RAND EUROPE

The moral component of cross-domain conflict

Lucia Retter, Alex Hall, James Black, Nathan Ryan

For more information on this publication, visit www.rand.org/t/RR1505

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

RAND Europe is a not-for-profit organisation whose mission is to help improve policy and decisionmaking through research and analysis. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Preface

This is the final report of a study commissioned by the UK Ministry of Defence (MOD) through the Defence Human Capability Science and Technology Centre (DHCSTC) framework. The study was conducted over a period of six weeks and examines the academic debate pertaining to the moral landscape of conflict that spans different military domains (air, maritime, land, space, cyber). The investigation which is the subject of this report was commissioned by the Programme and Delivery Directorate of the Defence Science and Technology Laboratory (Dstl).

RAND Europe is an independent, not-for-profit policy research organisation that aims to improve policy and decision-making in the public interest through research and analysis. RAND Europe's clients include European governments, institutions, NGOs and other organisations with a need for rigorous, independent, interdisciplinary analysis.

For more information please contact:

Alex Hall

Research Leader, Defence and Security Programme

RAND Europe

Westbrook Centre, Milton Road

Cambridge CB4 1YG

United Kingdom

Tel. +44 (1223) 353 329

ahall@rand.org

Abstract

This study was commissioned to examine the academic debate pertaining to the moral landscape of cross-domain conflict (i.e. a conflict that spans two or more military domains (land, maritime, air, cyber, space)). The study: considers the body of work on morality and armed conflict in the future operating environment; provides insights on the ways in which new ways of fighting may challenge traditional moral principles; and identifies areas that may be underexplored in the body of work on morality or may merit further analysis. The study considered two emerging technologies (cyber and autonomous systems) to derive practical insights on the ways in which new technologies could challenge traditional thinking about morality. The work involved a systematic review of relevant literature, a programme of interviews and a one-day workshop with academic experts.

The study finds that: the majority view among consulted experts was that existing moral frameworks and principles continue to apply; there is a considerable disparity in the legal interpretations applied to the term 'armed attack' and in deliberations regarding what constitutes 'harm' (including both physical and non-physical effects). Theorists generally agree that there is no particular moral barrier to responding to a non-kinetic attack – once confirmed as constituting an 'armed attack' – with kinetic force if this is considered the most appropriate course of action under the specific circumstances. Revisionist approaches to just war theory challenge the legal distinction between combatants and non-combatants since it does not account for the moral intentions of individuals party to a conflict. Under this line of thinking, non-combatants may render themselves liable to harm if their actions infer their support for an 'unjust war'. Both cyber and autonomous systems were considered to present challenges to a number of the principles underpinning traditional moral and legal frameworks.

Table of Contents

Figures

Tables

Executive Summary

This study examines the academic debate on the subject of morality in conflict

The nature of conflict is always changing, underpinned by cultural, military and technological evolution. In the last 20 years, the pace of change has accelerated, due in no small part to the advent of new technologies that are transforming the way conflicts are fought, as well as the operating environment in which they take place. Against this backdrop of continuous change, the traditional morality frameworks that underpin conduct in conflict have been subject to increased scrutiny. A lively academic debate has emerged on the enduring relevance of traditional morality frameworks and explores the challenges posed to them by new ways of waging war.

This 'quick look' study was commissioned to examine the academic debate pertaining to the moral landscape of cross-domain conflict (i.e. a conflict that spans two or more military domains (land, maritime, air, cyber, space)). The study: considers the body of work on morality and armed conflict in the future operating environment; provides insights on the ways in which new methods of fighting may challenge traditional moral principles; and identifies areas that may be underexplored in the body of work on morality. The work involved a systematic review of relevant literature, a programme of interviews and a one-day workshop with academic experts. As a 'quick look' rather than an in-depth study, the work focused on morality frameworks in the western tradition (the just war theory and international humanitarian law) and centred around two technological areas (cyber and autonomous systems).

Future morality judgements will be made in an environment characterised by complexity and uncertainty

While morality judgements are often inherently complex in nature, several features of the future operating environment further complicate the context for moral decision-making. An example of this is the increasing blurring of distinctions between war and peace, between the different domains of conflict (land, maritime, air, space, cyber) and between kinetic and non-kinetic effect. This lack of tangible boundaries can present profound challenges for law and morality, making it difficult to determine what conduct would be legally sanctioned and morally justifiable. Despite – and perhaps because of – the rise of novel technologies, moral reasoning skills will continue to be important, at the individual as well as the collective level. This is relevant not only to ensure the morality of individual acts but also to respond to greater external scrutiny of military and individual actions that will result from the spread of surveillance technologies and the increasing relevance of social media.

The academic debate about morality in future conflict coalesces around several principal issues

Much of the academic body of work on the subject of morality in conflict takes either the just war theory or international humanitarian law as its frame of reference, with the debate revolving around the applicability of these existing moral frameworks to new ways of waging war. The debate reflects on whether existing definitions or legal provisions require amendment to respond to the rise of new technologies, whether because of their inherent characteristics or the nature of their use in conflict. There is an increasing orientation towards the moral responsibility of the individual (as opposed to the state) as the primary actor in moral deliberation.

Key findings:

- It was generally agreed by study participants that the 'cross-domain' aspect of conflict (which was an initial focus for this study) is less helpful as a framework for deliberation about morality than a focus on effects (kinetic and non-kinetic) and technologies (their inherent characteristics and application).
- Existing moral frameworks were not generally considered to have outlived their usefulness: the majority view was that existing moral frameworks and principles continue to apply. That said, some advocate for a new interpretation of existing principles or amendment to or a confirmation of underpinning definitions.
- There is a considerable disparity in the legal interpretations applied to the term 'armed attack' (which is critical in determining the legality of a resort to force) and in deliberations regarding what constitutes (sufficient) 'harm' (including both physical and non-physical effects). This is particularly contentious in relation to cyber.
- There was general consensus among those consulted during the study that asymmetry in conflict does not, in and of itself, pose a moral problem. In other words, the exploitation of asymmetric advantage is not de facto a moral concern.
- Similarly there appears no moral obligation to respond 'in kind'. Theorists generally agree that there is no particular moral barrier to responding to a non-kinetic attack – once confirmed as constituting an 'armed attack' – with kinetic force if this is considered the most appropriate course of action under the specific circumstances.
- While there exists in the academic body of work some consideration of whether a moral obligation exists to employ technologies that offer greater accuracy than other options (e.g. an automated or autonomous capability may be able to undertake targeting more accurately than a human in advance of a kinetic strike), strong counterarguments may be discerned against this view, particularly in relation to the use of unmanned aerial combat vehicles.
- Revisionist approaches to just war theory challenge the legal distinction between combatants and non-combatants since they do not account for the moral intentions of individuals party to a conflict. Under this line of thinking, non-combatants may render themselves liable to harm if their actions infer their support for an 'unjust war'.

The study's two case studies (on cyber and on autonomous systems) explore specific practical moral considerations

The study case studies provide insights into the ways in which specific technologies challenge current morality frameworks. Two technology areas were selected: cyber and autonomous systems. The selection of these technologies does not imply that they pose more challenges or more difficult challenges than other technological areas, rather that they received the most coverage in the sources considered.

Cyber capabilities challenge the core principles of morality frameworks in a number of ways

Cyber contributes to the blurring of the distinction between peace and war by creating uncertainty as to what constitutes conflict (as opposed to crime or other activities) in cyberspace and, in turn, the kinds of response that are morally appropriate. Cyber does not conform neatly with the central tenets of international law, not least because of the debate over whether a cyber attack can constitute an 'armed attack' under international law. Its transcendence of the notion of physical distance sets it apart from conflict in all other domains. Cyber's perceived ease of use may lower the threshold for the resort to force, albeit that the novelty of cyber means that its offensive or defensive use may set an enduring precedent. This increases the moral significance of decisions about its use.

Cyber prompts particular consideration of the following core morality principles *inter alia*:

- **Just cause**. The existence of a just cause is critical to the moral arguments associated with engaging in conflict. The right to self-defence is predicated on having been subject to an 'armed attack'. The question of whether a cyber attack constitutes an 'armed attack' is therefore pivotal to whether or not just cause exists and the resort to force can therefore be justified. An associated challenge is the issue of attribution. Cyber attackers may not be conclusively identifiable and the just cause principle rests – in part – on there being a readily identifiable opponent against whom it is justifiable to enter into conflict.
- **Last resort**. Cyber poses a challenge to the principle of last resort (or necessity), the notion that conflict should only occur as a last resort once all other reasonable alternatives have been exhausted. Since cyber operations may cause widespread disruption but relatively little destruction, they may be considered an easier and less destructive option for responding either to a cyber attack or to other kinds of armed attack.
- **Proportionality**. Under this principle, the use of force employed should be proportionate to the harm suffered. It is difficult to determine what constitutes a proportionate response to a cyber attack. This will depend on the harm caused by the original attack which may itself, be difficult to quantify. The possible escalation chain should also be central to proportionality considerations; that is, the expected escalation ladder that might emerge as a result of a cyber attack and response to it. Last, employing or responding to force in the cyber domain is likely to set a precedent and thus carries additional moral responsibility.
- **Discrimination**. Under this principle, war must be discriminate in nature, distinguishing between legitimate targets and non-combatants. While the intent may be for a cyber operation to be discriminate, the inter-dependent nature of the cyber domain may result in unintended consequences whereby civilians or non-military infrastructure are affected.

Autonomous systems raise questions in relation to the principles of legitimate authority, last resort and proportionality

The issues surrounding autonomous systems has attracted much attention in the public consciousness. While a prominent question in the public debate is whether morality can be reduced to an algorithm (in other words, whether a machine can ever be capable of moral deliberation), the body of academic work on the subject is more nuanced. It acknowledges that the relationship between levels of autonomy and moral permissibility is non-linear and complex. While increasing a system's autonomy raises heightened concerns regarding the lack of human oversight and moral agency, it also reduces the influence of human error: there are likely to be moral benefits and risks associated with both low and high autonomy systems. Much of the debate on autonomous systems centres on where responsibility lies for a machine's actions and mistakes, exploring the issues related to liability (whether product liability, criminal negligence or responsibility for war crimes) and standards (how to articulate and program the ethical standards that should govern the use of autonomous capabilities).

The nature of autonomous systems challenges conventional thinking in relation to, *inter alia*, the following principles:

- **Legitimate authority**. The use of autonomous systems challenges the principle of legitimate authority which is concerned with the right to wield force. For fully autonomous systems, concerns revolve around whether a machine can ever have authority to take a life or start a war as an agent of state policy.
- **Last resort**. Some argue that the extreme asymmetry of recent conflicts involving armed unmanned aerial vehicles means that the historic use of these technologies has rarely, if ever, represented a 'last resort'. Others worry that the removal of humans from the battlefield may lead policymakers to resort more readily to the use of force in preference to non-military instruments.
- **Proportionality**. Some experts have expressed concerns that the distance involved in the use of autonomous systems could lead to moral desensitisation and disengagement. A counter view to this is that the use of autonomous systems frees the operator from the 'fog of war', allowing for a decision-making process to emerge that may be more sensitive and morally engaged. Others question the moral premise under which an individual may be killed by a machine without human involvement citing an infringement of basic human dignity. A counter argument runs that the precision offered by machine may result in cleaner targeting, resulting in less human suffering.

The study identifies areas meriting further exploration and suggests priority areas for MOD

The study identifies a number of areas that may merit further analysis and exploration:

- Many experts consulted during this study considered that existing legal (and underpinning moral) frameworks have enduring utility but may need to be interpreted differently or extended to take account of new operating norms. A more detailed examination of the 'grey areas' in international law is recommended, specifically addressing the challenges posed by particular technologies. This would assist in identifying areas where there is tension, shortfall or ambiguity and could be used to improve the applicability of the law in current and future operations.

- Much of the literature has examined the increasing prominence of the individual as the key actor (rather than the state) in moral behaviour. A more practical, applied consideration of what this means and might mean in future warfighting would be beneficial to derive practical insights for recruitment, training, command and control, and other areas.
- Given the apparent preponderance of work on cyber and autonomous systems, a focus on technological areas beyond the two examined here would be helpful in enriching the wider debate. Examples could include: direct energy weapons, nanotechnology and non-lethal weapons.
- For practical reasons, this study focused solely on Western perspectives and the Western traditions of morality-based thinking. A detailed analysis of morality frameworks and systems of belief beyond this Western-centric view is recommended. An understanding of alternative morality frameworks – and the challenges posed to them by the changing nature of conflict – may offer further assistance to inform thinking morality in conflict and offer insights into the morality considerations of current and future UK allies, adversaries and target audiences.

Areas in which MOD might wish to focus its efforts in advancing its thinking on morality include the following:

- MOD should ensure that the contemporary discourse on morality is integrated in the wider dialogue about military strategy in a meaningful way. Evidently the UK will wish to be – and to be perceived as – a moral actor. Greater, more holistic consideration should be given to what this means in practice and what safeguards and frameworks need to be put in place to allow the UK to accomplish this.
- Work on current and emerging 'grey areas' in international law would be instrumental in helping MOD determine current areas of vulnerability and anticipating challenges that might be posed/precedents in the event of a future attack.
- A greater emphasis on policy development in relation to cyber and to autonomous systems would help focus on the specific morality issues associated with the UK's likely use of these capabilities in the future, as well as shaping wider global norms.
- Reflecting the apparent shift away from state agency to a focus on individuals as moral actors, MOD should take steps to ensure that morality is embedded in every individual service member. In doing so, MOD should encourage discussions on morality and consider whether amendment may be required to the existing recruitment, training, education and command and control regime in order to facilitate this.
- Examination of potential changes in the future moral operating landscape could be integrated into wider horizon-scanning and strategic force development work to assess Defence planning against moral assumptions and attempt to generate a more robust evidence base to inform decision making.

Acknowledgements

The study team owes a debt of gratitude to the many organisations and individuals who supported this study.

Our thanks are due firstly to Dstl for their sponsorship of this study.

We would like to thank all experts consulted in the course of this short study for their time, flexibility and valuable insights: General Sir Hugh Beach, Prof Eyal Benvenisti, Prof Nigel Biggar, Dr William Boothby, Prof Helen Frowe, Dr Adam Henschke, Prof Don Howard, Prof Anthony Lang, Dr Patrick Lin, Prof Jeff McMahan, Prof Mary Ellen O'Connell, Prof Sir David Omand, David Ronfeldt, Major Jackie Schiller and Dr Jim Walsh.

We would also like to thank all experts who participated at the expert workshop and contributed to a stimulating and though-provoking discussion: Prof Isabelle Duyvesteyn, Dr Christopher Finlay, Prof Mervyn Frost, Tom McKane, Dr Esther D. Reed, Dr Massimo Renzo, Paul Schulte and Dr Mariarosaria Taddeo.

Within RAND Europe, we would like to acknowledge the support of Prof Paul Cornish who kindly facilitated contact with many of the experts consulted in the study. We thank Dr Chris Giacomantonio and Dr Giacomo Persi Paoli for their contribution to the work in their capacity as Quality Assurance reviewers. We are also indebted to Sarah Grand-Clement for providing invaluable assistance to the study team.

Abbreviations

AI	Artificial Intelligence
ICRC	International Committee of the Red Cross
IHL	International Humanitarian Law
JWT	Just War Theory
LAWS	Lethal Autonomous Weapons Systems
NSA	Non-state Actor
POW	Prisoner of War
ROE	Rules of Engagement
UAV	Unmanned Air Vehicle
UNIDIR	United Nations Institute for Disarmament Research

Definitions

Armed Conflict	Pursuit of objectives through violence
Cross-Domain Conflict	For the purposes of this study, this term refers to a conflict that takes place across two or more military domains: air, naval, land, cyber, space
Hybrid Warfare	A type of warfare that incorporates a full range of different modes of warfare including conventional or asymmetrical modes executed by classic military forces that can include, in an extreme approach, terrorist acts and violence on the population and actions to favour public disorder. These activities are operational and tactical directed to achieve synergistic effects in the physical and psychological dimensions of conflict. (Source: Barbu, 2015)
jus ad bellum	Refers to the conditions under which states may resort to war or to the use of armed force in general
jus in bello	Regulates the conduct of parties engaged in an armed conflict
Non-State Actors	All those actors that are not (representatives of) states, yet that operate at the international level and that are potentially relevant to international relations. Non-state actors can be divided into the following categories: 1) Intergovernmental organisations 2) International non-governmental organisations 3) Corporate interest groups and transnational corporations 4) Epistemic communities 5) Remainder category (including terrorist networks, professional organisations, scouts, churches, etc.) (Source: Arts, 2005)
War	Extreme form of armed conflict that usually takes place between states

1. Introduction

1.1. Context

The cultural, military and technological developments of the last twenty years have presented new challenges to the traditional distinctions that underpin conventional legal, moral and strategic thinking. With the rise of Non-State Actors (NSA),[1] the conflation of different types of hostile groups (e.g. links between terrorism and criminal networks) and the increasing use of non-traditional weapons (e.g. cyber, tactical targeting), distinctions between the state of war and the state of peace have become more fluid, resulting in a change in the nature (and threshold) of conflict.[2] Technological advances in autonomy bring together humans and machines in an unprecedented way.[3] The contemporary and future battlespace encompasses forms of conflict that may transcend or blur the distinctions between the military 'domains' (air, land, sea, space, cyber) and involve the application of both kinetic (physical) and non-kinetic (virtual, intangible) effects.

As a result of the changed characteristics of the operating environment[4] and the wider trends outlined above, the principles that constitute the building blocks of traditional moral codes applying to war and conflict have come under scrutiny. These new developments have prompted new questions for reflection. Are traditional moral frameworks still relevant in relation to the new ways of conflict and war? What are the most difficult moral challenges faced by decision-makers in relation to tomorrow's conflict? What will the future moral operating environment look like for the UK and its allies? These and similar questions are at the heart of the research effort undertaken in this study.

---

[1] Non-state actors (NSAs) include 'all those actors that are not (representatives of) states, yet that operate at the international level and that are potentially relevant to international relations' (Arts 2005). NSAs can be divided into the following categories (see Arts 2005 for detailed references to relevant literature on these categories):

1) Intergovernmental organisations
2) International non-governmental organisations
3) Corporate interest groups and transnational corporations
4) Epistemic communities
5) Remainder category (including terrorist networks, professional organisations, scouts, churches, etc.).

[2] Global Strategic Trends, p. 96.

[3] Ibid., p. 69.

[4] As outlined in Future Operating Environment 2035.

1.2. Purpose of this study

The purpose of this study is to examine the academic debate pertaining to the moral landscape of cross-domain conflict'; that is, a conflict that spans two or more military domains. More specifically, this work considers:

- The extant and emerging body of work on morality in relation to armed conflict and war in the future operating environment.
- Any apparent 'disconnect' between new ways of fighting and traditional notions of morality surrounding war and armed conflict.
- Insights on the moral principles that are challenged by the new ways of fighting and high-level implications (legal, policy, cultural, military, societal).
- Specific areas that may currently be underexplored in the body of work on the subject of morality in cross-domain conflict.

1.3. Assumptions and caveats

The study is future-focused, discursive in nature and focuses on mapping the landscape of relevant research, seeking to outline the main discussion points. It is a high-level synopsis of the debate to help policymakers understand the academic landscape and areas where further focus may be worthwhile. It is not intended as a conclusive or exhaustive analysis.

In this study, *war* is a 'state of armed conflict between different countries or different groups within a country. War remains constant under all circumstances.'[5] 'If differences cannot be resolved satisfactorily by other means, confrontation deteriorates into armed conflict. *Conflict* is characterised as a resort to violence to gain advantage and achieve desired outcomes.'[6]

For the purposes of this study, 'morality' and 'ethics' will be used interchangeably.[7]

Due to the time constraints of this study, the review of literature was limited to articles and grey literature (e.g. policy reports, UN documents) and the study team was not able to review books or edited volumes.

While the study team has sought to include a non-Western perspective wherever practicable, given the short and discursive nature of the study, any such engagement has been limited to secondary literature and information obtained from experts consulted in this study – all of whom came from a Western perspective. Please refer to Chapter 2 for further discussion on the non-Western perspectives.

This study does not specifically focus on 'hybrid warfare'[8] and unconventional modes of warfare such as use of social media, albeit some aspects related to the military combat effort within 'hybrid warfare' are

[5] Joint Doctrine Publication 0-01 (2014). UK Defence Doctrine. p. 18.

[6] Ibid.

[7] Some philosophers indicate that morality describes a code of conduct of a society or another type of group (Gert 2002). Ethics is then constructed as the critical reflection on morality. In this study, the terms 'morality' and 'ethics' are used interchangeably.

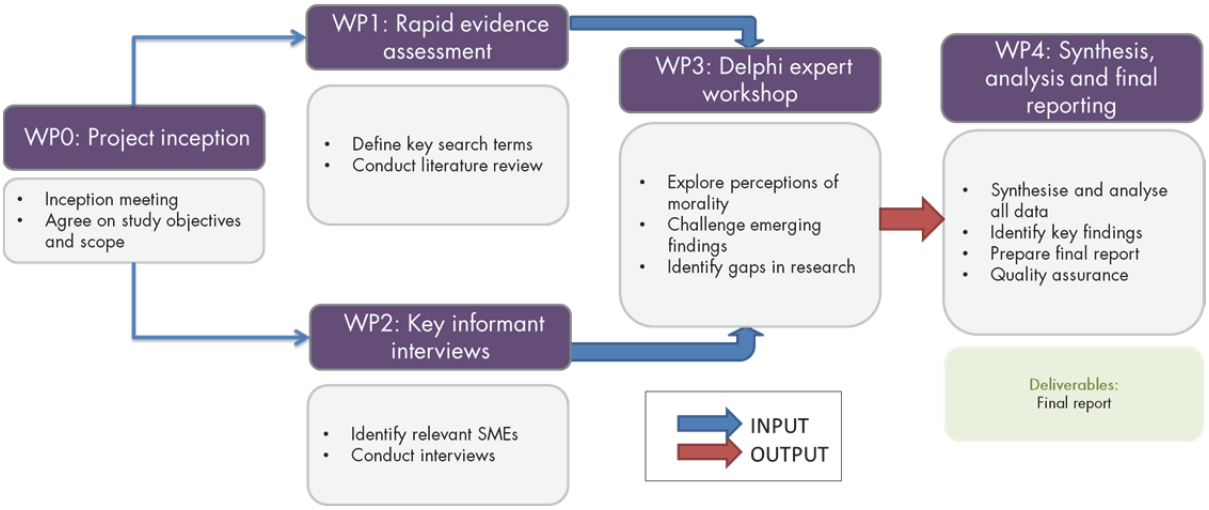
[8] A 'hybrid war' includes actions that 'incorporate a full range of different modes of warfare including conventional or asymmetrical modes executed by classic military forces that can include, in an extreme approach, terrorist acts and

relevant to the examination of moral questions within this study. A short section on 'hybrid war' is included in Chapter 2 but considerations of morality in relation to unconventional methods of fighting are beyond the scope of this study.

1.4. Methodology

The study was conducted over a period of six weeks and relies heavily on input from academic literature and experts, most of whom have worked on the topic of morality and conflict for several years, some even decades. This input was collected in three ways: (1) through a systematic review of literature, (2) interviews with experts, (3) and a one-day expert workshop. Figure 1.1 presents a graphical outline of the tasks and methodologies employed in this study.

Figure 1.1 Project plan and methodology



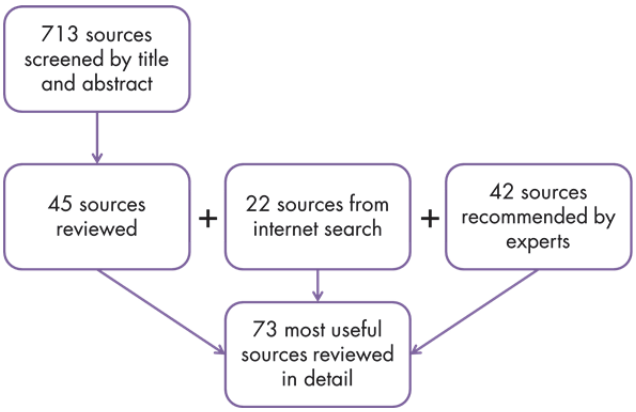
As part of the literature review phase, a systematic search was performed in the following databases: EBSCOHost, JSTOR, PolicyFile, Proquest, ROCs, SCOPUS, SCS, Web of Science and Google Scholar. An initial set of 446 references related to ethics or morality and 'cross-domain' conflict and another 267 sources related to ethics or morality and 'hybrid war' were screened by title and abstract to identify sources relevant to the topic of ethics or morality and cross-domain conflict. Forty-five sources were identified in this way. An additional 22 sources were identified through internet searches and 42 more were recommended by experts consulted in the course of the study. In general, this latter category proved of highest relevance and provided the most useful insights. In total, 109 sources were reviewed in detail, out of which 73 were deemed most relevant for the purposes of this study as they were future-focused and specifically addressed morality and conflict. The review of literature was captured in a literature review matrix to ensure a systematic way of capturing data.[9] Figure 1.2 summarises the literature review process.

---

violence on the population and actions to favour public disorder. These activities are operational and tactical directed to achieve synergistic effects in the physical and psychological dimensions of conflict.' (Barbu 2015).

[9] The literature review matrix captured the following information: 1) Author, year, title, journal; 2) Study purpose; 3) Relevant moral framework (e.g. the just war theory); 4) Key military domain; 5) Key technology; 6) Case study or country study; 7) Main thesis of the article; 8) Specific policy implications; 9) Peer reviewed (Yes/No); 10) RAND

Figure 1.2. Literature review process



To validate and supplement the material from the literature review, the study team conducted 17 interviews with experts from the US, UK and Australia who are active in research on the topic of morality and new ways of warfighting. These experts were identified through: (a) RAND's internal networks, (b) the literature review, and (c) recommendation from experts. The interviews were conducted using a semi-structured interview protocol. The data from interviews was captured in a data extraction matrix.[10]

Finally, the study team organised an expert workshop in London, which focused on the following tasks:

- Discussion on the landscape in relation to the question of morality within cross-domain conflict.
- Identification of the main issues around which the debate is centred.
- Small group discussions to test the application of moral frameworks against specific vignettes outlining a hypothetical future situation.

The study team used two separate vignettes – one focused on cyber, the other on autonomous systems – as an exercise in practical reasoning. The rationale of using hypothetical case-studies or vignettes is to examine frameworks of moral reasoning in the light of concrete examples. In this exercise, the study team gained insight into how participants perceived the challenges posed to the underlying principles of the JWT, International Humanitarian Law (IHL) and virtue ethics[11] by the novel use of emerging technologies.

Reviewer. Depending on the topic of the article, some columns were left blank for some articles. Some article, for example, did not mention any case studies or country studies. Therefore, this column was left empty.

[10] The interview data extraction matrix captured the following information: 1) Interviewee (name, position); 2) Date of interview; 3) Relevant moral framework (e.g. the just war theory); 4) Main thesis (in relation to novel ways of conducting warfare); 5) Noting any specific policy/military implications/specific moral dilemmas; 6) Specific views on the implications of novel ways of fighting for: a) conflict escalation, b) self-defence, c) necessity, d) pre-emption, e) discrimination and f) proportionality; 7) Views on the relationship between morality and law; 8) RAND interviewer

[11] A useful summary of virtue ethics is presented in Reding (2014): 'Virtue ethics claims that each individual holds virtues that allow them to lead a 'good' life (Sandel 2012). These virtues consist of desirable character traits that are expressed in individual actions and that are durable, omnipresent and influential – but only applied where necessary. The virtues have traditionally been classified into intellectual virtues such as practical wisdom; and moral virtues such as courage, justice, honesty and integrity (MacIntyre 1984).

The workshop participants were sent preparatory reading materials in advance and thus had the opportunity to reflect on some of the questions. During all of the discussions, both consensus and divergence of arguments were captured to illustrate the breadth and depth of the debate.

1.5. Principles underpinning the analysis

Throughout the study, the study team has been acutely aware of the fact that the topic of morality in conflict has been approached from a primarily Western perspective. This perspective is steeped in the JWT and recognises the importance of IHL in regulating behaviour prior to and during combat.

While the study team recognises and references other ethical frameworks that can apply to the conduct before and during war or armed conflict (see Chapter 2 for more detail), the analysis in this study is structured along the principles underpinning the JWT, many of which are also reflected in IHL. The reference to these principles ensures that this study is grounded on solid analytical foundations and reflects the fundamental commitments (and accountability) of the UK military to IHL.[12]

For the sake of uniformity, the study team adopted the set of Just War principles that are outlined in the Stanford Encyclopedia of Philosophy[13] – an online resource populated by experts in relevant fields of philosophy. The study team appreciates that these principles may be known under different names and/or may be merged together in sources dealing with the JWT. IHL principles referred to in this study are taken from the website of the International Committee of the Red Cross (ICRC).[14] Table 1.1 summarises the core principles of the JWT and Table 1.2 outlines the principles underpinning IHL.

With reference to Table 1.1, *jus ad bellum* 'refers to the conditions under which States may resort to war or to the use of armed force in general.'[15] The core components of *jus ad bellum* in IHL are: the prohibition against the use of force among States and the exceptions to it (self-defence and UN authorisation for the use of force), set out in the United Nations Charter of 1945.[16]

Jus in bello regulates the conduct of parties engaged in an armed conflict. According to the ICRC, it is synonymous with IHL. [17]

[12] See Future Operating Environment 2035, p. 6 for UK commitment to upholding international law.

[13] Stanford Encyclopedia of Philosophy, 'War'.

[14] ICRC. Fundamentals of IHL.

[15] ICRC. What are jus ad bellum and jus in bello.

[16] Ibid.

[17] Ibid.

Table 1.1. Principles of the Just War Theory[18]

Jus ad bellum	1. just cause – **self-defence and defence and protection of others against aggression and grievous wrongdoing**
	2. **last resort** – a state may resort to war only if it has exhausted all plausible, peaceful alternatives to resolving the conflict
	3. **proper authority** – decision to go to war must be made by appropriate authorities (usually specified in the constitution), in a proper process and publicly announced
	4. **right intention** – must ensure there is a just cause, no ulterior motive
	5. **reasonable chance of success** – states may resort to war only if there is a probability of measurable impact on resolution of the conflict
	6. **proportional to the means used** – before initiating war, states must weigh the goods expected to result from it against evils expected to result (e.g. casualties)
Jus in bello	1. **obeying all international laws on weapons prohibition**
	2. **discrimination and non-combatant immunity** – use of (non-prohibited) weapons is only permitted against combatants
	3. **proportionality –** only force proportional to the ends sought is permitted
	4. **benevolent quarantine for prisoners of war (POWs) –** persons no longer involved in combat cease being lethal threats to basic rights and should not be treated as active combatants
	5. **no means *Mala in Se* –** means that are evil in themselves are prohibited (e.g. genocide, ethnic cleansing, mass rape)
	6. **no reprisals** – violations of *jus in bello* in response to violations of *jus in bello* are prohibited

[18] Stanford Encyclopedia of Philosophy, 'War'.

Table 1.2. Principles of IHL[19]

1.	**distinction between civilians and combatants , civilian objects and military objects –** attacks may only be directed against combatants. Attacks must not be directed against civilians[20]
2.	**prohibition to attack those *hors de combat*** (i.e. anyone who is in the power of the adverse party; or anyone who is defenceless because of unconsciousness, shipwreck, wounds or sickness; or anyone who clearly expresses an intention to surrender)[21]
3.	**prohibition to inflict unnecessary suffering –** the use of means and methods of warfare that are of a nature to cause superfluous injury or unnecessary suffering is prohibited[22]
4.	**principle of necessity –** permits measures that are actually necessary to accomplish a legitimate military purpose and are not otherwise prohibited by international humanitarian law[23]
5.	**principle of proportionality –** attack that 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, is prohibited[24]

In addition to *ad bellum* and *in bello* principles, recent academic debate has also focused on the importance of '*jus post bellum*'. *Jus post bellum* is a term first presented by Brian Orend in his 2002 article 'Justice after war'.[25] It refers to the justice and law after war and the transition from conflict to peace and reconstruction.

1.6. Structure of the report

This report summarises the findings of the study. It contains five chapters and three short appendices. Figure 1.3 presents the report structure and outlines the logical links between chapters and appendices.

[19] ICRC. Fundamentals of IHL.

[20] ICRC. Rule 1. The principle of distinction between civilians and combatants.

[21] ICRC. Rule 47. Attacks against persons hors de combat.

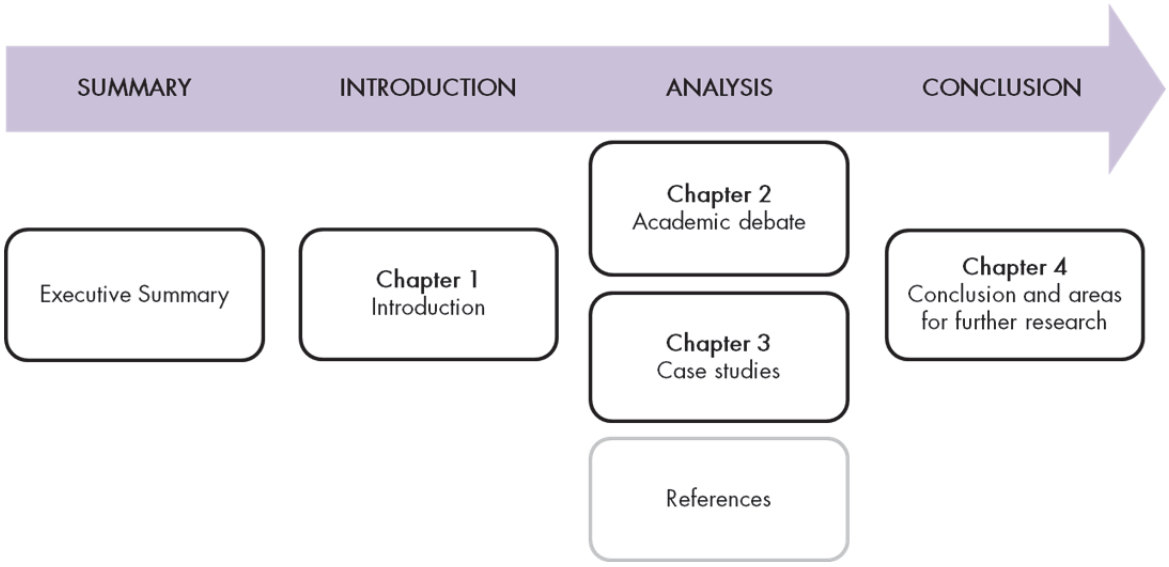
[22] ICRC. Rule 70. Weapons of a nature to cause superfluous injury or unnecessary suffering.

[23] ICRC. Military necessity.

[24] ICRC. Rule 14. Proportionality in attack.

[25] Orend (2002).

Figure 1.3. Report structure



2. Academic debate

2.1. Future Moral Operating Environment

This section outlines some of the contextual factors that have emerged throughout the research activity of the study team. These considerations often stem from current scenarios but are seen by experts as applicable to likely future conflicts and wars affecting the UK. This chapter draws on material from the literature review, expert interviews and discussions at the expert workshop.

2.1.1. Blurring of distinctions between war and peace

The blurring of national and overseas threats[26] and the rise of NSA present the UK and its allies with situations in which the distinction between peace, conflict and war can be unclear (see Chapter 1, for a distinction between war and armed conflict). A war is often no longer 'declared' and a tangible boundary between peacetime and wartime have become difficult to draw. A cyber 'attack' on critical national infrastructure illustrates this dilemma as the attack may not be easily attributable, or cause any direct physical harm, yet could lead to casualties due to an ensuing collapse of a power grid, and consequent effects on hospitals and other facilities. Determining whether a hostile act or a conflict rises to the level of an 'armed attack' and whether there is a justifiable reason to resort to the use of force can be problematic.[27]

Some of these developments can be described as a rise in the so-called 'hybrid warfare',[28] with a mix of conventional and asymmetric means of combat to undermine the opponent's combat efforts.[29] From the perspective of morality, 'hybrid warfare' uses 'tactic success to obtain strategic effects by rapid exploitation of the advantages within cognitive and moral field.'[30] 'Hybrid warfare' often includes the use of political, economic, social, humanitarian, diplomatic and informational measures, alongside the participation of the

[26] Future Operating Environment 2035, p. 32.

[27] Schmitt (2012), Interview with William Boothby, Tallinn Manual (2013).

[28] A comprehensive definition of actions within a 'hybrid war' is provided in Barbu (2015): 'Hybrid actions incorporate a full range of different modes of warfare including conventional or asymmetrical modes executed by classic military forces that can include, in an extreme approach, terrorist acts and violence on the population and actions to favour public disorder. These activities are operational and tactical directed to achieve synergistic effects in the physical and psychological dimensions of conflict.'

[29] Munteanu (2015), Hoffman (2007), Barbu (2015).

[30] Barbu (2015).

local population by the state or NSA involved in conflict.[31] As such, moral considerations are extended beyond those of military combat action to those of a political or economic or humanitarian nature, which go beyond the scope of this study.

The existence of this 'grey area' in conflict[32] has profound implications for law and morality as well as for the question of what may be the desired end of a conflict. If the attack does not constitute 'use of force' under Art 2(4) of the UN Charter, do the principles of *jus ad bellum* still apply?[33] If the conflict does not constitute 'war', are *in bello* principles relevant to guide the conduct of those participating in the conflict?[34] What alternative measures, short of war, should be considered without significantly increasing the risk of becoming more vulnerable to a greater future harm as a result of waiting? What is the desired outcome *post bellum* of this conflict? Is it justice? Is it peace?

There are no simple answers to these questions and academics, lawyers and Western governments engage in extensive debates trying to identify the appropriate legal framework (e.g. IHL, domestic criminal law, international human rights law) to govern their conduct in these 'grey' areas. Moreover, since conflict is dynamic, the legal and moral considerations also evolve. As a conflict progresses with time, it is the task of decision-makers to continuously re-evaluate the situation.[35] They need to consider whether there are alternative approaches to the present situation that are preferable from a legal and moral standpoint (even if the initial resort to force was legal under *jus ad bellum* principles).

2.1.2. Moral uncertainty inherent to war and conflict

Added to the uncertainty over the appropriate legal framework applicable in a given situation, there is also the ever-present uncertainty over what conduct is morally right. This is subject to extensive debate, which is beyond the scope of this study and covers considerations related to combat environment, situation, mental health and others. Within the context of this study, this section serves as a reminder about the importance of individual moral decision-making, rather than as a source of a comprehensive analysis of individual moral deliberation in war.

Determining whether conduct is morally right is made more challenging in the 'fog of war' where information is imperfect and a thorough assessment of consequences is very difficult.[36] In war, which may include a large number of agents, it becomes difficult to determine the implications of moral principles.[37] Moral decision-making in the context of war and armed conflict, as in other areas such as counterterrorism and health care, requires an individual to make trade-offs between moral values such as

[31] Munteanu (2015).

[32] Term discussed at the expert workshop.

[33] Whetham (2016).

[34] Ibid.

[35] Interview with Eyal Benvenisti.

[36] Morkevicius (2013), Cornish (2002, 2007, 2013).

[37] Interview with Jeff McMahan, see also Cornish (2002, 2007).

life, health, preservation of culture and others.[38] As with other areas of applied ethics, ethical decisions in war and armed conflict require context-specific deliberation.[39]

As shown in section 2.2.4 in greater detail, there is a consensus in the literature reviewed for the purposes of this study and among interviewees that the context of new ways of warfighting does not mean that traditional moral principles of the JWT and IHL cease to apply.[40] Yet, it is only retrospectively (*ex post*), that the judgement of the commander or soldier can be properly evaluated and assessed with reference to IHL or a broader set of moral principles.[41] As such, the decision-maker (strategic, operational or tactical commander as well as individual soldier) in any given situation is entrusted with the duty to exercise discretion when choosing the course of action.[42] Most experts consulted in this study agree that moral agency resides in the individual – the commander as well as the individual soldier.[43] It is these actors who engage in combat themselves who are in the best position to ensure that action is undertaken in line with legal and moral principles of the JWT and IHL.[44] Aiding this effort is a strong moral strategic and operational level leadership and rules of engagement (ROE) that enable individual moral deliberation within the remit of legality (with tactical level commanders only allowed to refine ROE to make them more restrictive, not less).[45]

Most of the experts consulted and referenced in this study agree that moral deliberation and prudential decision-making in a situation like conflict or war is complex. It requires an informed moral conscience and the ability to reason morally.[46] Most of the experts also agree that moral deliberation is only possible by humans.[47] As illustrated in the Chapter 3 case study on autonomous systems, this view presents a strong counterargument to the view that it may be possible to program 'morality' and/or 'legality' into an autonomous machine. Based on the information from expert interviews, the ability to reason morally can develop through appropriate formation and training[48] and can be facilitated by emphasis on virtues in the

[38] Reding (2014).

[39] Ibid.

[40] For example: Lucas (2013a,b, 2014), Eberle (2013), O'Connell (2011, 2012, 2015), Jastram (2011), also argued in interviews with Jeff McMahan, Helen Frowe, Mary Ellen O'Connell, Nigel Biggar.

[41] Interview with Eyal Benvenisti. It is important to note that when exercising ex post assessment of the soldier's decision to act, what is morally and legally relevant is the information that was available to her/him at the time of acting (and not new information received after the attack).

[42] Cornish (2002 and 2007).

[43] For example, interviews with Jeff McMahan, Helen Frowe, Don Howard, Jackie Schiller, Anthony Lang.

[44] Cornish (2002).

[45] Interview with Jackie Schiller.

[46] Detailed account in Morkevicius (2013); also highlighted in workshop discussions.

[47] Morkevicius (2013), Lucas (2013b), highlighted in interview with Eyal Benvenisti and workshop discussions.

[48] For example, interview with Helen Frowe and Don Howard.

context of the military profession.[49] As one of the experts noted, 'the important thing is not to tick ethical boxes, but to apply the underlying thinking.'[50]

2.1.3. Importance of public perceptions

As noted in *Future Operating Environment 2035*, public attitude and reaction to military operations is likely to impact governments' willingness to deploy forces in the future.[51] The growth of surveillance technologies like body cameras and the spread of information on social media are likely to result in greater external scrutiny of the military and individual actions in combat.[52] Autonomous technologies with their precision targeting ability may lower inhibitions against war[53] but may, at the same time, make the public more sensitive to civilian casualties.[54] Faced with more 'indirect' threats to security, interests and prosperity, for example, a cyber threat to the national banking system, public opinion is likely to vary as to the justifiability of a military response.[55]

Public perceptions affect the moral considerations both in relation to *jus ad bellum* and *in bello*. Public opposition to war may pressure governments to consider alternative responses short of military action. Public endorsement, on the other hand, may reinforce the narrative of a Just War. Survey-based research shows that even if public inhibitions to war are lowered (e.g. by the use of unmanned combat vehicles), this effect is less significant than the role of the overall policy justification for the resort to the use of force.[56]

The role of public perceptions is particularly notable in the debate on the morality of lethal autonomous weapons systems (see Chapter 3 for more detail) and on the interpretation of the Martens Clause in this context.[57] The so-called Martens Clause first appeared in the preamble to the 1899 Hague Convention (II) and places emphasis on the importance of taking into account public conscience when determining the appropriate regime to govern the use of new weapons. It reads as follows:

> 'Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the *public conscience*.'[58]

---

[49] Myers (1997) (for an article claiming the opposite, see Toner (2006)).

[50] Interview with Sir David Omand.

[51] Future Operating Environment 2035, p. 7.

[52] Ibid., p. 42, also a subject of workshop discussions .

[53] Walsh, Schultzke (2015), O'Connell (2011).

[54] Walsh (2015a,b).

[55] Future Operating Environment 2035, p. 7.

[56] Walsh, Schultzke (2015).

[57] Lin (2015).

[58] ICRC. The Martens Clause and the laws of armed conflict. Authors' emphasis.

Article 36 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Geneva, 8 June 1977 (API) requires all signatory states to subject all new weapons (including non-lethal) to a legal review.[59] Without such a review and without a developed body of law to govern the use of new weapons (such as lethal autonomous weapons and cyber), based on the Martens Clause, combatants and non-combatants should remain under a protective regime that is informed by the public conscience. To illustrate by means of an example, an indication of 'public conscience' may be the emerging consensus among experts and the general public on the requirements of 'meaningful human control' to be involved in operations of semi-autonomous systems.[60] A sense of morality present in the 'public conscience' can, therefore, have influence on the legal and government deliberations over the use of new technologies in conflict and war.

2.1.4. Appreciation of non-Western perspectives

As noted in the introduction, this study has examined and used in its analysis moral principles that stem from the Ancient Greek and Roman and Christian JWT; the principle tenets of IHL and the framework of virtue ethics. Although there are similarities between the Christian JWT and the governance of war in Islam, there are also substantive differences,[61] the examination of which is beyond the scope of this study. Similarly, even though the UN Charter and the Geneva Conventions were agreed to by representatives of all major religions, cultures and nations after the Second World War, implying that these rules are universally binding,[62] some states choose not to abide by the law or interpret the law in a manner not initially envisaged by the signatories to the above agreements.[63] While this does not mean that the principles of IHL are more or less binding on different states, states' adherence to them and interpretation of them may differ from the interpretation adopted by the UK military and the UK government.

Crucially, NSA, in general, are not subjects under international law and are thus not obliged to abide by the principles of IHL. Some violent NSA involved in current and potential future conflicts adopt what may be called a 'tribal morality', which centres around protection of one's own against the other and on retaliation in kind.[64] Another view emphasises that adversaries involved in today's and tomorrow's warfare engage in setting 'ethical traps' as a source of their power.[65] These 'traps' are set to prompt the UK and its allies to act in a way that undermines the core values and moral principles that the 'West' defends.[66] One interviewee noted that there is, essentially, a 'moral asymmetry' in which western professional armies are tightly bound by the constraints of IHL, while their opponents (often NSA) are not held accountable by

[59] ICRC. The review of weapons in accordance with Article 36 of Additional Protocol I.

[60] UNIDIR (2015).

[61] Kelsay (1990).

[62] O'Connell (2015).

[63] Ibid., elaborated on in workshop discussions.

[64] Interview with David Ronfeldt.

[65] Frost (2012), elaborated on by author during workshop discussions.

[66] Ibid.

the same standards.[67] Any meaningful assessment of this asymmetry, however, as well as of the relationship between the principles of the JWT, IHL and the ethical frameworks adopted in the 'West' would require a dedicated research effort.

2.2. Debate related to morality in future conflict

One of the principal aims of this study is to map the landscape of the academic debate with regard to morality and cross-domain conflict. This section provides an overview of this debate, outlining areas of convergence and divergence. It also outlines a set of key areas of research and captures the diversity in views on the application of existing moral frameworks to current and future conflict. Chapter 4 complements this chapter in that it identifies gaps in research and knowledge and proposes areas for further research.

2.2.1. Key questions

The academic debate related to morality and future conflict is wide-ranging, lively and encompasses diverse perspectives. The last 10 to 12 years have seen a convergence of thinking on the ethics of war beyond the discipline of moral philosophy, reaching out to law, religious studies and political science. The research conducted by the study team shows that the majority of experts operate either within the framework of the JWT or IHL or both (seen as complementary and mutually reinforcing). In general, there has been an increase in scholarship on the moral responsibility of the individual as the moral actor; to contrast and complement analyses that see the state as the principal moral 'actor' in war. The key questions with which academics in this field engage are broadly similar; yet, the answers they supply vary significantly. Based on the literature and interviews, the study team's analysis suggests that these questions have emerged as most pertinent in relation to morality and future conflict:

- To what extent are existing moral frameworks (e.g. JWT and IHL) applicable to the new ways of conducting warfare?
- What adjustments (if any) are required to the legal definitions of 'armed conflict', 'just cause' and 'harm' to more accurately reflect new technological developments?
- What is the appropriate moral and legal framework to account for situations of non-kinetic hostile action with non-physical consequences? What, if any, is the appropriate framework for responding to such an action?
- What are the moral implications related to the inherent characteristics of new technologies themselves and what are the moral implications of their use?
- How might response options be constrained, given the risks associated with the new ways of conducting warfare? For example, what might be the implications of a particular response for conflict escalation?

In addition to these general questions, as mentioned in section 2.1.1, several legal questions arise as a result of the blurring of distinctions between 'war' and 'peace'. These are;

- If the attack does not constitute 'use of force' under Art 2(4) of the UN Charter, do the principles of *jus ad bellum* still apply?[68]

[67] Interview with Nigel Biggar.

- If the conflict does not constitute 'war', are *in bello* principles relevant to guide the conduct of those participating in the conflict?[69]
- What alternative measures short of war should be considered without significantly increasing the risk of becoming more vulnerable to a greater future harm as a result of waiting?
- What is the desired outcome *post bellum* of this conflict? Is it justice? Is it peace?

2.2.2. The role of the cross-domain factor in reflections on morality in conflict

At the outset, it was intended that this study focus on the moral considerations associated with what could be called 'cross-domain conflict'. In the course of the research it became clear that considerations of difficult moral questions related to future conflict and war are largely unaffected by the cross-domain element of conflict. Rather, any assessment of legality or morality with respect to warfare will depend on the following criterion: is the use of force lawful – that is, is it a self defence response to an 'armed attack' (as reflected in Art 51 of the UN Charter)? In other words, does the resort to the use of force meet the principles of JWT (listed in Table 1.1)? If the use of force is legal and moral, the choice of weapons or domains, within the constraints of IHL, does not by itself affect the moral judgement.[70]

In discussions with the study team, several experts have suggested that, in considerations of morality, the distinction between kinetic and non-kinetic effects proves more useful than the 'cross-domain' perspective as it captures the distinction between physical and non-physical harm.[71] In addition to *jus ad bellum* considerations, this distinction facilitates thinking through some of the moral questions in relation to the conduct *in bello*, specifically regarding the principles of proportionality and discrimination. The most obvious case in point here is the use of the cyber domain for military purposes and the moral considerations raised in relation to the 'harm' done and what constitutes a 'proportionate' (kinetic or non-kinetic) response. These questions are examined in Chapter 3.

Based on the literature review, the study team noted that the vast majority of academic writers tackle the questions on morality in future conflict with reference to specific technologies that are already on the rise or are likely to be used widely in the future. Although the terms 'emerging technologies' or 'new weapons' or 'new means of fighting' capture a wide range of technologies and specific weapons,[72] the majority of the literature sources and interview discussions have centred around two areas: (1) cyber and (2) autonomous systems. While this may be a result of a hidden bias in the literature search, it may also be an indication that these two technologies pose significant moral dilemmas and are therefore brought up as examples in the majority of research on the topic of morality and future conflict.

---

[68] Whetham (2016).

[69] Ibid.

[70] Interviews with William Boothby, Jeff McMahan.

[71] Workshop conversations.

[72] During the expert workshop, the experts identified the following key future technologies likely to be used in conflict and war: artificial intelligence (AI used in a lethal way), directed energy, cloning, pharma, advances in biomedical technologies, computer viruses, GPS, social media, internet of things, space, chemical warfare, nanotechnology, biological, drones, non-lethal weapons.

As experts point out, moral considerations emerge both as a result of the inherent characteristics of a technology and in relation to its specific use.[73] Reflecting on future conflict through the lens of emerging technologies thus appears to be another useful way to assess the moral dilemmas posed by new ways of fighting. Chapter 3 takes this approach, assessing the moral challenges posed by two novel technology areas: (1) cyber and (2) autonomous systems.

2.2.3. Diversity of legal interpretations

The first criterion of legality of the use of force may seem relatively straightforward. However, the rise of new technologies that may be used in current and future conflict, such as cyber, autonomous systems, non-lethal weapons, directed energy weapons, nanotechnology and others, present several challenges to the meaning of the terms 'armed attack', 'harm' and the notion of a 'just cause'. Specific to cyber, for example, both treaty law and customary international law are silent on the meaning (if any) of an 'armed attack'.[74] As the consequences of a cyber 'attack' are less likely to be lethal and physical than those of a conventional kinetic attack, the meaning of 'harm', traditionally referring to violent consequences of an attack such as physical harm and loss of human life, is challenged.[75]

Some progress has been made in the development of a 'soft law'[76] on cyberwarfare in the form of the Tallinn Manual, which summarises a set of rules that, based on a consensus of a group of international law experts, arise from customary international law.[77] Many experts have reflected on the kinds of criteria that may engage a *jus in bello* analysis;[78] however, disagreement over the meaning and applicability of the term 'armed attack' to cyber remains. Additionally, some experts argue that the Internet was not conceived as a battlefield.[79] It has been argued that most hostile activity facilitated in cyberspace should be viewed as criminal activity and handled under criminal law (domestic and international).[80] Cyber activity such as direct denial of service, cyber espionage or GPS jamming may constitute a coercive act, but it often falls short of qualifying as an act of war.[81] Most cyber activity will be in the realm of espionage and sabotage, which are less physically destructive than traditional means of warfare, yet may cause significant (non-physical) harm.[82] Based on this view, under most circumstances, IHL would not be applied in response to a cyber operation. In other words, short of identifying a cyber 'attack' as an 'armed attack',

[73] Workshop discussions.

[74] Schmitt (2012); Tallinn Manual (2013), elaborated on in interview with William Boothby.

[75] Workshop discussions.

[76] 'Soft law' are 'rules of conduct which, in principle, have no legally binding force but which nevertheless may have practical effects' (Source: Snyder 1993 cited in Cini (2001)).

[77] Tallinn Manual (2013).

[78] Lucas (2013a, 2014), Bethlehem QC cited in Jastram (2011), Allhoff (2014).

[79] O'Connell (2012).

[80] Ibid., Reed (2015).

[81] Schmitt (2012); Tallinn Manual (2013), Allhoff (2014), Henschke (2014), elaborated on in interview with Anthony Lang.

[82] Interview with Adam Henschke.

only measures short of war such as, for example diplomatic sanctions or criminal prosecutions, would represent an appropriate response.

2.2.4. Applicability of existing moral frameworks

With a few notable exceptions,[83] the majority of literature sources and experts consulted in this study argue that existing moral frameworks based on the JWT, IHL and virtue ethics are broadly applicable to what may be future ways of fighting. While they may agree that there is no need to scrap everything and start from scratch, or that existing moral frameworks have no relevance to current and future warfighting, their views, naturally, fall on a spectrum. Some experts argue that elements of the extant moral frameworks require an overhaul and some principles a reinterpretation in light of new developments such as cyberwarfare and autonomous systems.[84] Experts whose position might be described as 'revisionist JWT' argue that the existing principles of JWT need to be interpreted in relation to individual moral action and moral responsibility.[85] Others still emphasise the universal character of the moral principles of the JWT underpinning IHL and consider that there is no need for new principles or a major overhaul of this framework.[86] Rather, what is required, they argue, is a renewed focus on the original intentions behind the law governing the use of force, which were those of post-Second World War political leaders who sought to set up a system that would protect a long-lasting peace.[87]

While the research conducted in this study suggests that extant moral frameworks remain broadly useful when examining future ways of conflict and warfighting, two separate and novel trends have also emerged in relation to the morality in future conflicts. These were mostly reflected in the discussions held at the expert workshop. First, new technologies might not necessarily bring up 'new' moral issues, yet they tend to expose existing moral problems in a more obvious way.[88] The moral dilemmas related to the use of lethal autonomous weapons systems, for example, are by some experts considered in a certain sense to be the same as those related to 'brainwashed soldiers' who are less capable of independent moral reasoning but are 'programmed' to follow orders, moral or not.[89] Contrary to this argument, however, it needs to be noted that, though 'brainwashed', soldiers still remain human beings with an inherent capability to reason morally. However, autonomous systems are not human beings and do not have an inherent 'moral compass'. Second, the way in which new technologies are used in combat, especially if such a use occurs for the first time, increases the moral responsibility of the user as their choice may set the trend for further, potentially escalatory, behaviour.[90]

---

[83] For example Dipert (2010) as the most prominent, to an extent Arquilla (1999).

[84] For example: Patrick Lin, Adam Henschke, Edward Barrett, George Lucas, Michael Schmitt, David Whetham. See References for a list of relevant works.

[85] For example: Jeff McMahan, Helen Frowe, similar position held by Valerie Morkevicius.

[86] For example: Mary Ellen O'Connell, Esther Reed. See References for a list of relevant works.

[87] Ibid.

[88] Workshop discussions.

[89] Ibid.

[90] Ibid.

Even if there may be agreement in principle on the applicability of JWT principles to current and future conflict, academic journals are replete with different interpretations of these principles. The theory has developed over centuries and academics and practitioners have taken different approaches when interpreting them. On the one hand, there is a more rules-based, legalistic interpretation that frames morality as directed by rules, guidelines and laws. On the other hand, the JWT principles may be applied casuistically, whereby the starting point is an individual engaging in practical moral reasoning on a case-by-case basis, reaching beyond law and guidelines.[91] A combination of these two approaches is a natural 'resolution' in practice and several experts consulted in this study believe that a combination enable individuals' moral reasoning to take place, particularly in complex situations of war and conflict.[92] As mentioned in paragraph 2.2.1, effective moral reasoning requires formation of a moral conscience.[93] Some experts argue that, with the increased use of autonomous and remotely piloted systems, constant media surveillance and a general 'micromanagement' of combat, alongside a generally rules-based approach to decision-making, individuals' capacity for judgement and decision-making may become restricted and their ability to deliberate along the lines of a casuistic approach to JWT may be undermined.[94] Some experts have argued that the use of remotely piloted and autonomous systems may lead to 'moral de-skilling' of human soldiers, i.e. the loss of the ability to make moral judgements,[95] although others argue that practical usage of remotely piloted aircraft seems to suggest a high level of moral deliberation among soldiers as well as a more extensive engagement of legal advisors.[96] Further elaboration of these issues is found in Chapter 3.

2.3. Impact of new military developments on moral principles

The previous two sections have outlined the general context and nature of the academic debate surrounding the issue of morality and new ways of fighting. In this section, the analysis is structured around the principles underpinning JWT and IHL, specifically focusing on those principles that seem to be most 'under pressure' when considering new technologies and new ways of conducting warfare. Chapter 3 provides a more detailed analysis of how these principles are affected by two new technologies: (1) cyber and (2) autonomous systems.

2.3.1. Action in 'unjust wars'

One of the key tenets of IHL is the distinction between 'combatants' and 'non-combatants'.[97] This distinction has fundamental implications for the treatment of people involved in or affected by conflict. In general, the same treatment is to be given to combatants and non-combatants on both sides of the

[91] Rengger (2002).

[92] For example: Paul Cornish, Anonymous, Jeff McMahan, Helen Frowe.

[93] Morkevicius (2013). 'Conscience' may be seen as a synonym of a 'soul' (term used in traditional JWT discussion).

[94] Cornish (2002), Vallor (2013).

[95] Vallor (2013).

[96] Workshop discussions.

[97] ICRC. Rule 1. The principle of distinction between civilians and combatants.

conflict, regardless of whether they are actively or passively involved in a war that is 'unjust', i.e. one that does not meet the *ad bellum* criteria for a 'just war' (see Table 1.1). From a 'revisionist' JWT perspective, individuals who have made a free choice to participate in an 'unjust war' that causes unjustifiable harm to innocents, may make themselves liable to be harmed regardless of whether, under IHL, they would qualify as 'non-combatants'.[98] As a consequence, from this perspective, all action undertaken in the context of an 'unjust war' would be seen as morally unjustifiable. For example, consider a civilian IT hacker secretly acting on behalf of a state when conducting a series of distributed denial of service (DDOS) attacks on critical national infrastructure of another state which is not (yet) involved in a state of conflict (and so the hacker may not qualify as a 'direct participant in hostilities' under IHL). This hacker may, based on the 'revisionist' JWT perspective make themselves liable to be harmed if their attack causes grave harm to innocent civilians.

From a practical point of view, however, discerning whether a war is 'just' or not is difficult and soldiers in combat have to rely on the judgement of political and military leadership. Due to the inherent uncertainty in war (see section 2.1.2), imperfect information and imperfect moral deliberation as well as the legal distinction between 'combatants' and 'non-combatants' remains a useful, albeit not a flawless principle to guide action in war and armed conflict.

2.3.2. Moral 'obligation' to reduce 'risk' in war

Some new technologies already in use or likely to be used more in future conflict, such as remotely piloted and autonomous systems and cyber, have raised a question of whether there is a moral obligation to reduce the risk faced by own forces by means of a technology that helps prevent or completely avoid casualties. Those who argue strongly in favour of such a moral obligation rely on what can be called 'the principle of unnecessary risk'.[99] The principle ascertains that: 'in trying to accomplish some objectively good goal, one must, *ceteris paribus*,[100] choose means that do not violate the demands of justice, make the world worse or entail more risk than necessary to achieve the good goal.'[101] This argument is most prominent in relation to unmanned combat vehicles and increasingly autonomous weapons. It relies on an interpretation of the principle of applying a response proportional to the means used and the requirement of a reasonable chance of success under *ad bellum* JWT principles. Moreover, the principle of discrimination may also be invoked: in addition to reducing the risk to own forces, some argue, fully autonomous weapons in particular may be capable of targeting in a much more discriminate way, therefore reducing civilian casualties.[102] If such weapons were to be programmed to comply fully with IHL, the case for a 'moral obligation' to use autonomous weapons instead of any others would be strengthened further.[103]

---

[98] Interviews with Jeff McMahan and Helen Frowe.

[99] Strawser (2010) cited in Galliott (2012).

[100] 'All things being equal'.

[101] Strawser (2010) cited in Galliott (2012).

[102] UNIDIR (2015).

[103] UNIDIR (2015).

There are three principal counterarguments to the above claims. First, while none of the experts consulted in this study claims there is a moral 'obligation' to have boots on the ground (in the form of a physically present combatant) there is an argument that the use of unmanned and autonomous weapons may devalue the martial virtues (particularly courage)[104] and could be seen as 'less honourable'.[105] There is also evidence to show that the use of unmanned combat vehicles can lower the threshold of using force. This can lower the threshold at which decision-makers resort to force through, for example, unmanned combat vehicles (as they will not be sacrificing own soldiers) which is contrary to the general prohibition on the use of force in the UN Charter.[106] Given the potentially negative impact on virtues and the evidence to the unintended consequences of unmanned combat air vehicles, it is difficult to argue that their use is morally 'obligatory'.

Second, as shown in the United Nations Institute for Disarmament Research (UNIDIR) publication on *The Weaponization of Increasingly Autonomous Technologies in the Maritime Environment: Testing the Waters*, some experts argue that even if a future autonomous system were able to function in a manner fully compliant with IHL, the requirements of the Martens Clause to consider the view within the 'public conscience' would still remain. Some of the issues falling under the 'public conscience' are questions like 'is it acceptable that human life – even if a legitimate military target – is taken by a 'robot' in absence of human intent?' and 'what are the implications for human dignity?'[107] As long as these remain unresolved, it is difficult to argue in favour of a 'moral obligation' to use autonomous technologies in combat.[108]

Finally, short to medium term, it is crucial to remember that, in practice, autonomous technology is insufficient to calculate accurately proportionality and collateral damage and thus cannot be deemed to be fully compliant with IHL.[109] 'The only way (at the moment) that the use of such a system would be legal is if its area of search and times of search for targets were to be confined to space where there are no civilians, no civilian objects, no historical or cultural heritage and no objects or persons entitled to special protection under the law.'[110] Several experts agree that the current level of sophistication is far off a fully autonomous system that would be able to conduct moral deliberation necessary to satisfy the requirements of IHL.[111] At this point in time and for the foreseeable future, based on the literature and expert opinions consulted in this study, it is therefore incoherent to argue that there is a 'moral obligation' to use autonomous weapons.

---

[104] Kirkpatrick (2015) citing Sparrow (2013) as the only author (besides himself) exploring the relationship between martial virtues and 'drones'. However, it is worth noting that Kirkpatrick (2015) argues explicitly that martial virtues do apply to the use of 'drones'.

[105] Discussions at the workshop.

[106] O'Connell (2011); Walsh, Schultzke (2015), elaborated on in interview with Mary Ellen O'Connell.

[107] UNIDIR (2015).

[108] Ibid.

[109] Interview with William Boothby, also argued during workshop discussions, detailed insights in Lin (2008).

[110] Interview with William Boothby.

[111] Interview with William Boothby, also argued during workshop discussions, detailed insights in Lin (2008).

2.3.3. Considerations on 'asymmetry' in conflict

Much has been written on the topic of 'asymmetric warfare' and especially in the last two decades, 'asymmetric wars' and conflicts have invited analyses from both strategic and ethical points of view. The moral questions debated in the literature reviewed for the purposes of this study are: (1) whether asymmetry in and of itself in warfare poses a moral problem and (2) whether asymmetry is inherently immoral. These questions are usually considered in relation to unmanned combat vehicles and autonomous systems but they could also apply to offensive (and defensive) cyber capabilities, as well as other novel technologies. The so called 'asymmetry objection'[112] relies on an argument that the use of technologically superior capabilities against an adversary without such (or even remotely equivalent) technology makes the fight 'intrinsically unfair' and therefore unjust.[113] In such a fight, following this line of thought, the risk is disproportionately laid on the force[114] without the technological capabilities and it is implausible that such a war constitutes a proportional response to the means used. Though not a military ethicist, Clausewitz wrote about a situation of radical asymmetry (usually after one force had suffered military defeat but the war had not yet ended) where 'war' is no longer 'war' but, rather, becomes 'administration' and the winning force operates almost entirely risk-free.[115] One of the interviewees in this study commented that the risk that exists in warfighting is part of the moral character of war: if it is taken away, the nature of war changes.[116]

In a sense, however, it can be said that all conflicts are asymmetric in that there is never parity in the means and capabilities employed in the fighting.[117] Several interviewees consulted in this study argue that asymmetry of means in and of itself does not pose a moral problem.[118] Furthermore, an insistence on symmetry in conflict might result in the prolonging of human suffering as it could lead to entrenchment rather than rapid resolution.[119] What matters from a moral perspective is whether the party using technologically more advanced means is doing so with a just cause and in a proportionate and discriminate manner. Some experts suggest that the opponent without the technological means and without a just cause has made themselves liable to be harmed and that there might even be a moral obligation to use technologically more advanced weapons if they are proven to reduce the risk to combatants on the side of the actor who has a just cause.[120]

---

[112] Galliott (2012).

[113] Galliott (2012).

[114] Ibid.

[115] Clausewitz (originally published 1832).

[116] Anonymous.

[117] Workshop comment.

[118] For example, interviews with Jeff McMahan, Helen Frowe, Mary Ellen O'Connell, Nigel Biggar, David Ronfeldt.

[119] Workshop discussions.

[120] Interviews with Jeff McMahan and Helen Frowe.

2.3.4. Proportionality of response

Related to the question of the moral implications of asymmetry of capabilities is the question of what constitutes a proportionate response, particularly in cases involving non-kinetic attacks coming from another state. This applies to cyber attacks in particular. The first step in answering this question is to determine whether the 'attack' constitutes an 'armed attack' and, as such, whether it triggers the invocation of IHL.[121] As outlined above (section 2.1.1), short of an 'armed attack', the situation is not governed by IHL and the permitted response would have to be in line with criminal law and international human rights law.[122]

Several experts argue that if the state does determine that an 'armed attack' had occurred and it is able to attribute this to a state or a non-state actor, the response may take either a kinetic or a non-kinetic form as long as the legal criteria of proportionality are met and that such a response constitutes a last resort, that is, all other options having been exhausted.[123] Essentially, based on this view, the military response may take either form as long as the *jus ad bellum* requirements are fulfilled.

In the case of a cyber attack, however, the moral deliberation assumes a special degree of gravity. While a cyber attack can cause significant damage and, by second-order effects, can even cause lethal damage, a moral challenge emerges as to when this damage is great enough to warrant a response?[124] Also, if the response takes on a kinetic form, what precedent does that set for future action?[125] And, following from that, what implications might this have for potential conflict escalation?

In theory, a kinetic response to a non-kinetic attack does not, by itself, present moral challenges to the principles of last resort or proportionality. In practice, however, there would be a need for extensive legal and moral deliberation to determine whether the attack qualified as an 'armed attack' and whether no alternative responses were possible to achieve the desired outcome. Also, it would be important to consider the probability of escalation and take into account any harm that could be created by a disproportionate and potentially illegal counter-attack (e.g. by use of nuclear weapons or by an overwhelming kinetic response).[126] Lastly, the government would also need to consider the importance of setting a precedent, which, in itself, brings with it special moral responsibility.

2.4. Key findings

This section provides a brief summary of the key findings from an analysis of the academic debate on the topic of morality and cross-domain conflict. Each of the findings is based on and supported by the analysis presented earlier in this chapter.

---

[121] Schmitt (2012), Tallinn Manual (2013), Bethlehem QC cited in Jastram (2011), also discussed in interview with William Boothby.

[122] Bethlehem QC cited in Jastram (2011) elaborated on in interview with Sir David Omand and interview with Mary Ellen O'Connell.

[123] Lucas (2013a), Allhoff (2014).

[124] Allhoff (2014), point also raised in interview with Sir David Omand.

[125] This point was raised during workshop discussions.

[126] Interviews with Jeff McMahan and Helen Frowe.

1. The blurring of distinctions between peace, conflict and war creates a 'grey area' in which the appropriate application of legal and moral principles requires careful and ongoing deliberation, including a periodic revisiting of a question of whether there are any alternatives (military/non-military) to the status quo.
2. Given the uncertainty created by war, moral deliberation is difficult and the exercise of discretion is crucial. There is convergence in academic thinking, focusing on the moral responsibility of the individual (whether in command or direct combat action). Developing individuals' ability to apply practical moral reasoning is key to ensuring that decisions taken within the context of conflict are in line with the principles of the JWT and IHL. Development of practical moral reasoning can be facilitated by training, education, good leadership and allowing individuals to apply moral reasoning without unnecessary external interference.
3. In a world of social media and the high speed of information exchange, public perceptions can serve as an indication of 'public conscience' and can have a positive or negative effect on the government's willingness to use force as well as on the manner in which force is used. As such, they can significantly alter the *jus ad bellum* and *in bello* assessments of a given conflict.
4. Recognising that all parties signatory to the Geneva Conventions and other instruments of IHL are bound by it, it must be noted that NSA and also some state actors do not (fully) abide by these principles and, instead, apply a different ethical framework to their military decisions. This study was undertaken from a Western perspective and moral questions are deliberated with reference to the JWT and IHL. All findings and analyses in this report should be interpreted in light of this caveat.
5. There is general agreement among experts that focusing on the 'cross-domain' aspect of conflict is less helpful in deliberating on moral questions compared with a focus on effects (kinetic vs non-kinetic) of a military operation or a focus on technologies (both their use and their inherent characteristics).
6. The academic debate displays great diversity in legal interpretations of 'armed attack' as well as on the appropriate application of international law to different situations that cause physical or non-physical harm. The most contentious area here is cyber.
7. The majority of experts involved in this study believe that existing moral frameworks and principles apply to current and future forms of warfighting, albeit some advocate a new interpretation of existing principles, while others argue these principles are inviolable.
8. A 'revisionist' approach to JWT holds that the legal distinction between combatants and non-combatants may not account for the moral intentions of individuals involved in conflict. Based on this view, even 'non-combatants' may make themselves liable to be harmed if their actions are such that they support an 'unjust war' and cause great harm. Following this logic, there may be an argument to support a more nuanced understanding of 'non-combatants'.
9. Some experts argue that there is a 'moral obligation' to use weapons that lower the risk of casualties and are more discriminate. Strong counterarguments can be put forward against this view, particularly in relation to the use of unmanned aerial combat vehicles, the use of which raises a number of moral challenges.
10. The research suggests there is a consensus among academics consulted in this study that asymmetry in conflict does not, by itself, pose moral problems. Practical concerns raised by the

use of unmanned combat air vehicles do not stem from the asymmetric technological advantage but, rather, from their use against adversaries and civilians not involved in an armed conflict.

11. There is a general agreement in theory that a non-kinetic attack, once determined to constitute an 'armed attack' may merit a kinetic response. In practice, however, it may be that measures short of war would be considered more appropriate. Also, any such case would need to be considered in light of a moral responsibility of precedent-setting.

3. Case studies

3.1. Rationale

This chapter examines the academic debate surrounding two technological areas: cyber; and autonomous systems. It provides a synthesis of the current thinking on the moral considerations associated with these capabilities and identifies those issues that emerged – either in the literature review or through contact with study experts – as being most morally complex.

The inclusion of case studies is intended to explore the 'practical' moral considerations linked to specific technologies as well as to consider the more abstract elements of the debate. By examining the ways in which specific technologies challenge current morality frameworks and schools of thought, it is possible to derive insights that may not be apparent solely through studying the wider morality debate.

The selection of these specific technologies as 'case studies' does not imply that they pose more or more difficult challenges than other technological areas. These technology areas were selected principally because they received the most coverage in the sources considered by the study team.

3.2. Cyber

3.2.1. Context

Cyberspace may be defined as a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[127] A cyber attack may be defined as a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to (physical or virtual) objects.[128] However, as indicated in section 2.2.3, determining whether a cyber 'attack' constitutes an 'armed attack' is subject of an ongoing and contentious debate.

Cyberspace is a thing of contrasts: it is a space and is thus similar to other domains of contention such as the land and maritime environments. It is also a space unlike any other, a new domain of objects and entities with both physical and virtual properties,[129] making it dissimilar to other domains. Cyberspace,

[127] Joint Publication 1-02 (2008), DoD Dictionary of Military Terms.

[128] Tallinn Manual, (2013).

[129] Barrett (2013).

therefore, has to be appreciated on its own merits,[130] not least with the increasing militarisation of cyberspace, as states have begun to project 'cyberpower' within the international system.[131]

Some view 'cyberwarfare' as the first major new form of warfare since the development of nuclear weapons. As such, there currently exists a policy vacuum with absence of an informed, open, public or political discussion of what an ethical policy for the use of cyber weapons might be.[132] Cyberspace has been called a 'lawless wild-west' in which 'anything goes'.[133] This has led some scholars to urge states to set a positive precedent through the establishment of mutually beneficial relationships and approaches to conduct in cyberspace.[134] Others have argued that cyberwarfare is not amenable to regulation by international pacts and that long periods of low-level, multilateral cyberwarfare are likely until such point that a game-theoretic equilibrium is sought.[135] In other words, only through the application of game theory principles will strategies be discovered that are both moral and effective in suppressing overall harm to all parties in the long run.[136]

A number of contextual factors were discernible in the debate on morality in relation to cyber:

- **Cyber contributes to a blurring of the distinction between peace and war.** The nature of the cyber domain creates uncertainty as to what acts constitute conflict (as opposed to crime or other offensive or threatening activities) in cyberspace and, in turn, the kinds of actions that are morally appropriate in response (since these will depend on whether a conflict or law enforcement moral framework applies).
- **Cyber does not conform neatly with the central tenets of international law**. One of the morality questions often encountered in the debate is whether a cyber attack can constitute an 'armed attack' under Articles 2.4, 39 and 51 of the UN Charter, thereby establishing *casus belli*[137] and legitimising a kinetic or non-kinetic response. Cyber operations can cause dire consequences but do not fit neatly into the notion of an attack that is 'armed' in the kinetic sense. This raises the question: at what point does the damage caused by a cyber attack become sufficiently great to warrant a kinetic response?[138] Various sources concur with Schmitt's view that, within the spirit of the law, armed attack in the cyber context can be interpreted as encompassing any acts that result

[130] Libicki (2009).

[131] Nye (2010). Nye provides the following definition of cyberpower: 'the ability to use cyberspace to create advantages and influence events in other operational environments and across the instruments of power. Cyberpower can be used to produce preferred outcomes within cyberspace or it can use cyber instruments to produce preferred outcomes in other domains outside cyberspace.'

[132] Dipert (2010).

[133] Cornish (2010).

[134] Ibid.

[135] Dipert (2010).

[136] Ibid. Game theory is a branch of mathematics that is concerned with strategic decisions in competitive situations where the outcome of participant's choice of action depends on other participants' choices. Game theory can be applied to strategic decisions in business, economics and war, among others.

[137] Latin meaning 'the case for war'.

[138] Interview with Nigel Biggar.

in consequences analogous to those caused by the kinetic actions originally envisaged by the term 'armed attack'.[139] The majority of the International Group of Experts involved in drafting the Tallinn Manual did not believe that the term 'armed' necessarily requires the employment of 'weapons': they considered that the critical factor was whether the effects of a cyber attack were comparable to those resulting from a kinetic attack. An opposing view to this conception of cyber holds that it is not IHL that has primary application to cyber activity; rather, these activities fall under international law governing economic and communications activity.[140] From this point of view, cyber 'attacks' are considered primarily criminal acts to be handled under the regime of sanctions, countermeasures, criminal prosecutions, and not responded to in a military way.[141]

- **If occurrence of a cyber 'attack' is established, response can be kinetic or non-kinetic**. Once the occurrence of a cyber 'armed attack' is confirmed, an appropriate response – whether kinetic or non-kinetic – may be morally justifiable. As indicated in Chapter 2 (section 2.3.4), however, it is important to consider the potential practical implications of kinetic response to a non-kinetic attack that may involve conflict escalation and repercussions in public perceptions and public support of the government's actions.
- **Cyber is still sufficiently new that its offensive or defensive use may set an enduring precedent**. As with any novel capability, the first or early use of, or response to, the capability represents a morally important choice since it may set a precedent for its future use. Some sources were supportive of a moratorium on the use of cyber until an appropriate framework is established for the moral application of cyber effect.[142] This would prevent the establishment of dangerous 'knee-jerk' precedents that could pose significant problems downstream. It was acknowledged, however, that the development of such a framework would require more political will than is currently thought to exist, not least given the inherent difficulty of the task.[143]
- **Cyber challenges temporal and spatial considerations and involves a large number of state and NSA, potentially challenging the state monopoly on the use of force**. Cyber represents a departure from traditional forms of conflict in two distinct areas. First, cyber reduces the time available for decision-making. This is apparent both in traditional forms of conflict that are now underpinned by information systems and in cyber conflict. There may be less time available to consider the moral dimension of available options and it may be necessary to pre-programme some decisions. The near-instantaneous nature of cyber may also erode distinctions between *ad bellum*, *in bello* and *post-bellum* as a cyber conflict could be initiated and completed in a matter of milliseconds. Second, cyber collapses and transcends the notion of physical distance, which is a critical constraint in the conduct of conflict in all other domains. It also creates new potential zones of conflict and targets including server facilities and cyber operatives as well as private

[139] Schmitt (2012).

[140] O'Connell (2012).

[141] Ibid., also mentioned by a workshop attendee.

[142] Workshop attendee.

[143] Workshop discussions.

corporations.[144] Since cyber 'weapons' may be employed without the knowledge or approval of the state, the state's monopoly on the use of force is challenged.

- **Cyber may lower *ad bellum* threshold and may alter *post bellum* considerations**. As argued in detail below, the relatively lower levels of harm caused, the relative 'ease' of deployment of cyber weapons and the challenges posed by attribution may lower the threshold of the government's resolve to use force.[145] The *jus ad bellum* principles can therefore be deemed to deserve a refined or even a completely new interpretation. Additionally, some argue that the reversibility of a cyber 'attack' may make the *post bellum* reconstruction significantly easier compared with a kinetic attack.[146] A counter-argument to this view holds that evidence shows how easily such an 'attack' may spiral out of control.[147] As such, determining not just what the attacked targets are but also the degree of damage may be difficult, making it impossible to 'reverse' the damage in any meaningful way.[148]

3.2.2. Challenges posed to morality principles by cyber conflict

Conflict in cyberspace appears to challenge – or at least complicate – a number of the central principles of existing moral frameworks. In particular, cyber does not allow for the straightforward application of the principles of just cause, proportionality, legitimate authority, last resort, discrimination and right intent.

The following matrix explores in brief the challenges posed to the morality principles by cyber conflict. More detailed descriptions of some of these challenges may be found below.

Table 3.1. Ways in which cyber challenges morality principles

Principles	Challenges posed
Just cause	Does a cyber attack constitute an 'armed attack'? Can the perpetrator of the original attack be reliably identified?
Legitimate authority	Since cyber operations may be conducted by many actors, does the notion of the state's monopoly on the use of force withstand scrutiny?
Right intent	Can the motives underlying a cyber attack be determined or proven?
Necessity/Last resort	Does cyber represent an 'easy option, lowering the threshold for policymakers to use force? Could a pre-emptive cyber attack prevent worse harm being caused later and what would be the moral implications?
Probability of success	How far can the outcomes of an attack be predicted? Can damaging

[144] Interview with Anthony Lang.

[145] Arquilla (1999).

[146] Lin (2012).

[147] Ibid.

[148] Ibid.

	effects be limited? What is the likely response of the adversary?
Proportionality	What would be a proportionate response to an attack and how can this be determined (given the difficulty associated with quantifying harm caused)?
Discrimination	Given the potential for cascading effects and unintended consequences, can cyber ever be truly discriminate? Does cyber challenge the current definition(s) of 'non-combatant' with implications for non-combatant immunity?

Just cause

The existence of a just cause for going to war is the central tenet of the JWT: to lack just cause would render all actions thereafter in war immoral. The Tallinn Manual considers that a state that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence.[149] As explored above, the question of whether a cyber attack constitutes an 'armed attack' (or commensurate harm) is pivotal to whether or not just cause exists and whether the resort to force can therefore be justified. Some experts have suggested that a more nuanced understanding of 'attack' be embraced whereby cyber operations causing serious harmful consequences such as severe economic effects or significant disruption of societal functions may be characterised as 'armed attack' even where these do not result in death, injury, damage or destruction.[150].

Some commentators contend that the threshold at which an attack becomes an 'armed attack' should not be made public, arguing that, for deterrence to be effective, the adversary should not have a clear appreciation of where the boundaries lie.[151] Others posit that without a shared understanding of where the boundaries lie, a credible deterrent cannot be established.[152]

A further problem in determining just cause in cyber conflict is the issue of attribution. The just cause principle rests, in part, on there being a readily identifiable protagonist against whom it is justifiable to enter into conflict. A primary facet of cyber operations is that they often offer plausible deniability such that determining with any certitude the actors and agents culpable presents a challenge.[153] In many cases, states can plausibly claim that attacks may be shown to have originated in their territory but that they were not sanctioned by the government. This represents a problem: if the perpetrator of the original attack cannot be reliably identified, the argument follows that it is not morally permissible to respond by attacking the suspected source of that attack.

This raises the question of whether it is ever morally justifiable to respond to a cyber attack where there is uncertainty regarding the identity of the perpetrator. If conclusive proof is required, the time taken to

[149] Tallinn Manual (2013).

[150] Schmitt (2012).

[151] Lucas (2013a).

[152] Mazo (2011).

[153] Arquilla (1999).

acquire this may pose a delay, which may in turn erode the operational advantage or probability of success of any response: this presents a morality consideration of its own.[154] If conclusive evidence is not required, the 'certainty threshold' is likely to be case specific and will depend not only on the evidence of culpability, but also on the possible consequences or the escalation chain of a response (or non-response). Some experts believe that the challenge of attribution can be addressed in a manner similar to conventional conflict, threatening to regard the state suspected of hosting the hostile actor as 'complicit' unless they address the criminal behaviour within their borders.[155]

Right intent

For 'right intent' to exist, the resort to force must be for the sake of the just cause and without ulterior motive. The existence of a just cause for going to war is, in itself, insufficient, since the motivation or intent behind the resort to war must be morally justified too. It is not morally permissible, under traditional JWT, to engage in conflict for impure motivations such as territorial gain or to exact revenge, even if the cause is just.[156] In addition to just cause, to have right intent, the conflict activity must not exceed that which is necessary to vindicate the just cause and must be conducted in a manner likely to yield a 'just and lasting peace'.

Various sources concur that the use of cyber operations is permissible providing it is motivated primarily by the intent to cause proportionate harm to military (rather than civilian) infrastructure or to degrade an adversary's ability to undertake destructive offensive operations.[157] It is not permissible if harm to civilians or the destruction of civilian infrastructure is intended (rather than occurring as an unintended outcome).[158] If a 'just cause' can be established, the use of accurate non-kinetic cyber operations may allow for the cause to be vindicated while causing minimal loss of life or physical damage.[159] As a result of the limited harmful effects of a cyber 'attack', cyber weapons may become more attractive as a means to exercise pre-emptive or even preventive military operations.[160] This argument contends that the preventive use of cyber weapons could potentially reduce the probability of future harm, e.g. by disabling a kinetic capability or slowing the proliferation of weapons of mass destruction.[161] The Stuxnet case study (in which a malicious cyber worm was used to disrupt the Iranian nuclear enrichment programme) is cited to support this claim since the cyber operation resulted in a significant delay to Iranian nuclear enrichment.[162] In response to this argument, however, it must be remembered that 'preventive' operations

[154] Workshop discussions.

[155] Lucas (2013a).

[156] Burkhardt (2013).

[157] Lucas (2013a), Arquilla (1999).

[158] Lucas (2013a).

[159] Arquilla (1999), Lucas (2013a).

[160] Arquilla (1999).

[161] Ibid.

[162] Lindsay (2013).

are illegal under IHL and pre-emption is only allowed under very narrow circumstances, including an imminent attack.[163]

Last resort

Cyber poses a challenge to the principle of 'last resort', the notion that engagement in conflict should only occur as a matter of absolute necessity, all other reasonable alternatives having been exhausted and when further delay threatens to make the situation worse.[164] Since cyber operations may cause widespread disruption but relatively little destruction, they may be considered as an easier and less destructive option to address the harm done or intended.[165] Whether it can be argued that their use can qualify under the just war principle of 'last resort' will depend fundamentally on whether a 'cyber attack' qualified as 'armed attack' and thus whether the use of force is the morally right response (see section 3.2.1). As indicated earlier, the difficulty of identifying what international law framework applies to specific cyber activity is likely to make it very difficult to argue that a military response is one that constitutes 'last resort'. Before resorting to the use of military force, all other options available under international criminal law should be explored to respond to the harmful activity carried out against the affected state.

From the perspective of cyber offence, the principle of 'last resort' appears to be fundamentally undermined for the reasons outlined in the previous section: greater 'ease' of use due to limited damage; greater likelihood of using cyber in a preventive manner, with the intention of preventing 'greater harm'.[166]

Proportionality

Cyber poses a number of challenges to the principle of proportionality, which is inherently a difficult elastic concept and one that is not easily applied.[167] The research conducted in this study shows that it is difficult to determine what constitutes a proportionate response to a cyber attack.[168] As with the other principles analysed in this chapter, the determination of what constitutes a 'proportional' response will depend, to a large degree, on the definition and assessment of 'harm' caused by the original attack (see section 3.2.1 for detail). This may be, in itself, difficult to quantify. While the direct impacts of a cyber attack may, in some cases, be discernible, often the second- and third-order effects are less readily identifiable or their causality difficult to establish. Effects may be tangible (e.g. number of direct/indirect deaths, direct/indirect financial impacts) or intangible (e.g. psychological impacts).[169] Establishing whether these cascading effects were foreseen and intended by the adversary is also problematic.

---

[163] Interview with Mary Ellen O'Connell. A wider discussion on the morality of pre-emption and prevention falls outwith the bounds of this study.

[164] Lucas (2013a).

[165] Arquilla (1999).

[166] Ibid.

[167] Interview with Nigel Biggar.

[168] Workshop discussions and interviews.

[169] Workshop discussions.

When considering response options, the debate seems fragmented. In determining the type of response that might be proportionate, various sources suggest that it is the violence produced by the original attack rather than the technical nature of the attack that is critical.[170] Thus, it may be that a high level of disruption to a modern industrial state is sufficiently grave that the application of lethal kinetic force in response would be proportionate,[171] even when the original strike had not caused any direct lethal effects.

Under such circumstances, there appears no moral obligation for the attacked state to constrain itself to an 'in kind' response (see section 2.3.4).[172] In other words, it is not the case that the only proportional response to a cyber attack is a cyber counter-attack. Indeed, given the inherent inability to understand the full potential harm that could be caused by a cyber attack, an in-kind response might be high risk, increasing the possibility of becoming embroiled in an escalatory tit-for-tat cyberwar with an adversary. The Tallinn Manual offers the following guidance: 'a cyber attack that 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 is prohibited'. In practice, however, the effectiveness and scope of many cyber attacks cannot be known in advance, particularly if they have never been used before.[173]

The possible escalation chain should also be at the heart of proportionality considerations. The questions posed include: would no response encourage future attacks? Would a robust response be capable of suppressing the future threat from this adversary and deterring other would-be attackers? Would a robust response prompt escalation of the wider conflict? These questions all have moral considerations because of the obligation to minimise unnecessary harm implicit within the JWT and international law. If, by responding or not responding, the risk of unnecessary harm is increased, this should be taken into account also in response deliberations. Some strategists conclude that proportionate cyber responses are impossible because escalation control in this domain is too difficult.[174]

Discrimination

Traditional frameworks of morality dictate that war must be discriminate in nature, distinguishing between legitimate targets and non-combatants. This is echoed in soft law pertaining to cyber. The Tallinn Manual states that it is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature, i.e. if they cannot be directed at a specific military object or limited in their effects as required by the law of armed conflict.[175] However, while those executing a cyber operation may intend it to be discriminate in its effect, the inter-dependent nature of the cyber domain may result in unintended consequences whereby civilians or non-military infrastructure are affected. A cyber attack may

[170] Interview with William Boothby.

[171] Interviews and workshop.

[172] Lucas (2013a), Allhoff (2014).

[173] Henschke (2014).

[174] Mazo (2011).

[175] Tallinn Manual (2013).

proliferate beyond that which is anticipated or planned, causing cascading effects that affect those who are not legitimate targets within a conflict.

Cyber may erode the norm that civilians should not be considered permissible targets of war. According to the legal definitions within the Geneva Convention and its additional protocols, civilians directly participating in hostilities may be considered legitimate targets of war. Technology workers and others active in cyberspace (whether directly involved in cyber operations on behalf of a legitimate political authority or not) may increasingly find themselves targeted in adversary attacks and counterattacks.[176]

While some cyber attacks may have a degree of reversibility, this will not always be the case. *Jus post bellum* therefore needs to be considered early in the planning stages of a cyber operation (see section 3.2.1 for detail).

Challenges to other principles

According to JTW, political authorities within established political systems are the only actors with the legitimate authority to wield the use of force. In turn, such political authorities 'own' the instruments of violence (land, air, maritime and space assets). Cyber complicates this principle: unlike traditional military assets, cyber is a global commons, owned by no one and accessible by everyone from government agencies to NSA to private individuals.[177]

Under the JWT, a reasonable probability of success is necessary if a war is to be just. In other words, the benefits offered by engaging in a conflict must be judged attainable, balancing at least some of the suffering involved.[178] With cyber conflict, success itself may be difficult to define. Further, uncertainty surrounding the second- and third-order effects of cyber operations (compounded by their potential lack of visibility) may make probability of success more difficult to discern than in traditional forms of conflict or war.

3.3. Autonomous systems

3.3.1. Context

Alongside cyber, advances in military robotics have also been the subject of wide and lively debate among both military strategists and ethicists – with autonomous systems now the 'most controversial conventional weapons platform in the UK Armed Forces' portfolio'.[179]

The proliferation of autonomous technologies has brought a new urgency and practical dimension to longstanding theoretical discussions about machine morality and artificial intelligence (AI). According to the US Government Accountability Office, the number of countries operating unmanned air vehicles (UAVs) doubled in the period 2004–2012[180] – the UK Ministry of Defence (MOD) reports that around

[176] Henschke (2014).

[177] O'Connell (2012), Reed (2015).

[178] Harbour (2011).

[179] Birmingham Policy Commission (2014).

[180] US GAO (2012).

80 state militaries now possess an unmanned intelligence, surveillance, target acquisition and reconnaissance (ISTAR) capability, with around a dozen operating armed systems.[181] On land, unmanned systems have long been used for explosive ordnance disposal (EOD) purposes, with armed systems being deployed to guard borders and military facilities in Israel, Russia and South Korea. A number of countries, including the UK, are also making significant investments in development and testing of autonomous maritime systems – with the US Navy deploying its first unmanned underwater vehicles (UUVs) from a *Virginia-class* attack submarine in 2015.[182]

For the purpose of this study, the term 'autonomous systems' denotes a broad range of capabilities: from 'remotely piloted' systems reliant on human control; through 'automated' systems capable of conducting a limited number of tasks without human input; up to 'fully autonomous' systems equipped to operate without human direction for extended periods of time. These systems may operate in the land, air, maritime, space or cyber domains – the focus is on the capacity of the software for moral deliberation and Kantian moral agency, rather than on the hardware or platform itself.

Important outstanding questions include:

- Could and should a machine ever be capable of moral deliberation (from an ethical rather than technical standpoint)?
- What degree of human control is needed or desirable? Who is responsible for acts conducted by autonomous systems (including malfunctions, collateral damage, or war crimes)?
- Is morality something that can be programmed, or must it be learnt? What about legality?
- Are existing moral and legal frameworks adequate, or are new prohibitions and norms required? Should machines be held to the same standards as humans, or need they attain a higher standard?
- How can machines best be used to overcome the moral limitations of human warfighters?

These issues have prompted a wide range of responses. As with cyber, experts are divided as to whether autonomous systems represent a continuation, evolution or revolution in military ethics. This diversity of viewpoint is presented in section 3.3.2 below.

A number of contextual factors are relevant when considering this issue:

- **The relationship between levels of autonomy and moral permissibility is non-linear and complex**. Much of the strongest opposition to unmanned systems is focused on lethal autonomous weapons systems (LAWS) capable of operating and killing without human command. Such systems, with their sophisticated capacity for independent reasoning (moral or otherwise) throw questions of machine morality into the sharpest relief. However, literature and interviews also suggested it would be wrong to infer a simple, linear relationship between a given system's degree of autonomy and its moral acceptability. Though increasing a system's autonomy brings heightened concern over the lack of human oversight and the question of moral agency, it also reduces the influence of human error, fatigue or emotion, all of which may undermine moral decision-making. A robot soldier cannot feel anger, lust or a desire for revenge, nor experience

[181] Brooke-Holland (2013).

[182] Osborn (2015).

sleep deprivation or psychological trauma. Furthermore, as noted below, fully autonomous systems may be more effective on the battlefield in certain contexts, increasing the 'probability of success' discussed in JWT. As such, there are moral benefits and risks associated with both low (largely manual) and high (largely automated) autonomy systems, while mid-level systems may be affected by the drawbacks of both human fallibility and machine inflexibility.

- **Debates over autonomous moral agency raise questions over who is responsible for a machine's choices, actions and mistakes**. As Lucas (2013) reports, the use of autonomous systems prompts key questions over the chain of human responsibility for the moral deliberations of a machine. This raises issues over product liability and criminal negligence, meaning that the designers, programmers and exporters of any such technology could be liable for war crimes committed through the machine's malfunction, failure or poor design.[183] The UNIDIR report notes that a judgement is needed as to what level of technical compliance would be morally permissible in a lethal autonomous system in terms of its known error or fail rate. This debate over the chain of moral agency and responsibility for machines also flags up the fact that voters, policymakers, industry and others are also involved in shaping the moral deliberations (and failings) of human soldiers.[184]
- **Attempting to reduce morality to an algorithm is an exercise with implications for the wider Just War debate**. As Morkevicius (2013) observes, the very process of debating the potential for autonomous systems with the capacity for moral deliberation may throw wider, unresolved issues with JWT and IHL into focus: 'Developing fully autonomous military robots should be doubly desirable: the technical process of "teaching" robots ethics would finally systematise Just War thinking, while robots could uphold the rules of engagement even under the most emotionally trying of situations'.[185] Against this, however, are arguments that the morality of war is not meant to be systematised or rules-based; rather, it derives its potency and utility from being a 'living tradition'.[186]
- **The ethical standard to which autonomous systems should be held is subject to debate**. For some experts, the focus on the question of a machine's capacity for moral deliberation is overly speculative, or else a 'red herring' that distracts from more immediate concerns. Arkin (2007) suggests, for instance, that rather than trying to 'gold-plate' full moral deliberation into machines, both technologists and ethicists should instead focus on more achievable aims.[187] As Lucas (2013) argues, 'We neither want nor need our unmanned systems to be ethical, let alone more ethical or more humane than human agents. We merely need them to be safe and reliable, to fulfil their programmable purposes without error or accident, and to have that programming designed to conform to relevant international law (such as the IHL) and specific rules of engagement'.[188] This

[183] Lucas (2013b).

[184] Lin (2015).

[185] Morkevicius (2013).

[186] Anonymous.

[187] Arkin (2007).

[188] Lucas (2013b).

assumes that legal compliance may be more precisely defined and thus simpler to code than more casuistic, context-sensitive morality.

- **Deployment of fully autonomous systems may shape a wider precedent or moral norm**. Though remotely piloted systems have proliferated widely and seen extensive battlefield use, the future deployment of fully autonomous systems is likely to play an important role in shaping wider norms as to the technology's use. As such, civil society groups such as the Campaign to Stop Killer Robots or international bodies such as the United Nations (UN) Convention on Certain Conventional Weapons have discussed the possibility of a moratorium on development of such systems until their moral, strategic and political implications are fully understood. Crosston (2014) has noted that the proliferation of autonomous technologies means it would benefit early adopters (e.g. US, UK) to set an exemplar for responsible use before other states achieve technological parity.[189]

3.3.2. Challenges posed to morality principles by autonomous systems

Conflict involving autonomous systems appears to challenge – or at least complicate – a number of the central principles of existing moral frameworks. The following matrix explores in brief the challenges posed to the morality principles by autonomous systems. More detailed descriptions of some of these challenges may be found below.

Table 3.2. Ways in which autonomous systems challenge morality principles

Principles	Challenges posed
Just cause	Autonomous systems have been synonymous in recent years with breaches of sovereignty and targeted killings. What is an 'armed attack' or *casus belli* in relation to autonomous systems? Who is liable for a machine's atrocities?
Legitimate authority	How should 'meaningful human control' be defined in relation to autonomy? What independent authority should a machine hold? Does autonomy blur the distinctions between combatant and non-combatant?
Right intent	Can a machine possess intent or moral agency? Does use of autonomous systems entail a loss of martial virtues?
Necessity/Last resort	Do autonomous systems lower or raise the threshold for policymakers to use force? What are the implications for perceptions of a war's legitimacy?
Probability of success	Do leaders have a moral obligation to use autonomous systems to prevent friendly and civilian losses? Is there a threat of strategic backlash?
Proportionality	Do asymmetry and distance pose moral problems? Can a machine act in self-defence? Can an autonomous system use lethal force in line with principles of

[189] Crosston (2014).

	proportionality and human dignity?
Discrimination	Can autonomous systems be sufficiently discriminating to allow for independent moral agency? Are they better suited in certain domains?

Just cause

Discussing the morality of autonomous systems in relation to 'just cause' is often conflated with wider debates about the legitimacy of targeted or extrajudicial killing. The complex debate over the feasibility or desirability of moral deliberation in autonomous systems is further complicated by their recent role in controversial operations (particularly by the US) to target NSAas part of the so-called War on Terror. These raise questions related to the sovereignty of fragile states; the acceptability of states targeting their own citizens abroad; the place of non-military bodies (e.g. the Central Intelligence Agency) in operating unmanned systems; the risk of civilian casualties; and the wider role of military force in counterterrorism, as opposed to law enforcement or other paradigms. As Mayer (2015) notes, the focus of much public controversy and academic debate has therefore been 'primarily on policy decisions regarding how the platform has been employed rather than on the inherent characteristics of the technology itself. While well intentioned, the conflation of the use of armed drones with the tactic of targeted killing has muddled rather than clarified an important discussion regarding the strategic and sociological impact of next-generation unmanned combat air vehicles (UCAV) and machine autonomy'.[190]

Examining autonomous systems outside of this recent policy context suggests fewer inherent difficulties in relation to the notion of 'just cause'. Insofar as autonomy is dependent on the cyber domain, unmanned systems present new opportunities for non-lethal or a non-kinetic attack that may undermine the traditional definitions of 'armed attack' or 'harm' used to justify defensive war. Though partially autonomous or remotely piloted systems are unlikely to be subject to international ban, it may be that use of fully autonomous systems is judged '*mala in se*'[191] in future, much like use of chemical or biological weapons. If so, this could present a new category of *casus belli* for states seeking to defend international norms, prevent war crimes or counter proliferation. As noted above, there are also unresolved issues with the question of responsibility for the actions of autonomous systems that inflict unwanted destruction or fatalities through machine error – if state X procures a system from state Y, but the system accidentally conducts a strike against state Y, which country (if any) should be liable to retaliatory strike?

[190] Mayer (2015).

[191] Latin meaning 'wrong in itself'.

Legitimate authority

The use of autonomous systems poses a wide variety of questions about the relationship between human and machine authority. Even in the context of remotely piloted systems, operating with little or no autonomy, critics contend that the growing reliance on technical means may influence, cloud or desensitise human thinking. Even the design, assumptions and idiosyncrasies of the underlying algorithms that collect and analyse data to feed to pilots can bring their own 'techno-politics' that shape the way in which moral decision-making is framed.[192] Worryingly, data links can also be spoofed (i.e. falsified or forged) or hacked.[193] On the more positive side, by contrast, teaming humans with autonomous systems that will observe and record their every act may improve human compliance with IHL– though the effects of this surveillance on unit cohesion and morale may be less desirable.[194]

For fully autonomous systems, the concerns are more heightened still: can a machine ever have authority to take a life? If it can, does this logically entail that it could also have authority to start an entire war as an agent of state policy? Given these concerns, recent debate has coalesced around the notion of 'meaningful human control' – a concept that emerged as a major theme at the UN Convention on Certain Conventional Weapons in May 2014. As Horowitz and Scharre (2015) argue, 'one [particular] issue motivating the focus on meaningful human control is concern about a potential "accountability gap"'. To address this issue, experts argue for maintaining a human 'in the loop'; ensuring these human operators are adequately trained and have sufficient information to make moral, lawful decisions; and conducting rigorous testing of autonomous systems to ensure they are controllable and do not pose unacceptable risk.[195] Issues of this kind become even more complex as machines proliferate and are taken up in increasing numbers and sophistication by NSA; indeed, taken to their logical extreme then machines could themselves in future become a new category of legal actor (e.g. just as corporations can hold legal personhood), further complicating the consideration of moral and legal agency on the road to war.

There are related concerns about the balance between human and machine authority, which may affect not only the morality of decision-making, but also squad cohesion and chains of command. Lin (2015) posits that complex situations may emerge in the future context of manned-unmanned teaming where, for instance, a machine chooses to refuse an otherwise legitimate order from a human commander because it judges the order non-compliant with the ROE. 'How ought the situation proceed: should we defer to the robot who may have better situational awareness, or the officer who (as far as she or he knows) issues a legitimate command?'[196] Furthermore, it is not immediately clear who would be responsible for the events and unintended consequences that ensue from the machine's refusal to comply.

Importantly, too, the rise of autonomous systems not only raises questions about the relation between human and machine authority; it also complicates the relationship between humans themselves. As

[192] Introna (2004).

[193] For example: Blair (2011).

[194] Lin, Bekey and Abney (2008).

[195] Howard and Scharre (2015).

[196] Lin, Bekey and Abney (2008).

Galliott (2015) notes, the use of UAVs has in many countries been associated with the 'outsourcing' of the day-to-day authority for war to state-employed civilians or private contractors.[197] Removed from the battlefield, there is less urgent need for UAV pilots or support personnel to come from military institutions. In this context, critics of autonomous technologies caution that their use may serve to further erode the traditional distinctions between combatant and non-combatant; military and civilian; public and private actor. This would cast civilian personnel involved in designing, building or operating autonomous systems as legitimate potential targets, given their moral responsibility (at least in part) for that machine's actions and transgressions. A related argument draws a similar conclusion from a differing aspect of autonomy – specifically, arguing that the fact it removes human soldiers from risk leaves adversaries with little choice but to shift towards terrorism or strategic attacks on civilian populations as a means of inflicting human and political costs otherwise impossible on the battlefield.

Right intent

Proponents of the morality of autonomous systems note that a machine, if suitably programmed, cannot deviate from the stated goals of a conflict; having no self-interest of its own, it cannot corrupt or deviate from a 'just cause' and pursue anything other than 'right intent'.

Critics counter, however, that 'right intent' is a positive value, not merely the absence of malicious or unjust intentions; and that this capacity for intentionality presumes some sort of 'soul', 'conscience' or moral agency. Alongside debate over the capacity of a machine to possess right (or any) intent are wider concerns about the implications of this technology for human virtue and morality. As outlined in section 2.2.4., a number of experts argue that the increased use of autonomous systems – with the associated shift towards a rules-based approach to decision-making – may restrict opportunities for individual, casuistic moral deliberation and lead to a wider 'moral de-skilling'.[198] Certainly, the proliferation of autonomous technologies may diminish the role of other virtues that have traditionally been central to warrior culture, such as notions of 'courage' or 'honour'. However, some of the experts consulted in this study note that these virtues should not be treated uncritically; in the past, some military cultures have promoted vain pursuits of glory (e.g. medieval chivalry), pursued suicide and brutality (e.g. Imperial Japan) or else revelled in killing in the name of notions such as bravery. By contrast, machines are not capable of bloodlust, anger, fear; they have no incentive to rape, pillage or murder; they feel none of the hatred or trauma that can push a small minority of human soldiers to carry out battlefield abuses or atrocities. As such, it may be possible to program right intent (or, at very least, the absence of malicious intent) into autonomous systems to ensure slavish pursuit of the ROE.

Last resort

There is significant debate about the implications of autonomous systems for the notion of 'last resort'. Galliott (2015) argues that the extreme asymmetry of recent conflicts involving armed UAVs – typically against low-technology NSA in fragile states – means that the historic use of these technologies has rarely,

[197] Galliott (2015).

[198] Vallor (2013).

if ever, represented a 'last resort'. Other critics worry that the removal of humans from the battlefield may lead policymakers to resort more readily to the use of force ahead of non-military instruments.[199]

Empirical evidence for this hypothesis has shown mixed results, however. Walsh and Schulze (2015) have examined survey data from 3,000 civilians to show that public support for the use of force does increase when unmanned systems are involved. However, they found that policy objectives (e.g. counter-terrorism, humanitarian intervention, or support for an ally) and other demographic factors (e.g. gender) remained the largest determinants of public attitudes. As such, while 'critics of drones are correct in calling attention to the risk of drones lowering inhibitions against war… drones make other *jus ad bellum* considerations more important than ever'.[200] Equally, the focus of political leaders and public discourse on precision munitions and autonomy appears to make public opinion increasingly intolerant of civilian losses; this collateral damage may be accepted more willingly when human soldiers are at risk.[201]

Probability of success

Though the proliferation of autonomous systems in recent years has been driven by their operational and tactical utility, the question of military efficacy is not detached from moral deliberation. The conventions of just war theory dictate that actions must have a reasonable likelihood of success to be justifiable; otherwise, military leaders risk mission failure, collateral damage or other unintended consequences.

Certainly, autonomous systems offer a wide range of advantages over manned systems, which may boost the probability of operational success. At the strategic level, they offer reduced casualty rates and may thus prolong popular and political support for a conflict's aims. At the tactical level, the benefits of autonomy are particularly apparent in tasks deemed 'dull, dirty, dangerous, difficult or different'.[202] Freed from the constraints of human endurance, autonomous systems offer high levels of persistence – the unmanned Zephyr system recently acquired by UK MOD can fly continuously for up to 336 hours, for instance, operating safe from potential attack at over 60,000 feet.[203] Autonomy is not simply about lengthy surveillance missions, however. Without a human pilot, UCAVs currently under development are free to embrace advanced designs optimised for high-G manoeuvring[204] or low observability; alternatively, others focus on cheap, disposable platforms or networked 'swarm' tactics to overwhelm enemy defences. Unlike manned vehicles, these systems can be deployed quickly with limited logistical 'tail', or else left dormant and undetected in a potential conflict zone for activation at a later point, drastically reducing mobilisation times. Importantly, too, autonomous systems can operate in contested or denied areas without risk to human life, including environments contaminated by chemical, biological or radiological agents, or other extremes such as space.

---

[199] Interview with Anthony Lang.

[200] Walsh and Schulze (2015).

[201] Walsh (2015b).

[202] The Economist (2011).

[203] Quick (2014).

[204] Manoeuvres involving large amounts of G (i.e. gravitational) force, often associated with air combat.

In this context, a number of experts argue that militaries have a moral obligation to deploy autonomous systems, not merely to reduce immediate human losses but also to ensure the long-term success of the operation.[205] However, it is important to note that the deployment of unmanned systems may, given their controversial connotations, provoke a backlash of negative opinion from adversary groups, local populations or the domestic electorate. Critics cite the use of drone strikes as a symbol in anti-Western propaganda; or note that such tactics may be perceived as war without honour, courage or humanity. A number of studies have furthermore cited problematic health and psychological effects on populations 'living under drones', arguing that the sense of living with an all-seeing but unseen machine overhead – both 'panopticon' and 'sword of Damocles'[206] – can cause widespread distress and unrest, turning civilians against an otherwise Just War. The Birmingham Policy Commission has found, however, that more empirical study is required to assess the responses of different audiences to unmanned systems.[207]

Proportionality

The question of 'proportionality' is central to debate over the morality of autonomous systems. As noted in section 3.3.1, here the discussion of autonomy often focuses on the recent nature of the technology's use, as opposed to its intrinsic or abstract characteristics. As Frost notes, UAVs have to date primarily been deployed by Western governments with extensive economic, technological and military resources; they have supported discretionary operations against small, non-state adversaries that do not pose an existential threat.[208] Furthermore, some experts fear that the distance involved in the use of autonomous systems (either between pilot and platform or between the platform and its target) could lead to moral desensitisation and disengagement. As Coker (2001) has argued, attempts to make war bloodless, clinical and humane through the use of these sorts of technologies may, in fact, lead paradoxically to greater inhumanity – the human soldier becomes alienated from the battlefield, warrior culture is undermined and the two-way dialectic of strategy becomes the mere administration of violence.[209]

Strategic theorists argue, however, that all conflict is inherently asymmetric; furthermore, that distance has long been a feature of conflict (see also section 2.3.3 for discussions on asymmetry). As Crosston (2014) notes, the archer, artilleryman or pilot have long operated at a remove from the violence they execute – this is especially true of senior decision-makers, whose personal, proximate supervision of combat was at its peak in the Napoleonic era. Indeed, though land forces increasingly fight 'war among the people', significant advances in armour and force protection mean that soldiers can share close spatial proximity with adversaries but still operate with only limited vulnerability to attack.[210] This is not seen as morally

[205] Strawser (2010) cited in Galliott (2012).

[206] Foucault (1975).

[207] Birmingham Policy Commission (2014).

[208] Frost (2015), Galliott (2015).

[209] Coker (2001).

[210] Smith (2005).

problematic; states are well justified (both in moral and operational terms) in all reasonable attempts to reduce the risk to friendly losses.[211]

Importantly too, autonomous systems free operators from much of the chaos, emotion and 'fog of war', facilitating a decision-making process that may be more sensitive and morally engaged, rather than less. Exponents of Remotely Piloted Aerial Systems (RPAS) observe, for instance, that drone pilots may spend hours reconnoitring a target site; listening to individuals' conversations, learning their movements and developing a close understanding of the patterns of life. Furthermore, legal advisors and intelligence analysts are on hand to inform any decision to strike, as well as to provide scrutiny – with pilots aware that any and all decisions may need to be justified in court after the fact. This remote decision-making may thus support a more rational and strategic judgement of the 'proportionality' of any use of force.

Other criticisms of autonomous systems focus not on specific patterns of their use (e.g. targeted killings) but on the inherent characteristics of the technology. Important here are two concepts of 'human dignity' and of 'public conscience' as articulated in the Martens Clause of the Hague Conventions. Proponents of calls for a ban or moratorium on the use of LAWS argue that to be killed without human involvement infringes on basic human dignity, objecting that a machine cannot ever truly demonstrate 'accountability, remedy, and respect'.[212] On a technical level, however, the precision offered by machines may in fact offer opportunities for inflicting less protracted, messy or painful deaths; hitting targets more cleanly than a human shooter and avoiding superfluous injury or unnecessary suffering.[213] Lin (2015) also cautions that arguments that autonomous systems are '*mala in se*' may rest primarily on instinctive feeling or on anthropomorphic portrayals inappropriate for machines. Critics counter that this instinctive feeling may, even if illogical, still be sufficient to trigger the need for a reappraisal of the legality of autonomous systems, arguing that such weapons inflame widespread distaste and should thus be prohibited in the name of 'public conscience'.

The issue of proportionality is also recurrent in debates over the casuistic dilemmas attached to programming morality into a machine. If a fully autonomous system comes under attack, for instance, what is a proportionate response under IHL? Can a machine have a right to self-defence, in the absence of a Self? At the other end of the logical extreme, if technological barriers to full autonomy are overcome and a machine is able to achieve Kantian moral agency, then this raises a panoply of new issues, whereby the system might justifiably refuse orders that place it at risk or even turn on its makers to ensure its own survival at the point of attempted decommissioning.

Discrimination

The question of a machine's capacity for adequate discrimination is similarly central to debate over the moral permissibility of autonomous systems. Here, it is important to distinguish between related but distinct debates about remotely piloted and fully autonomous systems. Concerning the former, critics note that supposedly 'precise' strikes by armed UAVs have been responsible for significant civilian

[211] Interviews with Jeff McMahan and Helen Frowe.

[212] Lin (2015).

[213] Ibid.

casualties and collateral damage in recent years. Against this, however, other experts argue that persistent, remotely piloted systems afford time and space in which to make more informed and discriminating moral choices.[214]

When examining the more difficult question of fully autonomous systems, critics of the technology contend that morality is too contextual and casuistic to ever be programmed with satisfactory granularity into an autonomous machine. As such, it is argued that these systems cannot ever hope to be sufficiently discriminating to be allowed full moral agency. However, this assumes a top-down approach (e.g. programming morality into a machine as code); a more heuristic, bottom-up approach (e.g. machine learning) may in future enable autonomous systems to 'learn' morality in a casuistic manner, mirroring the development of ethical understanding in humans.[215]

If this remains a far-off prospect for now, then literature and interviewees suggest that highly autonomous systems may become more permissible in some domains than others as an interim measure to ensure their safe use. As the UNIDIR report notes, 'experts have suggested that fully autonomous weapons are likely to first appear in the relatively "uncluttered" maritime environment.' Where the number of parameters for a machine to compute is comparatively limited and there are few civilians to risk as collateral damage.[216] In this relatively simple context, internationally declared fields of autonomous underwater vessels could operate and respond without human instruction to noise signatures matched with known enemy military vessels; this field might simply be deactivated when hostilities ceased.[217] With appropriate safeguards in place to guard against system malfunction (for example with human checks on activation/deactivation), the proliferation of anti-access, area denial (A2AD) capabilities such as sophisticated anti-ship and air defence systems may make fully autonomous systems essential to maritime, space and combat air; by contrast, the land domain and close air support missions are likely to prove more challenging given the heightened risk of civilian collateral damage.

[214] Interview with Nigel Biggar.

[215] Lin, Bekey and Abney (2008).

[216] UNIDIR (2015).

[217] Interview with Sir David Omand.

4. Key conclusions

4.1. The academic landscape

This brief study of the academic landscape relating to morality in conflict indicates that there is a lively and wide-ranging debate on issues such as:

- The enduring applicability of existing morality frameworks in an evolving operational context
- The constraints and shortfalls of the international legal regime in current and future conflict
- The role of the state and that of the individual as moral actors
- The morality considerations arising from the increasing use of new technologies in conflict.

This body of work is categorised largely by its focus on either a particular morality framework (e.g. JWT) or on a particular technology area (e.g. the morality of cyber conflict). That said, a number of sources transcend these categories, considering a moral framework and technological area in tandem. The literature varied in its specificity: many of the sources were very general in nature. By contrast, some of the technology-oriented sources were highly specific. As expected, this study having been confined to academic sources, the work tended to be theoretical rather than empirical in tone. From the literature sample identified in support of this work, cyber and autonomous systems were the two technology areas that received most attention with other technologies such as nanotechnology, biological engineering, non-lethal capabilities also mentioned, but receiving comparatively little detailed analysis.

4.1.1. Principal research questions

As illustrated in previous chapters, the topic of morality and future conflict presents academics and practitioners with a range of different questions. In Boxes 1–4, these questions have been assembled for the purpose of overview, broken down by a relevant thematic area. The aim of collecting these questions in one place is to help identify what future research questions could be useful to pursue.

Box 1. Research questions related to future moral operating environment

- Are traditional moral frameworks still relevant in relation to the new ways of conflict and war?
- What are the most difficult moral challenges faced by decision-makers in relation to tomorrow's conflict?
- What will the future moral operating environment look like for the UK and its allies?

Box 2. Research questions related to the application of existing legal and moral frameworks

Application of existing legal and moral frameworks

- To what extent are existing moral frameworks (e.g. JWT and IHL) applicable to the new ways of conducting warfare?
- What adjustments (if any) are required to the legal definitions of 'armed conflict', 'just cause' and 'harm' to take into account new technological developments?
- What is the appropriate moral and legal framework to account for situations of non-kinetic hostile action with non-physical consequences? What, if any, is the appropriate framework for responding to such an action?
- What are the moral implications related to the inherent characteristics of new technologies themselves and what are the moral implications of their use?
- How might response options be constrained, given the risks associated with the new ways of conducting warfare?

Box 3. Research questions related to the blurred lines between 'war' and 'peace'

Blurred distinctions between 'war' and 'peace'

- If the attack does not constitute 'use of force' under Art 2(4) of the UN Charter, do the principles of *jus ad bellum* still apply?
- If the conflict does not constitute 'war', are *in bello* principles relevant to guide the conduct of those participating in the conflict?
- What alternative measures should be considered without significantly increasing the risk of becoming more vulnerable to a greater future harm as a result of waiting?
- What is the desired outcome *post bellum* of this conflict? Is it justice? Is it peace?

Box 4. Research questions related to case studies on cyber and autonomous systems

Cyber case study

- Does a cyber attack constitute an 'armed attack'? Can the perpetrator of the original attack be reliably identified? Can the motives underlying a cyber attack be determined or proven?
- Since cyber operations may be conducted by many actors, does the notion of the state's monopoly on the use of force withstand scrutiny?
- Does cyber represent an 'easy option', lowering the threshold for policymakers to use force? Could a pre-emptive cyber attack prevent worse harm being caused later and what would be the moral implications?
- How far can the outcomes of an attack be predicted? Can damaging effects be limited? What is the likely response of the adversary?
- What would be a proportionate response to an attack and how can this be determined (given the difficulty associated with quantifying harm caused)?
- Given the potential for cascading effects and unintended consequences, can cyber ever be truly discriminate? Does cyber challenge the current definition(s) of 'non-combatant' with implications for non-combatant immunity?

Autonomous systems case study

- What is an 'armed attack' or *casus belli* in relation to autonomous systems? Who is liable for a machine's atrocities?
- How should 'meaningful human control' be defined in relation to autonomy? What independent authority should a machine hold? Does autonomy blur the distinctions between combatant and non-combatant?
- Can a machine possess intent or moral agency? Does use of autonomous systems entail a loss of martial virtues?
- Do autonomous systems lower or raise the threshold for policymakers to use force? What are the implications for perceptions of a war's legitimacy?
- Do leaders have a moral obligation to use autonomous systems to prevent friendly and civilian losses? Is there a threat of strategic backlash?
- Do asymmetry and distance pose moral problems? Can a machine act in self-defence? Can an autonomous system use lethal force in line with principles of proportionality and human dignity?
- Can autonomous systems be sufficiently discriminating to allow for independent moral agency? Are they better suited in certain domains?

4.1.2. Areas meriting further exploration

This study identified a number of areas perceived as requiring further analysis and exploration:

- Many of the experts consulted during this study considered that existing legal (and their underpinning moral) frameworks continue to withstand scrutiny in the light of the changing character of conflict, but may need to be interpreted differently or extended to take account of these new operational norms. It would be beneficial for a more detailed examination to be undertaken of the 'grey areas' in international law, specifically in relation to the challenges posed to international law by particular technologies. Such analysis would be critical in identifying areas where there is tension, shortfall or ambiguity and in which change or expansion could therefore improve the applicability of the law in current and future operations. Examples include: the expansion of the criteria relating to 'armed attack'; amendments to the notion of 'harm' and the more robust articulation of *jus post bellum*.
- Much of the literature has examined the increasing prominence of the individual as the key actor (rather than the state) in moral behaviour. A more practical, applied consideration of what this means – and might mean – in future warfighting would be beneficial. A move away from state-based morality could have implications for recruitment, training, command and control and support systems for combatants.
- The body of work seems heavily oriented to the morality implications of the cyber and autonomous systems technology areas. It would benefit from an extended focus on technology areas of interest, beyond the two examined here. Examples might include directed energy weapons, non-lethal capabilities or synthetic biology. It is acknowledged that the volume of literature sourced in this study on these topics may reflect an inherent research bias. That said, it is also possible that the prevalence of literature on these two areas may be due to their 'in vogue'

attractiveness arising from their perceived game-changing potential or from their comparative maturity when considered alongside other emerging technologies such as synthetic biology. In any case, the debate would likely be enriched by the inclusion of broader considerations as would be introduced by other emerging technologies. These might reinforce the shortcomings of particular elements of existing morality frameworks or legal regimes and provide further indicators as to ways in which these might be made more relevant.

- As emphasised previously, due to the practical constraints of time and language, this study focused on Western perspectives and the Western traditions of morality-based thinking. There would be merit in a detailed analysis being conducted of morality frameworks and systems of belief beyond this Western-centric view and the challenges posed to these alternative frameworks by the changing nature of conflict. Alternative morality frameworks may offer both practical assistance in thinking about the moral implications of future conflict and offer important insights into the morality considerations of current and future UK allies, adversaries and target audiences.
- Further exploration of the extent to which morality can be weaponised and moral questions used as munitions in future war would be valuable. Some experts described the 'ethics trap', the risk that the UK and its allies be drawn into conflicts or engagements that breach self-imposed moral standards by opponents whose behaviour is configured specifically to elicit this response, thereby undermining the UK's occupation of the moral 'high ground'.
- Further exploration of the influence of social media on the perception of morality and just war by domestic and international audiences. Social media presents key challenges, including the risk of (negative) group thinking, but also potentially presents unrivalled opportunities for shaping public perception of specific actions or measures.

4.1.3. Suggested priority areas for MOD

Areas in which MOD might wish to focus its efforts in advancing its thinking on morality include the following:

- The MOD should ensure that the contemporary discourse on morality is integrated in the wider dialogue about grand and military strategy in a meaningful way. Evidently, the UK will wish to be – and to be perceived by domestic and international audiences as – a moral actor in its conduct in conflict but greater, more holistic consideration should be given to what this means in practice, given the changing character of conflict, and what safeguards and frameworks need to be put in place to allow the UK to accomplish this.
- Work on current and emerging grey areas in international law (suggested above), would be instrumental in helping MOD determine current areas of vulnerability and anticipating challenges that might be posed or precedents that might be set in the event of a future attack. Pre-emptive thinking on these issues would be of tremendous value, especially in the face of potential 'lawfare' (i.e. the use of domestic or international law to damage, distract or occupy an opponent) from revisionist or obstructionist adversaries.
- A greater emphasis on policy development in relation to cyber and to autonomous systems would help focus on the specific morality issues associated with the UK's likely use of these capabilities in the future, as well as shaping wider global norms. Similarly, MOD should consider the

ramifications of the purposeful cultivation of ambiguity and uncertainty (e.g. 'hybrid warfare' and information operations) for moral norms.

- Reflecting the shift away from state agency to a focus on individuals as moral actors, MOD should take steps to ensure that morality is embedded in every individual service member, supported by an organisational 'moral culture', rather than relying on a top-down, compliance-, orders- or rules-based approach. In doing so, MOD should consider any changes or amendments that may be necessary to its existing recruitment, training and education and command and control regime in order to facilitate this. For instance, given the concern expressed by experts over the potential for new technologies to exceed or in some way complicate traditional moral frameworks and definitions, MOD should ensure that training techniques used to embed moral and lawful conduct in service personnel explore the specificities of these new challenges (e.g. considering the morality of cyber actions in war-gaming).
- Examination of potential changes in the future moral operating landscape could be integrated into wider horizon-scanning and strategic force development work to assess defence planning against moral (as well as social, economic and military) assumptions and attempt to generate a more robust evidence base to inform decision-making.

References

Allhoff, Fritz and Ryan Jenkins. 2014. 'The Facebook war: Would taking down a social network justify a real-world attack?' Slate, June 11. As 10 March 2016: http://www.slate.com/articles/technology/future_tense/2014/06/cyberwar_ethics_when_is_a_real_world_response_to_a_cyberattack_justifiable.html.

Arkin, Ronald C. 2007. 'Governing lethal behavior: Embedding ethics in a hybrid deliberative/reactive robot architecture.' Georgia Institute of Technology, Technical Report GIT-GVU-07-11.

Arquilla, John. 1999. 'Ethics and information warfare.' In Strategic Appraisal: The Changing Role of Information in Warfare, edited by Zalmay Khalilzad, John White and Andy W. Marshall, chapter 13. Santa Monica, Calif.: RAND Corporation.

Arts, Bas. 2005. 'Non-state actors in global environmental governance: New arrangements beyond the state.' In Palgrave volume on global governance, edited by M. Koenig-Archibugi and M. Zürn.

Barbu, Florin-Marian. 2015. 'Considerations concerning hybrid war.' Strategic Impact 55 (2): 50.

Barrett, Edward T. 2013. 'Warfare in a new domain: The ethics of military cyber-operations.' Journal of Military Ethics 12 (1): 4–17.

Birmingham Policy Commission. 2014. The Security Impact of Drones: Challenges and Opportunities for the UK. Birmingham: University of Birmingham. As of 17 March 2016: http://www.birmingham.ac.uk/research/impact/policy-commissions/remote-warfare/index.aspx

Blair, D. 2011. 'Iran shows off captured US drone', The Daily Telegraph, 8 December. As of 17 March 2016: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8944248/Iran-shows-off-captured-US-drone.html

Brooke-Holland, L. 2013. Unmanned Aerial Vehicles (Drones): An Introduction. London: House of Commons Library.

Burkhardt, Allan. 2013. 'Just War and Human Rights: Fighting with Right Intention.' University of Tennessee. As of 14 March 2016: http://trace.tennessee.edu/cgi/viewcontent.cgi?article=2840&context=utk_graddiss

Cini, Michelle. 2001. 'The soft law approach: Commission rulemaking in the EU's state aid regime.' Journal of European Public Policy 8 (2): 192–207.

Clausewitz, Carl von, [1832] 1976. On War. Michael Howard, and Peter Paret, eds. And trans. Princeton, NJ: Princeton University Press.

Coker, C. 2001. Humane Warfare. London: Routledge.

Cornish, Paul and Frances V. Harbour. 2003. 'NATO and the individual soldier as moral agents with reciprocal duties: Imbalance in the Kosovo Campaign.' In Can Institutions Have Responsibilities? Edited by Toni Erskine, 119–137. London: Palgrave Macmillan.

Cornish, Paul, Livingstone, David, Clemente, Dave, Yorke, Claire. 2010. 'On Cyber Warfare'. Chatham House. As of 17 March 2016: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r1110_cyberwarfare.pdf

Cornish, Paul. 2002. '"Cry, 'Havoc!' and Let Slip the Managers of War": The Strategic, Military and Moral Hazards of Micro-managed Warfare.' NATO.

Cornish, Paul. 2003. 'Myth and reality: US and UK approaches to casualty aversion and force protection.' Defence Studies 3 (2): 121–128.

Cornish, Paul. 2007. 'The ethics of 'effects-based' warfare: The crowding out of jus in bello?' In The Price of Peace: Just War in the Twenty-First Century, edited by Charles Reed and David Ryall, 179–200. Cambridge: Cambridge University Press.

Crosston, M. 2014. 'Pandora's presumption: drones and the problematic ethics of techno-war.' Journal of Strategic Security 7 (4): 1.

Danks, David and Joseph H. Danks. 2013. The moral permissibility of automated responses during cyberwarfare. As of 10 March 2016: https://www.andrew.cmu.edu/user/ddanks/papers/AutomatedResponses-Final.pdf

Dipert, Randall R. 2010. 'Ethics of cyberwarfare.' Journal of Military Ethics 9 (4): 384–410.

Donaldson, Peter. 2015. 'Less-lethal roundup: On the cusp of something with much promise but level of uncertainty.' Military Technology 39 (11): 57–61.

Duyvesteyn, Isabelle. 2012. 'Escalation and de-escalation of irregular war: Some observations and conclusions.' Journal of Strategic Studies 35 (5): 601–611.

Eberle, C. J. 2013. 'Just War and Cyberwar.' Journal of Military Ethics 12 (1): 54–67.

Finlay, Christopher J. 2013. 'Fairness and liability in the Just War: Combatants, non-combatants and lawful irregulars.' Political Studies 61 (1): 142–160.

Foucault, M. 1975. Discipline and Punish: The Birth of the Prison. New York: Pantheon Books [in English].

Frost, Mervyn. 2012. 'Ethics, foul play and war in international relations.' Research seminar, University of Hull.

Frost, Mervyn. 2015. 'Mervyn Frost reviews Military Robots: Mapping the moral landscape, by Jai Galliott.' RUSI Journal, 1 December.

Future Operating Environment 2035. UK Ministry of Defence. 2015. As of 10 March 2016: https://www.gov.uk/government/publications/future-operating-environment-2035

Galliott, Jai C. 2012. 'Viewpoint article closing with completeness: The asymmetric drone warfare debate.' Journal of Military Ethics 11 (4): 353–356.

Galliott, Jai C. 2015. 'Military robots: mapping the moral landscape.' Ashgate.

Gert, B. 2002.'The Definition of Morality.' The Stanford Encyclopedia of Philosophy.

Ministry of Defence. 2014. 'Strategic Trends Programme: Global Strategic Trends – Out to 2045.' Development, Concepts and Doctrine Centre. Fifth edition.

Gregory, Derek. 2010. 'War and peace.' Transactions of the Institute of British Geographers 35 (2): 154–186.

Harbour, Frances. 2011. 'Reasonable probability of success as a moral criterion in the Western Just War tradition.' Journal of Military Ethics, 10 (3): 230 –241.

Henschke, A. and Patrick Lin. 2014. 'Cyberwarfare ethics, or how Facebook could accidentally make its engineers into targets.' Bulletin of Atomic Scientists, August 29. As of 10 March 2016: http://thebulletin.org/cyberwarfare-ethics-or-how-facebook-could-accidentally-make-its-engineers-targets7404

Hoffman, Frank G. 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies.

Horowitz, M.C. and P. Scharre. 2015. 'Meaningful Human Control in Weapon Systems: A Primer.' Center for a New American Security. As of 10 March 2016: http://www.cnas.org/human-control-in-weapon-systems

Hyten, John and Robert Uy. 2004. 'Moral and ethical decisions regarding space warfare.' Air & Space Power Journal. 18 (2): 52.

The Economist. 2011. 'Flight of the drones'. 8 October. As of 17 March 2016: http://www.economist.com/node/21531433

International Committee of the Red Cross (ICRC)

- Fundamental principles of IHL. As of 17 March 2016: https://www.icrc.org/casebook/doc/book-chapter/fundamentals-ihl-book-chapter.htm#d_iii
- Rule 1. The principle of distinction between civilians and combatants. As of 17 March 2016: https://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1
- Rule 14. Proportionality in attack. As of 17 March 2016: https://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter4_rule14
- Rule 47. Attacks against persons hors de combat. As of 17 March 2016: https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule47
- Military necessity. As of 17 March 2016: https://www.icrc.org/casebook/doc/glossary/military-necessity-glossary.htm
- Rule 70. Weapons of a nature to cause superfluous injury or unnecessary suffering. As of 17 March 2016: https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule70
- The Martens Clause and the laws of armed conflict. As of 17 March 2016: https://www.icrc.org/eng/resources/documents/misc/57jnhy.htm
- The review of weapons in accordance with Article 36 of Additional Protocol I. As of 17 March 2016: https://www.icrc.org/eng/resources/documents/misc/5pxet2.htm
- What are *jus ad bellum* and *jus in bello*? As of 17 March 2016: https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0

Introna, L.D. and D. Wood. 2004. 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems.' Surveillance & Society 2 (2/3): 177-198.

Jastram, Kate and Anne Quintin. 2011. The Internet in Bello: Cyber War Law, Ethics and Policy. Seminar held 18 November 2011, Berkeley Law. As of 10 March 2016: https://www.law.berkeley.edu/files/cyberwarfare_seminar--summary_032612.pdf

Joint Doctrine Publication 0-01. 2014. UK Defence Doctrine. 2014. p. 18. As of 10 March 2016: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf

Joint Publication 1-02. 2008. DoD Dictionary of Military Terms. Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7.

Kelsay, John. 1990. 'Religion, morality, and the governance of war: The case of classical Islam.' The Journal of Religious Ethics 18 (2): 123–139.

Kirkpatrick, J. 2015. 'Drones and the martial virtue courage.' Journal of Military Ethics 14 (3-4): 202–219.

Libicki, Martin. 2009. 'Cyberdeterrence and cyberwar.' RAND Corporation, Santa Monica.

Lin, Patrick, Fritz Allhoff and Neil C. Rowe. 2012. 'Computing Ethics. War 2.0: Cyberweapons and Ethics.' Communications of the ACM 55 (3).

Lin, Patrick, G. Bekey and K. Abney. 2008. 'Autonomous Military Robotics: Risk, Ethics and Design.' California San Luis Obispo: Polytechnic State University.

Lin, Patrick. 2010. 'Ethical blowback from emerging technologies.' Journal of Military Ethics 9 (4): 313–331.

Lin, Patrick. 2015. 'The Right to Life and the Martens Clause.' Convention on Certain Conventional Weapons (CCW) meeting of experts on lethal autonomous weapons systems (LAWS), at United Nations in Geneva, Switzerland on 13–17 April 2015. As of 10 March 2016: http://ethics.calpoly.edu/ccw_testimony.pdf

Lindsay, Jon R. 2013. 'Stuxnet and the limits of cyber warfare.' Security Studies 22 (3): 365–404.

Lucas, George R. 2011. '"New rules for new wars". International law and Just War Doctrine for irregular war.' Case Western Reserve Journal of International Law 43 (3): 677–705.

Lucas, George R. 2013. 'Ethics and cyber conflict: A response to JME 12:1 (2013).' Journal of Military Ethics 13 (1): 20–31.

Lucas, George R. 2013a. 'Just War and cyber conflict. Can there be an "ethical" cyber war?' As of 10 March 2016: http://www.usna.edu/Ethics/_files/documents/Just%20War%20and%20Cyber%20War%20GR%20Lucas.pdf

Lucas, George R. 2013b. 'Legal and ethical precepts governing emerging military technologies: research and use.' Amsterdam Law Forum. As of 10 March 2016: http://amsterdamlawforum.org/article/viewFile/330/498

Lucas, George R. 2014. 'Permissible preventive cyberwar: Restricting cyber conflict to justified military targets.' In The Ethics of Information Warfare, edited by Luciano Floridi and Mariarosaria Taddeo, 73–83. London: Springer.

MacIntyre, A. 1984. 'After Virtue: A Study in Moral Theory.' Notre Dame, Indiana: University of Notre Dame Press.

Mayer, Michael. 2015. 'The new killer drones: Understanding the strategic implications of next-generation unmanned combat aerial vehicles.' International Affairs 91 (4): 765–780.

Mazo, Vincent. 2011. 'Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?.' Washington: Institute for National Strategic Studies.

Morkevicius, Valerie. 2013. 'Tin men: Ethics, cybernetics and the importance of soul.' Journal of Military Ethics 13 (1): 3–19.

Munteanu, Razvan. 2015. 'Hybrid warfare – the new form of conflict at the beginning of the century.' Strategic Impact 56: 19–26.

Myers, Charles R. 1997. 'The core values: Framing and resolving ethical issues for the Air Force.' Airpower Journal 11 (1).

Nye, Joseph. 2010. 'Cyber Power'. Belfer Center for Science and International Affairs (Harvard Kennedy School). As of 17 March 2016: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

O'Connell, Mary Ellen. 2011. 'Seductive drones: Learning from a decade of lethal operations.' Journal of Law, Information & Science, Notre Dame Legal Studies Paper. 11–35.

O'Connell, Mary Ellen. 2012. 'Cyber security without cyber war.' Journal of Conflict and Security Law 17 (2): 187–209.

O'Connell, Mary Ellen. 2015. 'Myths of hybrid warfare.' Ethics and Armed Forces 2 (1): 1–5.

Orend, Brian. 2002. 'Justice after war.' Journal of Social Philosophy. 31 (1): 117–137.

Osborn, K. 2015. 'Navy to Deploy First Underwater Drones from Submarines', Military.com, 13 April. As of 17 March 2016: http://www.telegraph.co.uk/news/worldnews/middleeast/iran/8944248/Iran-shows-off-captured-US-drone.html

Quick, D. 2014. 'Zephyr UAV continues to break records on first authorised civil flight', Gizmag. 28 September. As of 17 March 2016: http://www.gizmag.com/zephyr-uav-civil-test-flight/34010/

Reding, A. et al. 2014. 'Handling ethical problems in counterterrorism. An inventory of methods to support ethical decisionmaking.' Santa Monica, Calif.: RAND Corporation.

Reed, Esther D. 2015. 'Just War reasoning in an age of risk.' New Blackfriars 96 (1062): 206–222.

Rengger, Nicholas. 2002. On the Just War tradition in the twenty-first century. International Affairs (Royal Institute of International Affairs 1944-). 78 (2): 353–363.

Sandel, M. 2012. 'Justice: What's the Right Thing to Do?' New York: Farrar, Straus and Giroux.

Schmitt, Michael N. 2012. 'Attack' as a Term of Art in International Law: The Cyber Operations Context. Proceedings of the 4th International Conference on Cyber Conflict 283–293.

Schmitt, Michael N., ed. 2013. 'Tallinn Manual on the International Law Applicable to Cyber Warfare.' New York: Cambridge University Press.

Smith, M. L. R. 2012. 'Escalation in irregular war: Using strategic theory to examine from first principles.' Journal of Strategic Studies 35 (5): 613–637.

Smith, R. 2005. The Utility of Force: The Art of War in the Modern World. London: Allen Lane.

Stanford Encyclopedia of Philosophy. 2005. 'War'. As of 18 March 2015: http://plato.stanford.edu/entries/war/#2.1

Stone, John. 2012. 'Escalation and the War on Terror.' The Journal of Strategic Studies 35 (5): 639–661.

The United Nations Institute for Disarmament Research (UNIDIR). 2015a. The Weaponization of Increasingly Autonomous Technologies: Considering Ethics and Social Values. UNIDR Resource, No. 3.

The United Nations Institute for Disarmament Research (UNIDIR). 2015b. The Weaponization of Increasingly Autonomous Technologies: Considering how Meaningful Human Control might move the discussion forward. UNIDIR Resources No. 2.

The United Nations Institute for Disarmament Research (UNIDIR). 2015c. The Weaponization of Increasingly Autonomous Technologies in the Maritime Environment: Testing the Waters. UNIDIR Resources No. 4.

Toner, Christopher Hugh. 2006. 'A critique of the air force's core values.' Air & Space Power Journal, winter 2006.

US Government Accountability Office (GAO). 2012. Non-Proliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports. GAO-12-536. Washington, DC: US GAO. As of 17 March 2016: http://www.gao.gov/assets/600/593131.pdf

Vallor, S. 2013. The future of military virtue: Autonomous systems and the moral deskilling of the military. Cyber Conflict (CyCon), 2013 5th International Conference.

Walsh, James Igoe and Marcus Schulzke. 2015. The ethics of drone strikes: Does reducing the cost of conflict encourage war? Strategic Studies Institute and U.S. Army War College Press.

Walsh, James Igoe. 2015a. 'Political accountability and autonomous weapons.' Research and Politics 1–6.

Walsh, James Igoe. 2015b. 'Precision weapons, civilian casualties, and support for the use of force.' Political Psychology 36 (5): 507–523.

Whetham, David. 2016. 'Are we fighting yet? Can traditional Just War concepts cope with contemporary conflict and the changing character of car?' The Monist 99 (1): 55–69.