
Enforced Equations

Dino Kritsiotis*

Abstract

This contribution to the symposium on Michael Walzer's Just and Unjust Wars: A Moral Argument with Historical Illustrations (1977) engages with Jack Goldsmith's assessment of cyber warfare in the context of both the jus ad bellum and the jus in bello. In so doing, its purpose is to register the intended significance of the moral argument contained in Walzer's text from the meaning of 'war' that emerges from its pages; however, international law has long since abandoned this concept as the operational premise for the regulations offered by way of the jus ad bellum and the jus in bello, and Just and Unjust Wars is opened up to a much more rigorous reading of its contents – including the Afterword on 'Nonviolence and the Theory of War' as well as a fuller inventory of the precedents actually used by Walzer in original and subsequent editions – that argue for a significance of the lessons of this work altogether more encompassing and enduring than may greet the reader on initial contact.

Michael Walzer's trade in *Just and Unjust Wars* is past precedent: whether comparing Operation Iraqi Freedom with the occupation of Germany after World War II,¹ or assessing how 'genuine democracies' have treated their respective peoples through time,² or addressing the deadliness of Hiroshima,³ his entire thesis is proclaimed on the back of human experience after blood-soaked human experience.⁴ As the subtitle of this volume makes admirably clear, this is after all a work of moral argument with *historical* illustrations, which draws not on 'thinking about war in general, but about particular wars, above all about the American intervention in Vietnam'.⁵ The general is thus forged from the morsels and solemn lessons of each particular in setting out its programme of 'practical morality',⁶ and from the first moments of connecting with

* Professor of Public International Law, University of Nottingham. Email: dino.kritsiotis@nottingham.ac.uk.

¹ M. Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (4th edn, 2006), p. ix. All subsequent references are to the 4th edn of this work.

² *Ibid.*, at xi ('even if their record abroad is less than satisfactory').

³ *Ibid.*, at 269.

⁴ *Ibid.*, at xx.

⁵ *Ibid.*, at xix.

⁶ *Ibid.*, at xxiii; also at xxiv.

this modern classic, it is apparent how much each of these precedents has been carefully chosen and constructed out of a certain appreciation of the concept of ‘war’: the preface to the fourth edition is littered with references to ‘wars declared’⁷ and to ‘resistance to [armed] aggression’⁸, to ‘military attack’,⁹ ‘intervention’,¹⁰ ‘military action’,¹¹ and ‘military defeat’,¹² as well as to ‘forcible democratization’,¹³ ‘forcible transformation’,¹⁴ and ‘the coercive imposition of foreign ideas and ideologies’¹⁵ – but, invariably, also to ‘acts of war’.¹⁶ If one harbours any uncertainties as to the scope of the study from its title, then those soon vaporize as an implicit consensus is reached with the reader as to the organizing intellectual interest and imperative of this work.¹⁷

Two further sets of observations work towards the reinforcement of this appreciation, but also become the occasion for questioning the scope of the premise that underpins *Just and Unjust Wars*: one comes in the preface to the fourth edition after the elaboration of the containment system adopted against Iraq following the eviction of its armed forces in February 1991 from their occupation of Kuwait. Walzer describes the arms embargo, the system of weapons inspection, and the establishment of no-fly zones in Iraq north of its 36th parallel and south of its 32nd parallel, as ‘measures short of war’,¹⁸ and, then, as ‘force-short-of-war’.¹⁹ Common sense dictates, or so he writes, that these responses are all ‘very different from actual warfare’,²⁰ from which they must thus be kept analytically separate, but they also inspire his claim that ‘[t]he argument about *jus ad bellum* needs to be extended ... to *jus ad vim*’ – as ‘[w]e urgently need a theory of just and unjust *uses of force*’.²¹ The second set of observations arises

⁷ *Ibid.*, at x.

⁸ *Ibid.*

⁹ *Ibid.*

¹⁰ *Ibid.*, at x and xi.

¹¹ *Ibid.*, at x.

¹² *Ibid.*

¹³ *Ibid.*, at ix; also at xvii.

¹⁴ *Ibid.*, at x.

¹⁵ *Ibid.*, at xi.

¹⁶ *Ibid.*, at xii.

¹⁷ The preface to the most recent (i.e., fourth) edition is much more pronounced in this respect than the preface to the original edition, although the latter did provide that ‘[w]hen we talked about aggression and neutrality, the rights of prisoners of war and civilians, atrocities and war crimes, we were drawing upon the work of many generations of men and women, most of whom we had never heard of’: *ibid.*, at xix. And, at xxii, ‘[t]hroughout the book, I treat words like aggression, neutrality, surrender, civilian, reprisal, and so on, as if they were terms in a moral vocabulary – which they are, and always have been’.

¹⁸ Walzer, *supra* note 1, at xiv. The latter no-fly zone was extended to the 33rd parallel in Sept. 1996: MacIntyre, ‘France refuses to patrol widened Iraq No-fly zone: split allies’, *The Times*, 6 Sept. 1996, at 15.

¹⁹ *Ibid.*, at xv (for, ‘[i]n fact, they all involved the use (or, in the case of inspections, the threat) of force’: *ibid.*, at xiv). Also at xvi and xvii. And, at xvii, ‘the use of force-short-of-war’.

²⁰ *Ibid.*, at xv.

²¹ *Ibid.* (emphasis added; which, he maintains, ‘shouldn’t be an overtly tolerant or permissive theory, but it will certainly be more permissive than the theory of just and unjust war’). Of course, international law effected precisely such a change almost seven decades or so ago now when it shifted from the concept of war to the concept of force in Art. 2(4) of the UN Charter, but it seems rather pointless to recall this fact in view of Walzer’s position – set out in the preface to the original edition – that ‘[t]o dwell at length upon the precise meaning of the Charter is today a kind of utopian quibbling’: *ibid.*, at xx. See, also, Brierly, ‘International Law and Resort to Armed Force’, 4 *Cambridge LJ* (1932) 308. Perhaps one is best left to

from the afterword that appeared in the original edition of *Just and Unjust Wars*, entitled 'Nonviolence and the Theory of War',²² concerning the possibilities for 'war without weapons',²³ or war without fighting and killing: non-violence is defined by what it is (e.g., disobedience, non-cooperation, boycott, and general strike),²⁴ but also by what it is not – and it is *not* or does not involve 'military advance',²⁵ 'military occupation',²⁶ 'aggressive war',²⁷ military intervention,²⁸ the taking up of arms,²⁹ invading armies,³⁰ or 'armed insurrection'.³¹ These are all intended as evocative examples of the sort of 'historical cases'³² that matter to us or should matter to us in mapping out the parameters of this field of knowledge, thought, and enquiry – but they are also palpable testaments to the fluidities and flexibilities of disciplinary boundaries, whether we are working in the realm of moral philosophy or positive international law.

* * *

The advent of the digital revolution and associated 'vulnerabilities' is what engages the concern of Jack Goldsmith in his very useful contribution to this symposium, 'How Cyber Changes the Laws of War',³³ which marks out separate possibilities for human and state action in this emerging sphere of activity: cyber attacks ('an act that alters, degrades, or destroys adversary computer systems or the information in or transiting through those systems')³⁴ and cyber exploitations ('merely monitoring and related espionage on computer systems')³⁵ both carry the whiff of warmaking about them and come with their own unraveling line of precedents: that catalogue now includes the actions taken against Estonia (2007), Georgia (2008) and Iran (2010). New forms of power and new forms of asserting power have come to exploit these vulnerabilities

remark upon the ironical turn occasioned by the first and most recent prefaces of *Just and Unjust Wars*, the former of which declared that 'this is not a book about the positive laws of war' (*ibid.*, at xx), and the latter of which does seem to seek some sort of emulation with the positive law itself.

²² Walzer, *supra* note 1, at 329–335.

²³ *Ibid.*, at 329. Also at 331 and 334.

²⁴ *Ibid.*, at 330 (methods by which 'the citizens of the invaded country transform the aggressive war into a political struggle').

²⁵ *Ibid.*

²⁶ *Ibid.*

²⁷ *Ibid.*

²⁸ *Ibid.*, at 331.

²⁹ *Ibid.* (or, at 332, 'armed resistance').

³⁰ *Ibid.*, at 331, 332, and 333.

³¹ *Ibid.*, at 334. Although the issue of suicide is raised at one point – *à propos* Mohandas Gandhi's advice to the Jews of Germany to commit suicide rather than take up arms against Nazi tyranny – where Walzer concludes that '[h]ere nonviolence, under extreme conditions, collapses into violence directed at oneself rather than at one's murderers': *ibid.*, at 332.

³² *Ibid.*, at xxiv. Hence Walzer's emphasis on 'actual judgments and justifications', although he does remark at one point that '[r]eaders upset by my failures [of abridgement] might usefully treat the cases as if they were hypothetical – invented rather than researched – though it is important to my own sense of enterprise that I am reporting on experiences that men and women have really had and on arguments that they have really made': *ibid.*, at xxiv.

³³ Goldsmith, this volume, at 129.

³⁴ *Ibid.*, at 130.

³⁵ *Ibid.*, at 130.

– or, as it is put elsewhere in the article, ‘[t]he inherent insecurity of computer systems’.³⁶ Does international law fall readily silent on such occasions?

One approach is to treat any or all of these occurrences within the existing infrastructure provided by international law in the form of the *jus ad bellum* and the *jus in bello*, which Walzer deals with under the rubrics of ‘the theory of aggression’ and ‘the war convention’³⁷ respectively.³⁸ This requires us to probe the actual scope of concepts such as the ‘use of force’ and ‘armed attack’ (for the *jus ad bellum* of the Charter of the United Nations) and ‘armed conflict’ (for the *jus in bello* of the Geneva Conventions and Additional Protocols), a comparison that might create the impression that there are greater possibilities for accommodating these developments under the law of the Charter: for one thing, there is no explicit statement in Article 2(4) of the Charter that this force be *armed* as there is with the taxonomy of conflicts set out in the Geneva Conventions,³⁹ and there are three other occasions when the Charter does in fact enter the qualification that the force be *armed* (its preamble provides that ‘armed force shall not be used’; Article 41 concerns ‘measures not involving the use of armed force’, and, finally, Article 46 regulates the relationship between the Security Council and the Military Staff Committee in respect of ‘the application of armed force’).⁴⁰ Sheer inference, then, suggests the adaptabilities of the Charter’s prohibition of force, but this reasoning comes up against the general and immediate background of the Charter’s regulation of force that really leaves no room for doubt regarding the purity of the proposition then at stake – and it is not one that set out to encompass either political or economic forms of force.⁴¹

The great value of the assessment under review is that it brings more fully to life the *qualitative* differences of cyber warfare when compared with political or economic force: ‘the cyber context’, Goldsmith writes at one point, ‘changes the scale and consequences of theft and espionage to a degree that can result in harm to the country at least as severe as a physical attack’.⁴² The possibilities of scale – but also of the instantaneousness, the immediacy of consequence – of a cyber attack makes us think anew about the appropriateness of any normative likeness to acts of armed force,⁴³ and of

³⁶ *Ibid.*, at 131.

³⁷ For a detailed depiction of ‘the war convention’ see Walzer, *supra* note 1, at 44–47 (which is to be kept keenly separate from positive international law: *ibid.*, at 199). Walzer later levels the charge that aspects of the positive canon known as the laws of war ‘are radically incomplete’: *ibid.*, at 288. See also *supra* note 21.

³⁸ Appearing as Parts II and III of *Just and Unjust Wars*, and reinforced by Walzer’s comparative treatment of belligerent and ‘peacetime’ reprisals: *supra* note 1, at 216.

³⁹ And, of course, the First Additional Protocol – although, curiously, Goldsmith persists in using the anachronistic formulation of the ‘level of war’: *supra* note 33, at 131, 132, 133 and 138.

⁴⁰ These are separate invocations to the armed forces of member states or those placed at the disposal of the SC – mentioned in Arts 43(1), 44, and 47(3) of the Charter.

⁴¹ A point with which Goldsmith accords, and which, he suggests, holds good to this day: *supra* note 33, at 134. Consider, too, Farer, ‘Political and Economic Coercion in Contemporary International Law’, 79 *AJIL* (1985) 405, at 410.

⁴² *Supra* note 33, at 133. And described, with potent effect, in Hersch, ‘The Online Threat’, *New Yorker*, 1 Nov. 2010, at 48.

⁴³ Anew because D.W. Bowett had contemplated this possibility in his seminal work *Self-Defence in International Law* (1958), at 113: ‘the rôle of self-defence will not, except in the most exceptional circumstances, be to sanction the use of force’. Note, however, that ‘a country as fiercely controlled as Iraq could

bringing this aspect of human relations within the Charter's governance of force. The argument for making this equation is sharpened by contrasting a hypothetical cyber attack 'that renders the electricity grid or air traffic control system inoperable, and that results in many deaths' with one 'that merely involves espionage' with 'a slow disruptive cyber attack on critical infrastructure' and '[the] "mere" destruction of critical economic or military data'.⁴⁴ At the very least, the first of these rather potent examples seems to me to be of a very different order from instances of political force (e.g., transnational propaganda or to the projection of words across borders) – but even to 'detailed instructions for organizing an uprising' in another country,⁴⁵ and, quite possibly, to extreme instances of economic force.⁴⁶

That said, we should recall that the Charter itself does envisage the possibilities for what it calls 'demonstrations' and 'blockade[s]' in Article 42 – but these are notably *not* part of the measures envisaged 'not involving the use of armed force' designated under Article 41 of the Charter.⁴⁷ To be clear, the importance of these juridical classifications cannot be overstated, for whatever classifies as 'force' for the purposes of Article 2(4) of the Charter may yield a response *in kind* from the aggrieved state – but it could also conceivably open the door to a possible 'military response'⁴⁸ as part of the Charter's framework for prohibited as well as *permissible* force. An alternative interpretation is to keep the *modalities* of force rigorously apart from one other – so that political, economic, and armed instruments of action and response are never mixed in practice – but where the language of the Charter is used for making the legal justification and assessment of a given action and the

have lasted years under sanctions without being forced to withdraw from Kuwait': J. Simpson, *From the House of War* (1991), at 380 – an observation made after the SC's adoption of comprehensive economic sanctions against Iraq on 6 Aug. 1990 (Res. 661) and of the subsequent naval interdiction it imposed on Iraq on 25 Aug. 1990 (Res. 665).

⁴⁴ All examples from Goldsmith, *supra* note 33, at 134 (where the former hypothetical 'would count as a use of force'). Consider the impressive recounting of the joint cyber programme of the United States and Israel ('Olympic Games') developed against the nuclear capabilities of Iran in D.E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (2012), at 188–225.

⁴⁵ The hypothetical examples of Farer in his discussion of political aggression: Farer, *supra* note 41, at 407.

⁴⁶ Such as the liquidation of a state, or an action designed to 'reduce that state to the position of a satellite' – further examples provided by Farer, *supra* note 41, at 413. Goldsmith reminds us that the latter (the 'wreaking of economic havoc') can be actualized through cyber attack: Goldsmith, *supra* note 33, at 132. He also mentions the possibilities of 'widespread economic harm': *ibid.*, at 133.

⁴⁷ *Viz* the complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations. Used in this context, 'demonstrations' have been understood to refer to 'demonstrations of strength intended to discourage a potential peace-breaker from the use of armed force or its resumption, or to induce a change in its behaviour' – whereas blockades '[do] not assume a technical law-of-war sense, but rather points to military action with a view to sealing off particular coasts or land areas'. See Frowein and Krisch, 'Article 42', in B. Simma (ed.), *The Charter of the United Nations: A Commentary* (2nd edn, 2002), i, at 749, 755. Both of these formulations appear to implicate to greater or lesser degrees that other aspect of the Charter prohibition of force pertaining to the *threat* of force – but this does not have much hold on Goldsmith's position here, which appears to have been guided by the existence of a singular 'critical threshold' within Charter law: Goldsmith, *supra* note 33, at 134. See, further, the discussion accompanying notes 18 to 21 *supra*.

⁴⁸ Farer, *supra* note 41, at 408.

response it elicits.⁴⁹ State practice has thus far issued something of a split verdict on this matter: note how Syria recently considered the broad economic sanctions levelled against it by the League of Arab States as a declaration of ‘economic war’,⁵⁰ but only threatened kindred acts by way of response,⁵¹ whereas Israel invoked its right of self-defence against terrorist attacks as its justification for building the structure at the heart of *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (2004).⁵² More to the point for present purposes, the Pentagon has been prepared to consider cyber attacks as ‘acts of war’ – which, in its view, ‘may result in a military response’⁵³ – and, in October 2012, the US Defense Secretary Leon E. Panetta advised of the very real possibilities of ‘a cyber Pearl Harbor’ – a precedent once again rallied to frame the challenge or proposition before us – or of ‘an attack that would cause physical destruction and the loss of life’ which ‘would paralyze and shock the nation and create a new, profound sense of vulnerability.’⁵⁴ ‘Potential aggressors,’ he then warned, ‘should be aware that the

⁴⁹ This appears to be the thrust of Bowett’s position when he writes:

‘a State may justify unilateral economic measures which might otherwise be illegal if it can show that these measures are taken in self-defence. Of course, the essentials of self-defence must be proved. The State would have to show that it was reacting to a delict by another State, posing an immediate danger to its security or independence in a situation affording no alternative means of protection and, lastly, that the reaction was proportionate to the harm threatened’.

See Bowett, ‘Economic Coercion and Reprisals by States’, 13 *Virginia J Int’l L* (1972) 1, at 7. The choice of the word ‘delict’ is important here because it does not confine the right of self-defence to occurrences of ‘force’, let alone to those amounting to an ‘armed attack’. Bowett’s evidence for this claim, on offer at *ibid.* at 7–8, does not inspire confidence as these are not likely robust representations of the *opinio juris sive necessitatis* of East Germany, Spain, Indonesia, and Cuba regarding their respective rights of self-defence.

⁵⁰ MacFarquhar, ‘Syria calls the Arab League’s sanctions “economic war”’, *NY Times*, 29 Nov. 2011, at A6.

⁵¹ ‘As Effective as Bullets, Maybe’, *The Economist*, 3 Dec. 2011, at 41. Walid al-Moallem, the foreign minister of Syria, emphasized Syria’s geographic location as a ‘transit point for commercial traffic’, and mentioned Syrian air space and its road connections of Turkey and Europe; there was no suggestion of an armed response.

⁵² [2004] ICJ Rep 136, at 194, para. 138. Israel considered the structure to be ‘one of the most effective non-violent methods for preventing terrorism in the heart of civilian areas’, and Dan Gillerman, Israel’s Permanent Representative to the United Nations, informed an emergency special session of the GA that ‘[i]nternational law and Security Council resolutions, including resolutions 1368 (2001) and 1373 (2001), have clearly recognized the right of States to use force in self-defence against terrorist attacks, and therefore surely recognize the right to use non-forcible means to that end’: see UN Doc. A/ES-10/PV. 21 (20 Oct. 2003) (emphasis added). In her separate opinion to the advisory opinion, Judge Rosalyn Higgins remained ‘unconvinced that non-forcible measures (such as the building of a wall) fall within self-defence under Article 51 of the Charter as that provision is normally understood’: at 215–216, para. 35.

⁵³ Sanger and Bumiller, ‘Pentagon to consider cyberattacks acts of war’, *NY Times*, 1 June 2011, at A10. See, further, Osborne, ‘Pentagon warns that cyber-attacks will be seen as “acts of war”’, *Independent*, 2 June 2011, at 23.

⁵⁴ US Dept. of Defense, Office of the Assistant Secretary of Defense (Public Affairs), News Transcript: Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, available at: www.defense.gov/transcripts/transcript.aspx?transcriptid=5136 (11 Oct. 2012) (also: ‘[a] cyber attack perpetrated by nation states and violent extremist groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation’). See, further, Bumiller and Shanker, ‘Panetta warns of the dire threat of cyberattack on US’, *NY Times*, 12 Oct. 2012, at A1 and Lieberman and Collins, ‘The gathering cyberstorm’, *Int’l H. Trib.*, 8–9 Dec. 2012, at 6.

United States has the capacity to locate them and to hold them accountable for their actions that may try to harm America.⁵⁵

* * *

Walzer dissects the ‘initiation’ of force from how hostilities are conducted between states,⁵⁶ and it is this that occasions the shift from the law of the Charter to that presented in the Geneva Conventions (as well as the First Additional Protocol).⁵⁷ In *Just and Unjust Wars*, he betrays a general sense of when the rules of warfare might actually become applicable. This is his celebrated ‘war convention’ of moral persuasion,⁵⁸ and epithets such as ‘fighting’⁵⁹ and ‘firefight’,⁶⁰ ‘slaughter’⁶¹ and ‘mass destruction’,⁶² ‘combat’,⁶³ ‘kill’,⁶⁴ and ‘killing’⁶⁵ adorn much of the analysis. As Walzer himself admits at one point, his approach very much assumes ‘a conventional firefight’,⁶⁶ and it is this proposition that instructs numerous claims made throughout the work: ‘[t]he moral equality of the battlefield distinguishes combat from domestic crime’.⁶⁷

Yet, to develop the point made at the outset of this response, a more exacting engagement with the precise terms of *Just and Unjust Wars* makes clear that belligerent action can be manifested in very different ways, at one and the same time that we are taught to rethink the battlefield as the exclusive *locus* for hostile exchange: reference is made to ‘encompassable battles’ as but one example of warfare,⁶⁸ while Walzer also discusses sieges and blockades (‘[c]ollective starvation is a bitter fate: parents and children, friends and lovers must watch one another die, and the dying is terribly drawn out, physically and morally destructive long before it is over’)⁶⁹ and the rape of women

⁵⁵ *Ibid.* Within the same speech, Secretary Panetta referred to the relevance of the principles of the *jus ad bellum* as well as those of the *jus in bello* for any response of the United States: ‘[i]f we detect any imminent threat of attack that will cause significant, physical destruction in the United States or kill American citizens, we need to have the option to take action against those who would attack us to defend this nation when directed by the president’; ‘we will only [conduct effective operations to counter threats to our national interests in cyberspace] to defend our nation, to defend our interests, to defend our allies’ – and this would be done ‘in a manner that is consistent with the policy principles and legal frameworks that the [D]epartment [of Defense] follows for other domains including the law of armed conflict.’

⁵⁶ Walzer, *supra* note 1, at 127. Indeed, ‘the conduct of hostilities’ is referred to at one point – at 127 – on the first page introducing that part of the work devoted to ‘the war convention’.

⁵⁷ The extent of the coincidence between the concepts of ‘force’ (of the UN Charter) and of ‘all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties’ (of the Geneva Conventions and First Additional Protocol) remains a matter of some contention, which I have attempted to explore in ‘The Tremors of *Tadic*’, 43 *Israel L. Rev.* (2010) 262, at 278–279.

⁵⁸ *Supra* notes 37 and 56.

⁵⁹ Walzer, *supra* note 1, at 127.

⁶⁰ *Ibid.*, at 217.

⁶¹ *Ibid.*, at 109.

⁶² *Ibid.*, at 272.

⁶³ *Ibid.*, at 2.

⁶⁴ *Ibid.*, at 45.

⁶⁵ *Ibid.*, at 270.

⁶⁶ *Ibid.*, at 128.

⁶⁷ *Ibid.*

⁶⁸ *Ibid.*, at 109.

⁶⁹ *Ibid.*, at 161. ‘[I]ntentional deaths’, Walzer writes, that are ‘not ruled out by the laws of war’ (*ibid.*, at 162). In supporting this claim, reference is made to C.C. Hyde, *International Law* (2nd edn, 1945), iii, at

(‘[r]ape is a crime, in war as in peace, because it violates the rights of the woman who is attacked’).⁷⁰ On discussing nuclear weapons, we learn that ‘[i]t is in the nature of the new technology that we can be threatened without being held captive’.⁷¹ War or armed conflict has thus devised manners and means other than the orthodox ‘frontal assault’⁷² that has come to represent its glaring stereotype; what matters is how varied this frontal assault can actually be in real terms – against civilians, against women, against children, against the old and the infirm – and Walzer comes closer to the mark of his overall thesis when he writes of war as ‘an act of coercion, a violation of the *status quo*’⁷³ and ‘a world of duress, of threat and counter-threat’.⁷⁴ In other words, the war convention that he has invoked in this work is not and should not be confined to the occurrence of ‘conventional war’.⁷⁵

Cyber warfare thus enters this existing set of normative arrangements and possibilities, and two questions seem to be pertinent here: one concerns whether an act of cyber warfare (of the kind described by Goldsmith, e.g., the neutralization of an electricity grid or the blocking of military communications)⁷⁶ can actually be used to *initiate* an armed conflict between states,⁷⁷ that is to set the Geneva Conventions and the First Additional Protocol in motion, or whether it can only be regarded (in Walzer’s words) as ‘a form of action’ or ‘the mode or means of an attack’ during extant hostilities.⁷⁸ The other question relates to the sufficiency of the law as it now stands for regulating cyber warfare occurring in the course of an ongoing armed conflict. The leading effect of Goldsmith’s various hypotheticals is to think of cyber warfare as involving the instrumentalization of an existing resource as a weapon of warfare – the weaponization of the World Wide Web, if you will – as was done in December 1976 with the adoption of the Convention on the Prohibition of Military or Any Hostile Use of Environmental Modification Techniques. This forbids High Contracting Parties from engaging ‘in military or any other hostile use of environmental modification techniques having widespread use of environmental modification techniques having widespread, longlasting or severe effects as the means of destruction, damage or injury

1802. Yet, the year of the initial publication of *Just and Unjust Wars* – 1977 – marked the advent of the First and Second Additional Protocols, both of which outlawed starvation as a method of warfare.

⁷⁰ *Ibid.*, at 134.

⁷¹ *Ibid.*, at 271.

⁷² *Ibid.*, at 162.

⁷³ *Ibid.*, at 168.

⁷⁴ *Ibid.*, at 313.

⁷⁵ *Ibid.*, at 278 (and hence his reference to ‘the whole range of wartime activity’: *ibid.*, at 289). Indeed, on the other side of the war equation, Walzer asks ‘how responsibility for aggression is diffused through a political system’: *ibid.*, at 292.

⁷⁶ Goldsmith, *supra* note 33, at 130.

⁷⁷ *Supra* note 56. The topic of cyber warfare and non-international armed conflicts is not touched upon by Goldsmith, although, as early as 1997 the Tamil Tigers were reported to have shut down the servers and email capabilities of Sri Lankan embassies throughout the world: see Havelly, ‘When States Go to Cyber-war’, BBC News Online, 16 Feb. 2000, available at: <http://news.bbc.co.uk/1/hi/sci/tech/642867.stm>. Goldsmith does raise the spectre of denial-of-service cyber attacks: *supra* note 33, at 132. See, also, Schmitt, ‘Classification of Cyber Conflict’, 17 *J Conflict & Sec L* (2012) 245, at 255–259.

⁷⁸ Walzer, *supra* note 1, at 216. See also the discussion of Kritsiotis, *supra* note 57, at 281–282.

to any other State Party',⁷⁹ and represents a deliberate categorization of the environment as a *weapon* of warfare,⁸⁰ as opposed to its status as a *victim* of hostilities.⁸¹ One wonders whether legislative reform along these lines is at all required for acts of cyber warfare, and whether, in the interim, the First Additional Protocol becomes at all relevant with its provision that '[i]n the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party'.⁸²

For all of this, Walzer is in agreement that 'the crucial distinction in the theory and practice of war [is] not between prohibited and acceptable weapons but prohibited and acceptable targets'.⁸³ The emphasis, then, is very much on the actual *consequences* of warfare rather than on how these consequences might be actualized or come to pass. From the examples that have been provided, all acts of cyber warfare can hardly be counted as a 'bloodless strategy' in the overall scheme of things,⁸⁴ and it seems that the rules of warfare very much have their work cut out for them and that a new chapter in their history is in the process of being written – especially as to how determinations are to be made as to which dual use targets come within the law's depiction of permissible targets and which do not: the 'mingling' of civilian and military computer and telecommunication systems is taking warwaging to its next frontier.⁸⁵

* * *

The final matter to raise with respect to this contribution to the *EJIL* symposium concerns 'the attribution problem'⁸⁶ that befalls the victim state intent on responsive action, where Goldsmith's position is that 'traceback' in the context of sophisticated cyber warfare 'is neither fast nor remotely certain'.⁸⁷ He is right to point out of course the significance of this issue for both the *jus ad bellum* and *jus in bello*,⁸⁸ so prominent has it been since *Case Concerning Military and Paramilitary Activities in and against Nicaragua* in June 1986, where the International Court of Justice found for the *jus ad bellum* that an armed attack could include 'the sending by a State of armed

⁷⁹ Art. 1(1).

⁸⁰ The preamble to the Convention recognizes that 'scientific and technical advances may open new possibilities with respect to modification of the environment' and that 'military or any other hostile use of such techniques could have effects extremely harmful to human welfare'. See, further, Roscini, 'World Wide Warfare: *Jus ad bellum* and the use of Cyber force', 14 *Max Planck Ybk UN Law* (2010) 85.

⁸¹ As is envisaged in Art. 35 (3) of the First Additional Protocol, which prohibits the employment of 'methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment'.

⁸² Art. 36 (emphases added).

⁸³ Walzer, *supra* note 1, at 276.

⁸⁴ *Ibid.*, at 271. See, also, *supra* note 44.

⁸⁵ Goldsmith, *supra* note 33, at 134.

⁸⁶ *Ibid.*, at 135.

⁸⁷ *Ibid.*, at 134.

⁸⁸ See Brenner, "At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare', 97 *J Criminal L & Criminology* (2007) 379.

bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces',⁸⁹ and that, for the purposes of the *jus in bello*, 'United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the *contras*, the selection of its military or paramilitary targets, and the planning of the whole operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the United States the acts committed by the *contras* in the course of their military or paramilitary operations in Nicaragua'.⁹⁰ These *dicta* tell us a good deal about the statist thrust of international law in terms of its structures of argumentation and the evidence demands it makes, but it is worth recalling that in his discussion on the problem of peacetime reprisals, Walzer had also concluded that 'acts of force are not always acts of state in any simple sense': '[t]hey are not the work', he there wrote, 'of recognized officials and of soldiers acting on official orders, but (often) of guerrilla bands and terrorist organizations – tolerated, perhaps patronized by the officials, but not directly subject to their control'.⁹¹

It is moving beyond this simple sense of 'the state' that is of interest to us here, because connecting with the specifics of the *jus ad bellum* and the *jus in bello* – over and above the law of state responsibility⁹² – reveals how much the *lex specialis* has charted a much more varied and complex pragmatism for itself: the facts and law of its many precedents speak to matters other than the question of state attribution, and include the harbouring of terrorists by a state,⁹³ and, following on from Walzer's discussion of the December 1968 Israeli raid on Beirut International Airport,⁹⁴ the support or sympathy of a given state for operatives not acting in its name or with its official sanction.⁹⁵ States have been known to become complicit in the violence committed by non-state actors,⁹⁶ and even to afford subsequent validation to those actions,⁹⁷ and,

⁸⁹ [1986] ICJ Rep. 14, at 103, para. 195.

⁹⁰ *Ibid.*, at 64, para. 115.

⁹¹ Walzer, *supra* note 1, at 216.

⁹² And its 'criteria', posited by Goldsmith, *supra* note 33, at 135.

⁹³ Walzer, *supra* note 1, at 217.

⁹⁴ In response to the hijacking of a commercial El Al airliner at Athens airport, undertaken by two members of the Popular Front for the Liberation of Palestine: Walzer, at 218. The episode is analysed in some detail by Falk, 'The Beirut Raid and the International Law of Retaliation', 63 *AJIL* (1969) 415. On the relationship between Lebanon and the PFLP see Falk, at 420–421. Falk's interpretation, at 424, is that 'the politics of terror and the use of exile sanctuaries to disrupt "the enemy" society enjoys an ambiguous status in recent international experience'. On that occasion, Israel had contended before the SC that Lebanon was 'assisting and abetting acts of warfare, violence, and terror by irregular forces and organizations' against Israel: see UN Doc. S/8945 and UN Doc. S/8946 (both 29 Dec. 1968).

⁹⁵ For Falk, *ibid.*, at 425, 'there does exist a wide range of variation as to the extent and character of control (or even knowledge) possessed by the territorial government over the conduct of specific guerrilla operations and the formation of more general liberation strategy'. On relating this to the 'responsibility' of the Government of the Lebanon consider Falk, at 431–432 and 439–440.

⁹⁶ As occurred at an Entebbe Airport in Uganda in July 1976, after the hijacking of an Air France airliner by members of the People's Front for the Liberation of Palestine and the Baader Meinhof Gang: Y. Dinstein, *War, Aggression and Self-Defence* (5th edn, 2011), at 257.

⁹⁷ In its report to the SC on 25 Apr. 1980, the US reported that it had attempted a rescue mission in Iran 'in exercise of its inherent right of self-defence with the aim of extricating American nationals who have

as Thomas M. Franck advised over a generation ago now, there are thus a series of possible involvements by a state in initiations of force which are ‘generically related’ but, at one and the same time, ‘significantly dissimilar’ – ‘and the law, if there is to be one, cannot simply disregard the differences’.⁹⁸ This does seem to be a most useful refrain in shaping our thinking on cyber warfarers, as does the fact that the *jus in bello* is now accompanied by a raft of international criminal laws and infrastructures that redirect the focus from state to *individual* action. The challenge of traceback presumes, of course, that the identity of the perpetrator of an attack is known or might be knowable in the first instance – and Goldsmith is right to highlight the intractability of this challenge for cyber warfare.⁹⁹ For Walzer, concerned as he is in *Just and Unjust Wars* with the allocation of moral blame as opposed to any legal reckoning,¹⁰⁰ ‘[t]here can be no justice in war if there are not, ultimately, responsible’ – let us also add identifiable – ‘men and women’.¹⁰¹ Anonymity is the enemy of the good, at least in this instance, for his whole theory of justice rests on the possibilities – or, better, the premise – of identification from those ‘whom we can rightly demand an accounting’.¹⁰²

been and remain the victims of the Iranian armed attack on our Embassy’: see UN Doc. S/13908 (25 Apr. 1980).

⁹⁸ Franck, ‘Who Killed Article 2 (4)? Or: Changing Norms Governing the Use of Force by States’, 64 *AJIL* (1970) 809, at 813–814.

⁹⁹ Although, in Oct. 2012, US Defence Secretary Panetta noted how the Department of Defence ‘has made significant advances in solving a problem that makes deterring cyber adversaries more complex: the difficulty of identifying the origins of that attack’ by making ‘significant investments in forensics to address this problem of attribution.’ *Supra* note 54. This point is picked up by Goldsmith in his discussion of the main elements of Panetta’s speech:

‘The [Department of Defence] has previously said that it is trying to improve its attribution capabilities and in conversation officials have noted some success. Panetta goes further, saying concretely and definitively that ... “significant advances [have been made] in solving” the attribution problem, presumably through a combination of tracing back the source of a cyber attack and identifying the attacker through “behaviour-based algorithms” and human and electronic intelligence. Panetta does not tell us how good, or fast, [the Department of Defence] is at attribution, and he may to some unknown degree be puffing. Nonetheless, this is a potentially big deal for cyber deterrence.’

See Goldsmith, ‘The Significance of Panetta’s Cyber Speech and the Persistent Difficulty of Deterring Cyberattacks’, *Lawfare* www.lawfareblog.com/2012/10/the-significance-of-panettas-cyber-speech-and-the-persistent-difficulty-of-deterring-cyberattacks/ (15 Oct. 2012). See, also, Hopkins, ‘Britain’s enemies accused of cyber-attacks on infrastructure’, *Guardian*, 3 Dec. 2012, at 8.

¹⁰⁰ Walzer, *supra* note 1, at 291.

¹⁰¹ *Ibid.*, at 288. Reading Goldsmith’s article makes us appreciate the limitations of Walzer’s assessment of the war convention: ‘[w]hat is crucial is that [war criminals] can be pointed at; we know where to look for them, if we are ready to look’: *ibid.*, at 289.

¹⁰² *Ibid.*, at 287 (and, at 289, ‘it is not easy, perhaps, to mark out aggressors, though I think we should start with the assumption that it is always possible’).