**BOOK REVIEW**

***Technology and the Law on the Use of Force*** by Jackson Maogoto, Routledge Press, 2015, 111 pp., ISBN: 978-0-415-69433-9

The intersection between the *jus ad bellum* and technology represents a crucial topic *de nos jours*,for obvious reasons. As such, much recent literature and scholarly debate has focused on international law’s ability to respond to new and developing technologies, such as cyber warfare[[1]](#footnote-2) or combat drones (UAVs).[[2]](#footnote-3) As its title suggests, Jackson Maogoto’s *Technology and the Law on the Use of Force* looks to contribute to these debates, not by adopting the usual approach of considering a single ‘technology’, but, instead, by assessing the application of the *jus ad bellum* to modern technological threats more generally.

This underlying ambition is most welcome, but, somewhat strangely, Maogoto ultimately only considers two ‘types’ of technology in his book: the militarisation of outer space and cyber warfare (and, it must be said, the latter of these is dealt with rather cursorily). This immediately leaves one questioning why other technologies, such as, say, UAVs or battlefield ‘robots’[[3]](#footnote-4) were not included. Nevertheless, while the intersection of cyber warfare and the *jus ad bellum* represents extremely well-trodden ground, Maogoto’s book might be seen as contributing to the *jus ad bellum*/technology literature because it predominantly focuses on the legal framework applicable to the militarised use of outer space; a ‘type’ of technological advancement that has been comparatively overlooked.[[4]](#footnote-5)

Maogoto states (5) that his book operates within the confines of two spectra. First, analysis is limited solely to exploring ‘only…those information intrusions that are instigated by or imputable to States…’ The implications of the forcible use of technologies by non-state actors are thus beyond the book’s scope.[[5]](#footnote-6) Secondly, it is said that the book’s coverage is restricted to the *jus ad bellum* (as opposed to the *jus in bello*). The majority of the book is, indeed, *jus ad bellum*-centric, and *jus in bello* concerns are entirely left aside; however, it is notable that the book also considers other legal areas in relation to force/militarisation too (such as, say, provisions relating to the *testing* of nuclear weapons, at 38-39, or the wider ‘space law’ regime more generally, at 34-43). It is therefore not the case that the book is merely confined to examining rules that can strictly be considered as ‘*jus ad bellum*’ in nature (at least, in the Charter-framework sense). This is no bad thing—indeed, the wider focus on norms of international law beyond just Articles 2(4) and 51 as applicable to the militarisation of outer space (in chapter 3) represent some of the most valuable elements of the book—but it is worth keeping in mind.

*Technology and the Law on the Use of Force* begins, in chapter 1, by familiarising the reader with the well-known tenets and framework of the *jus ad bellum*, which ultimately underpin later discussions concerning the extent to which that regime can adapt to the technologies considered. This is very much a framework chapter in which Maogoto seeks to ground his analysis. The starting point for any *jus ad bellum* discussion is, of course, the prohibition of the threat or use of force contained in Article 2(4) of the United Nations (UN) Charter. Considerable literature elsewhere has deconstructed this cornerstone prohibition in terms of its various component parts.[[6]](#footnote-7) Of particular note for Maogoto, however, is the fact that the meaning of the term ‘force’ in Article 2(4) has traditionally been interpreted based on the type of ‘forcible’ action undertaken (military/kinetic).[[7]](#footnote-8) This is contrasted with the fact that, for states, it is in reality the *consequences suffered*, rather than the weapon utilised for administering force, which is of importance.[[8]](#footnote-9)

Maogoto’s key message (see, for example, 12), within both chapter 1 and the book as a whole, is that while the UN Charter’s *jus ad bellum* legal provisions can ‘cope’ with conventional warfare, when it comes to more advanced weaponry things become more problematic. In Maogoto’s view, technological advances in warfare have ‘overtaken’ the international legal framework, which, he asserts, is now ill-equipped to regulate both aggressive cyber operations and attacks in/from outer space. For example, in relation to the right of self-defence, Maogoto argues (17) that the injury suffered by a state by virtue of intrusions into ‘the digital commons’ will likely not be sufficient to trigger Article 51: an attack that merely corrupts or ‘annoys’ rather than destroys would, in his view, fall short of a qualitatively grave use of force triggering a defensive response.[[9]](#footnote-10) The fear is that this may leave states with no defensive recourse in response to technological threats.[[10]](#footnote-11)

The application of the rules of the *jus ad bellum*, created prior to the advent of both space exploration and cyberspace, to the threats posed by these modern technologies will obviously be somewhat anachronistic.[[11]](#footnote-12) There is no question that the application of ‘old’ law to such threats is neither self-evident nor straightforward. Equally, in the view of the present reviewers, Maogoto’s core claim in this regard is somewhat overstated. New security threats have emerged in various guises throughout the UN era, and there is nothing so inherently unique about either cyberspace[[12]](#footnote-13) or the militarization of outer space[[13]](#footnote-14) that means that existing legal provisions are necessarily inapplicable to the threats that these technologies pose. It is also not the case that just because an action falls outside of the scope of the *jus ad bellum* it falls outside of the scope of *international law*. One must keep in mind that technological threats are still likely to be violations of the principle of non-intervention[[14]](#footnote-15) and/or the duty of due diligence.[[15]](#footnote-16) Even though the violation of these norms themselves does not allow for forcible responses in self-defence, states still have legal recourse to non-forcible countermeasures.[[16]](#footnote-17)

Chapter 2 of *Technology and the Law on the Use of Force* deals with the strategic consideration of the Revolution in Military Affairs (RMA) and, thus, underpins the book’s latter discussions in a theoretical/strategic sense. Indeed, there is a broad theoretical approach, underpinning the entire book, of fusing strategic considerations with international law. This attempt to buttress practical discussions with theoretical foundations had the potential to be of significant value: strategic considerations arguably should be at the heart of any *jus ad bellum* analysis, given the inextricably intertwined nature of these topics. While still a prominent fixture of strategic literature,[[17]](#footnote-18) the RMA rarely surfaces prominently in international legal debates.[[18]](#footnote-19) It is thus commendable that Maogoto considers this strategic perspective in chapter 2, but it is also something of a shame that—perhaps all too conscious of his audience, who will likely fall more readily into the ‘international lawyer’ rather than ‘strategist’ camp—his discussion of the RMA is so brief.

The RMA concept has been used in a range of ways in the strategic literature,[[19]](#footnote-20) but in the context of the topic of the book under review it denotes a ‘military-technical revolution’: a new, more efficient way of waging war.[[20]](#footnote-21) Ostensibly, Maogoto uses strategic thinking to revisit his earlier premise in chapter 1 that the applicable legal framework needs re-thinking in light of modern strategic goals (23). In relation to both outer space and cyberspace, the strategic goal on the part of an aggressor state, again, is not necessarily to cause physical damage but, rather, to ‘disrupt, deny, degrade or destroy information’ (28). All of which would seemingly fall outside the *jus ad bellum* regulatory framework.

The book’s second chapter is subdivided into two broader discussions on cyber warfare and outer space in relation to technological advances and the wider RMA. In the context of outer space, Maogoto argues (24-5) that the latest revolution in military affairs has been for states to develop appropriate strike platforms. The United States Space Command’s vision for 2020[[21]](#footnote-22) is employed (24) as a case in point, demonstrating states’ commitment to building strike platforms designed for use in outer space. The second part of the chapter briefly (25-27) signposts the RMA in cyberspace, recording the rise in recourse to cyber-attacks by noting *locus classicus* such as Estonia (2007).[[22]](#footnote-23)

Chapter 3 showcases Maogoto’s expertise in space law, in that it considers how the *jus ad bellum* framework regulates (or, indeed, *should* regulate) the potential militarisation of outer space. The chapter is undoubtedly the book’s most unique and interesting contribution to current literature.[[23]](#footnote-24) Maogoto traces the major treaties that regulate states’ activities in outer space (Outer Space Treaty, Limited Test Ban Treaty, Liability Convention and Anti-Ballistic Missile Treaty), and his analysis (32-43) of this treaty regime, and its potential to restrict the use of outer space as a theatre of war, is clear and well-reasoned.

The author convincingly argues that, while these conventions are emphatic in trying to prevent militarisation in outer space, the reality is that states are incrementally challenging the boundaries set by the regime. China’s recourse, in 2007, to an anti-satellite weapon to down one of its own defunct weather satellites adds credence to that position,[[24]](#footnote-25) as Maogoto notes (45). A similar perspective emerges when one poses the following hypothetical question. If an intercontinental ballistic missile/exoatmospheric missile was technically located in outer space before its re-entry, would that breach provisions of the existing legal regime? The answer would likely be no, at least if one considers the *travaux préparatoires* of the Outer Space Treaty from the 1960s.[[25]](#footnote-26) Maogoto’s argument (45) that the key tenets of space law do not preclude the broader ‘militarisation’ of outer space *per se* (in the sense of ‘military usage’, such as the deployment of intelligence satellites for military purposes) is difficult to dispute. Of course, militarisation of this kind is very different from ‘all out’ militarisation (in the sense of the direct use of force in/from space), and this distinction is helpfully drawn in chapter 3 (particularly at 43-47).

Having said all this, the arguments presented in chapter 3, as is indeed the case throughout *Technology and the Law on the Use of Force*, have a notable tendency to raise questions rather than resolve them. For example, given that the author persuasively asserts that the increased militarisation of outer space as an inevitability, he does not sufficiently engage with the question of *how* one might in fact ‘transpose’ the existing *jus ad bellum* regime to outer space. Certainty, from a conceptual perspective it would be more productive to recalibrate and interpret the existing parameters to fit the ‘uniqueness’ of outer space rather than simply to hold that the current regime is insufficient. The ‘peculiarities’ of outer space as a potential battlefield require a re-appraisal of the thresholds for the cardinal prohibition of the threat or use of force in Article 2(4) and a state’s lawful recourse to self-defence under both Article 51 and customary international law. Unfortunately the book under review does not do enough in terms of attempting to undertake such a re-appraisal.

One should note Maogoto’s caveat in the introduction to chapter 3 (31) that not every single relevant ‘space law’ instrument will be scrutinised therein. The absence in the discussion of, for example, the proposed Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT) can, therefore, be somewhat excused. Nonetheless, given the on-going conversations about the PPWT in the Conference on Disarmament[[26]](#footnote-27) and the European Union’s proposed Code of Conduct for Space Activities,[[27]](#footnote-28) Maogoto’s approach is regrettably narrow.

In chapter 4, Maogoto surveys (56) the applicable landscape surrounding the perennial difficulties with applying the law on the use of force to attacks occurring in cyberspace. These difficulties have been exhaustively and *exhaustingly* covered elsewhere,[[28]](#footnote-29) and it must be said that *Technology and the Law on the Use of Force* adds relatively little to the *jus ad bellum* literature concerning cyber warfare. At fewer than 20 pages, chapter 4, for the most part, merely acts as a summary of existing approaches. For example, Michael Sklerov’s important proposed typology for assessing cyber-attacks[[29]](#footnote-30) is set out (57). The approach taken by Sklerov—which to some extent was a refinement of earlier proposals by Michael Schmitt[[30]](#footnote-31)—is potentially extremely valuable and could benefit from further analysis. However, Maogoto does not *analyse* Sklerov’s typologies at all, he merely lists them. To an extent, this is symptomatic of the book as a whole, which is too often overly descriptive (rather than analytical) when it comes to the key issues with which it is grappling.[[31]](#footnote-32)

Chapter 4 (quite correctly) questions the extent to which different cyber operations fall within or without the purview of Article 2(4): this debate is perhaps still not entirely resolved, but it has existed since the 1990s and its parameters are well-known.[[32]](#footnote-33) Unfortunately, chapter 4 does not meaningfully advance this debate. Indeed, the chapter arguably clouds rather than elucidates matters, in that it at times unhelpfully blurs the questions of whether a cyber-attack does (or can) constitute an instance of ‘force’, ‘intervention’ and/or an ‘armed attack’. These are, of course, all different concepts with different thresholds.[[33]](#footnote-34) For example, Maogoto’s discussion of the Stuxnet virus[[34]](#footnote-35) references the notions of both ‘force’ and ‘armed attack’ in the same breath without apparently distinguishing them, and the chapter’s discussion of the 2013 Tallinn Manual[[35]](#footnote-36) and *Nicaragua* case[[36]](#footnote-37) (65) similarly seems to amalgamate the concepts of ‘force’ and ‘intervention’.

Ultimately, Maogoto reaches the almost indisputable (but relatively anodyne) conclusion in chapter 4 that ‘injurious physical impact on a State’s CNI would comfortably meet the threshold [for a breach of Article 2(4)]’ (65). However, he essentially brushes aside the more contentious and important question of whether cyber-attacks with *non*-kinetic results can qualify as a use of force (or, for that matter, as an armed attack). Commentators will be quick to point out that a cyber-attack that, for example, ‘corrupts data on a stock exchange and which in turn causes widespread economic harm but no direct physical damage’[[37]](#footnote-38) could have disastrous effects.[[38]](#footnote-39) It is precisely such attacks—that result in significant but ‘non-corporal’ damage— with which traditional conceptions of the *jus ad bellum* struggle. This categorisation problem is admittedly raised in the book (particularly at 60-2), but it is largely sidestepped.

Even more significant is the chapter’s failure to engage with the question of attribution/state responsibility. Much of the difficulty with applying the *jus ad bellum* to cyber-attacks concerns attribution (notably, because using proxy servers to hide the original IP address can comparatively easily mask the author of a cyber-attack).[[39]](#footnote-40) This crucial issue—which, perhaps more than any other factor, makes the application of the *jus ad bellum* to cyberspace problematic—is briefly alluded to by Maogoto (for example, at 85) but is not explored.[[40]](#footnote-41)

Chapter 5, alongside chapter 3, is one of the more interesting in the book. It provides the reader with a conceptual re-thinking of the existing parameters/framework previously discussed. While such exercises are, of course, necessarily more theoretical than practical, they can nonetheless provide valuable insight in terms of conceptualising *de lege ferenda*. Maogoto’s attempt in chapter 5 to provide ‘solutions’ to the problems that he has earlier identified certainly has some thought-provoking elements. For example, his consideration, rooted in environmental law, of outer space as a finite natural resource (79-82) makes an important (if frustratingly brief) contribution to the wider topic of the legal implications of the weaponisation of space.

As a whole, Chapter 5 is notably more analytical than the rest of the book. Having said this, the chapter, again, ultimately raises more questions than it answers. While it is not necessarily an academic’s job to answer all of their own rhetorical questions, the chapter does not offer the solutions that the reader craves, even tentatively.

To conclude, Jackson Maogoto is to be commended for attempting to tackle such a complex and broad topic. However, while the examples provided in the book are varied and thought provoking, *Technology and the Law on the Use of Force* has some significant weaknesses. With respect, it must be said that the book is not especially well-written (for example, the oxymoronic notion of ‘boundless boundaries’, at 3, is indicative of some quite poorly chosen phrases). Much more importantly, it does not do enough to support its core contention that the existing legal framework is necessarily unable to cope with modern technological advances. The book is short, at fewer than 100 pages (excluding bibliography). One could be charitable and see it as a succinct commentary but—given the scope of the topic with which the book looks to engage, and the lack of depth in which it does so—the unfortunate fact is that it is not ‘succinct’, it is lightweight. *Technology and the Law on the Use of Force* a notable disappointment, because it feels like a missed opportunity to contribute something really important to the various ongoing debates on technology and the *jus ad bellum*. The undeniably high quality of chapter 3 and its analysis of the space law regime shows just how good this book could have been, had the author adopted a more detailed and analytical approach throughout.

There is definitely scope for a book providing a truly rigorous examination of the ability (or inability) of the *jus ad bellum* to deal with modern technologies in a general sense. The literature similarly would benefit from a book that focused in depth on the legal regulation of the weaponisation of outer space in particular (something which has received comparatively little commentary the wider literature).[[41]](#footnote-42) Unfortunately, in the view of the present reviewers, this book—while it undoubtedly has its merits—does not sufficiently fill either gap.

Francis Grimal

*Book Review Editor*

*Senior Lecturer in Public International Law, The University of Buckingham*

*Email: francis.grimal@buckingham.ac.uk*

James A Green

*Co-Editor-in-Chief*

*Professor of Public International Law, University of Reading*

*Email: j.a.green@reading.ac.uk*

1. See, for example, James A Green, ‘The Regulation of Cyber Warfare under the *Jus ad Bellum*’ in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015), 96; Oona Hathaway, Rebecca Crootoof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue and Julia Spiegel ‘The Law of Cyber-Attack’ (2012) 100 *California Law Review* 817; Heather A Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012), 37-74; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014); and Matthew C Waxman, ‘Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)’ (2011) 36 *Yale Journal of International Law* 421. [↑](#footnote-ref-2)
2. See, for example, Marie Aronsson, ‘Remote Law-Making? American Drone Strikes and the Development of *Jus ad Bellum*’ (2014) 1(2) *Journal on the Use of Force and International Law* 273; Robert P Barnidge, Jr, ‘A Qualified Defense of American Drone Attacks in Northwest Pakistan under International Humanitarian Law’ (2012) 30 *Boston University International Law Journal* 409; Susan Breau and Marie Aronsson, ‘Drone Attacks, International Law, and the Recording of Civilian Casualties of Armed Conflict’ (2012) 35 *Suffolk University Transnational Law Review* 255; Max Byrne, ‘Consent and the Use of Force: An Examination of ‘Intervention by Invitation’ as a Basis for US Drone Strikes in Pakistan, Somalia and Yemen’ (2016) 3(1) *Journal on the Use of Force and International Law* 1 (page number for pre-issue online publication); and Sikander Ahmed Shah, *International Law and Drone Strikes in Pakistan: The Legal and Socio-Political Aspects* (Routledge, 2016). [↑](#footnote-ref-3)
3. See Armin Krishna, *Killer Robots: Legality and Ethicality of Autonomous Weapons* (Ashgate, 2009), particularly at 89-116. [↑](#footnote-ref-4)
4. Having said this, literature on the militarisation of outer space has remained constant since the advent of the space race. See, for example, Michel Bourbonnière, ‘Law of Armed Conflict (LOAC) and the Neutralisation of Satellites or *Ius in Bello Satellitis*’ (2004) 9 *Journal of Conflict Security Law* 43; Tare C Brisibe, ‘Customary International Law, Arms Control and the Environment in Outer Space’ (2009) 8 *Chinese Journal of International Law* 375; Blair S Kuplic, ‘The Weaponization of Outer Space: Preventing an Extraterrestrial Arms Race’ (2014) 39 *North Carolina Journal of International Law and Commercial Regulation* 1123; Jackson Maogoto and Steven Freeland, ‘The Final Frontier: The Laws of Armed Conflict and Space Warfare’ (2007) 23 *Connecticut Journal of International Law* 165; Zachos A Paliouras, ‘The Non-Appropriation Principle: The Grundnorm of International Space Law’ (2014) 27 *Leiden Journal of International Law* 37; Michael N Schmitt, ‘International Law and Military Operations in Space’ (2006) 10 *Max Planck Yearbook of the United Nations Law* 89; and Fabio Tronchetti, ‘The Right of Self-Defence in Outer Space’(2014) 63 *German Journal of Air and Space Law* 92. [↑](#footnote-ref-5)
5. On this issue, see, for example, Nicolò Bussolati, ‘The Rise of Non-State Actors in Cyberwarfare’ in Jens David Ohlin, Kevin Govern, and Claire Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (Oxford University Press, 2015), 102. [↑](#footnote-ref-6)
6. See, for just a few examples, Olivier Corten, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Hart, 2010), 50-197; Thomas M Franck, *Recourse to Force: State Action Against Threats and Armed Attacks* (Cambridge University Press, 2002), 11-9; and Nico Schrijver, ‘The Ban on the Use of Force in the UN Charter’ in Marc Weller (ed), *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press, 2015), 466. [↑](#footnote-ref-7)
7. On that traditional interpretation, see Daniel B Silver, ‘Computer Network Attack as a Use of Force under Article 2(4)’ (2002) 76 *International Law Studies* 73, 80-2; and Tom J Farer, ‘Political and Economic Coercion in Contemporary International Law’ (1985) 79 *American Journal of International Law* 405. [↑](#footnote-ref-8)
8. For the classic expression of this view, see Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press, 1963), 362. [↑](#footnote-ref-9)
9. This is the prevailing view in the literature. See, for example, Harrison Dinniss (n 1) 81. However, for a contrary position, see Nicholas Tsagourias, ‘Cyber-Attacks, Self-Defence and the Problem of Attribution’ (2012) 17 *Journal of Conflict and Security Law* 229, particularly at 231-2. [↑](#footnote-ref-10)
10. See, for example, Matthew C Waxman, ‘Self-Defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions’ (2013) 89 *International Legal Studies* 109 (echoing this concern). [↑](#footnote-ref-11)
11. See Russell Buchan, ‘Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions’ (2012) 17 *Journal of Conflict and Security Law* 212, 212-13 (specially making this point in relation to cyber-attacks). [↑](#footnote-ref-12)
12. See Wolff Heintschel von Heinegg, ‘Territorial Sovereignty and Neutrality in Cyberspace’ (2013) 89 *International Legal Studies* 123, 123-4; and Christopher P M Waters, ‘New Hacktivists and the Old Concept of *Levée en Masse*’ (2014) 37 *Dalhouse Law Journal* 771, 773-5. [↑](#footnote-ref-13)
13. See Schmitt (n 4) 102 (noting that Article III of the 1967 Outer Space Treaty is to be interpreted in light of the existing *jus ad bellum* framework). [↑](#footnote-ref-14)
14. See Buchan (n 11). [↑](#footnote-ref-15)
15. See James A Green, ‘Disasters Caused in Cyberspace’ in Susan C Breau and Katja L H Samuel (eds), *Research Handbook on Disasters and International Law* (Edward Elgar, forthcoming 2016); and Michael N Schmitt, ‘In Defense of Due Diligence in Cyberspace’ (2015) 125 *Yale Law Journal Forum* 68. [↑](#footnote-ref-16)
16. See Mary Ellen O’Connell, ‘Cyber Security without Cyber War’ (2012) 17 *Journal of Conflict and Security Law* 187, 204-205. [↑](#footnote-ref-17)
17. See, for example, Andrew Futter and Jeffrey Collins (eds), *Reassessing the Revolution in Military Affairs: Transformation, Evolution and Lessons Learnt* (Palgrave Macmillan, 2015); and Special Issue: The Information Technology Revolution in Military Affairs, (2010) 33(4) *Journal of Strategic Studies*. [↑](#footnote-ref-18)
18. Although, see, for example, Francis Grimal, *Threats of Force: International Law and Strategy* (Routledge, 2012). [↑](#footnote-ref-19)
19. See, for example Andrew N Liaropolous, ‘Revolutions in Warfare: Theoretical Paradigms and Historical Evidence – The Napoleonic and First World War Revolutions in Military Affairs’ (2006) 70 *Journal of Military History* 363; and Richard Stiennon, ‘A Short History of Cyber Warfare’ in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015), 7, 14-6. [↑](#footnote-ref-20)
20. Eliot A Cohen, ‘A Revolution in Warfare’ (1996) 75 *Foreign Affairs* 37. [↑](#footnote-ref-21)
21. *Long Range Plan: Implementing USSPACECOM Vision for 2020* (United States Space Command, 1998). [↑](#footnote-ref-22)
22. For discussion of the cyber-attack on Estonia, see Lene Hansen, ‘Digital Disaster, Cyber Security, and the Copenhagen School’ (2009) 53 *International Studies Quarterly* 1155, 1168-71. [↑](#footnote-ref-23)
23. Although, note, for example, the sources cited at n 4. [↑](#footnote-ref-24)
24. Noting, of course, that in this context China could probably invoke Article VIII of the Outer Space Treaty, which would give it autonomy to dispose of its own ‘property’ in this way. [↑](#footnote-ref-25)
25. See, for example, Jonathan Halpern, ‘Antisatellite Weaponry: The High Road to Destruction’ (1985) 3 *Boston University International Law Journal* 167, 181; and the *travaux preparatoires* themselves: ‘Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies’ (16 September 1966) UN Doc A/AC.105/35 Annex III - WP.6/ Rev. 1 (note particularly the US’s interpretation of Art IV of the Outer Space Treaty). These sources are referenced by Maogoto himself in his doctoral thesis: *The Militersiation and Weaponisation of Outer Space—From Playground to Battleground: Legal Perspectives on the Use of Force* (Sydney, 2007), 24. [↑](#footnote-ref-26)
26. See United Nations, Conference on Disarmament, 2015, http://nti.org/18TAR (accessed 21 April 2016). [↑](#footnote-ref-27)
27. European Union External Action, ‘International Code of Conduct for Outer Space Activities’, (Draft) *European External Action Service* (31 March 2014) http://eeas.europa.eu/non-proliferation-and-disarmament/outer-space-activities/index\_en.htm (accessed 21 April 2016). [↑](#footnote-ref-28)
28. See, for example, the sources cited in n 1. [↑](#footnote-ref-29)
29. Michael J Sklerov, ‘Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent’ (2009) 201 *Military Law Review* 1, particularly at 54-5. [↑](#footnote-ref-30)
30. Michael N Schmitt ‘Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework’ (1999) 37 *Columbia Journal of Transnational Law* 885. [↑](#footnote-ref-31)
31. For some other notable examples in the book, see the accounts of the Soviet proposals relating to space attack weapons (74), or the US DoD’s approach to cyber activities (57 and 84). [↑](#footnote-ref-32)
32. The debate is set out in detail in Green (n 1) particularly at 98-107. [↑](#footnote-ref-33)
33. James A Green, *The International Court of Justice and Self-Defence in International Law* (Hart, 2009), 31-3. [↑](#footnote-ref-34)
34. On the Stuxnet virus, see Stiennon (n 19) 20-2. [↑](#footnote-ref-35)
35. Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (prepared by the International Group of Experts at the Invitation of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, 2013) [↑](#footnote-ref-36)
36. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (merits) [1986] ICJ Rep 14. [↑](#footnote-ref-37)
37. Jack Goldsmith, ‘How Cyber Changes the Laws of War’ (2013) 24 *European Journal of International Law* 129, 133. [↑](#footnote-ref-38)
38. See Vida M Antolin-Jenkins, ‘Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?’ (2005) 51 *Naval Law Review* 132, 155; and Stephanie G Handler, ‘New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare’ (2012) 48 *Stanford Journal of International Law* 209, 229. [↑](#footnote-ref-39)
39. See P W Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford University Press, 2014) 75. [↑](#footnote-ref-40)
40. On this issue, see, for example, Constantine Antonopoulos, ‘State Responsibility in Cyberspace’ in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015), 55. [↑](#footnote-ref-41)
41. See n 4 and accompanying text. [↑](#footnote-ref-42)