Introduction

Jens David Ohlin

1. THE FRAMEWORK OF REMOTENESS

The number of academic articles and books on drone warfare has increased exponentially in the last five years. Of course, this academic output is entirely justified, given the significance of drone technology—and the strategy of targeted killing—in modern warfare. Although there is much debate and little agreement in this literature, it is undeniable that the nature of warfare is changing, and the question addressed in this literature is how the current law, whether international humanitarian law (IHL), international human rights law, or jus ad bellum, should apply to drone strikes carried out in diverse operational situations.

In terms of sheer volume, the literature on cyber-war follows close behind. For some years, much of the literature offered legal analysis of hypothetical attacks. The coming age of cyber warfare was on the horizon, but had not yet appeared. The Stuxnet attack changed all of that. And now the cyber-intervention by Russia in the US election of 2016 has established that cyber activities (and cyber counter measures) will be ever-present in the strategic and diplomatic landscape. Whether one agrees that, on one end of the spectrum, the Russian hacking in that case constituted an 'act of war', as some US politicians declared, or on the other end of the spectrum perhaps simply a violation of standard 'norms' of international behavior, as President Obama indicated, the fact of the matter is that cyber interventions of all sorts will radically proliferate in the coming decade. With the advent of the *Tallinn Manual*, in its first and second manifestations, and other academic efforts, the invisible college of international lawyers is grappling with how to apply to cyberspace international legal norms whose foundation was laid many years ago when cyber-attacks were mostly the stuff of science fiction.[1]

Finally, the technological advances regarding Autonomous Weapons Systems (AWS) are perhaps less prevalent, though if one defines AWS sufficiently broadly, it is clear that current weapons development for the

[1] See M N Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

United States, Russia and China already includes a substantial AWS component, so that the legal literature on AWS is arriving on the scene just in time. Although the concept of AWS is often misunderstood in the popular imagination as involving robotic infantry, the more typical application of the technology involves missile systems with autonomous targeting protocols—something that is not so hard to imagine. (The other typical application is cyber weapons with independent or quasi-independent targeting protocols.) The number of legal issues posed by these applications is immense.

The goal of the present volume is not to rehash the existing issues, which are already usefully articulated and debated in the literature. Rather, the point is to cut across the traditional categories and analyze these developments conceptually. Much of the literature atomistically considers drones, while another segment analyzes cyber, and a third literature addresses AWS. The prime motive of this volume is to both aggregate and disaggregate these subjects at the same time. The subjects are aggregated by considering drones, cyber, and AWS altogether, but then disaggregated by slicing off one aspect that is common to all three and investigating it in more detail.

Here is where the concept of remoteness enters the picture. One crucial aspect that unites drones, cyber and AWS is their remote capability—a potentially new form of warfare that is allowing operators to use ever more discriminating force while also receding further in time and space from the target of the military operation. This one aspect of the new technology—its remoteness—deserves its own investigation, and this volume provides it. Under this rubric, many questions can and should be asked. Is the remoteness of these technologies that much different than what came before? If it is different, is the difference one of degree or of kind? If these new technologies require additional regulation, or if existing regulation is already adequate, does their remoteness constitute an additional hurdle towards effective regulation? Do these remote technologies change the risk calculus for going to war in ways that are ethically or legally problematic? Are these technologies being used in ways that comply with jus ad bellum? In particular, are we witnessing a new category of warfare: remote self-defense?

The point here is not to defend a particular position with regard to these issues, but simply to defend the need for a legal volume that focuses exclusively on the notion of remoteness per se, as a field of serious academic inquiry. The nature of the remoteness is the Elephant in the Room, the obvious common characteristic of these technologies that has, nonetheless, moral and legal implications that are not so easy to

trace or predict. Hopefully, the present volume is the beginning of that scholarly endeavor.

2. THIS VOLUME'S CONTRIBUTION TO THE DEBATE

In Chapter 1, 'Remoteness and reciprocal risk', I argue that reciprocal risk is not, and has never been, an essential component of IHL or the law of armed conflict. In canvassing the history of military technology, I argue that the strategic goal in all military engagements has been to maximize lethality to the target while minimizing risk to the operator. The most recent technologies, including drones, cyber-weapons, and AWS, are only the most recent (and extreme) versions of this familiar incentive that underlies all strategic warfare. In the chapter, I analyze the question of whether the radical *increase* in asymmetrical risk will make war too easy—and ultimately result in more warfare. I explore and respond to this objection. Along the way, the chapter also considers whether reciprocal risk is an essential component of ethical warfare—a possibility that is cautiously rejected. In the end, the chapter performs a debunking function by taking some of the most common complaints about these technologies—pertaining to their remoteness—in order to demystify them and provide the correct historical context for them. Seen in that light, drones, cyber-weapons, and even AWS start to look less like aberrations and more like the ultimate conclusion to the natural evolution of warfare.

In Chapter 2, 'The principle of distinction and remote warfare', Emily Crawford continues the discussion of remoteness by focusing on the fate of the 'intransgressible' principle of distinction in an era when military targeting technology is becoming ever more remote, with the operator of the weapon ever further in geographic distance from the target of the military strike. Crawford argues that this technological evolution carries both promises and perils for the principle of distinction. On the one hand, she takes seriously the argument that some remote technologies, including drones, allow for increased compliance with the principle of distinction, in part because of increased capacity to hover over a target and improved surveillance capacity: 'Drones, with the potential to spend days, even weeks observing a potential target, gathering copious data on the target, and allowing for complex and detailed assessments about the legality of a strike against such a target, without fear of discovery of such surveillance, thus may be exceptionally compliant with the principle of distinction.' On the other hand, she also warns that there are risks associated with remote attacks, whether by drone or cyber-weapons,

because the 'clarity and precision offered by drones by way of their "real-time" video feed of targets is undermined by the very real technological problem of "latency"—the time delay between activities observed and videoed at the target site and the arrival of that video image via satellite to the pilots'. Crawford does more than simply trade in generalities, but instead gives specific examples of strikes where technology either helped or hindered compliance with the principle of distinction.

In Chapter 3, 'Modern drone warfare and the geographical scope of application of IHL: pushing the limits of territorial boundaries?', Robert Heinsch examines the way that remotely piloted vehicles have expanded the geographical scope of armed conflict. With this expansion has come uncertainty over the geographical scope of IHL as a regulator of lethal conduct. Specifically, the legal question Heinsch examines is whether drone strikes alone, if piloted remotely from the United States but deployed in a foreign state against a non-state actor, are sufficient to place the United States in a non-international armed conflict with that non-state actor. If the answer to that question is yes, then presumably the IHL rules applicable to non-international armed conflicts (NIACs) will govern and restrict those drone strikes. That being said, many human rights lawyers would resist this conclusion because they view IHL as being too permissive and insufficiently restrictive. Heinsch argues that the correct standard is whether there is 'protracted armed violence' between the state and the non-state actor, and there is nothing in that standard that would prevent a series of drone strikes from satisfying that standard. When applied to the facts of most drone strikes conducted by the United States, however, Heinsch argues that many of the strikes fall below the threshold for the existence of an armed conflict, because the violence is not sufficiently protracted. In that case, International Human Rights Law governs the killings.

In Chapter 4, 'The characterization of remote warfare under international humanitarian law', Anthony Cullen examines the concept of armed conflict as a legal term of art, and how it applies in the context of drones, cyber-attacks, and autonomous weapons. Cullen argues that a proper definition of 'armed conflict' cannot be constructed in the abstract, but instead requires consideration of the object and purpose of IHL as a field of legal regulation. Cullen identifies that object and purpose as the protection of civilians in armed conflict. Based on this simple cannon of interpretation, Cullen argues that IHL should be interpreted in such a way that it applies to armed conflicts pursued primarily with drones, cyber-weapons, or AWS—precisely because these modalities have the capacity to negatively impact civilians. As Cullen

notes, 'If the law of armed conflict has a vanishing point in the 21st century, it is arguably that of remote warfare'. By this he means that the greatest risk of irrelevance for IHL is with regard to drones, cyber-weapons and AWS. This suggests that IHL as a discipline must pro-actively work to maintain its relevance as a source of constraint and regulation of the modalities of remote warfare. Since the future of armed conflict resides with these remote technologies, IHL risks irrelevance and obsoleteness if it does not rise to the challenge.

In Chapter 5, 'Remoteness and human rights law', Gloria Gaggioli asks whether, in contrast to Cullen's focus on IHL, human rights law has a distinct role to play in armed conflicts (or military force generally) that are characterized by the remote deployment of military assets, especially drones, but also to a lesser extent cyber weapons and AWS which also demonstrate degrees of remoteness. The author asks, critically, whether the human rights principles of legality, accountability, transparency, dignity and self-defense have a distinctive role to play in the regulation of remote force. Gaggioli moves away from the often-uncritical distrust of remote weaponry among human rights scholars and activists, and instead scrutinizes the very nature of remote force to determine whether—and to what degree—it offends these core principles of human rights law. The picture she paints is far subtler than that offered by some human rights activists, but it still recognizes a large conceptual space for human rights law to govern, and constrain, remote force.

In Chapter 6, 'Exploiting legal thresholds, fault-lines and gaps in the context of remote warfare', Mark Klamberg asks whether the current system of legal regulations regarding the use of force are adequate to the task of regulating military violence in a world of remote warfare. Specifically, Klamberg argues that the current scheme for regulating the use of force is full of gaps and thresholds that define what does—and does not—count as a use of force in the sense of the UN Charter or an armed conflict in the sense of IHL. It is precisely these gaps and fault lines that allow so-called gray conflicts to persist below the radar of particular legal regulations. Indeed, much of the rationale for states to deploy remote technologies, including drones, cyber-weapons and AWS, is that it might allow the state to project state interests while not triggering many of the legal restrictions that would attach to more conventional military interventions.

Part II of the Handbook focuses more specifically on the legal regulation of remotely piloted vehicles (drones) and cyber technology. In Chapter 7, 'Drone strikes: a remote form of self-defense?', Nigel D White and Lydia Davies-Bright argue that technological developments are changing the nature of international relations that give rise to the need

for legal regulations of jus ad bellum. Specifically, White and Davies-Bright note that the advancement of remote technology is facilitating the deployment of military force in ways that place existing notions of sovereignty under intense pressure. States with remote technology can now attack far-flung territories with drones, causing those targeted states to worry about how to protect their own sovereignty against these intrusions. The authors connect this development to a resurgence in 'primordial understandings of sovereignty based on preservation of the nation state'. On the other hand, one might also view remote technology not just as a cause to this problem but as a *response* to it. Non-state actors are using the tactics of terrorism to inflict damage on state authorities in an attempt to undermine traditional notions of Westphalian sovereignty, while (some) states are pushing back with an aggressive campaign of extraterritorial military force designed to protect state authority. The authors conclude that 'the return to absolute forms of sovereignty by technologically advanced states is something more profound and alarming' because 'it represents a reversion to a very primitive view of the state whereby its promise to protect its citizens at all costs is used to circumvent the basic rights of individuals'. The chapter by White and Davies-Bright represents a powerful corrective to uncritical acceptance of the fate of self-defense arguments in an age of remote technology.

In Chapter 8, 'Drone warfare and the erosion of traditional limits on war powers', Geoffrey Corn continues the discussion of whether remote technology in general, and drones in particular, are transforming traditional avenues of legal regulation. Specifically, Corn asks whether the ubiquity of drones as a military platform has rendered obsolete the traditional constraints in US and international law for limiting the executive branch's deployment (or the sovereign's deployment) of military force. With regard to international law, even a limited number of drone strikes might qualify as an extraterritorial or transnational NIAC, as long as it is accepted that a NIAC may cross international borders and not remain exclusively *internal* to the state. If that is the case, the applicability of the label 'NIAC' encourages the use of military force because IHL sanctions a huge amount of violence, especially so in NIACs, which are under-regulated compared to their international cousins. But even without considering the classification dilemma of whether such conflicts are best described as IACS, NIACs, or something in between, the fact that they are armed conflicts at all means that a large amount of military force is permitted, at least with regard to jus in bello. (Jus ad bellum might be a different story, though other doctrines, including the 'unwilling or unable' test, perform similar justificatory

work in that domain too.) With regard to national law, drone strikes might allow the executive branch to alleviate a national security threat while at the same time placing very few (or even no) service members in harm's way. This factor, inter alia, led Harold Koh and the Obama Administration to suggest that the War Powers Resolution 'clock' did not necessarily apply to military operations with few so-called 'boots on the ground'. For Corn, these factors, in separate legal domains, suggest a dangerous incentive to use drones and also suggest a weakening in the traditional resources of the legal system to constrain and discourage the use of military force. As Corn concludes, 'This advent of the transnational armed conflict theory, coupled with the capacity to conduct virtually risk-free attacks with decisive lethal force, has arguably incentivized an aggressive invocation of armed conflict'.

Chapter 9 switches gears and specifically covers the legal regulation of cyber conflicts as a form of cyber warfare. In 'Developing norms for cyber conflict', William C Banks provides a useful outline for how law of war doctrines will apply to cyber conflicts and the difficulty of translating, into the cyber domain, principles and norms that were originally developed for regulating traditional military activities. After outlining some of these interpretative difficulties, Banks notes that there are reasons for optimism. In particular, Banks notes that the US Department of Defense recently released its *Department of Defense Cyber Strategy*. In that document, which is admittedly a strategic rather than legal analysis, Banks sees the seeds of a burgeoning recognition that cyberwarfare will place immense pressure on the existing normative architecture and will require significant reconceptualization of classic IHL principles. For example, Banks believes that the traditional notions of 'use of force' and 'armed attack' are simply not useful for understanding cyber conflict, though they remain the central pillars of the existing jus ad bellum and jus in bello. As Banks concludes, the DoD *Cyber Strategy*, by moving away from such traditional notions, 'could provide a pillar of a normative architecture for cyber conflict' in the future.

In Chapter 10, 'Some legal and operational considerations regarding remote warfare: drones and cyber warfare revisited', Terry Gill, Jelle van Haaster and Mark Roorda argue that while drones advance the goals of range and covertness, cyber weapons advance the goals of anonymity, allowing the attacker to defeat the enemy's desire for attribution. Nonetheless, the authors paint a portrait of technological advances that can be, and should be, subject to the regular normative constraints of the law of war. In this sense, the authors disagree with those critics who argue that drones and/or cyber weapons require a radical re-working of jus ad bellum or jus in bello in order for these weapons to be effectively

regulated. As the authors note, 'despite the new and to an extent revolutionary impact of these modes of remote warfare, it is clear they are and are, in principle, capable of being governed by the framework of international law, including the law relating to the use of force and the legal regimes which govern how and against whom or what force may and must be applied, in particular the humanitarian law of armed conflict and international human rights law where these are applicable'.

In the next chapter, 'Remote and autonomous warfare systems: precautions in attack and individual accountability', Ian S Henderson, Patrick Keane and Josh Liddy focus on the remoteness of AWS and the challenges that this poses for meeting the obligations, imposed by IHL, during the targeting process. The authors engage in an intensive analysis of the relevant requirements codified in Additional Protocol I (API), and in so doing, insert themselves into a long-running debate between activists who argue that AWS should be banned because they will necessarily violate the obligations of API and military analysts who argue that API may even impose an *obligation* to use AWS where doing so would improve targeting compliance. The authors take stock of the classic objections to AWS and cautiously and moderately support the conclusion that, in some limited circumstances, an AWS might better identify military targets, especially in contexts where military hardware is utterly unique and there are no civilian counterparts to the military equipment. That being said, it will likely be much more difficult to design and build an AWS that can reliably determine whether a human being is 'directly participating in hostilities' and therefore a lawful target on that basis. For proportionality assessments, an AWS might be trained and tested to determine whether its proportionality determinations are accurate. Although the determinations would need to keep a human being 'in the loop' in the strictest sense of that expression, 'it can be argued that human judgement and discretion is being applied by human decision makers electing to employ AWS at a certain location or time, or against certain kinds of targets, with knowledge of how the system will operate in that environment'.

In Chapter 12, 'Autonomous weapons systems: a paradigm shift for the law of armed conflict?', Robin Geiß and Henning Lahmann focus on the inevitable rise of autonomy in military operations, because 'the de-humanization of warfare is already well underway' and there is only a 'small step left towards fully autonomous weapons'. The authors therefore place the rise of AWS in historical context and suggest that the coming technological developments are just the last stage in a progression that has been long in the making. After developing this account, the

authors turn their attention to the often-asserted problem of a responsibility gap for AWS—that is, the question of who will be held responsible when an AWS violates international criminal law or international humanitarian law. The authors concede that it is somewhat problematic to turn over responsibility for complying with IHL to a machine that operates according to an algorithm. On the other hand, the solution to this problem—insisting on 'meaningful human control' for all weapons—is inherently ambiguous because what counts as keeping a human 'in the loop' can mean many different things. However, the authors conclude that '[i]f an agreement on the concept of "meaningful human control" can be reached that comprises all of the three elements, then the risk of an allegedly insurmountable "accountability gap" becomes a non-issue'.

In Chapter 13, 'Making autonomous targeting accountable: command responsibility for computer-guided lethal force in armed conflicts', Peter Margulies argues that AWS will pose significant challenges for IHL compliance, though he sees the solution as active engagement rather than an outright ban on the new technology, which he equates with seeking to 'blink away the future of war'—a totally unrealistic proposition. Specifically, Margulies argues that the doctrine of command responsibility is the key to ensuring that deployment of AWS are IHL-compliant because command responsibility will ensure that those deploying the systems are held accountable for any violations that occur during the deployment. For Margulies, the correct standard will be 'dynamic diligence', which he defines as requiring ongoing: adjustments in the system's interface, assessments of its compliance with IHL, updates to its inputs, and flexibility in the parameters governing the system's operation. In this context, 'flexibility' means that the commander should not operate the system in situations where doing so would be inappropriate. The contribution of Margulies' intervention is that it provides concrete detail to explain how the doctrine of command responsibility could work in practice to ensure that military commanders do everything feasible to control and deploy AWS in a responsible manner.

The volume concludes with Chapter 14, 'The strategic implications of lethal autonomous weapons' by Michael W Meier. In the final chapter, Meier takes a more strategic perspective on AWS by combining strategic considerations with legal analysis. Meier focuses on four key issues: whether AWS make it easier for states to go to war, whether they promote 'unintended engagements', whether AWS will foster greater asymmetry in warfare and ironically spur more terrorist attacks in response, and whether AWS will proliferate and trigger a new arms race. Meier ends his chapter by suggesting diplomatic and regulatory actions that the United States might take in order to mitigate the potential

instability that could be caused by the growing development of AWS. These include, inter alia, restrictions in some circumstances on the export of AWS technology to other states, similar to the existing UAV (drone) export policy that the US government has already implemented.

3. FUTURE DIRECTIONS

In the coming decades, the law regarding remote warfare will inevitably sharpen, as more and more state practice, in response to specific situations, will clarify the scope of existing customary law. Although the common refrain is that *we need a new treaty*, and that always remains a possibility, the vast majority of technological developments are either subsumed under existing treaty regulations or governed by rules of customary international law. Either way, the responses of the world community to these technologies over the coming decades will help form the legal framework for regulating them.

Although the future is bright for legal clarifications, the time for conceptual clarification is now. With the advancement of each new technology, 'armed conflict' as a category paradoxically seems to expand and contract at the same time. There is expansion because remote technologies allow for geographical distance between operator and target, or, in the case of AWS, between commander and target. This widens the geography of armed conflict—indeed globalizes it—scattering the 'participants' across the globe and even across virtual and cyber divides. However, at the same time, there is contraction of armed conflict because remote technologies, *in theory*, bring the promise of razor accurate targeting that will reduce civilian collateral damage. Indeed, even targeting against lawful combatants may be reduced. It is no surprise or coincidence that the advent of drones has allowed for the shift from status-based targeting to conduct-based targeting. The result is that individual fighters are targeted based on their level of threat or dangerousness, rather than the wholesale slaughter of hundreds or thousands of enemy fighters who are killed *en masse* simply because they belong to the same organization, whether it is a conventional army or a terrorist organization. This new era of status-based targeting, which is intimately wrapped up with remote technology, clearly represents a contraction of warfare in this sense.

With AWS, remoteness reaches into its heavenly extreme because the operator fades away into nothingness. Or, perhaps more extravagantly, the weapon *is* the operator. Either way, the distance of the individuals running the show has reached a level of conceptual remoteness perhaps

unthinkable in past conflicts: a war without soldiers. If that sounds like an exaggeration, it certainly is. But perhaps it is more accurate to describe a discrete military *operation* launched without military personnel, who are remote in the sense of non-existent, because the AWS will execute the operation without significant human decision-making 'in the loop'. For some scholars, this remoteness is a recipe for a moral disaster because it will promote unrestrained killing without risk and atrocities committed without responsibility. For others, this remoteness holds the promise implicit in the humanitarian project itself: reducing the suffering on human beings by removing them from warfare as much as possible (at least on one side of the conflict, if not both). One could understand this classic dilemma in the AWS literature as a dispute about the value of remoteness in military engagements. Must humans remain intimately involved in each military operation, or conversely should we work as much as possible to get them removed from war, as long as we can maintain (or even improve) targeting accuracy? Boiled down to its guts, this is a dispute about *remoteness*.