1. Remoteness and reciprocal risk

Jens David Ohlin

1. INTRODUCTION

The history of modern weaponry involves the construction of the technological capacity to produce lethal results while exposing the operator to the least amount of risk of death or injury. The most recent examples of this phenomenon are three new weapon categories: remotely piloted vehicles (drones), cyber-weapons, and Autonomous Weapons Systems (AWS). Each of these categories of weapons allows the attacking force to inflict military damage while the operators of the weapon remain safely shielded from the theater of operations.[1] The technological goal is therefore to generate an inverse proportionality between risk to the operator and lethality to the target.[2] By this standard then, the overall strategy is to create a system that grants the operator total immunity from risk but still inflicts maximum damage to the enemy.[3]

Recent increased technological capabilities have generated a divergent set of intuitive responses from different constituencies. For military planners in the United States, as well as coalition forces allied with them, the advent of remote killing by drone is a source of great pride, because it allows for greater force protection while still accomplishing the

[1] It is perhaps not correct that the operators remain completely shielded from attack. Rather, it is more correct to say that, as a comparative and relative matter, the operators of these weapons are *much less* subject to attack than the operators of more conventional weapons systems. But as the following chapter will demonstrate, the association between remoteness and risk is a difference of degree—not kind—from prior weapon systems.

[2] See Megan Braun, 'Predator Effect: A Phenomenon Unique to the War on Terror' in Peter L Bergen et al (eds), *Drone Wars: Transforming Conflict, Law, and Policy* (Cambridge University Press 2015) 253, 278 (describing the development of insect-sized drones that will operate in locations too dangerous for individual soldiers).

[3] Andy Dougan, *Through the Crosshairs: A History of Snipers* (Carrol & Graf 2005) 16 ('What primitive mankind sought was a weapon that could be used from a distance, leaving its user exposed to minimal risk of injury.').

mission.[4] Moreover, advocates for drone operations often insist that the parameters of the drone platform, including increased surveillance capacities as well as the ability to hover or circle over an intended target for an extensive period of time, allow drone operators to kill enemy targets with an unparalleled level of discrimination. In other words, the capacity to reduce civilian collateral damage is greatly enhanced. In contrast, critics are often harsh in their criticism of American and allied reliance on drone technology. Among the complaints are that drone attacks violate jus ad bellum in many instances, that the attacks produce collateral damage in the absence of risk, and that US military planners are all too willing to shift the risk of death from friendly military forces to enemy civilians who will be killed in the attack. The common assumption that resides beyond these diverse intuitions—both positive and negative—is that drone operations have transformed contemporary military engagements by changing the risk calculation.

For cyber-war, the calculation is slightly different. It is true that cyber-weapons involve remote operators who are physically distant from the scene of the ultimate attack. For example, the operators who designed and launched the Stuxnet computer virus against the Iranian nuclear power plant were nowhere near the centrifuges that were ultimately disabled and destroyed.[5] There is, however, a difference between drones and cyber-weapons: the United States and its allies view the latter not just as an opportunity for strategic force multiplication but also as an area of intense vulnerability and therefore a cause for grave concern. In particular, China, North Korea and Iran have remotely deployed, and threaten to deploy, cyber-weapons that the United States and other allied nations may only partially defend against.[6] Consequently, the risk is asymmetrical only in the following sense. China could launch a cyber-attack against US forces without endangering its Chinese cyber-soldiers, thus generating an asymmetry of risk. However, the United States could

---

[4] Ryan J Vogel, 'Drone Warfare and the Law of Armed Conflict' (2010) 39 Denv J Intl L & Policy 101, 102 ('Drone targeting has proven to be spectacularly successful—both in terms of finding and killing targeted enemies and in avoiding most of the challenges and controversies that accompany using traditional forces.').

[5] However, it should be noted that the virus might have entered the physical computer system through the connection of an infected USB device to a local computer. See Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014) 47–8.

[6] See David E Sangerjune, 'As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy' *New York Times* (16 June 2016).

do the same and launch a cyber-attack against Chinese forces without endangering American cyber-soldiers. The situation is therefore best described as 'reciprocal asymmetrical risk'.

It is unclear how the advent of AWS will transform reciprocal risk.[7] Just as in drone and cyber capabilities, some military nation-states will have the capacity to exploit the technology while others will not—at least not yet. The animating impulse behind AWS is to allow the 'operator' to remain further remote from the field of operation by transiting most of the operator tasks to the system itself.[8] One of the central reasons why the soldier—the human soldier—usually needs to be close to the kinetic effect is because the soldier needs to assess the situation and determine how to destroy the enemy. Air and naval power stretch that capability but they are only as effective as the intelligence regarding the target and they are only effective against some types of target. However, if a weapon system could—by itself—make strategic, legal, and even moral determinations about how to engage the target, the human soldier could remain safely out of harm's way in a remote location. Indeed, it would seem as if the whole strategic point of AWS is its promise of force protection combined with an argument that, like drones, they could reduce civilian collateral damage. Unlike drones, where the argument for lowering collateral damage is their ability to pin-point particular targets, the argument in favor of AWS is more specifically that their computerized algorithms would be immune from heuristic biases and other cognitive defects that infect human reasoning.[9] Like cyber-weapons, however, the asymmetrical risk would be balanced—it would be reciprocal in a deeper sense—in conflicts between military powers that both deploy AWS against each other.

The technological advances just described are novel, but the focus on reciprocal risk is not. The following section seeks to put these technological developments in historical context and will investigate the

---

[7] In using the phrase 'reciprocal risk', I follow George Fletcher's invocation of the term in a different context. See George P Fletcher, 'Fairness and Utility in Tort Theory' (1972) 85 Harv L Rev 537, 549 (strict liability and negligence as solutions for the unfairness of 'unexcused, nonreciprocal risk-taking').

[8] See Marco Sassoli, 'Autonomous Weapons—Potential Advantages for the Respect of International Humanitarian Law', Profiles in Humanitarian Assistance and Protection (2 March 2013); Christopher P Toscano, '"Friend of Humans": An Argument for Developing Autonomous Weapons Systems' (2015) 8 J Natl Security L & Policy 189, 213.

[9] See Gregory P Noone and Diana C Noone, 'The Debate over Autonomous Weapons Systems' (2015) 47 Case W Res J Intl L 25, 32 ('human error causes untold deaths—perhaps AWS can perform better').

moral and legal consequences of every belligerent's desire to reduce risk while maximizing lethality. In short, this chapter will investigate whether reciprocal risk is an essential component of ethical and lawful warfare, whether the technological capacity to produce asymmetrical risk through remoteness is historically novel or continuous, and whether recent advances on that front should be celebrated or criticized. For example, should we view the desire to create asymmetrical risk as fundamentally different from, or of a piece with, the shift from swords to guns? Are we witnessing a fundamental shift in warfare, or are we reading just the latest chapter in the same old story?

Specifically, this chapter will propose, explain and critically examine the concept of reciprocal risk. It will seek to determine whether there is, in fact, a historical norm in favor of reciprocal risk in warfare, and how the advent of drones, cyber-weapons and AWS have impacted this putative norm. After evaluating the alleged and often assumed rupture to reciprocal risk caused by technological innovation in weapons design, this chapter will then examine two familiar objections to these technologies. The first is whether the weapons will, by creating a severe asymmetry in risk, allow states to exercise force cavalierly, and remove an important check on warfare that helps limit the number of jus ad bellum violations across the globe. Having examined that anxiety, the final part of this chapter will ask whether reciprocal risk is an essential ethical component of basic norms of chivalry. This latter analysis will require an examination of legal principles under the Law of Armed Conflict (LOAC) and ethical principles embodied in just war theory.

2. A BRIEF HISTORY OF MILITARY RISK MANAGEMENT

Is it really true that the rapid development of drones, cyber-weapons and AWS has eroded reciprocal risk? A brief analysis of the history of weaponry suggests that the production of asymmetrical risk is not an outlier.[10] In fact, it has been the goal of weapon design ever since the abandonment of the club as an instrument of blunt-force killing.

Historians of weaponry generally regard the bow as the signature development in early weaponry. It allowed individuals to launch a deadly

[10] See Gabriella Blum, 'The Dispensable Lives of Soldiers' (2010) 2 J Legal Analysis 115, 132 ('governments try to protect their soldiers, partly by employing more aggressive force toward the enemy (including by "risk-transfer" from soldiers onto enemy forces and civilians)').

attack from a distance, perhaps even from a location hidden from view.[11] A target might be felled by an arrow without ever looking his killer in the eye. The attacker could therefore inflict a lethal result while minimizing, though not entirely erasing, his exposure to a lethal counter-attack. As one historian explains:

> At once safe and deadly, it was the ideal weapon of harassment. A combatant might spend an afternoon shooting away at long range with little fear of injury. Yet if the opportunity arose, he could move in closer and swiftly, silently dispatch an enemy with a single shot. It is not surprising, therefore, that the earliest actual image of combat, a Mesolithic cave painting at Morela la Vella in Spain, depicts men fighting with bows. Conceptually at least, the picture is a familiar one. The action is confused. The participants appear to be on the run, perhaps hoping to rip off a few quick shots before retreating. Moreover, all the combatants are armed symmetrically; only the bow is used.[12]

The advantage of bow and arrows over their predecessors—primarily fixed blades—was their ability to inflict damage at a distance.

It is important to recall that many of these early technological developments were motivated just as much by the requirements of hunting as they were by the requirements of warfare.[13] Action at a distance was crucial for catching prey. Managing risk was important in this endeavor as well, but not the primary motivating factor. While a few animals could harm a hunter during a close-quarters confrontation, most animals would simply flee. The real benefit of action at a distance was stealth and surprise. Regardless of its original motivation, the bow and arrow transformed warfare and effectively ended the paradigm of personal confrontations where soldiers were required to look the enemy in the eye before killing or injuring them.[14]

The introduction of guns accelerated the process that was first introduced with the bow and arrow.[15] Large-scale cannons used in the defense

---

[11] The javelin might be considered a forerunner of the bow and arrow and was used by the Mycenaeans for hunting but 'very rarely' in war. See A M Snodgrass, *Arms and Armour of the Greeks* (Cornell University Press 1967) 17.

[12] See Robert L O'Connell, *Of Arms and Men: A History of War, Weapons, and Aggression* (Oxford University Press 1989) 26.

[13] Ibid.

[14] The Mycenaeans probably used bows for warfare, even though the ancient Greeks who came later 'did not think highly of the bow for military use'. See Snodgrass (n 11) 17.

[15] See Malcolm Vale, *War and Chivalry* (University of Georgia Press 1981) 129 (discussing Don Quixote's complaint that war had become impersonal and

of fixed dwellings,[16] or used offensively in naval warfare, allowed armies to launch an explosive device over long distance with the artificial enhancement of explosive powder. The 'action' of action at a distance was no longer powered by human strength but by chemical ingenuity.[17]

Miniaturization of gun-power devices so that they could be carried by individual soldiers proved to be difficult to design and even more difficult to deploy. As the British historian John Keegan notes, hand-held firearms 'remained relatively ineffective' because they were 'fired by applying a burning match to an open touchhole, both prone to malfunction in wet weather, and they threw comparatively light balls only a short distance'.[18] The better option was the crossbow, a hybrid invention that had combined the propulsion of the firearm with the arrow, producing a deadly weapon: 'Armed with a crossbow a man might, without any of the long apprenticeship to arms necessary to make a knight, and equally without the moral effort required of a pike-wielding footman, kill either of them from a distance without putting himself in danger.'[19] In other words, crossbowmen were probably 'the first users of firearms'.[20] Consequently, the modern-day firearm was just the logical conclusion of a technological process first begun with the deployment of bows and arrows in battle.[21]

In conceptual terms, modern-day ordnances are basically improvements on the same paradigm. Artillery produces greater destruction, with greater accuracy, and at a greater distance than cannon fire. The strategic goal of artillery combat is to inflict damage from a range or location that

---

mechanical). See also J R Hale, 'Fifteenth and Sixteenth Century Public Opinion and War' (1962) 22 Past and Present 18, 21 ('by the beginning of the sixteenth century the gun had acquired a rich store of symbolic and associative overtones and was already rivalling the sword as the embracing symbol of war itself').

[16] Vale (n 15) 130–31.

[17] O'Connell (n 12) 162 ('Yet again, the great stabilizer was the imposition of the generic solid-firing smoothbore gun as the standard naval engine of destruction. So armed, all ships differed basically in degree rather than kind—the more guns, the more fighting power.').

[18] John Keegan, *A History of Warfare* (Knopf 1993).

[19] Ibid.

[20] Ibid. See also Jean Liebel, *Springalds and Great Crossbows* (Royal Armouries 1998) 23 (dating crossbows to the 10th century); Blum (n 10) 75.

[21] See Andrew Ayton, 'Arms, Armour, and Horses' in Maurice Keen (ed), *Medieval Warfare: A History* (Oxford University Press 1999) 186, 203–4 ('Massed archery by men able to unleash perhaps a dozen shafts a minute would produce an arrow storm, which at ranges of up to 200 yards left men clad in mail and early plate armour, and particularly horses, vulnerable to injury, while causing confusion and loss of order in attacking formations.').

is relatively immune from counter-attack by return fire. Cruise missiles launched from naval ships operate from the same strategic premise. Indeed, the logical culmination of this remoteness is Intercontinental Ballistic Missiles (ICBMs), which allow destruction of an enemy location without having to deploy mobile forces at all.

Before one gets to ICBMs, however, the game-changer for remote warfare came with the advent of air and naval power. One cause of World War II was a long-simmering dispute between Japan and the United States over naval power in the region. Japan needed naval dominance to transport ground troops to neighboring countries in pursuit of its imperial ambitions. The United States built a naval presence in the Pacific Ocean to counter this threat and check Japanese expansionism. The American capacity to deploy a massive naval presence was in one sense remote and in another sense not remote. It was not remote because the naval operators were located in the Pacific Ocean and subject to great risk. However, the use of naval power allowed the United States to project military force well beyond the American homeland, thus producing an element of remoteness that struck the Japanese as strategically intolerable, in turn leading to their decision to attack Pearl Harbor and start a conflict that they viewed, perhaps erroneously, as inevitable.

The specifics of naval warfare depend on remoteness. Aircraft carriers allow the major powers to deploy air assets—fighter jets—off the coast of the target state so that the strikers can move quickly to attack. At the same time, however, the aircraft carrier can in theory remain outside the direct radius of the target state's land-based defensive weapon systems, thus allowing the aircraft carrier to launch airstrikes from a safe and remote distance. Of course, if the target state has naval destroyers or air assets of its own, the aircraft carrier then becomes vulnerable, and must travel with an entire battle group of destroyers whose main purpose is to prevent enemy naval and air assets from getting within striking distance of the aircraft carrier. The carriers were originally conceived and designed at a time when they could produce an asymmetry of risk, although that advantage was quickly closed among major military powers; however, the asymmetry still persists in conflicts between major and lesser military powers.

3. MODERN TECHNOLOGICAL DEVELOPMENTS FOR REMOTE KILLING

Our next task is to determine whether the latest advancements in military technology are only the most recent examples of strategic asymmetries of

risk, or whether new technology represents a fundamental breakdown in the paradigm of reciprocal risk.[22]

A. Drones

The deployment of remotely piloted vehicles produces a number of strategic advantages. First, it allows the projection of force without risking a human pilot. Second, since there is no human pilot, the drone can stay in the sky for an extensive period of time, allowing both increased surveillance and the ability to strike within minutes. Third, the increased surveillance allows the attacking force to ensure that they are hitting the right target. Fourth, the use of precision warheads with small yields serves the goal of discrimination, thus reducing the number of civilians potentially killed in the strike as collateral damage. Fifth, drones have a small footprint, therefore facilitating covert or clandestine action. These advantages are all contingent rather than intrinsic features of the drone platform, with the possible exception of the elimination of risk to the human operator.

Switching now to the legal criticisms mounted against targeted killing by drone, the vast majority of the objections have no direct connection to the remoteness of the pilot, which is the defining characteristic of drone operations, though some of the legal criticisms might be *indirectly* linked to remoteness. Consider the objections outlined below.

First, some critics argue that drone attacks violate the sovereignty of the territorial state where the strikes occur.[23] In this regard, strikes in Yemen, Pakistan and Somalia are sometimes referenced.[24] The United States has asserted that the strikes are justified by self-defense against al-Qaeda, a non-state actor, or associated forces that are co-belligerents of al-Qaeda in its non-international armed conflict against the United

---

[22] For example, Paul Kahn argues that war without mutual risk produces 'an image of warfare without the possibility of chivalry'. See Paul Kahn, 'The Paradox of Riskless Warfare' (2002) 22 Phil & Pub Policy Quarterly 2, 4, cited in Blum (n 10) 137.

[23] See Mary Ellen O'Connell, 'Unlawful Killing with Combat Drones: A Case Study of Pakistan, 2004–2009' in Simon Bronitt et al (eds), *Shooting to Kill: Socio-Legal Perspectives on the Use of Lethal Force* (Hart Publishing 2012) 263, 264 (discussing drone strikes in Pakistan).

[24] For a discussion, see Sikander Ahmed Shah, *International Law and Drone Strikes in Pakistan: The Legal and Socio-Political Aspects* (Routledge 2015) 32.

States.[25] Of course, the drones cross the territorial borders of the territorial state, and if there is no self-defense argument against the territorial state, there is a non-trivial argument that the self-defense argument is inapplicable against the territorial state.[26] The United States has forcefully argued that self-defense is applicable in this context when the host state is unwilling or unable to redress the threat itself.[27] Formally speaking, the unwilling or unable test is a gloss on the necessity requirement for self-defense; if the host state is capable or willing to stop the threat, intervention by the foreign power is not necessary, and therefore self-defense is unavailable.[28] It is unclear, though, whether the US government views the infringement of the territorial state's sovereignty as a 'use of force' in violation of Article 2, thus requiring some Article 51 justification sounding in self-defense, or whether the infringement of sovereignty falls below the threshold of what would be considered an 'armed attack' under international law. Perhaps it is a mere counter-measure.[29] Without taking a view of the substance of this jus ad bellum debate, it is sufficient to note here that there is no *direct* connection between the remoteness of the pilot and the alleged jus ad bellum violations here. The issue would come up just as surely with a purportedly defensive attack carried out with manned aircraft or infantry

---

[25] See Harold Hongju Koh, Legal Adviser, US Department of State, Speech to the Annual Meeting of the American Society of International Law, Washington, DC (25 March 2010) ('As I have explained, as a matter of international law, the United States is in an armed conflict with al-Qaeda, as well as the Taliban and associated forces, in response to the horrific 9/11 attacks, and may use force consistent with its inherent right to self-defense under international law.').

[26] See Michael N Schmitt, 'Drone Law: A Reply to Un Special Rapporteur Emmerson' (2014) 55 Va J Intl L Dig 13, 16–17 ('Absent an "operational nexus" to the host State, the restrictive view would preclude an extraterritorial RPA strike, not because the individuals are unlawful targets, but rather because it is unlawful for the attacking State to cross the border in self-defense.').

[27] See Brian J Egan, Legal Adviser, US Department of State, Speech to the American Society of International Law, Washington, DC (1 April 2016) ('In particular, there will be cases in which there is a reasonable and objective basis for concluding that the territorial State is unwilling or unable to effectively confront the non-State actor in its territory so that it is necessary to act in self-defense against the non-State actor in that State's territory without the territorial State's consent.').

[28] See Ashley S Deeks, '"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense' (2012) 52 Va J Intl L 483, 522.

[29] For a discussion of countermeasures, see Sheng Li, 'When Does Internet Denial Trigger the Right of Armed Self-Defense?' (2013) 38 Yale J Intl L 179, 215.

(as was the case with the Bin Laden raid in Pakistan). To the extent that there is any connection at all, it is an *indirect* one. Perhaps the remoteness of the pilot removes an inherent constraint on using force cavalierly, thus giving the United States another incentive to violate jus ad bellum.[30] Since pilots will not be put in harm's way, there is less reason to be concerned about launching an international attack that could, according to some critics, violate jus ad bellum. This indirect argument will be evaluated in full in Section 4.

Second, drone attacks allegedly cause too much collateral damage to civilians.[31] Both journalists and legal scholars have reported on the vast human toll inflicted on the local population in areas where drone strikes have occurred.[32] Of course, collateral damage is not per se illegal unless it is disproportionate to the anticipated value of the military target. Moreover, even in cases where there are credible allegations of violations of the principle of proportionality, there is little to no evidence that the remoteness of the pilot is directly relevant to the production of the disproportionate collateral damage.[33] An air strike performed with a manned aircraft would have produced the same amount of collateral damage or, if one believes the US military, it is perhaps the case that the manned airplane might have produced *more* collateral damage. The same conclusions apply to criticisms that a particular drone strike violates international human rights law (IHRL). Under this argument, the strike is not governed by international humanitarian law (IHL) at all, and the more restrictive norms of IHRL apply, which prevent status-based targeting and would require capturing the target, using more traditional law enforcement methods, before lethal measures are employed against a

---

[30] See O'Connell (n 23) 267.

[31] Compare Shah (n 24) 28–9 ('A well-planned, targeted ground offensive with commando units would have been more effective in battling Al-Qaeda and sympathetic armed militias, and would have kept collateral damage, including civilian casualties, to a minimum.') with Jane Stack, 'Not Whether Machines Think, but Whether Men Do' (2015) 62 UCLA L Rev 760, 772 ('drones generate fewer civilian casualties than ground troops').

[32] See O'Connell (n 23) 271.

[33] See Stack (n 31) 772. One difficulty with assessing this question is the classified nature of the underlying data, which is rarely acknowledged or released by the US government. See Steven J Barela, 'Strategic Efficacy: The Opinion of Security and a Dearth of Data' in Steven J Barela (ed), *Legitimacy and Drones: Investigating the Legality, Morality and Efficacy of UCAVs* (Ashgate 2015) 271, 296 ('Secrecy of the drone program has rendered the necessary data for full assessment unattainable, and selective disclosures have only distorted an already fragmented picture.').

target that represents an imminent threat. But the same arguments could all be made—and have been made—against strikes carried out by manned vehicles.

There is one argument that asserts an indirect relationship between the remoteness of the killing and the alleged disproportionate collateral damage or the violation of human rights law. One could argue that the use of an unmanned aerial vehicle makes it more likely that civilians will be killed by collateral damage. The effect here would be to *transfer* risk from friendly forces *to* enemy civilians.[34] As noted above, it is empirically doubtful whether the move from manned aircraft to unmanned aircraft has this effect.[35] However, if one broadens the lens, a more defensible hypothesis emerges: that the selection of unmanned aircraft as compared to ground infantry forces, reduces the risk to friendly forces but dramatically increases the risk to enemy civilians.[36]

To answer this question, one must determine whether there is a legal obligation for attacking forces to use an alternative military tactic—such as ground forces—that would reduce collateral damage when compared to the default option, in this case a drone campaign. The question is whether this normative obligation is codified in existing law. Certainly, Additional Protocol I codifies a restrictive customary norm that requires attacking forces to take all reasonable precautions to reduce collateral damage as far as 'feasible'—an evaluative term that says little about how much attacking forces are permitted to prioritize friendly forces over enemy civilians.[37] Does this legal requirement *require* attacking forces to

---

[34] See O'Connell (n 23) 271 ('In the trailer in Nevada, the pilot knows she will not be attacked. She will go home to her family at the end of the day, coach a soccer game, make dinner, and help with homework.').

[35] For a discussion of this issue in the AWS context, see R Crootof, 'War, Responsibility, and Killer Robots' (2015) 40 North Carolina J Intl L & Commercial Reg 909, 923 (noting possibility for increased civilian harm but also concluding that this result is 'far from certain').

[36] See Stack (n 31) 772 ('The primary argument advanced to this end is that drones' significant reduction of the cost of war to the United States in terms of both "blood and treasure" will seduce policymakers into expanding the limits on what constitutes a "legitimate target," and engaging in more, longer, and less legitimate wars.').

[37] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 57. Although the United States is not a party to Additional Protocol I, many of its provisions are widely regarded as having ripened into customary international law, especially the provision requiring attacking forces to take all feasible precautions to reduce collateral damage.

forego unmanned aircraft in favor of ground forces where doing so would reduce collateral damage?[38]

The issue is contested. The US Law of War Manual recognizes an affirmative obligation to use a particular weapons platform to reduce collateral damage as far as possible, but 'the decision of which weapon to use will be subject to many practical considerations, including effectiveness, cost, and the need to preserve capabilities for other engagements'.[39] More importantly and convincingly, some IHL scholars who have considered this legal requirement believe that the obligation resides at the tactical level of the battlefield commander. In other words, a commander in a particular military engagement has an obligation, when presented with multiple weapons choices *at his or her disposal*, to select the option that will reduce collateral damage as far as possible, provided that the selection does not endanger friendly forces.[40] However, there is a question whether the normative obligation applies to strategic choices that are *not* within the purview of the battlefield commander. For example, if there are other weapons that *could* be deployed to the theater of operations, but remain warehoused far from the battlefield, is the nation in question responsible for its failure to bring the more discriminating weapons to the battle? No, argue several scholars.[41] Judged from this standard, a state cannot be faulted because it has decided, at the political level, to engage in an air-power campaign and has refused to

---

[38] In *Necessity in International Law* (Oxford University Press 2016), Larry May and I argue that attacking forces are under a moral obligation to subject themselves to a level of 'reasonable risk' in pursuit of their reduction of collateral damage.

[39] US Department of Defense, Law of War Manual (2015) § 5.11.3. The manual also notes that 'there would be few, if any, instances in which the use of a particular weapon system, such as precision-guided munitions or cyber tools, would be the only legally permissible weapon'. Ibid.

[40] See Michael N Schmitt and Eric W Widmar, '"On Target": Precision and Balance in the Contemporary Law of Targeting' (2014) 7 J Natl Security L & Policy 379, 402 ('Of course, attackers need only select less harmful means or methods that do not involve sacrificing military advantage and that are feasible. As an example, an attacker does not have to use a less powerful bomb against an insurgent leader in a building in order to avoid civilian casualties if doing so would significantly lower the likelihood of success (assuming all other IHL requirements are met).').

[41] Ibid ('For instance, although precision weapons may be available for an operation, they may be more useful at later stages of the campaign and thus need to be preserved, or the employment of a precision weapon may be infeasible because it would require increased risk to ground forces in order to designate a target.'). Compare with Shah (n 24) 28–9.

commit ground troops to the military operation, despite the fact that ground forces might do a better job of reducing civilian collateral damage. There is, of course, a strong moral argument for such an obligation, residing at the political level, but it is probably correct to conclude that mainstream international law is not yet prepared to recognize it as binding.

B. Cyber-weapons

Compared with remotely piloted vehicles, cyber-weapons involve an even further regression in the location of the combatant.[42] While the pilot of a drone might be far removed from the forward area of deployment, it is nonetheless the case that drones have a limited tactical range. Somewhere within a relatively close distance to the theatre of operations, the drone will need a base from which it can takeoff, land, refuel, and be repaired if necessary. These facilities are usually carefully sited to be out of harm's way, though they are still foreign military installations subject to discovery and attack in the event of an armed conflict. Though the pilot per se might remain in the United States, the actual deployment of the drone remains foreign.

In contrast, a cyber attack could, in theory, involve personnel who are all safely located in the United States and removed from the field of operations. Moreover, the target of the attack would have grave difficulty

---

[42] The application of the war paradigm to cyber warfare is contested, with some scholars believing that many cases of cyber attacks should be evaluated as 'actions short of armed conflict'. See Michael Newton and Larry May, *Proportionality in International Law* (Oxford University Press 2014) 280 (most cyber attacks are more analogous to embargoes than they are to traditional military attacks). Similarly, Mary Ellen O'Connell has argued that evaluating cyber attacks under the law of war paradigm only facilitates military control over cyber defenses. See Mary Ellen O'Connell, 'Cyber Security without Cyber War' (2012) 17 J Conflict Security L 187 ('The evidence shows that the USA, in particular, is building capacity and developing strategies that make the Department of Defense a major player in Internet use and protection. The concern with this development is that the Pentagon will conceive of cyber space as it does conventional space, with war fighting in mind. Yet, the international legal rules on the use of force, especially the rules on self-defence, raise important barriers to military solutions to cyber space problems. Indeed, the law of self-defence should have little bearing in discussions of cyber security. Even if some cyber incidents could fit a solid definition of what constitutes an armed attack, responding to such an attack will rarely be lawful or prudent if the response is a use of force. The emphasis, therefore, in terms of legal norms and commitment of resources should be in the non-military sphere.').

tracing and locating the source of the attack and the location of the hackers who launched the attack.[43] They might be located at the NSA headquarters (home of US Cyber Command), or they might be located in another installation. They might be located abroad, or they might even be civilian contractors (or hackers) hired by the attacking state to launch a particular cyber-attack.[44] In this sense, the offensive personnel might be located anywhere on the globe.[45]

Traditionally, scholars focus on this fact in the context of the attribution problem—the inability to determine which country launched the attack, which country is legally responsible for the infringement of the target state's sovereignty (assuming that the attack is not justified by principles of jus ad bellum articulated in the UN Charter), and by extension which state is subject to counter-attack as a right of response in legitimate defense.[46] However, it is less common for scholars to focus on remoteness as a risk-reducing strategy—though perhaps it was just too obvious to garner serious conceptual attention.[47] The risk-reducing nature of cyber-war is important, though, because it highlights the degree to which modern methods of attack are placing combatants at increasingly remote locations from the effects of their attacks.

One notable difference between drones and cyber is that for the former, the risk-reducing nature of the platform was the inspiration for its development, while for the latter, the risk-reducing nature of the platform

---

[43] See Scott J Shackelford and Richard B Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 Geo J Intl L 971, 1016.

[44] See Nicolò Bussolati, 'The Rise of Non-State Actors in Cyberwarfare' in Jens David Ohlin et al (eds), *Cyberwar: Law and Ethics for Virtual Conflicts* (Oxford University Press 2015) 103.

[45] See Heather Harrison Dinniss, 'Participants in Conflict: Cyber Warriors, Patriotic Hackers and the Laws of War' in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff 2013) 251, 258 (arguing that cyber warriors often work at great distances that alleviate them from the requirements of wearing uniforms or distinctive emblems); Mark Shulman, 'Discrimination in the Laws of Information Warfare' (1999) 37 Columbia J Transnational L 939, 956.

[46] See, eg, Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 J Conflict Security Law 229, 233; M C Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2 (4)' (2011) 26 Yale J Intl L 421, 445; T Rid and B Buchanan, 'Attributing Cyber Attacks' (2015) 38 J Strategic Stud 4, 5.

[47] But see Patrick Lin, George Bekey and Keith Abney, 'Robots in War: Issues of Risk and Ethics' in Rafael Capurro and Michael Nagenborg (eds), *Ethics and Robotics* (Akademische Verlagsgesellschaft 2009) 49.

is a mere by-product of the weapons system. The whole point of developing drones was to create a platform whereby the pilot would no longer be located on the aircraft. However, a cyber weapon is designed with the goal of launching an attack against a computer-based network in order to destroy or manipulate any civilian or military system that is partially controlled by, or connected to, a computer network or other device subject to manipulation. It just so happens that the deployment of such an attack almost never requires that the cyber attack be located in the general vicinity of the attack (although there might be some exceptions to this observation for so-called 'closed' systems). Generally speaking, though, cyber attackers can be located anywhere where there are sufficient network facilities to generate the attack. Usually, this location will be far removed from the location of the attack itself. But it would be wrong to describe this as a goal of cyber-warfare; rather, it is a happy coincidence (for the attacking force). The real goal is to attack computers and the systems that rely on them, and it just happens that the best way to do so is from the relatively safe confines of an office.

The target of a cyber attack might be a military installation, but the greatest utility of the cyber strategy is against dual-use (civilian and military) infrastructure as well as against revenue-enhancing operations that either directly or indirectly support the enemy's capacity to support its military. Both of these areas are controversial under existing law.[48] It might be objected that cyber will give attacking forces a greater incentive to attack such targets with little risk, and thus promote greater collateral damage on the part of civilians. The legitimacy of this argument depends, in part, on whether these attacks are lawful or not.

Consider first the question of attacking dual-use infrastructure targets.[49] Important examples include electrical grids, power plants, oil refineries, railroads, and bridges—all of which support both civilian and

---

[48] For a discussion of the legality of bombing dual-use infrastructure targets, see Henry Shue and David Wippman, 'Limiting Attacks on Dual-Use Facilities Performing Indispensable Civilian Functions' (2002) 35 Cornell Intl LJ 559, 575 ('Under our approach, if the advantage of attacking an indispensable object cannot be viewed as compelling in relation to the anticipated direct and indirect civilian harm, the military functions served by the indispensable object may still be thwarted, but must be thwarted by some other means. For example, if the electricity plant serves command and control, as well as water-purification, the attacks will need to target the command and control facilities directly rather than indirectly by way of the facilities' energy source.').

[49] See Eric Talbot Jensen, 'Unexpected Consequences from Knock-On Effects: A Different Standard from Computer Network Operations?' (2003) 18 Am Univ Intl L Rev 1160–68.

military operations. Under the governing standard announced in Additional Protocol I, objects are defined as military objects—and subject to attack—if 'their nature, location, purpose or use make an effective contribution to military action' and their 'total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'.[50] Under that definition, all of the dual-use infrastructure targets would seem to qualify as military targets, since it is clear that the destruction of a bridge, railroad, oil refinery, or power plant would certainly offer a 'definite military advantage'. It is therefore unlikely that such attacks are categorically prohibited by IHL. The most that can be said is that such attacks are subject to an additional constraint, the principle of proportionality, and that attacks are impermissible if the collateral consequences to the civilian population in destroying, say, the oil refinery or bridge, are disproportionate to the contemplated military advantage to be gained by their destruction.[51] However, even this is controversial.[52] The other position is that the principle of proportionality

---

[50] Additional Protocol I (n 37) Article 52(2).

[51] For a discussion of targeting dual-use infrastructure targets with cyber weapons, see Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 185 (concluding that '[t]he fact that an object is *also* used for civilian purposes does not affect its qualification under the principle of distinction: if the two requirements provided in Article 52(2) of Additional Protocol I are present, the object is a military objective but the neutralization of its civilian component needs to be taken into account when assessing the incidental damage on civilians and civilian property under the principle of proportionality').

[52] In 2013, an ICTY Trial Chamber held that the destruction of the old Stori Most Bridge used by military and civilian personnel was a violation of IHL because it violated the principle of proportionality. See *Prosecutor v Prlic*, Trial Chamber Judgment, ICTY Case No IT-04-74 (29 May 2013) para 1584 ('The Chamber therefore holds that although the destruction of the Old Bridge by the [Croatian armed forces] may have been justified by military necessity, the damage to the civilian population was indisputable and substantial. It therefore holds by a majority, with Judge Antonetti dissenting, that the impact on the Muslim civilian population of Mostar was disproportionate to the concrete and direct military advantage expected by the destruction of the Old Bridge.'). For a discussion of this case, see Martin Lederman, 'Is it Legal to Target ISIL's Oil Facilities and Cash Stockpiles?' *Just Security* (27 May 2016).

applies only to civilian collateral deaths and cannot transform what would otherwise be a lawful military *object*.[53]

The second example is the even more controversial question of targeting revenue-enhancing operations whose destruction would inhibit the *capacity* to launch and sustain a military campaign by denying a regime the capacity to develop the necessary financial and other resources to sustain the military.[54] Recent examples include the United States decision to target ISIS oil supplies and cash stockpiles.[55] In the case of the oil supplies, the oil was not necessarily destined for military vehicles but was instead to be sold in return for cash payments that might fund military operations. By destroying both oil and cash, the attacking forces denied to their enemy the ability to *fund* military operations.[56] This argument, if accepted, turns many proto-typically *economic* activities into legitimate military objectives. Again, this theory represents a slippery slope and is highly controversial, in part because so much of the citizenry's daily life is wrapped around economic activity, and at least one animating impulse of IHL is to protect the civilian population from the horrors of armed conflict. The targeting of objects involved in economic activity threatens that basic goal of the regulatory enterprise.

Both examples discussed above (dual-use and revenue-enhancing targets) are highly relevant for the case of cyber attacks, because it is plausible that a cyber-weapon might be ideally suited to go after either a dual-use infrastructure target such as an electrical grid, or to go after a war-sustaining economic activity, such as a financial system (for

---

[53] In *Prlic*, Judge Antonetti dissented and concluded, simply, that the Stori Most Bridge was a 'military objective' and 'there is no such thing as proportionate destruction'. *Prosecutor v Prlic*, Separate and Partially Dissenting Opinion of Presiding Judge Jean-Claude Antonetti, ICTY Case No IT-04-74 (29 May 2013) 325.

[54] In a recent article, Ryan Goodman argues that such attacks are, in principle, consistent with IHL, as long as they also meet other conditions, including the principle of proportionality. See Ryan Goodman, 'Targeting "War-Sustaining" Objects in Non-International Armed Conflict' (2016) 110 Am J Intl L (discussing precedent of Union destruction of cotton during the Civil War because it funded Confederate military operations).

[55] See Matthew Rosenberg, 'U.S. Drops Bombs Not Just on ISIS, but on Its Cash, Too' *New York Times* (20 January 2016).

[56] Goodman (n 54).

example, stock market operations).[57] If a cyber attack allows the attacking force to launch these questionable attacks, with limited risk to the attacking hackers, then the future of warfare might be waged with an ever-increasing impact on the civilian population who are more affected by the destruction of dual-use infrastructure targets and war-sustaining economic activity targets than by the destruction of traditional military targets.[58] This would be a worrisome result and perhaps reason to criticize, rather than celebrate, the increase in cyber attacks by virtue of their risk-free operation. In these situations, lowering risk to military personnel may come with a resulting, albeit indirect, increase in harm to the civilian population.[59]

So cyber attacks potentially allow a greater number of risk-free attacks against infrastructure targets that civilians rely on. The one thing holding militaries back, at this point, is the fear of cyber reprisals. If one country launches a cyber assault, one's enemies, provided that they are cyber-enabled, could potentially launch a brutal cyber-retaliation.[60] The result is a steady détente for the time being. However, that détente is only viable for states with adequate non-cyber military capabilities that can afford to forgo using cyber weapons. The real promise of cyber weapons is that they may represent a force multiplier—even a force equalizer—for states with the inability to spend their way to military dominance using conventional weapons. With no resources to win a typical arms race, a minor military power may view cyber weapons as its one shot to level the

---

[57] For example, a cyber attack could damage an irrigation system that is reprogrammed to flood crops that will feed the civilian population. See William Boothby, *The Law of Targeting* (Oxford University Press 2012) 398.

[58] See David Turns, 'Cyber War and the Concept of "Attack" in International Humanitarian Law' in David Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff 2013) 209, 224–5 (noting risk of 'slippery slope towards a potential expansion of legitimate targets that would simultaneously expand the possibilities for indiscriminate attacks while curtailing the operation of the fundamental principle of distinction').

[59] See Turns (n 58) 224 n 77 (noting that an attack against an electricity generator may cause no initial physical damage but 'later down the line, such basics for the civilian population as water purification plants would shut down, leading to epidemics of disease from water contamination').

[60] However, it appears that some nations are better equipped than others to play this cat-and-mouse game. See David E Sangerjune, 'As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy' *New York Times* (16 June 2016) (reporting that while the US has substantial cyber offensive capabilities, NATO at the present moment has few options to engage in low-level cyber retaliation for attacks coming from Russia or China).

playing field with traditional military powers. Using this calculation, some states may not only utilize cyber-weapons but may wish to accelerate the transition to cyber conflict, a domain where they are more likely to succeed. This would represent a negative outcome for civilians who might be disproportionately harmed in a cyber conflict based on the likelihood that some civilian infrastructure targets may be tempting targets for a cyber offensive.

C. Autonomous Weapons Systems

Autonomous weapons involve the greatest attenuation of human operators; the level of risk to the operator could be reduced to zero by removing human beings from the 'loop' entirely.[61] While there are human beings involved in the design and construction of AWS, the systems could be deployed—at least in theory—without a human operator.[62] First, we should scrutinize whether this is an intended or unintended consequence of AWS. Like drones, it might be argued that AWS are designed to reduce risk to the human operator by turning over essential tasks to the weapon itself, thus allowing the relevant human beings to remain far from the field of battle.[63] However, this is probably an incorrect assumption. The animating impulse behind AWS is the promise that artificial intelligence is better equipped to make quick life-or-death decisions than a human operator, at least in certain operational contexts in which the AWS is designed to succeed.[64] For example, if an AWS could better distinguish between civilian and military aircraft, this would argue in favor of giving autonomous targeting protocols to an anti-aircraft

---

[61] See Daniel N Hammond, 'Autonomous Weapons and the Problem of State Accountability' (2015) 15 Chi J Intl L 652, 656 ('Unlike the activities of human-operated drones, an AWS's actions are not easily attributable to a particular person.').

[62] For a discussion, see David Akerson, 'The Illegality of Offensive Lethal Autonomy' in David Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff 2013) 65, 86; Peter Asaro, 'Jus Nascendi, Robotic Weapons and the Martens Clause' in Ryan Calo et al (eds), *Robot Law* (Edward Elgar 2016) 367, 386 (concluding that a requirement of meaningful human control is suggested by ethical principles of humanity that were preserved by the Martens Clause).

[63] Crootof (n 35) 920–23.

[64] See Mark Klamberg, 'International Law in the Age of Asymmetrical Warfare, Virtual Cockpits and Autonomous Robots' in Jonas Ebbesson et al (eds), *International Law and Changing Perceptions of Security* (Brill Nijhoff 2014) 152, 167.

missile system.[65] The goal of this autonomous targeting would have nothing to do with reducing risk to human operators but rather would be inspired by the goal of reducing human error.[66] In this respect, it would appear that AWS should be grouped with cyber weapons where the reduction of risk to the combatants on the attacking side should be viewed as a collateral consequence rather than the animating impulse for the development of the weapon.

However, it is possible to imagine future applications of AWS where the goal is to reduce risk by achieving the ultimate degree of remoteness, that is, removal of the human operator entirely. This would, in fact, transcend remoteness entirely and transform it into pure disappearance.[67] This would be particularly desirable in the infantry context. That being said, for the moment the majority of contemplated AWS applications involve missile-targeting programs that would be deployed by land, sea or air. The other major area for AWS application is cyber. A cyber weapon could include an algorithm that identifies and assesses the nature of a particular computer system, whether it is military or civilian, for example, and then disables the computer system without requiring an executive command for an operator. In this respect, a cyber weapon might be more or less autonomous, thus suggesting that the most important development in the future of warfare might not be cyber or AWS but in fact the *combination* of the two strategies.

The infantry context, though a source of popular imagination, represents the future of AWS deployment, not its present. In the future, if AWS technology is sufficiently advanced, it could be deployed in the infantry context as a risk-management tool.[68] Robotic infantry devices, operating autonomously, could roam a city street and eliminate any and

---

[65] Robert Sparrow, 'Building a Better Warbot: Ethical Issues in the Design of Unmanned Systems for Military Applications' (2009) 15 Science & Engineering Ethics 169.

[66] Another benefit is the ability of an AWS to continue operating even when its communication link is severed. See Jeffrey S Thurnher, 'Examining Autonomous Weapon Systems from a Law of Armed Conflict Perspective' in Hitoshi Nasu and Robert McLaughlin (eds), *New Technologies and the Law of Armed Conflict* (Asser Press 2014) 213, 217. Compare with Peter Asaro, 'On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making' (2013) 94 Intl Rev of Red Cross 687, 691.

[67] See Markus Wagner, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems' (2014) 47 Vand J Intl L 1371, 1373.

[68] See Wagner (n 67) 1380 ('Moreover, the use of UMS reduces the risks to a military's own troops.').

all enemy combatants within a defined parameter.[69] The device could be programed to forego attacks that violate the principle of proportionality or other operational or legal (or moral) constraints. Advocates for AWS point out that such a system could increase IHL compliance since human beings during infantry deployments are subject to cognitive errors or weakness of the will. Using a robotic infantry device would avoid these difficulties. On the other hand, there is a grave risk that states might rush to deploy an AWS that is *less* capable of complying with IHL, when compared to its human counterparts, simply to avoid risk to its own troops.[70] In this situation, the lowering of risk to the attacking force would be accompanied by an increase of risk to the civilian population based on the possibility of errors committed by the system. Since infantry deployment of AWS is only a future possibility, and not a present reality, this problem should be classified as a hypothetical consequence of the AWS paradigm, and one that naturally flows from the incentives created by the risk reduction for the attacking force.[71]

Taken together, remotely piloted vehicles, cyber and autonomous weapons represent the logical culmination of a process that first began when human beings started using tools as weapons of warfare.[72] The goal

---

[69] See Heather M Roff, 'The Strategic Robot Problem: Lethal Autonomous Weapons in War' (2014) 13 J of Military Ethics 211, 212 ('Assuming that such machines will be able to identify correctly *combatants*, which is certainly questionable, we face an additional set of constraints: identifying legitimate objects/targets and setting military objectives.').

[70] Cf Jack M Beard, 'Law and War in the Virtual Era' (2009) 103 Am J Intl L 409, 423.

[71] I leave aside for the moment whether it is sufficient to generate an argument for banning AWS outright. See Human Rights Watch & Intl Human Rights Clinic, Harvard Law School, *Losing Humanity: The Case Against Killer Robots* (2012) 1–2. For a discussion, see Tyler D Evans, 'At War with the Robots: Autonomous Weapon Systems and the Martens Clause' (2013) 41 Hofstra L Rev 697, 730–31 ('However, HRW's "humanitarian" recommendation to preemptively ban AWS could actually result in a counter-humanitarian outcome: machines may "reduce risks to civilians by making targeting more precise and firing decisions more controlled [ ]especially compared to human-soldier failings that are so often exacerbated by fear, panic, vengeance, or other emotions …"'); Michael N Schmitt, 'Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics' (2013) 2 Harvard National Security J 1, 3 ('*Losing Humanity*'s recommendation to ban the systems is insupportable as a matter of law, policy, and operational good sense').

[72] D'Aspremont reads the current academic debate skeptically and suggests that international lawyers are predisposed to think of cyberspace as a 'problem' or 'gap' that can be resolved by 'intervening' with the tools of international law

of these technological advances consistently has been to increase lethality while reducing risk to operators. The major strategy for achieving this balance is physical distance: when the weapon can travel long distances, the operator can remain far from the target and out of harm's way. What recent technological advances demonstrate, however, is a capacity to lower risk asymmetrically—using methods that transcend mere physical or geographic remoteness. True, drones represent the logical culmination in risk reduction through physical remoteness, but cyber and autonomous weapons have achieved risk reduction in ways that have fundamentally transformed, or even eliminated, the significance of physical distance. In the case of AWS, the operator has not just moved from the front lines, but has been replaced entirely—the strategy of risk reduction taken to its logical conclusion.

4. OPTIMAL OR SUB-OPTIMAL LEVELS OF ASYMMETRIC RISK IN ARMED CONFLICT

Having established that the process of lowering asymmetrical risk through remoteness is a common but now accelerating aspect of modern warfare, our task is now to determine whether this process is normatively undesirable. In the prior section, we considered isolated arguments, within the context of each weapons platform, that lowering asymmetrical risk might have the perverse effect of increasing IHL violations. But now we consider a much larger and more powerful objection: that lowering asymmetrical risk will inevitably result in more jus ad bellum violations.[73] In other words, the advent of risk-free warfare will allow rogue states to launch attacks in violation of jus ad bellum.[74] In the past, what kept states in check—in addition to formal or informal international legal sanctions—was the possibility that states would not want to sacrifice a large percentage of their personnel in order to launch an attack. In a

(either existing frameworks or new rules). See Jean D'Aspremont, 'Cyber Operations and International Law: An Interventionist Legal Thought' (2016) 21 J of Conflict & Security L.

[73] The most sophisticated analysis (and critique) of this objection was offered in Kenneth Anderson, 'Efficiency *in Bello* and *ad Bellum*: Making the Use of Force too Easy?' in C Finkelstein, J D Ohlin and A Altman (eds), *Targeted Killings: Law and Morality in an Asymmetrical World* (Oxford University Press 2012) 374, 389 ('Resort to force is "too easy" if it results in unjust interventions; otherwise not.').

[74] For an example of this argument, see M Shane Riza, *Killing without Heart* (Potomac 2013) 77–80.

sense, the personal costs of war were the greatest check on jus ad bellum violations. With risk-free warfare possible, what is to stop rogue nations from unleashing a continuous stream of jus ad bellum violations?[75]

This objection presupposes that states care about their own citizens. If a despotic tyrant rules a state, the authority to decide whether to resort to force may be concentrated in a particular individual who is indifferent to the suffering his decisions impose on his subjects. Consequently, the reduction of asymmetrical risk would have little impact on the tyrant's calculation regarding the costs of potentially violating jus ad bellum. The same argument might apply even when the state is relatively democratic, as long as membership of the armed forces is not distributed equally across the population. If the decision-making authority is concentrated among political elites who are less likely to serve—or have family members who serve—in the military, they may be insensitive to the costs associated with warfare.[76] Again, in this situation, the reduction in asymmetric risk may have limited impact on the decision-making process of the policy elites. The elites may already be predisposed to the use of force and the risks on the domestic population may not be decisive for their selfish calculus.

For the sake of evaluating the jus ad bellum argument against remote warfare, I will assume that there are a non-trivial number of states where the risk to the military is important to the ruling class, and where the reduction of asymmetrical risk will remove an important barrier to the exercise of force. This rhetorical assumption is important for purposes of evaluating the objection on its own terms. Does it succeed? Does remote warfare risk increasing jus ad bellum violations?

Consider the following hypothetical. Assume for the sake of the argument that State A is deciding whether to launch an invasion against State B. Let us also presuppose that State A is aware that the majority of the world community will criticize the attack as a violation of core principles of jus ad bellum under public international law generally and the UN Charter specifically. Although State A is concerned about the reputational costs associated with a perceived violation of the UN Charter, the officials leading State A are more concerned about a report from their own military generals that the military campaign will result in an initial loss of life estimated between 500 and 2,000 military personnel, during the first two weeks of the military campaign. This news may not

---

[75] See Crootof (n 35) 923–6.

[76] This has led some to suggest that the US should reinstate a universal draft. See Kathleen Frydl, 'Why America Needs the Draft' *The American Interest* (16 January 2014).

necessarily change the decision of State A, but it is enough to give its leaders pause before deciding to proceed. It makes it less likely, ceteris paribus, that State A will decide to go ahead with the invasion. Now, let us change the hypothetical and assume that the military deaths are reduced to near zero because of the remote technologies that will be used during the two-week military campaign. It is not controversial to assume that this decision will make it more likely that State A will launch the military campaign. It is important not to exaggerate the point. This does not mean that this one factor is the sole criterion that will influence the outcome of the decision. Rather, it simply means that, ceteris paribus, State A will be more likely to launch the invasion with the remote technology than they would if they had no access to the remote technology. This provides ample illustration of the oft-heard objection that access to technologies that lower asymmetrical risk will inevitably make it easier for states to go to war in violation of the UN Charter.

In evaluating the legitimacy of this objection to remote weapons, it is important to separate out the two elements of the argument. The first element is the claim that lowering asymmetrical risk will encourage more states to launch more attacks. The second element is the claim that lowering asymmetrical risk will mean more attacks in *violation of the UN Charter*. I concede the first element of the argument but wish to question the second element. Simply put, there is strong reason to think that remote technology will increase the number of attacks, but there is no reason to think—absent other information—that remote technology will increase the number of jus ad bellum violations.[77]

How can we put a wedge between these two different elements of the argument? The answer depends on recognizing the exact opposite scenario: some states forego the use of military force, even in situations when principles of jus ad bellum suggest that they are entitled to launch an attack, simply because the costs of vindicating their jus ad bellum rights are inappropriately high. Consider the following situation: State B is situated close to a belligerent and aggressive neighbor, State C. The government officials in State C are in an expansionist mood and seek control over their neighbor, State B, even though State C has no viable claim under international law to the territory of State B. Consequently, State B is in a position of having to decide whether it will expend military resources in fighting off State C's aggression. Now let us also assume that State C has substantial military assets, and with it, the capacity to undertake an unambiguous injustice against State B.

---

[77] See Anderson (n 73).

In deciding whether to resist, State B will be guided by, inter alia, two considerations. The first is whether it can actually succeed in repelling State C's aggression, that is, whether it has sufficient military strength to push back State C's military advance. The second consideration is the cost that it must bear, in terms of the human lives of its own military personnel, in repelling the aggression (assuming that its defensive effort will succeed). This last consideration is especially relevant in the context of our discussion. One could well imagine State B deciding that so many of its personnel will be killed during the operation that it is not worth fighting back. Consequently, it will forego violence and effectively accede to State C's wishes. The result is that State B puts down its weapons and decides to let its country be annexed by State C.

Assuming that defensive force is permitted against politically motivated military aggression, the result here is troubling.[78] We have constructed the hypothetical in such a way that it is assumed that State B has a jus ad bellum right to defend itself against an unlawful aggression. However, because the costs of exercising that right are too high, State B declines to exercise the right. From the perspective of jus ad bellum, this has to be counted as a poor outcome.

Now imagine, for the moment, that State B has significant remote capabilities as part of its arsenal, and that it can defend itself using technology that reduces asymmetrical risk, thus giving it either strategic parity or even strategic advantage over State C. Now, the disincentive to exercising its jus ad bellum right is removed. State B may now decide that the cost of exercising its inherent right of legitimate defense is bearable. This is only made possible because of the advent of remote technology: drones, cyber weapons or AWS. In this situation, this would be an enhancement to jus ad bellum, not a negative.

How realistic is this hypothetical? Would it ever happen in reality? My own view is that it happens more often than we are comfortable recognizing. In Crimea, the Ukrainian government basically gave up

[78] Not everyone follows this assumption. For example, the philosopher David Rodin has argued that military force is not morally justified when used against political aggression—one country's invasion of a sovereign state in order to rule it rather than destroy it. See David Rodin, 'The Myth of National Self-Defense' in Cécile Fabre and Seth Lazar (eds), *The Morality of Defensive War* (Oxford University Press 2014) 69, 70–75.

control over Crimea, while Russian troops, engaged initially in unacknowledged force, were already on the territory of Crimea.[79] The position of the Ukrainian government, as well as at least some international law scholars, was that Russian attempts to annex Crimea were illegal, and that the Ukrainian government would have been justified under the UN Charter in using military force to protect its sovereign borders, which included Crimea. However, the Ukrainian government did not launch a counter-attack and surrendered the territory to Russia. At least part of the concern was the loss of life to individual Ukrainian soldiers who would have died during the conflict.[80] If the Ukrainian government could have entertained an armed conflict with a lower risk to its own troops, it might have been more willing to exercise its jus ad bellum rights. In this case, lowering asymmetrical risk would have promoted—rather than obstructed—Charter values.

A similar story could be told regarding Nazi aggression in Europe during World War II. It was clear to almost everyone involved that Nazi aggression in Europe was illegal. First, Hitler moved into the Rhineland, despite prior treaty obligations not to do so; his forces then pursued the Anschluss with Austria. After that, Hitler annexed the Sudetenland, which had been under the control of Czechoslovakia. At least one of the reasons Hitler was not stopped earlier was because the human toll of resistance was too high. Sometimes, jus ad bellum principles allow war, rather than condemn it, so any military advantage that promotes the recourse to war could, in these scenarios, actually maximize the principles embedded within jus ad bellum.

Again, a similar story could be told regarding humanitarian intervention, though this point is subtle because arguably unilateral humanitarian intervention violates the UN Charter and its promotion of state sovereignty and territorial integrity. However, many international lawyers support humanitarian intervention in limited cases,[81] even though the weight of today's legal doctrine is against such intervention. There may be cases where humanitarian interventions are not pursued because the risk to military personnel performing the intervention is just too high.

---

[79] David M Herszenhorn, Patrick Reevell and Noah Snieder, 'Russian Forces Take Over One of the Last Ukrainian Bases in Crimea', *The New York Times* (22 March 2014).

[80] For a discussion of the capitulation, see Patrick Reevell and Noah Sneidermarch, 'For Ukraine Military in Crimea, Glum Capitulation and an Uncertain Future' *The New York Times* (22 March 2014).

[81] See Jens David Ohlin, 'The Doctrine of Legitimate Defense' (2015) 91 Intl L Stud 119, 121.

And if remote technology could reduce that risk, the reduction in risk would increase the number of humanitarian interventions. Whether this is a good thing or not depends on the legality of humanitarian intervention.

This is no mere theoretical point. Neither the United States nor the world's other major powers engaged in any significant military intervention in Rwanda during its genocide. This was so despite the fact that many individuals, at the United Nations and elsewhere, were aware of the coming slaughter.[82] Why was nothing done? A military intervention large enough to stop the genocide would have put American lives at risk, and there was little appetite in the United States for more war casualties. The military intervention in Somalia had been particularly difficult for the Clinton Administration, leading to both military disaster and a sense that American troops were being sacrificed for an ill-conceived mission with limited connection to American interests.[83] The Clinton Administration was not interested in replicating this result and consequently failed to intervene in Rwanda. Had there been an opportunity to intervene in Rwanda with lower asymmetrical risk, through drones or AWS, perhaps the United States could have averted the genocide. Of course, these military technologies did not exist then, but the next time a 'Rwanda' occurs, the available military options will include options to lower risk. A similar story can be told with regard to Serbia. Although in that case the United States did intervene, the intervention came late and was hampered by various concerns over risk to US personnel. With more technological options to reduce risk, the United States might have intervened earlier, and more aggressively, against Serbia (or other actors) during the Balkan conflicts.

Expressed abstractly, the point here is simple: remote technologies reduce the costs associated with going to war. However, they reduce the costs associated with *all* wars, both good and bad. And unless one is a pacifist who believes that all wars are bad, then we should be concerned about a situation where we inhibit morally necessary, or legally authorized wars, by over-regulated warfare.[84] The goal of international law should be to reduce war to zero, but in the absence of that utopia, it

---

[82] For a first-hand account, see Roméo Dallaire, *Shake Hands with the Devil: The Failure of Humanity in Rwanda* (Random House Canada 2003) 240.

[83] The specifics of the Somalia intervention are detailed in Mark Bowden, *Black Hawk Down* (Grove Atlantic 1999).

[84] Pacifism is poorly understood as a philosophical doctrine. The best and most recent account of the theory is found in Larry May, *Contingent Pacifism: Revisiting Just War Theory* (Cambridge University Press 2015).

should reduce all illegal wars but not discourage lawful wars—or at the very least an important subset of them.

Is there any reason to think that enforcing a system of reciprocal risk would somehow discourage illegal wars but encourage lawful wars? I see no intuitive reason why this would be the case. It would seem, rather, that tinkering with reciprocal risk is a blunt tool in the regulator's toolbox—it would simultaneously discourage morally odious and morally commendable conflicts. To correctly determine the soundness of this proposal, one ought to tally up the benefits of preventing the odious conflicts and then subtract the harm associated with preventing morally beneficial counter-attacks. Whether this would be an improvement in the status quo would be anyone's guess—this hypothetical calculation is incredibly difficult to envision. From this vantage point, the discouragement of morally and legally appropriate wars ought to count as a serious deficit in the proposal and would be an example of the perverse effects of over-regulating warfare. At the very least, this problem ought to sound a cautionary note into the argument that remote technologies ought to be restricted because they make the resort to armed force too easy.[85] As the preceding analysis has shown, sometimes making the resort to force easier is, all things considered, a better result—depending on whether the conditions for jus ad bellum are satisfied or not.

5. RECIPROCAL RISK AS AN ETHICAL REQUIREMENT FOR CHIVALRIC KILLING

The final objection to remote warfare is that its reduction of asymmetrical risk is fundamentally incompatible with deeper norms of chivalric warfare—norms that are either codified in existing provisions of IHL, embedded ethical norms stemming from the moral requirements for belligerency, or 'professional' norms that attach to soldiers.[86] In the following section, I canvass each of these domains but conclude that the reduction of asymmetrical risk, while intuitively troubling, does not violate norms of chivalric warfare.[87]

---

[85] See Anderson (n 73) 389–90.

[86] Riza (n 74) 88. See also Martin L Cook, 'Drone Warfare and Military Ethics' in David Cortright et al (eds), *Drones and the Future of Armed Conflict: Ethical, Legal, and Strategic Implications* (University of Chicago 2015) 46, 60–61.

[87] The concept of chivalry, as a social institution, dates back to the year 1000. For a discussion, see Georges Duby, *William Marshal: The Flower of*

First, consider the codified requirements of IHL. Although chivalry is clearly a background principle that helps explain the historical development of IHL, few scholars view it as a guiding principle equal in significance to the principles of humanity or necessity. Those principles have a determinate legal status that structure and inform the analysis of particular rules in IHL. The principle of necessity was explicitly codified in Articles 12, 13, and 14 of the Lieber Code, and forms the foundation for the rule that allows privileged combatants to kill enemy combatants. Similarly, the principle of humanity also emanates from the structure and penumbra of existing IHL. Just as the principle of necessity was explicitly referred to in the Lieber Code, so too the principle of humanity was referred to in the Martens Clause, and provides the analytical foundation for the rules that regulate unnecessary suffering of soldiers, the protection of POWs and the prohibition against killing them, and in general the rules that seek to insulate the civilian population, as much as possible, from the horrors of warfare.

Can the same thing be said of the principle of chivalry? Probably not, though it may still be a *background* legal principle in IHL.[88] Soldiers meet each other on the battlefield as equals. Indeed, this is the foundation for the moral equality of combatants—the rule that extends immunity to all privileged combatants for their acts of battlefield killing, regardless of whether they are parties to the 'right' or 'wrong' side of the conflict as far as jus ad bellum is concerned. If this is what is meant by the principle of chivalry, then yes, combatants meet each other as equals on the battlefield. But if 'chivalric warfare' means an equality of arms, a

---

Chivalry (Pantheon 1987); Antonio Santosuosso, *Barbarians, Marauders, and Infidels: The Ways of Medieval Warfare* (Westview 2004) 172.

[88] For example, see Terry Gill, 'Chivalry: A Principle of the Law of Armed Conflict?' in Marcel Brus and Brigit Toebes (eds), *Armed Conflict and International Law: In search of the Human Face: Liber Amicorum in memory of Avril McDonald* (Asser Press 2013). Gill argues that chivalry retains its significance for contemporary IHL and provides the foundation for many particular rules codified in existing treaties. However, Gill does not identify killing at a distance as a violation of chivalry: '(Long range) missile warfare, whether by means of ballista, long or crossbow, musket, artillery, machinegun or sniper rifle (or for that matter helicopter gunships or missile armed unmanned aerial vehicles or "drones"), has been part of warfare for centuries and is the "great leveler", making no distinction between rank, class, skill or bravery of the recipients … In short, chivalry and martial honour have never precluded maximizing one's advantages and neutralizing those of the opponent …' Ibid 47.

personal connection between killer and killed,[89] or a symmetrical assumption of risk, there is simply no way to logically deduce this more extensive notion of chivalry from the moral equality of combatants.

It is true, however, that chivalry may help explain other rules in international law that remain viable, notably the extensive protections that IHL extends to civilian populations.[90] Some of these requirements may owe their existence to requirements of chivalry.[91] For example, the law requires combatants not to engage in attacks that will cause disproportionate collateral damage—a requirement that places soldiers in some degree of risk at the expense of protecting the civilian population. In some cases, soldiers may even be under an obligation to take all feasible measures to reduce civilian casualties as far as possible—again a requirement that imposes demands on soldiers that may cause them harm. Similarly, in IHL, a soldier may not assert duress or necessity as an excuse to the war crime of killing innocent civilians. Traditionally, these rules are justified by reference to the inherent dignity or moral worth of civilians. But for each of these rules, the law's prioritization of the civilian (even an enemy one) over the soldier could be seen as a partial outgrowth of the principle of chivalry; it is dishonorable for a soldier to put himself or herself above the civilian, and sacrifices may be required. Again, though, there is nothing in this notion of chivalry that requires soldiers to bear additional risk simply because lowering asymmetrical risk is *inherently* dishonorable.[92]

Second, we should consider whether established norms of warfare, stemming either from moral philosophy or professional standards,[93]

---

[89] See O'Connell (n 23) 271; see also David Grossman, *On Killing: The Psychological Cost of Learning to Kill in War and Society* (Back Bay 1996) 187; Jennifer M Welsh, 'The Morality of "Drone Warfare"' in Cortright et al (n 86) 24, 43–4 (concluding that drone pilots are simultaneously far removed and 'quite close' to their targets at the same time).

[90] Gill (n 88) 47.

[91] See Thomas Wingfield, 'Chivalry in the Use of Force' (2001) 32 U Tol L Rev 111, 136 ('This quest for honor—the desire to fight with swords, both literally and metaphorically—counterbalances the dark side of armed conflict, the base desire to destroy, simply because one can. In this struggle, the law of chivalry is an elegant weapon, for a more civilized age.').

[92] Another example is the prohibition against perfidy. See Walter G Sharp, 'The Effective Deterrence of Environmental Damage During Armed Conflict: A Case Analysis of the Persian Gulf War' (1992) 137 Mil L Rev 1, 31.

[93] Some have argued that the principle of necessity could be constrained by interpreting it through the lens of professional standards and discipline. See Yishai Beer, 'Humanity Considerations Cannot Reduce War's Hazards Alone:

require reciprocal risk. This argument implies that killing from a distance while remaining out of danger is cowardly and that 'real men' put themselves in harm's way when they engage in lethal attacks during combat.[94] For example, after the 9/11 attacks, author and cultural critic Susan Sontag offered the following observations in *The New Yorker*:

> Where is the acknowledgment that this was not a 'cowardly' attack on 'civilization' or 'liberty' or 'humanity' or 'the free world' but an attack on the world's self-proclaimed superpower, undertaken as a consequence of specific American alliances and actions? How many citizens are aware of the ongoing American bombing of Iraq? And if the word 'cowardly' is to be used, it might be more aptly applied to those who kill from beyond the range of retaliation, high in the sky, than to those willing to die themselves in order to kill others. In the matter of courage (a morally neutral virtue): whatever may be said of the perpetrators of Tuesday's slaughter, they were not cowards.[95]

Although Sontag did not come out and say explicitly that American pilots are cowards, she did say that they are more appropriately considered cowards than are suicide bombers. Why? The relevant difference between the two is that the suicide bomber not only risks his life but in fact *sacrifices* it, while the pilot risks little or nothing. And Sontag said this before the great proliferation of drone strikes. With those technological advancements, Sontag might have been even more categorical in her condemnation of the 'cowardly' actions of drone pilots, who basically risk nothing of their own personal safety.

Sontag's tone-deaf assessment was met with predictable outrage. Coming on the heels of the worst terrorist attack on American soil, it is no surprise that the public had little interest in her apparent lionization of suicide bombers and her criticism of American military personnel. However, the public reaction is neither here nor there. The more important question is whether Sontag was on to something or not from the perspective of moral or political theory. And in this regard, it does

---

Revitalizing the Concept of Military Necessity' (2015) 26 Eur J Intl L 801, 805 ('Constraining the brute force of a military is in its own self-interest and enhances its operational effectiveness.'). This example is an attempt to make professional standards morally and legally relevant. The question is whether that methodology is generalizable to other contexts.

[94] For a contrasting view, see Drone Pilot, 'It is War at a Very Intimate Level' in Peter L Bergen et al (eds), *Drone Wars: Transforming Conflict, Law, and Policy* (Cambridge University Press 2015) 113, 116 ('Just because you are separated by technology does not mean you are separated emotionally.').

[95] Susan Sontag, 'Tuesday, and After' *The New Yorker* (New York, 24 September 2001).

seem odd to suggest that there is a 'morally neutral virtue' that would require personal risk in the fighting of war. The most that can be said in favor of the position is that: fighting in a war while risking one's life is particularly courageous, but failure to do so should not be considered a moral deficit. In other words, courage is supererogatory; its presence should be celebrated but its absence is no reason to condemn an action as immoral or illegal. Indeed, there are many situations, such as duress, where we celebrate those who demonstrate moral heroism but refuse to condemn those who fail to live up to that unreasonably high standard. The second insight one might draw from Sontag's exposition is that the United States is quick (perhaps too quick) to act as the world's 'self-proclaimed superpower' simply because it can project military force without risk—an argument that we already considered above and mostly rejected.

Finally, consider reciprocal risk from the perspective of professional standards of conduct that reign among soldiers. When the technology of guns advanced enough, in both range and precision, to allow for a practice that could fairly be called sniping, it immediately drew attention as a questionable practice.[96] Over time, the unease remained because some soldiers consider it a 'dirty practice' or 'cold-blooded'.[97] But for others, snipers are virtuous because they are more capable of respecting the principle of discrimination.[98]

The use of snipers was specifically designed to be a force equalizer—to counter the enemy's strategic advances in other domains.[99] Also, the use of the sniper was intimately wrapped up with a new

---

[96] See Michael E Haskew, *The Sniper at War: From the American Revolutionary War to the Present Day* (Macmillan 2005) 8; Andy Dougan, *The Hunting of Man: A History of the Sniper* (Fourth Estate 2004).

[97] See Joanna Bourke, *An Intimate History of Killing: Face-to-face Killing in Twentieth-century* (Basic 2000) 54. See also Robert Graves, *Good-Bye to All That* (1957) 132 ('While sniping from a knoll in the support line, where we had a concealed loop-hole, I saw a German, about seven hundred yards away, through my telescopic sights. He was taking a bath in the German third line. I disliked the idea of shooting a naked man, so I handed the rifle to the sergeant with me. "Here, take this. You're a better shot than I am." He got him; but I had not stayed to watch.'), quoted in Michael Walzer, *Just and Unjust Wars* (Basic Books 2000) 140.

[98] Dougan (n 3) 295 ('The sniper is the smartest of "smart" weapons. Through the fog of war he is able to distinguish friend from foe, target from survivor, in confused surroundings.').

[99] For example, the British used snipers to counter Napoleon's army. See Brandon Webb, *The 21st Century Sniper: A Complete Practical Guide* (Skyhorse

development that saw a change in practice regarding who was targetable in warfare. In the past, officers and other military personnel who held support positions were usually not targeted in battle; the advent of sniping coincided with a breakdown of that cultural norm, leading some to suggest that snipers had 'foresworn the chivalrous code of battle from the old days'.[100] For example, during the US military engagement in Somalia, a young woman was killed by an American sniper, which provoked a public outcry. One soldier, responding to the event, wrote:

> Although I am a proponent of the employment of snipers, I believe that most people feel there is something unclean—unsporting or not chivalrous—about their use. Some see sniping as a dishonorable method of prosecuting war and expect more from our military. The alleged killing of the young Somali woman only reinforced the skeptics' view and illustrated how a misplaced round can instantly result in human tragedy.[101]

However, what was problematic about that event was uncertainty over the status of the target, not the manner in which the target was defeated. If there is a chivalric code of warfare that requires reciprocal risk, and prohibits killing at a distance, it is an element of the chivalric code that has long since been abandoned,[102] a development that was already well underway by the time of the US Civil War.[103] Sniping was rampant

---

2010) 11. See also Dougan (n 3) 9 (discussing snipers used during the siege of Lichfield in 1643).

[100] Webb (n 99) 11. See also Blum (n 10) 75 (noting that crossbows allowed commoners to strike knights from a distance—an earlier example of a similar problem).

[101] Lawrence E Casper, *Falcon Brigade: Combat and Command in Somalia and Haiti* (Lynne Rienner 2001) 134.

[102] See Allen J Frantzen, *Bloody Good: Chivalry, Sacrifice, and the Great War* (University of Chicago Press 2004) 1–3 (arguing that chivalry continued as an important concept during World War I, despite the popular assumption that when 'young men filled with illusions of chivalry were ordered to walk into machine-gun fire, an ancient brotherhood fell before the weapons of a new age').

[103] See Adrian Gilbert, *Stalk and Kill: The Sniper Experience* (St Martin's Press 1997) 27 (describing the American Civil War as a 'golden age for the military rifle' but noting that 'this simple yet profound transformation in the conduct of war was not realized at the time, and massed columns of brightly uniformed soldiers were regularly slaughtered by devastating fire from a single line of riflemen'); Matthew J Grow, *'Liberty to the Downtrodden': Thomas L. Kane, Romantic Reformer* (Yale 2009) 223 (noting that Thomas Kane believed that it was fundamentally dishonorable for General Ashby to have been felled by a sniper's bullet). Grow writes that 'The Incident not only demonstrates how chivalry defined appropriate action in combat for Kane, but also how the chaos

during World War I.[104] If the chivalric code defined honorable killing as personal, that was the chivalric code of a prior era.[105]

6. CONCLUSION

Reduction of asymmetrical risk is, in many ways, the goal of strategic warfare.[106] The preceding analysis has demonstrated a historical continuity in every army's attempt to project military power but remain at arm's length from the enemy's strategic capabilities. Drones, cyber weapons and autonomous weapons are just the latest instantiation of an ancient imperative of strategic warfare. The goal of combat is to exploit the gap between one's own zone of lethality and the enemy's—projecting power while reducing or eliminating risk. Indeed, military experts recently warned the US government that China's development of a new missile would allow the Chinese military to strike an American base in Guam that was previously beyond the range of Chinese missiles—negating the point of locating the base in Guam.[107] The desire to reduce asymmetrical risk is ever-present both in new technological platforms but also in more conventional assets, such as ballistic missiles.

Reduction of asymmetrical risk has consequences, though the preceding analysis has demonstrated that, contrary to received intuitions, none of these consequences run afoul of either jus in bello or jus ad bellum considerations. While risk-free weapon platforms might raise the risk of more armed conflict, this fact applies equally to good and bad wars, thus

---

of battle and the bitterness of the war rendered such concern for chivalry increasingly antiquated and impractical for most soldiers as the war wore on.' Ibid.

[104] Gilbert (n 103) 53. See also Adrian Gilbert, *Sniper: The Skills, the Weapons, and the Experiences* (St Martin's Press 1994) 37–68.

[105] See Matthew Strickland, *War and Chivalry: The Conduct and Perception of War in England and Normandy, 1066–1217* (Cambridge University Press 1996) 17, 30 (discussing the chivalric code among captured knights which broke down with regard to the treatment of external enemies who were slaughtered upon capture); John Gillingham, '1066 and the Introduction of Chivalry into England' in George Garnett and John Hudson (eds), *Law and Government in Medieval England and Normandy* (Cambridge University Press 1994) 31, 32–3.

[106] Gill (n 88) 47.

[107] See Brad Lendon, 'U.S. must beware China's "Guam killer" missile', CNN.com (15 May 2016) ('Guam, home to Andersen Air Force Base and Apra Naval Base, has been as a place from where the U.S. could project power across the Pacific while having its forces at relatively safe distance from possible threats, including North Korea and China.')

leading to the inescapable conclusion that in some circumstances, remote technology has salutary benefits. As for jus in bello, reduction of risk is only problematic if it comes with an increase in risk to the civilian population that is greater than what the law allows. If, however, the level of risk to civilians complies with the law, the lowering of risk to friendly troops is not, itself, a legal vice.