The use of cyber force: Is the *jus ad bellum* ready?

Christian Henderson[*]

The issue of international cyber attacks has given rise to discussions within and between many academic disciplines,[1] has been discussed within international fora,[2] and is never far away from the headlines of the global media.[3] There are many explanatory reasons for this interest; the fact that such attacks involve computers which, today, we all use in some form, the fact that they are relatively new and continuing to evolve, their often unidentifiable nature, and their variety of form, from 'simple' hacks into domestic computers to 'distributive denial of service' attacks, to sophisticated intrusions into bank and state systems. However, it is their potential for physical devastation and destruction, and perhaps an ensuing cyber war, that undoubtedly continues to stoke the greatest amount of interest.

While a cyber attack that can unequivocally be described as a use of force for the purposes of international law, let alone one that has led to a cyber 'war', is yet to occur, it is such a prospect that has been the focus of attention from the academic legal community of late. Two relatively recent publications on this topic are Heather Harrison Dinniss' *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012)

[*] Professor, University of Sussex.

[1] See, for example, JA Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015).

[2] For a discussion of this issue in the context of the United Nations, see C Henderson, 'The United Nations and the Regulation of Cyber-security', in N Tsagourias, R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) 465.

[3] See, for example, BBC News, 'US Cyber-attacks: Iranians Charged by Department of Justice', 24 March 2016, available at <www.bbc.co.uk/news/world-us-canada-35893040>.

and the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), although interest in the topic dates back to the 1990s.[4] The book under review, Marco Roscini's *Cyber Operations and the Use of Force in International Law* (Oxford University Press, 2014), follows in a similar vein to these two publications, addressing both the law governing the use of force (the *jus ad bellum*) *and* the laws of armed conflict (the *jus in bello*). The work of the author has led to him becoming a recognized expert on both aspects in general, and also in the cyber context.[5]

The focus of this short piece is the book's coverage of the *jus ad bellum* aspects, which consumes approximately one third of the book. There are, in this respect, two notable points that attention should initially be drawn to. The first is that international law provides no *lex specialis* rules directly and expressly addressing the use of force in cyberspace. The general rules regulating the use of force within the international community are relatively old, but the question is whether due to technological and other advances they have become dated. The 'contemporary' prohibition of the use of force and its associated exceptions of individual or collective self-defence and actions mandated by the United Nations Security Council date back to 1945 and were devised in an era of conventional armies crossing borders and weaponry that consisted of tanks, bombers, warships, etc. The reason today for a lack of dedicated rules regulating cyber force may simply be due to the fact that the international community is yet to catch up and develop *lex specialis* rules regulating actions within this specific field. However, it may also be because states, as with Roscini, feel that the existing rules are adequate and capable of being applied to developments and actions within cyber space. As Roscini states in the conclusion to this section of the book:

> 'In the current absence of specific *jus ad bellum* rules applicable to cyber operations, we are left with the provisions contained in the UN Charter and in customary international law. These rules are flexible

[4] See, for example, TA Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the UN Charter' (1998) 30 Case Western Reserve J Intl L 567.

[5] See, for example, M Roscini, 'World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force' (2010) 14 Max Planck Yb United Nations L 85.

> enough to be extended to means that did not exist when they were adopted.'[6]

The second, and related point, is the generally prospective nature of the analysis and discussion. While there have been several relatively recent high profile cyber attacks, such as in Estonia in 2007, in Georgia in 2008, and in Iran in 2010, which are referred back to, referenced, and utilized frequently throughout this section of the book, if one is looking to see how existing international law has been interpreted, applied and developed in connection with these types of attacks there is not a great deal of state or institutional practice to work with. The discussion is, therefore, to an extent of a hypothetical nature. This does not in itself devalue the book in that it delves into and surveys in good detail the minutiae of the existing rules of the *jus ad bellum* to address the underlying question of whether international law and the international legal system is ready and equipped to competently address and provide the necessary tools of critique and regulation for the inevitable reality of large scale cyber attacks and, potentially, cyber warfare. In this sense the objective of Roscini's work is to, on the one hand, strip back the rules to get to their essence and, on the other, see how they have been interpreted and developed over the past 70 years to discern firstly whether they are able to regulate cyber uses of force and to then gauge the legality of certain actions under them.

Overall, Roscini does a commendable job. The approach of the book is firmly doctrinal in nature and is, as is the case with much of Roscini's work, extremely well researched. While one may not always agree with the positions adopted or arguments made, Roscini nonetheless generally provides excellent authority and support for these, utilizing both primary and secondary legal sources. In particular, there is generally extensive engagement with, and utilization of, verbal state practice, in connection with the few cyber attacks that have been witnessed over recent years, in the abstract, and in various military manuals and official state documents.

This methodology does, of course, have its limitations, as one of the key criticisms of the ways in which international law is formed and in-

[6] M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP, 2014) 115.

terpreted, and in particular the way customary international law is developed, is that it is these more powerful states that are able to make their voices heard. In this respect, while the section attempts to include the views of a broad range of states, it is very often the practice and views of certain usual suspects, in particular the United States, that are drawn upon by Roscini to illustrate his points. While one might argue in certain contexts that there are 'specially affected' states whose views and opinions should be given special weight, it is difficult to sustain such an argument in the cyber context as today most states rely to some degree on computers, including in operating and protecting critical national infrastructure. However, one should not be too quick to criticize Roscini here as he is, after all, only able to utilize the information that is available.

The book is also well researched in regards to secondary legal sources, and refers to and makes use of a broad range of literature. In particular, while Harrison Dinniss' book and the *Tallinn Manual* may be seen as direct competitors to Roscini's, potentially leading to some authors shying away from referencing them, Roscini cites and utilizes them liberally in substantiating, and juxtaposing, his own positions.

In the earlier stages of this section of the book Roscini sets out whether cyber operations can engage the prohibition of the threat or use of force. In this respect three preconditions are advanced as being necessary:

> 'First, the cyber operation needs to be attributed to a state: private individuals or armed groups do not fall within the scope of the provision, not even when they can inflict damage comparable to that caused by states. Secondly, the cyber operation must amount to either a "threat" or a "use of force". Thirdly, the threat or use of force must be exercised in the conduct of "international relations".'[7]

The first and third of these conditions are closely related, as while the first makes the point that the actions of non-state actors are not (as yet, at least) covered by the prohibition, the third highlights that the prohibition is of an inter-state nature, and actions solely against non-state actors are in and of themselves insufficient to engage the prohibi-

[7] ibid 44.

tion. A notable element of this section of the book is the relative focus that is placed upon providing a textual analysis of Article 2(4)'s application in this context, while the customary international law source of the norm is not something that Roscini openly engages with to any significant degree. Issue may be taken with this, as while Article 2(4)'s application is in the realms of states, being expressly addressed to 'members' of the UN operating in their 'international relations', it is quite possible that developments regarding the cyber field have taken – or could take – place within the realms of the customary form of the prohibition. Yet, given that virtually all states are a party to the UN Charter, and Article 2(4)'s weighty status within this instrument, it is unlikely that any changes to the customary prohibition could take place which are inconsistent with the strictures of Article 2(4), or a reasonable interpretation of them, thereby justifying Roscini's narrow focus on the treaty form of the norm.

As mentioned above, Roscini maintains that attribution to a state is necessary in any assessment as to whether a cyber attack constitutes a prohibited use of force for the purposes of Article 2(4). Roscini sets out well the 'effective control' standard of attribution and the 'clear and convincing' standard of evidence for such control and how they apply in the cyber context. Yet, while *legal* attribution is one thing, some of the problems with meeting these on a *factual* level could have been provided more attention. Indeed, given the very nature of cyber operations, actually being able to establish effective control by a state over non-state actors who have engaged in a cyber use of force through evidence that could be described as clear and convincing, is particularly problematic and raises question marks over the viability of the application of such standards in the cyber context.

The second of Roscini's requirements above – that the cyber operation must amount to either a threat or use of force – is where the discussion is focused. There is much to agree with in Roscini's analysis, such as the way that he separates the discussion up into the various levels of seriousness that a cyber operation may take. However, one issue excluded from the discussion in connection with the prohibition of the threat or use of force is the *mens rea* issue of intention,[8] which is, by

[8] This is mentioned in passing twice ibid, at 46.

contrast, given some attention in connection with the issue of self-defence. Indeed, in the context of self-defence Roscini states that:

> 'When the damage caused to a certain state or its nationals is however not intended (a situation that is particularly likely in the cyber context), it is doubtful that self-defence can be invoked by the accidental victim … [A]n armed attack is nothing else than a form of aggression, it requires *animus aggressionis.* Indeed, according to the ICJ, an armed attack must be carried out "with the specific intention of harming". *Animus aggressionis* means a deliberate intention to cause damage to property, people or systems of a certain state. In the cyber context, this hostile intention can be inferred from "such factors as persistence, sophistication of methods used, targeting of especially sensitive systems, and actual damage done"'. [9]

The requirement that an armed attack must be shown to be intended before self-defence can be invoked could be doubted upon the basis that the right exists first and foremost for states to defend themselves, without them having to first engage whether the attack was intentional or not. This argument applies equally in the cyber context. However, it is not clear why the same attention is not given to the issue of intention in regards to the prohibition of the threat or use of force. Granted, this is not an issue that many authors have dedicated much time to, including the *Tallinn Manual*. But hostile intent, and means of discerning it within the cyber context, would seem a particularly important element in determining whether a forcible action comes within the realms of the prohibition of the threat or use of force.[10] For example, Roscini is clear that a threat or use of force must be exercised in the conduct of 'international relations'. Yet, it becomes apparent that this will often be determined upon the basis of the intent of the attackers. If an analogy is to be made with the non-cyber context, a forcible measure against a private foreign individual, aircraft or ship within a state's territory or territorial airspace or waters would not likely in and of itself constitute a use of force, given that international relations have not become engaged. But if it becomes clear that the individual, ship, or aircraft has been

[9] ibid 76-77 (footnotes omitted).

[10] See, for example, T Ruys, 'The Meaning of "Force" and the Boundaries of the *Jus ad Bellum*: Are "Minimal" Uses of Force Excluded from the UN Charter Article 2(4)?', (2014) 108 AJIL 159, 189-191.

employed as a proxy for the state of nationality of the individual or state of registration of the ship or aircraft, then a hostile intent towards another state becomes discernable, thus engaging the international relations between the two states. This issue, including the prospect for a mistaken use of force (which, as Roscini notes is 'a situation that is particularly likely in the cyber context') [11] would have been a welcome addition to the analysis and discussion here. Of course, problems of evidence in establishing this *mens rea* element will necessarily be present.

In the section of the chapter on self-defence Roscini on the whole provides an excellent survey of the relevant law and its applicability in the cyber context. In doing so, Roscini adopts the 'scale and effects' standard in distinguishing uses of force from armed attacks giving rise to a response in self-defence.[12] Yet, while this standard has been laid down by the International Court of Justice, and a common sense approach would dictate that there must at least be some distinguishing elements between the two types of force which should, in theory, give rise to very different responses by a victim state, it is not clear that this has been witnessed in practice. Indeed, states have resorted to self-defence in varying circumstances, not necessarily solely in response to those attacks possessing what one would consider scale, effects or gravity. In addition, a former president of the ICJ, Rosalyn Higgins, has subscribed to the view that the legality of an action in self-defence is more about the proportionality of the forcible response, than the scale and effects of the use of force giving rise to it.[13] Although it is easy to see the policy aspects behind trying to restrict the possibility for a forcible response,[14] addressing nuances such as this in practice would have been a nice addition to the book.

There were other aspects in the book's discussion of self-defence where perhaps a more nuanced approach in assessing state practice might have been warranted. One such area is in the discussion on non-state actors. Given that such actors may well be behind many cyber attacks today and those in the future, Roscini duly gives attention to this

[11] Roscini (n 6) 76.
[12] ibid, eg at 75.
[13] R. Higgins, *Problems and Process: International Law and How We Use It* (Clarendon Press, 1994) 250-251.
[14] As Christine Gray has set out. See C Gray, *International Law and the Use of Force* (OUP, 2008) 147-148.

issue. In contrast to his position noted above regarding whether non-state actors can be responsible for a use of force, Roscini adopts the position – correctly in the current reviewer's view – that non-state actors can by themselves be responsible for an armed attack, as opposed to a victim state having to pin the armed attack carried out by a non-state actor upon another state under the law of state responsibility in order to justify a response in self-defence. However, in Roscini's view, before doing so it must be demonstrated that the host or harbouring state is either 'unable or unwilling' to take action against the non-state actors, thus making the action in self-defence justifiable under the customary 'necessity' criterion. Two nuances might have been drawn out in this respect by the author. First, and as Roscini continues, '[t]he requirement of necessity also entails that the defensive reaction must be directed exclusively against the non-state actors when it is only them that are responsible for the armed attack, and not also the harbouring state.'[15] The problem here is that state practice paints this is something of a grey area. Yes, much recent practice would seem to support Roscini's position that any action in self-defence must be limited to the non-state actors themselves. But it was also not that long ago that following the events of 11 September 2001 the US's position of bundling in the harbouring state with the non-state actors for the purposes of self-defence, which was witnessed in practice in *Operation Enduring Freedom* in Afghanistan in 2001, was overwhelmingly endorsed by virtually the entire international community. Roscini does not acknowledge this, and some of the remnants felt in state practice from this episode, and what the consequences might be of this 'harbouring' standard in the cyber context. Given that there will be even greater difficulty in distinguishing non-state actors from their harbour states than in the kinetic context, this would have been an interesting discussion.

Furthermore, while a commendable aspect of Roscini's book is the extent to which it attempts to utilize the practice and views of states in supporting the positions adopted, this was not the case in the book's adoption of the applicability of the 'unable or unwilling' standard. Indeed, while the discussion here could be read as accepting this standard as *lex lata*, the only support advanced in support of its utilization in the

[15] Roscini (n 6) 86.

cyber context is that of the US.[16] The general absence of support in the *opinio juris* of states has been one of the key problems to date in the discussions regarding this standard. As such, Roscini's claim that '[t]he application of the unable or unwilling standard … in the cyber context finds support in … state practice'[17] is far from substantiated. If Roscini wished to paint a fully accurate picture of the *lex lata* in regards to this area of the *jus ad bellum*, some qualifications would have been welcome in his apparent support for this standard.

Overall, the sections of Roscini's book on the *jus ad bellum* cyber aspects are well-written, engaging, and thoroughly researched. They will also be accessible to non-lawyers, which makes this book particularly appealing. It is not easy to pick apart rules that were designed and adopted in a different era before the prospect of cyber attacks were even conceivable, and accurately apply them at a time before cyber uses of force have become a concrete reality, and overall Roscini has done a commendable job. With perhaps a few minor exceptions, the book establishes that the contemporary *jus ad bellum* rules are ready in theory for the challenge of cyber uses of force. Whether this will be borne out in practice, however, awaits to be seen.

[16] ibid 86-87.
[17] ibid 86.