Chapter 5

The Regulation of Cyber Warfare under the *Jus ad Bellum*

James A. Green

International Law

Introduction

Most interaction between cyberspace and 'the law' occurs at the national level (Remus, 2013: 180). This is largely appropriate, as a significant proportion of such actions either involve criminal activity by individuals or private groups for personal gain (Roscini, 2014: 4) or take the form of a plethora of other 'non-criminal' activities in cyberspace (commercial transaction, advertising, defamation, etc.) that are all best regulated by domestic law. Cyber warfare, however, is inherently 'international' in nature, and thus requires an international legal response (Morth, 1998: 581). Yet, at present, there are no specific rules of international law governing the interstate use of cyber force. The only treaty regulating cyberspace *per se* remains the 2001 Budapest Convention on Cybercrime, and there are no treaties at all that deal directly with cyber warfare, nor are there any specific provisions of customary international law on the topic (Shackelford, 2009: 219).

The first notable works in the international law literature relating to the problem of cyber warfare appeared in the late 1990s (e.g., Morth, 1998; Schmitt, 1999; Sharp, 1999), at a time when the discussion over how to deal with interstate cyber-attacks within the framework of international law was largely hypothetical. By the late 2000s, the need for international law to engage with the issue became rather more urgent, particularly following the various Distributed Denial of Service (DDoS) attacks directed at Estonia in 2007 (a series of attacks discussed in detail in both chapters 1 and 4 of this volume). Nonetheless, international law has not caught up with this modern form of conflict: cyber warfare, at least at first glance,

remains insufficiently regulated by the law. On this basis, cyber warfare has been described as existing 'in a legal netherworld' (Hoisington, 2009: 440; see also discussion by Danny Steed in Chapter 4 of this volume).

Having said this, in contrast, the recent *Tallinn Manual on the International Law Applicable to Cyber Warfare*, prepared by an international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (2013: 5), argues that '[t]his uncertainty does not mean cyber operations exist in a normative void.' Indeed, the *Tallinn Manual* represents the majority view in the literature on this point, which is that the existing rules of international law are applicable to the threat posed by cyber warfare (see, e.g, Harrison Dinniss, 2012; Benatar, 2009: 395; Schmitt, 2013: 176-177; Tubbs *et al.*, 2002: 15).

This chapter evaluates the potential for legal regulation of the resort to cyber warfare between states under the '*jus ad bellum*'. This branch of international law – also called the law on the use of force – deals with the initial decision as to whether or not to use military force: the question of *when* the use of force by a state may be lawful, if at all. This is as opposed to the legal regulation of the conduct of cyber hostilities under the '*jus in bello*': the question of *how* conflict must be conducted once force has already been initiated (for further discussion of this distinction, see Waters and Green, 2010: 292). The application of the *jus in bello* to cyber warfare is examined by Heather A. Harrison Dinniss in Chapter 6.

In the context of the *jus ad bellum*, the main approach in the existing scholarship to resolve the lacuna left by the lack of specific international legal regulation has been to try to adapt the existing prohibition of the use of force under Article 2(4) of the United Nations (UN) Charter to cover cyber warfare. Debate in the literature has therefore largely concerned whether

cyber warfare falls within the scope of Article 2(4). The first part of this chapter sets out in some detail this debate as to the correct interpretation of Article 2(4) with respect to cyber warfare. The application of Article 2(4) here is obviously somewhat anachronistic: cyber-attacks were not considered by those who drafted the Charter in 1945 (Buchan, 2012: 212-213). It has been traditionally agreed that the prohibition of the use of force in Article 2(4) includes physical armed force, but excludes non-physical acts, such as economic or political coercion. The question is therefore whether the modern phenomenon of cyber warfare should be correctly analogised with physical violence or with 'non-physical' methods of interstate coercion. However, as 'cyber warfare' covers a huge range of actions, it is not a simple matter to analogise it – wholesale – to other 'types' of intervention. It is, thus, extremely difficult to determine whether Article 2(4) clearly encompasses (or clearly *excludes*) the concept of aggressive cyber operations (Kodar, 2009: 138).

This chapter goes on to argue that the 'Article 2(4) debate' often misses the fact that an act of cyber warfare can be considered a breach of a different legal rule: the principle of non-intervention. This principle is a rule of customary international law, rather than being found in the UN Charter, but it is wider in scope than the prohibition of the use of force: for example, it covers economic and political coercion, in addition to physical military attacks. Therefore, irrespective of the applicability of Article 2(4), resort to cyber warfare will in most cases be unlawful under the principle of non-intervention. Yet, there are good reasons why the legal debate has focused upon Article 2(4) and has so often overlooked the principle of non-intervention: most importantly, this is because the principle is a demonstrably 'weaker' norm of international law, which often struggles to restrain state behaviour.

Next, this chapter considers some of the issues in applying either the prohibition of the use of force or the principle of non-intervention to cyber warfare. In particular, it is argued that there are significant problems in attributing aggressive cyber actions to a state, as a matter of either law or fact. The chapter concludes by reflecting upon proposals for a bespoke cyber warfare treaty and argues that – given the unlikelihood of such a treaty being agreed upon any time soon – the debate should be reoriented to focus on another existing international legal obligation: the duty to *prevent* cyber-attacks, or what is sometimes called the 'duty of duty diligence'.

The 'Article 2(4) Debate' on Cyber Warfare

The Prohibition of the Use of Force

Article 2(4) of the UN Charter has long been at the centre of the legal literature on cyber warfare. It is the key legal provision setting out the prohibition of use of force in modern international law:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.

The prohibition contained in Article 2(4) is unquestionably one of the most fundamental rules of the UN system and is commonly referred to as a 'cornerstone' provision (Dinstein, 2002: 99; Harrison Dinniss, 2012: 40). Additionally, alongside its inclusion in the Charter, the prohibition is also a norm of customary international law, meaning that even non-UN member states (of which there are, in any event, very few), are similarly bound (Bothe, 2003: 228). As such, the prohibition binds all the states of the world.

The prohibition is also a relatively simple rule on its face: Article 2(4) bans the use of force by one state against another (as does the parallel prohibition under customary international law). There are, of course, exceptions to this rule that are found elsewhere in the Charter. Article 51 provides for a right to use force in self-defence and, under Articles 39-42, the UN Security Council can authorise the lawful use of force. Nonetheless, the general rule is that force is prohibited.

It is additionally worth noting that the majority view is that the prohibition of the use of force is a rule of a 'peremptory', or *jus cogens*, nature (see, e.g., Orakhelashvili, 2006: 50). In other words, it is usually seen as having achieved a special status within the international legal system, whereby it cannot be altered or derogated from except by a newer rule of the same 'super-norm' sort (VCLT, 1969: Article 53). Rules of international law that have acquired this special peremptory character are extremely rare, and the present author has elsewhere questioned whether the prohibition of the use of force has in fact achieved *jus cogens* status (Green, 2011). In any event, whether or not the prohibition of the use of force is a *jus cogens* norm or not, no state in the world argues against its existence and general applicability.

Viewing cyber warfare through the prism of Article 2(4) presents an immediate problem, however. While a few writers have simply assumed that the prohibition of the use of force covers acts of cyber warfare (Graham, 2010: in general, but particularly at 88), it is, in fact, far from straightforward to apply Article 2(4) to cyber-attacks.

The 'Qualifying Terms' in Article 2(4)

A preliminary point of concern in relation to the applicability of Article 2(4) to cyber warfare is whether there is a loophole in the wording of Article 2(4) through which cyber-attacks might squeeze. The provision prohibits the 'use of force *against the territorial integrity or political independence of any state*' (emphasis added). On the basis that the prohibition of 'force' is qualified by this language, it may be argued that certain uses of force may not go 'against the territorial integrity or political independence' of the victim state and, thus, would not be covered (Gray, 2008: 31-33). If this interpretation is correct, it could be a particularly acute issue within the context of cyber warfare, which will likely not physically involve territorial incursion in the traditional sense (Schmitt, 1999: 888). For example, the DDoS attacks on South Korea and the United States in July 2009, for which it was alleged that North Korea was responsible, affected thousands of computers in the two states concerned. However, the attack did not involve territorial incursion into either state, at least in a physical sense: the botnet of hacked computers that was the source of the attacks was remotely activated (Sudworth, 2009). One might perhaps argue on this basis that the attacks in question were not 'against the territorial integrity' of either South Korea or the United States.

However, it is actually fairly clear that the prohibition of the use of force was always meant to be comprehensive in nature, in the sense that any and all uses of force fall under its purview (Franck, 2002, 12). The 'qualifiers' in Article 2(4) were intended by the Charter's drafters to be demonstrative of its all-encompassing scope, not exclusionary in this way (see UNCIO vol. VI, 1945: 334-335). It is worth remembering that the terms 'territorial integrity' and 'political independence' are presented in the alternative in Article 2(4) by the use of the word 'or'; it is rather difficult to conceive of a forcible state action, taken without the consent of the state against which it is directed, that does not in some way act against *either* that state's territorial integrity *or* its political independence. Moreover, as the *Tallinn Manual*

(2013: 43) notes, even if one could identify a forcible action of this sort, Article 2(4) also includes the 'catch all' phrase 'or in any other manner inconsistent with the Purposes of the United Nations'; and one of the purposes of the UN is the peaceful settlement of international disputes (UN Charter, 1945: Article 1). The majority view, therefore, is overwhelmingly that *all* uses of force fall foul of the prohibition.

The Meaning of 'Force'

While it can be said that all 'uses of force' are covered by Article 2(4)'s prohibition, this begs a much more problematic question for the regulation of cyber warfare under the *jus ad bellum*: do interstate cyber-attacks qualify as 'uses of force' in the first place? The primary debate in the international law literature, which has raged since the late-1990s, is whether a cyber-attack equates to 'force' as per Article 2(4). If so, then such action is prohibited by that article; if not, rather obviously, it falls outside of its reach. Unfortunately, Article 2(4) itself does not define what it means by 'force'. Long before the advent of cyberspace, states and scholars therefore debated what was included in the term and what was not. In particular, the question was whether actions such as economic and political coercion should be considered 'force' for the purposes of Article 2(4), or whether the provision is restricted to what might be termed '*armed* force' (i.e., troop movements, gunfire, explosives and so on) (on this debate, see Silver, 2002: 80-82).

The starting point for interpreting the meaning of provisions of a treaty is to consider the 'ordinary meaning to be given to the terms of the treaty in their context and in light of their object and purpose' (VCLT, 1969: Article 31). In other words, international law takes a 'common-sense' approach to determining the meaning of terms found in a treaty. A reading of Article 2(4) based on the ordinary meaning of its wording might well suggest that actions

beyond just ‘armed force’, such as coercive economic action, should be covered by its prohibition. It is certainly arguable that aggressive economic sanctions, for example, are ‘forcible’ under a normal understanding of the word.

Elsewhere in the UN Charter the qualified term ‘armed force’ is explicitly used (e.g., in the Preamble, as well as in certain articles in Chapter VII). Some scholars have pointed this out in support of a wide understanding of ‘force’ as used in Article 2(4). This is on the basis that – by deciding to use the term ‘force’ *in abstracto* in that article, but ‘armed force’ elsewhere – the drafters intended Article 2(4) to cover actions beyond just armed force (see, e.g., Benatar, 2009: 382). Otherwise, those taking this stance argue, why was the term ‘armed force’ not simply used consistently throughout the Charter?

Other scholars, however, have used the presence of the term ‘armed force’ elsewhere in the Charter to support an entirely contradictory, narrower understanding of force as being restricted to ‘armed force’ only. Harrison Dinniss (2012: 41-42), for example, argues that ‘force’ is also used in an unqualified form in Article 44, an article that refers to the decision of the UN Security Council ‘to use force’. Article 44 is directly linked to the powers of the Council to use all measures necessary to avert threats to international peace and security in Article 42, in contrast to its power to authorise ‘measures *not involving the use of armed force*’ in Article 41 (emphasis added). This strongly indicates that the unqualified use of the term ‘force’ in Article 44 should be read as meaning ‘armed force’ and thus, by analogy, so perhaps should the unqualified use of the same word in Article 2(4).

Also potentially supporting a more restrictive reading of ‘force’ in Article 2(4) is the fact that the ‘ordinary meaning’ of terms in a treaty must be interpreted in the context of the

broader principles and purposes of the convention in question (VCLT, 1969: Article 31). It is evident from reading the Preamble to the Charter that its core object and purpose is to limit the use of military force between states (key goals mentioned therein being to 'save succeeding generations from the scourge of war' and 'to ensure…that armed force shall not be used, save in the common interest'). As such, reading the word 'force' in the context of the goals of the Charter might similarly indicate that it should be limited to armed force (Buchan, 2012: 216).

These various attempts at interpretive gymnastics in the literature are ultimately inconclusive (Roscini, 2010: 104). In the end, Article 2(4)'s 'ordinary meaning' can be read as pointing in either direction. As such, a secondary method of treaty interpretation, when the ordinary meaning is not entirely clear (as is the case here), is to examine the *travaux préparatoires* of the treaty in question: that is, the debates over its drafting involving the drafters themselves (VCLT, 1969: Article 32). When one considers the *travaux préparatoires* of the Charter, it is evident that states at the time took a restrictive view of what they meant by 'force', in that they saw acts of economic or political coercion as falling outside of the concept.

Various actions that were of concern in 1945 and that could have been viewed as being 'forcible' – such as economic or political coercion – were explicitly excluded from the generally agreed upon and understood meaning of 'force' in Article 2(4) in 1945. There were a number of proposals advanced by states in 1945 to include such actions within the scope of the article. The most famous of these was a proposal by Brazil (UNCIO vol. VI, 1945: 334, 558-559), but similar suggestions were also made by Ecuador (UNCIO vol. III, 1945: 399,423; UNCIO vol. VI, 1945: 561-562) and Iran (UNCIO vol. VI, 1945: 563). All such proposals were firmly rejected by the vast majority of other states at the time (UNCIO vol.

VI, 1945: 720; see also Benatar, 2009: 383-384). Reference to the recorded views of the state drafters of the UN Charter, therefore, clearly indicates that the provision was originally intended to cover *armed* force only.

Perhaps more importantly, the drafters' interpretation of 'force' has been repeatedly confirmed in state practice over subsequent years. State practice is the core element of customary international law (Akehurst, 1974), and it is also a factor in determining the correct contextual development of the meaning of treaty provisions (VCLT, 1969: Article 31 3(b)). The restrictive view of the meaning of 'force' subsequently taken by states was particularly evident in the drafting of the UN General Assembly's Declaration on Friendly Relations (UN Doc. A/RES/25/2625, 1970). In that context, states formally debated whether 'economic, political and other forms of pressure against the territorial integrity or political independence of any state were illegal uses of force' (UN Doc. A/7619, 1969: para. 86). While a small number of states argued in the affirmative, the general view of the plenary sessions was clearly that they did not (see UN Doc. A/7619, 1969: paras. 86-93). A similarly restrictive understanding of 'force' can also be seen in the UN General Assembly's Definition of Aggression, adopted in 1974 (UN Doc. A/RES/3314, 1974).

Reflecting the position of states, the vast majority of writers now argue – and have done since at least the 1970s – that 'force' in Article 2(4) means 'armed force' and, thus, excludes such activities as economic or political coercion (for the classic expression of this view, see Farer, 1985). Despite ambiguities in the wording of Article 2(4), therefore, for decades there has been little question that economic and political coercion are excluded from the prohibition of the use of force. Armed force is covered, and economic and political 'force' is not.

The Meaning of 'Armed Force'

Simply put, by the 1970s, it was clear: force means armed force. Which seems simple enough until one asks: what counts as armed force? Specifically, are cyber-attacks 'armed force', or are they 'non-armed force'? The same textual ambiguities that plagued early interpreters of the Charter in relation to actions like economic coercion today exist within the context of cyber warfare. Those considering the application of the *jus ad bellum* to the emerging concept of technological force therefore began by trying to analogise such actions to existing forms of 'force', where agreement had already been reached as to Article 2(4)'s (in)applicability.

Analogy to the Nature of the Attack

The traditional way of defining the distinction between 'armed force' and 'other force' was based on armed force being an action of an 'explosive [nature, involving] shockwaves and heat' (noted by Brownlie, 1963: 362). In other words, the distinction was seen as being based upon the physical, kinetic *nature* of the force used. Cyber warfare does not, of course, involve such kinetic, physical action. The nature of (or what might be called the 'act of launching') the majority of cyber-attacks will have rather more in common with economic attacks (Goldsmith, 2013: 133). On this basis, in the early literature on cyber warfare, some writers argued that cyber aggression should rightly be analogised to economic or political coercion and, thus, excluded from the Article 2(4) prohibition (e.g., Kanuk, 1996: 289). In contrast, others took the view that cyber warfare has more, or certainly *can have* more, in common with the destruction caused by physical attacks, and so should be analogised to conventional warfare (e.g., Morth, 1998: 591). Analogising the nature of the force used simply brought the debate to another impasse.

Analogy to the Effects of the Attack

Long before the birth of the Internet, concerns had already been advanced that the traditional approach to understanding what was covered by the notion of 'armed force' for the purposes of Article 2(4) was insufficient. Most famously, Brownlie (1963: 362) took the view that a distinction based on the *nature* of the action missed a crucial point, namely its *effects*. Brownlie had in mind actions such as the use of 'bacteriological, biological and chemical devices', rather than cyber warfare, but the point he made is today equally relevant in the cyber context. The use of biological, chemical and radiological weapons can ultimately have devastating *physical effects* without necessarily being 'kinetic actions' in themselves (Schmitt, 2010: 154). Yet, even when Brownlie was writing in the 1960s, it was already unquestionable that states considered the use of such weapons by one state against another to be a breach of Article 2(4) (Roscini, 2010: 106). As such, Brownlie argued that the distinction should be – or, rather, already *was* – one based on the effect of an attack and not its nature.

It is clear that a majority of writers in the field have adopted an 'effects-based' approach to the meaning of 'force' in Article 2(4), including in the context of cyber warfare (e.g., Goldsmith, 2013: 133; Haslam, 2000: 165; Kodar, 2009: 139; Silver, 2002: 84-92). Certainly, analogising the effects of a cyber-attack seems to better encapsulate the wide spectrum of activities that can be considered 'cyber warfare' than the all-or-nothing categorisation approach of referencing the nature of force used. An 'effects-based' understanding of what constitutes 'force' for the purposes of Article 2(4) provides a more nuanced way of assessing whether cyber warfare qualifies. Instead of analogising cyber warfare to the nature of an existing action (a near impossible task as cyber-attacks have their own unique nature), one can instead look at the *results* of a cyber-attack and compare this to

the *results* of other types of action. Taking this approach, it would seem that cyber-attacks that have notably injurious consequences would constitute 'force' and, thus, would be a breach of Article 2(4); interstate cyber aggression resulting in less severe damage would not.

However, despite its widespread adoption in doctrine, problems still exist with a test based on the effects of a cyber-attack. One such issue is that by focusing on effects, breaches of the law may in part be determined by the 'durability' of the victim state (Nguyen, 2013: 1124). More powerful states are likely to be better able to defend themselves against cyber aggression, either because their more advanced cyber security programmes can stop an attack prior to its having had any 'effects' at all, or because the infrastructure of the state is better able to deal with the implications of a cyber-attack that does in fact 'hit' (meaning that where one state might suffer devastating effects, another may suffer far less damage from the same sort of attack). If 'effects' are what matter, an attack that might not be considered as falling within the scope of Article 2(4) if directed at a powerful state may incongruously qualify if the victim was a weaker one.

A related concern is that a test based on effects is *reactive* to force rather than *prescriptive*. One cannot know exactly what is prohibited, or – more pertinently – what responses may be available in relation to a violation, until after it has occurred. This is a concern somewhat amplified in the cyber arena by the potentially instantaneous nature of cyber-attacks (Hoisington, 2009: 452).

Perhaps most problematically of all, the effects approach leads the discussion down yet another interpretive rabbit-hole. To the 'effects' of what exactly are the effects of cyber warfare to be analogised? Or, to put it rather more simply: where is the threshold? Writing

in the 1960s, Brownlie (1963: 362) indicated that the weapon used needed to cause 'destruction to life and property' to qualify as 'force'. More recently, and specifically in relation to cyber warfare, Dinstein (2011: 88) has argued that 'the term "force" in Article 2(4) *must denote violence*. It does not matter what specific means – kinetic or electronic – are used to bring it about, but the end result must be that *violence occurs*' (emphasis added).

Under such an understanding, a cyber-attack that results in physical damage or physical violence qualifies, and all other cyber-attacks do not. The sorts of 'cyber doomsday scenarios' that are set out in the literature with increasing regularity, such as the use of computers to melt down a nuclear power plant, turn a state's unmanned military drones against it, drop its planes form the sky and so on (see, e.g., Clarke and Knake, 2010: 64-68), would clearly be covered. The effects of such actions would equate to, and could even exceed, the physical consequences of a use of traditional military force. Indeed, even below the level of such ultimate doomsday cyber-attacks, actions like the use of the Stuxnet virus against Iran in 2010 would also probably qualify because Stuxnet led to physical damage to property (Buchan, 2012: 219-221. For detailed discussion of the Stuxnet virus, see chapters 1 and 4 of this volume).

However, the vast majority of interstate cyber-attacks, at least of those that have so far transpired, would probably not meet Dinstein's 'occurrence of violence' version of the effects-based test for inclusion in the Article 2(4) prohibition. Attacks such as those against Estonia in 2007, or Georgia in 2008 (discussed in Chapter 1 of this volume), can be devastating in many ways, of course, but only in terms of disruption of infrastructure and economic loss (Nguyen, 2013: 1127-1128). In instances where no physical destruction

results the consequences of the cyber aggression would be analogised to the effects of economic force, which, as has been discussed above, is not covered by Article 2(4).

Dinstein's approach has thus been criticised by a number of writers on the basis that it is 'under inclusive' (e.g., Handler, 2012: 229). Looking only at violent, physical effects is too limiting, it has been argued, as this excludes too many cyber-attacks from the reach of Article 2(4) (Antolin-Jenkins, 2005: 155). For example, a cyber-attack 'that corrupts data on a stock exchange and which in turn causes widespread economic harm but no direct physical damage' would have devastating effects but would not be considered a breach of Article 2(4) (Goldsmith, 2013: 133). Thus, some – still following an effects-based approach – argue that cyber-attacks that are particularly severe *in spite of not leading to physical destruction* should be included (e.g., Waxman, 2011: 435-436).

The counter-argument to this, perhaps inevitably, is that economic actions can also have devastating, albeit non-physical, effects. Purely economic attacks are, as has been noted, excluded from Article 2(4) *per se*, however severe their consequences. To allow certain acts of cyber warfare to be included in Article 2(4)'s scope on the basis that their (non-physical) effects were particularly devastating would be to arbitrarily ignore the fact that equally injurious actions have long been considered excluded. This could lead to a slippery slope down which any and all 'forcible' action would be included in the prohibition (Hoisington, 2009: 447, at note 64). It can be argued that the strength of Article 2(4) is that it is reserved for the very worst forms of force – physical military action between states – and that it would devalue its normative weight to allow other actions to be included (e.g., Banks, 2013: 163). Indeed, the present author has suggested elsewhere that the debate over whether cyber-attacks

with non-physical consequences fall within the prohibition's scope could undermine its apparent *jus cogens* status (Green, 2011: 239-240).

The 'Schmitt Criteria'

The most famous attempt to remedy this uncertainty, by providing some guidelines and *principled* distinction to this interpretive minefield, is a set of criteria developed by Michael Schmitt (1999: 914-915). Schmitt may perhaps be considered the 'father' of the international legal scholarship on cyber warfare, and his criteria have been adopted by numerous scholars writing on the topic (e.g., Moore, 2013: 237; Murphy, 2013: 313; Dunlap, 2011: 85-86; Papain, 2011: 40-45; Remus, 2013: 182). The commentary to the NATO-commissioned *Tallinn Manual* (2013: 48-51) similarly references them with approval (although this is perhaps not especially surprising given that Schmitt was the director of the *Tallinn Manual* project). Schmitt has also recently re-stated his criteria in his own work (Schmitt, 2011: 576; Schmitt, 2010: 155-156) and has noted that they have 'generally withstood the test of time' (Schmitt, 2011: 575).

The Schmitt criteria are: 1) *Severity* (the effects must be particularly severe – this will most commonly involve physical damage but is not necessarily restricted to it); 2) *Immediacy* (the speed of the cyber-attack should preclude resort to a peaceful response); 3) *Directness* (the consequences are clearly caused by the cyber-attack); 4) *Invasiveness* (the effects should be felt within the target state and be notably invasive); 5) *Measurability* (it should be possible to measure the scale and effects of the attack); and 6) *Presumptive Legitimacy* (cyber-attacks should be presumed to fall outside of the scope of Article 2(4) unless their effects can be equated to those of other prohibited actions, most notably the use of traditional military force).

These criteria give a comparatively detailed, formalised way of justifying why one cyber-attack is included and another is not, because they break down 'many of the underlying characteristics that define an act as armed force' (Nguyen, 2013: 1123). They undoubtedly provide a useful starting point from which to undertake analysis of the lawfulness under Article 2(4) of any given cyber-attack, and the adoption of the criteria by scholars has helped to inject a degree of much needed coherence into the possible regulation of cyber-attacks by the *jus ad bellum*.

Schmitt has noted that 'severity is self-evidently the most significant factor for the analysis' (Schmitt, 2011: 576): in other words, 'effects' remain his primary benchmark. However, instead of focusing on 'severity' alone – which may to an extent be in the eye of the beholder – the criteria combine this initial criterion with other factors indicative of the overall 'intention' and 'consequentiality' of the attack in question, thus giving a more nuanced means of assessment. It is also worth noting (*Tallinn Manual*, 2013: 51-52) that the criteria are presented both as being non-exhaustive (meaning other factors can be taken into account if they can help analysis) and as operating 'in concert' (meaning that an action need not meet *all* of the criteria, just that reference to them, taken together, provides a strong indication of whether or not a cyber-attack falls within the prohibition).

Perhaps the most important point of departure from many other analytical approaches is that the criteria potentially allow for certain cyber-attacks with severe but non-physical consequences to qualify as a breach of the prohibition of the use of force (*Tallinn Manual*, 2013: 52). They do so not just by reference to damage caused, however, but by distinguishing such actions from other forms of coercion in a principled way, based upon

various factors indicating what 'sort' of action any given cyber-attack really is. On this basis, most non-physical cyber-attacks would probably be excluded, but not all of them.

Extremely helpful as they are, however, it is important to keep in mind that the Schmitt Criteria *are not law*. Even the impressive *Tallinn Manual*, where they have recently appeared, is not a binding legal document but a set of suggested guidelines prepared by experts (Roscini, 2014: 31). The writings of scholars can be considered an interpretive, secondary source of international law (Statute of the ICJ, 1945: Article 38.1(d)), but they should never be considered formal 'law' as such. Similarly, while there are some suggestions that states have referred to the criteria on a few occasions (see, e.g., Remus, 2013: 183), there is nowhere near enough evidence to conclude that states have adopted the criteria with sufficient consistency and regularity for them to have crystallised into customary international law.

It is also worth noting that Schmitt's criteria have come under some academic criticism, particularly on the basis that the last of them – 'presumptive legitimacy' – is self-referential (Barkham, 2001: 85-86; Hoisington, 2009: 452). This criterion bases its test for the legitimacy of cyber force on whether it is analogous to other actions that are considered to be legitimate. This is clearly a circular criterion, which takes things perilously close to previous debates analogising cyber force to other 'forcible' actions. Indeed, other scholars have questioned whether the criteria as a whole are simply another version of the existing 'categorisation-by-analogy' debate. It could be argued that the criteria merely provide *more* ways of analogising cyber warfare to other types of force, without taking sufficient note of the unique nature of cyber operations (see, e.g., Harrison Dinniss, 2012: 63).

Perhaps the most notable criticism that can be levelled at the criteria is that, for all the increased certainty that they provide, they are still ultimately rather vague (Benatar, 2009: 391). For example, Nguyen (2013: 1123-1124) notes that, in 2011, Schmitt applied his own criteria to the 2007 attacks against Estonia and concluded that five of his six principles were met. On this basis, Schmitt concluded that the DDoS actions against Estonia constituted a breach of the prohibition of the use of force (Schmitt, 2011: 577). Yet, Nguyen himself convincingly applies the criteria to the Estonia attack in a manner that indicates an entirely contradictory conclusion: i.e., he demonstrates that the criteria can credibly be applied to Estonia so as to support the view that it did *not* qualify as a use of force. Nguyen thus concludes that '[t]hese two contradictory interpretations of the same cyber attack demonstrate that Schmitt's six criteria can be too easily manipulated to create results supporting the geostrategic goals of the nation conducting the enquiry' (Nguyen, 2013: 1124). Schmitt himself has conceded that '[t]he criteria are admittedly imprecise' (Schmitt, 2011: 577).

Ultimately, the Schmitt criteria provide helpful guidance, but they are not 'the law', at least not yet; they are the thoughts of just one scholar (however influential they have been). The criteria are also arguably insufficiently precise and not 'cyber-centric' enough. The present author would thus agree with Benatar (2009: 391) that '[a]lthough Schmitt's model remains the most refined theory to date for addressing the legality of cyber attacks under the *jus ad bellum*, this is not to say that it has resolved the issue definitively'. The Schmitt criteria are not 'the answer' to the issue of cyber warfare and the *jus ad bellum* but are, rather, an important instance of interpretative legal triage.

The Forgotten Rule: The Principle of Non-Intervention

The Nature of the Principle and its Applicability to Cyber Warfare

The exhaustive and exhausting debate over the applicability of Article 2(4) is the focus of much of the legal literature on cyber warfare, which is why it has formed a significant part of this chapter. However, Article 2(4) is not the only rule of international law that is applicable to the resort to cyber warfare. As Russell Buchan (2012: particularly at 221-226) has importantly discussed, just because a cyber-attack fails to meet the test to constitute a breach of Article 2(4) (assuming that it can be agreed what this test is) *does not mean that it is lawful*. There is another rule of international law – the principle of non-intervention – that most acts of cyber warfare will fall foul of. Buchan (2012: 221) notes that many international law commentators 'have focused exclusively on Article 2(4), failing to consider the wider customary principle of non-intervention.'

The principle of non-intervention is not provided for as such in the UN Charter (other than in Article 2(7), which specifically requires *the United Nations* to refrain in intervening in the domestic affairs of states). The wider principle of non-intervention that applies to states *per se* can instead be found in customary international law (Schmitt, 2014: 143-145). This customary law principle has been confirmed by the International Court of Justice (ICJ) (*Nicaragua* case, 1986: para. 205), but is perhaps most notably set out in a number of declarations adopted by the UN General Assembly, which – while non-binding in themselves – reflect, and have contributed to the formation of, the binding customary international law rule (see, e.g., UN Doc. A/RES/25/2625, 1970; UN Doc. A/RES/31/91, 1976: particularly paras. 1, 3 and 4; UN Doc. A/RES/36/103, 1981: paras. 1 and 2). For example, the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty (UN Doc. A/RES/20/2131, 1965: paras. 1 and 2) holds that:

> No state has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other state…No state may use or encourage the use of economic, political or any other type of measures to coerce another state in order to obtain from it the subordination of the exercise of its sovereign rights or to secure from it advantages of any kind.

The principle of non-intervention means that one state cannot intervene in the domestic affairs of another state, so as to coerce it to act in a certain way. As such, both 'forcible' (in the sense of Article 2(4)) and 'non-forcible' coercive measures (such as economic and political interference) are prohibited by the principle. All uses of force in violation of Article 2(4) are also considered prohibited 'interventions', but the non-intervention principle is wider: not all unlawful interventions also breach Article 2(4). Thus, instances of coercive economic or political pressure are contrary to the non-intervention principle but not the prohibition of the use of force.

In the cyber context, it is likely that most interstate cyber-attacks – *including* those that fall short of being considered a breach of Article 2(4), whether based on the Schmitt criteria or other interpretative approaches – will be considered breaches of the principle of non-intervention. Admittedly, not all interstate cyber operations will violate the principle (Haslam, 2000: 163). For example, 'cyber espionage and cyber exploitation operations lacking a coercive element do not *per se* violate the non-intervention principle' (*Tallinn Manual*, 2013: 44). Only those cyber-attacks that are of a coercive nature (aiming to 'subordinate' another state in relation to matters within the domestic competence of that state) will breach the principle of non-intervention (Roscini, 2014: 65). However, while not

all cyber operations will qualify, acts of cyber *warfare* – as defined in the Introduction to this volume – will in virtually all instances.

Why has the Debate Overlooked the Principle of Non-Intervention?

It is true, as Buchan (2012: 221) argues, that many scholars have entirely overlooked the principle of non-intervention in their analysis of cyber warfare. Barkham (2001: 94), for example, argues that, if found to fall outside of the scope of Article 2(4), 'IW [information warfare], like economic sanctions, *would become a legal act* under international law' (emphasis added). This, of course, entirely misses the fact that neither coercive economic sanctions nor cyber-attacks are 'legal acts' at all: they are breaches of the principle of non-intervention.

However, it is worth noting that the principle of non-intervention has not been entirely ignored in the literature. A number of writers do in fact take note of the principle, and further conclude that most acts of cyber warfare are likely to constitute a breach of it (e.g., Roscini, 2014: 63-65; Harrison Dinniss, 2012: 73; Hathaway *et al.*, 2012: 843; Haslam, 2000: 160 and 163-164; Kodar, 2009: 140; Schmitt, 1999: 123). Yet, as Buchan (2012: 221) points out, 'these authors do not engage in a sustained analysis of how the non-intervention principle may apply to cyber attacks'. Consideration of the principle in the context of the legal regulation of cyber warfare, to the extent that it has occurred at all, has tended to be cursory.

One might well question why this is the case. The principle of non-intervention is wider in scope than the prohibition of the use of force, which means that it is much easier to conclude that the majority of interstate cyber-attacks are covered. If cyber-attacks are ultimately unlawful irrespective of the applicability of Article 2(4), why has the legal debate focused so

much on whether such attacks qualify as a use of 'force' for the purposes of that article? After all, a breach of international law is a breach of international law: the principle of non-intervention already exists and, 'on paper' (using that term figuratively, given that the principle is technically a rule of customary international law and, thus, unwritten), would appear to be sufficient to regulate cyber warfare.

The Weakness of the Principle of Non-Intervention and the Special 'Weight' of Article 2(4)

The literature's focus on Article 2(4) stems, in part, from the fact that the principle of non-intervention is often seen by states and writers as a 'weaker' rule of international law. As noted, the principle is a rule of customary international law rather than a treaty-based norm. While custom and treaties are hierarchically equal in the international legal system as a formal matter (Boas, 2012: 47), rules of custom are often, quite understandably, viewed as being inherently vaguer in nature (Sullivan, 2013: 667). Perhaps more importantly, the principle of non-intervention is also a rule that has long been regularly breached by states – at least in relation to the 'non-forcible' actions that it covers – without much in the way of legal, or even political, consequence (Henderson, 2013: 642-645; Krasner, 1999: 20-25). It is a simple matter to identify numerous instances where states 'coerce' one another on matters that theoretically are within their domestic spheres: the principle is regularly breached in the day-to-day reality of international relations.

Of course, Article 2(4) is at times breached too, but the principle of non-intervention is not particularly well 'respected' by states in comparison. On this basis, Banks (2013: 170) has argued that, '[a]lthough the non-intervention norm has the potential to serve as a legal barrier to disruptive cyber intrusions, there is no indication that any state has relied on Buchan's argument, or that any court has credited it in the cyber context.' To some extent, this

overstates the matter: just because states (and courts) have not referred to the principle of non-intervention in the cyber context does not mean that it is inapplicable or that they cannot do so in the future. Nonetheless, the basic point that Banks makes is correct. Despite the fact that the principle is a 'universally accepted [legal] norm in inter-state relations' (Wu, 2000: 38), it is a rule that struggles to restrain state behaviour, and has been marginalised both in academia and practice. Its potential to effectively restrain interstate use of cyber force can, therefore, be seriously brought into question.

In contrast, Article 2(4) has special 'weight' within the international legal system. It has already been noted that the prohibition of the use of force is usually viewed as being a 'superior' rule of *jus cogens*, which means that it cannot be altered or derogated from. Whether one accepts the peremptory status of the prohibition or not, there is no question that holding that cyber-attacks contravene Article 2(4) is rather more likely to stimulate state compliance than saying that it breaches the principle of non-intervention (Morth, 1998: 590). This helps to explain why writers have focused on Article 2(4) as the core of the debate: it is a rule that is rather more likely to restrain behaviour in practice. As Schmitt (1999:909) has phrased this, violating Article 2(4) is a 'normatively more flagrant act' than violating the principle of non-intervention.

Self-Defence

Self-defence is an inherent legal right of all states, and constitutes an exception to the prohibition of the use of force in Article 2(4). In simple terms, the right allows states to lawfully use force – which would otherwise be unlawful under the prohibition – in response to an armed attack (or, some would argue, the threat of an imminent armed attack) (see generally, Tibori Szabó, 2011).

Given that the right of self-defence is an exception to the prohibition of the use of force, Article 2(4)'s prohibition acts as an important 'gateway' to the responses available to a state that has suffered a cyber-attack. Violations of the principle of non-intervention do not trigger the right to use defensive force unless they *also* constitute a prohibited use of force (Roscini, 2014: 71). Thus, those who are concerned about states being left with no viable response to a crippling cyber-attack against them must clear the first hurdle of situating such attacks within the framework of Article 2(4). This, then, also helps explain why the core debate has been so focussed on that article and not the wider principle of non-intervention.

It is important to note that not all 'uses of force' will trigger the right of self-defence. The responding state must have suffered an 'armed attack' (UN Charter, 1945: Article 51). If an 'armed attack' has occurred, then the state may defend itself with the use of force (Corten, 2010: 402-406), subject to further requirements – stemming from customary international law – that the response be both necessary and proportional (Alexandrov, 1996: 20). Just as not all 'interventions' are 'uses of force', not all 'uses of force' are 'armed attacks'. The ICJ has made it clear that an 'armed attack' is not the same as any use of force, but represents instead 'the most grave form of the use of force' (*Nicaragua* case, 1986: para. 191; *Oil Platforms* case, 2003: para. 51).

Figure 5.1 (previously employed by the present author elsewhere, Green, 2009a: 33) usefully demonstrates the relationship between the three concepts of 'armed attack', 'force' and 'intervention'. The widest concept, and outermost circle, is the notion of intervention, within which both of the other two concepts fall; the narrowest concept – armed attack – is

represented by the innermost circle, falling within the notion of force (which is itself encompassed by the concept of intervention).

<*Figure 5.1* HERE>

Given that self-defence is only triggered by the occurrence of the narrowest of these concepts – an 'armed attack' – a secondary debate within the *jus ad bellum* scholarship on cyber warfare has been whether an act of cyber warfare can constitute an armed attack, thus allowing for a defensive response (see, e.g., Antolin-Jenkins, 2005: 162-172; Waxman, 2013: 110-116; Hathaway *et al.*, 2012: 843-848; Dinstein, 2002: 100-102). In many ways this debate mirrors that concerning Article 2(4)'s applicability to cyber warfare already discussed, and so it will not be repeated in detail here. Simply put, however, the question has been whether the effects of certain cyber-attacks can be seen as being severe enough not just to be treated as 'uses of force' but also as *grave* uses of force: that is, 'armed attacks'. If so, then states can potentially respond in self-defence not just by meeting cyber-with-cyber, but by defending themselves by means of conventional military force.

The general consensus in the literature is that, at least when it comes to the 'doomsday'-type scenarios discussed above (i.e., attacks with significant physical consequences), cyber-attacks can constitute armed attacks that trigger self-defence (e.g., *Tallinn Manual*, 2013: 54-61; Graham, 2010: 90-92). As with the popular 'effects-based' approach to the interpretation of 'force' discussed above, it is argued by a number of commentators that it would undermine the purpose of the right of self-defence to hold that states have a right to respond with force to large-scale conventional attacks leading to death and destruction but not to cyber-attacks that have exactly the same results, simply based on the *method* of attack (e.g., Banks, 2013: 162).

In other words, it is commonly argued that the *raison d'etre* of the right of self-defence is to enable states to protect themselves from serious attack and, in relation to attacks with severe physical effects, it is illogical to hold that the victim state's defensive imperative is any way lessened just because the attack was perpetrated by cyber (rather than conventional) means.

Therefore, the points of controversy are, as one might expect, at the margins. In particular, what of cyber-attacks which are devastating but 'non-physical' in effect? For example, Harrison Dinniss (2012: 81) argues that only cyber-attacks that cause 'damage to property or persons of sufficient scale' can trigger the right of self-defence; in contrast, Tsagourias (2012: 231-232) takes the view that, so long as its effects are significant, a cyber-attack can be an 'armed attack' irrespective of whether those effects are 'physical'.

It quickly becomes apparent, then, that – other than it involving a somewhat higher threshold – the debate on which acts of cyber aggression should or should not be considered an 'armed attack' triggering self-defence in many ways resembles the debate that has already been examined in detail on whether and which cyber operations qualify as 'force' for the purposes of Article 2(4). Self-defence will therefore not be explored further in this chapter. It should nonetheless be noted that additional issues exist in relation to exercising the right of self-defence in the cyber context, which have all been discussed to varying degrees in the literature. These include: the difficulties in applying the customary international law criteria of necessity and proportionality; whether states can respond in self-defence to cyber-attacks perpetrated by non-state actors; whether a number of comparatively 'minor' cyber-attacks can cumulatively equate to an armed attack; and the possibility of *anticipatory* defensive force being used in response to a cyber-threat (see, e.g., Harrison Dinniss, 2012: 82-106, who discusses all of these questions).

Problems with the Existing Approaches Taken in the Literature

In previous sections, it has been shown that there exist notable problems in the ability of either Article 2(4) or the principle of non-intervention to effectively regulate cyber warfare. In relation to the former, the unique nature of cyber warfare (in terms of the *range* of activities it encompasses, amongst other things) means that it is extremely difficult to fit such actions within the scope of Article 2(4), created, as it was, without cyber warfare in mind. Despite inventive attempts at interpretation and contextualised analogy, when trying to apply Article 2(4) there remain significant problems of *clarity* and *consistency* – both of which should be high up in any legal regime's bucket list. Similarly, resort to the under-discussed principle of non-intervention seems insufficient for a different reason. The *applicability* of the principle to cyber warfare is relatively straightforward, but the extent to which it will in fact restrain interstate cyber-attacks is highly questionable: it is a comparatively weak rule of customary international law, often violated and rarely leading to condemnation when breached.

The Issue of Attribution

Beyond the problems already discussed, however, perhaps the biggest issue with regard to the interaction of the *jus ad bellum* with cyber warfare relates to questions of *attribution*. In terms of determining state responsibility for breaches of international law, the International Law Commission's Draft Articles on State Responsibility (which are non-binding in themselves but which are largely reflective of binding customary international law) set out in detail how legal attribution is to be established. States are, fairly obviously, responsible for the actions of their organs (ASR, 2001: Article 4), including unauthorised acts (ASR, 2001: Article 7). Thus, cyber-attacks perpetrated by members of a state's armed forces will be

considered actions of the state. This also holds true for civilian hackers or programmers working directly for the state (ASR, 2001: Article 4; Roscini, 2010: 98).

In addition, actions of groups or persons 'acting on the instructions of, or under the direction or control of' the state are attributable to that state (ASR, 2001: Article 8). However, there is some debate as to exactly what standard of 'control' is necessary to attribute acts of cyber aggression by a non-state actor to the state (for discussion of this debate, see Shackelford and Andres, 2011: 984-993). Two possible, competing tests for the necessary standard of control can be found in case law. The first of these is an 'effective control' test, which requires that the state has specific, practical control over the actor concerned before that actor's actions can be viewed as being attributable to it (*Nicaragua* case, 1986: paras. 100-115). The second approach is the wider 'overall control' test, which requires a general level of control – going beyond mere support or provision of funds – but not necessarily specific direction or instruction in each particular instance (*Tadić* case, 1999: paras. 116-145).

The present author shares Roscini's view that the *Nicaragua* 'effective control' test is the more appropriate way of attributing cyber operations. This is because the effective control test offers a narrower understanding of what 'control' entails, and so 'would prevent states from being frivolously or maliciously accused of cyber operations', potentially leading to 'abuse of the right of self-defence' (Roscini, 2014: 38). Doubts nonetheless remain as to the appropriate test for determining 'direction or control'. Indeed, Margulies (2013) has recently suggested a third, wider approach of 'virtual control', specifically for attributing cyber-attacks. Under this test, the mere provision of finances or support would amount to sufficient 'control'. At present there is little basis for Margulies' 'virtual control' test in law, however. In any event, despite this fuzziness in terms of its correct implementation, the rule itself is

fairly straightforward: the conduct of actors controlled or directed by the state constitutes 'state conduct' as far as international law is concerned.

There is a further legal question in terms of attributing responsibility to the state. This is the necessary *evidentiary standard* required to establish that an act was perpetrated by the state (either directly by one of its organs, or indirectly by an entity under its direction/control). Evidentiary standards for international law generally, and the *jus ad bellum* in particular, are notoriously unclear, and different standards have been applied inconsistently (Green, 2009b). Generally speaking, though, there is a spectrum of three possible evidentiary standards that could be adopted in relation to attributing cyber-attacks to a state. The first, and strictest, possible standard is that the evidence must establish 'beyond a reasonable doubt' that an actor for which the state is responsible undertook the action: the evidence must be indisputable. The second possibility, falling in the middle of the spectrum, is a 'clear and convincing' test: that is, evidence must be *compelling*, but not necessarily indisputable. The third possibility would be a less onerous 'balance of probabilities' standard; under this approach, the evidence would have to establish that it was 'more likely than not' that the state was responsible for the action.

While it cannot be said with any certainty which of these evidentiary standards is the most appropriate for attributing acts of cyber warfare to a state (or which might be adopted in the future in that context), a number of writers have persuasively argued that 'clear and convincing' evidence should be the standard (e.g., O'Connell, 2012: 202; Roscini, 2014: 97-103). In other words, they argue that the compelling-evidence test, which sits in the middle of the spectrum, is the most suitable. Those supporting the adoption of this 'clear and convincing' standard do so on the basis that it is the test most commonly adopted by states

and because, from a policy perspective, it is also the most suitable: it avoids an onerous requirement for the evidence to be indisputable, but also guards against 'specious claims and false attribution' (Roscini, 2014: 102). Avoiding such incorrect attribution to a state is a particular issue in the cyber context, as false evidentiary trails are comparatively easy to lay in cyberspace (Kodar, 2009: 140-142).

Thus, if there is 'clear and convincing' evidence that a state organ or entity that the state directs or controls has perpetrated a cyber-attack against another state, then the state will be legally responsible either for a breach of Article 2(4) or the principle of non-intervention (Schmitt, 2011: 579). The significant difficulty with this, however, is that such *legal* attribution is predicated upon *factual* attribution. Even if it is agreed that the legal standard is that 'clear and convincing' evidence is required, this necessitates that actual evidence of this sort can in fact be obtained.

Questions of factual (or what might also be called 'forensic') attribution of course exist in all attempts to determine state responsibility for breaches of international law, but the problem of obtaining evidence is particularly pronounced in the cyber context (Tsagourias, 2012: 233). As Neil C. Rowe has already examined in Chapter 3 of this volume, there are significant technical uncertainties in attributing cyber activities to any particular actor. This is not the place to discuss these technical issues concerning factual attribution in any detail, but it is clear that, to some extent at least, 'the Internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers and you can surreptitiously enslave computers to do your dirty work' (Brenner, 2011: 32).

As Rowe discusses in his chapter, problems in technically attributing cyber-attacks to any particular actor are not always entirely insurmountable; they are, nonetheless, considerable, and are amplified in relation to technical attribution to a *state*. Thus, even if it can be agreed which actions are covered by Article 2(4) and which are not, and can then be agreed that the 'clear and convincing' approach is indeed the correct evidentiary standard for legally attributing such actions to the state (directly or indirectly), the chances of that standard being *reached* in terms of reliable forensic evidence will, in most instances in the cyber context, be extremely small (O'Connell, 2012: 202). Legally, '[t]here has to be compelling proof…[meaning that] in these cyber situations, one can point the finger, but not with the needed precision' (Singer and Friedman, 2014: 75). This issue is fundamental to the effectiveness of international law in the cyber context (Goldsmith, 2013: 136) and it is telling that, as yet, *no* act of cyber aggression has been conclusively factually (and, as a consequence, legally) attributed to a state (Harrison Dinniss, 2012: 53).

The Militarisation of Cyberspace

In addition to the attribution problem, significant concerns may also be raised about what might be termed the 'militarisation' of cyberspace. The *jus ad bellum* is a branch of international law that specifically deals with the use of military force. By situating interstate cyber operations within this area of the law at all, the legal literature can be seen as skewing focus towards a military approach to cyber security. Admittedly, the 'blame' for this cannot be laid entirely at the feet of lawyers: the reality is that states have predominantly engaged with cyber threats through military discourse and procedures, and the legal debate is, to some extent, simply reflecting that reality. Nonetheless, as has been eloquently discussed by Mary Ellen O'Connell (2012), by focusing on the *jus ad bellum* as the applicable legal regime,

there is a real concern that the law is (at least partially) responsible for 'feeding' a cyber arms race and contributing to the potential for military escalation.

In particular, one might argue that the possibility of forcible responses to cyber-attacks occurring under the right of self-defence is troubling in terms of the escalation of the use of force. While few would question that states should have some forcible recourse in response to the most extreme cyber-attacks causing death and destruction (Waxman, 2013: 111), most aggressive cyber operations will likely not come close to causing this kind of effect. By starting from the perspective of situating cyber warfare within the *jus ad bellum*, international law may be inherently inviting forcible responses to non-forcible actions (Tubbs *et al.*, 2002: 16). Once self-defence is entertained as an option – however much the majority of lawyers might say that it must be reserved only for the most devastating scenarios – this opens the door to states considering the 'military option' in response to lesser actions.

After all, as noted previously, the severity of a cyber-attack is in the eye of the beholder: a case can always be made that an attack is damaging enough to require a military response. Furthermore, concerns relating to the escalation of force used in self-defence in response to cyber aggression are amplified when one considers the problems associated with the factual attribution of cyber operations. If a state cannot accurately identify the source of an attack against it, how can it possibly know against which state to launch its responsive strikes?

Conclusion: A Shift of Focus towards the Duty to Prevent?

The previous section highlighted a number of issues with current attempts to apply the *jus ad bellum* to interstate cyber-attacks. In response to these sorts of concerns, a number of writers have argued that there is a need for a new bespoke cyber warfare treaty. Indeed, various

academic proposals now exist for such a treaty (see, e.g., Brown, 2006; Moore, 2013; Hathaway *et al.*, 2012: 880-884). Some states have also produced such plans. Most notably – and somewhat ironically, given its prominent links to cyber (in)security at the international level (Clarke and Knake, 2010: 219) – Russia has been calling for a cyber warfare treaty since the late 1990s (see UN Doc. A/53/576, 1998). Indeed, Russia has recently drawn up a full draft treaty on the subject (Draft Convention on International Information Security, 2011).

Calls for a cyber warfare treaty are worth heeding, at least to an extent. A set of agreed rules on the extent to which the norms of the *jus ad bellum* are applicable – including provisions on what sorts of cyber actions qualify variously as 'force,' 'interventions' and 'armed attacks' – would undoubtedly bring an increased level of consistency and certainty to the legal regulation of cyberspace. As noted above, the majority view is that the existing law can, and does, regulate interstate cyber warfare. This view is, in itself, correct, but the intricacies of the debates discussed above equally show that applying the existing law is no easy matter. Just because there is already law that can be applied to cyber conflict is no reason to avoid reiterating, and providing more specific (and perhaps clearer and more refined) guidance as to how to apply that law in a binding international agreement. Such an agreement would be valuable for the sake of clarity, if for no other reason.

However, while a cyber warfare treaty is appealing in theory, in practice it is extremely unlikely to emerge (Nguyen, 2013: 1111; Waxman, 2011: 426). Getting states to agree to *any* large multilateral treaty is an extremely difficult task, and in the context of an issue that relates directly to questions of national security, the odds of agreement lengthen significantly (Murphy, 2013: 332-333). There are deep rooted differences of opinion as to how the *jus ad*

bellum rules should apply, as has been noted; crucially, states have 'divergent strategic interests that will pull their preferred doctrinal interpretations and aspirations in different directions, impeding formation of a stable international consensus' (Waxman, 2011: 425-426). This can be seen by the impasse over Russia's calls for a cyber treaty. In particular, Russia has sought an *arms control* agreement, while the United States favours a very different approach, more in line with the existing *jus ad bellum* rules (Ford, 2010).

The emergence of a treaty confirming the way in which the law is to apply to cyber warfare, at least at present, is therefore something of a pipedream. It is also important to note that a treaty that simply solidifies the majority consensus (to the extent that such a thing can be identified) on the application of the *jus ad bellum* to cyber-attacks would do nothing to alleviate the key issue of *attributing* such attacks to states, even were it to be agreed upon (Barkham, 2001: 98-99).

Placing the notion of a cyber warfare treaty on the legal backburner for the foreseeable future, then, this chapter concludes with a tentative suggestion to try to alleviate some of the issues associated with the application of the *jus ad bellum* to cyber warfare. It is submitted that it would be desirable to promote a reorientation of focus towards another existing rule of international law: the duty that states take appropriate and reasonable steps to protect the sovereign rights of other states. This duty is already legally incumbent upon states. There is an existing requirement in international law that states take reasonable steps to ensure that their territory is not used in a manner detrimental to other states (see, generally, Barnidge, 2006). The ICJ confirmed, way back in 1949, that states cannot 'allow knowingly its territory to be used contrary to the rights of other states' (*Corfu Channel* case, 1949: 22). This general rule has subsequently been embraced, for example, in the international

environmental law context (see, e.g., ILA Study Group, First Report, 2014). It could be similarly emphasised in relation to acts of cyber warfare.

The suggestion here is, therefore, not to introduce 'new' law, but to refocus the cyber warfare debate around an existing legal duty. As with the principle of non-intervention, the applicability of the 'duty to prevent' to cyber warfare has been generally overlooked in the literature. Even when it has been referred to, it has, at times, been applied incorrectly. For example, Graham (2010: particularly at 92-96) argues that if a state breaches the duty to prevent, then this in itself means that the state is legally responsible for the cyber-attacks emanating from its territory that it has failed to prevent, whether or not it directed or controlled the perpetrator. This is entirely incorrect: on the basis of this 'duty to prevent', states are legally responsible, not for a breach of the prohibition of the use of force (or the principle of non-intervention) *per se*, but of a separate duty to take reasonable steps to prevent such attacks (Roscini, 2014: 40). The perpetrator is responsible for the act; the state is responsible for something else: the 'act', as it were, of not taking reasonable measures to stop the act.

A few writers have taken note of the duty in relation to cyber operations and correctly identified its implications (e.g., Tsagourias, 2012: 242; Roscini, 2014: 40, 80-88). The UN General Assembly's 'Group of Governmental Experts' also recently reaffirmed the duty in the context of cyber warfare (UN Doc. A/68/98, 2013: para. 23), as have some individual states (see, e.g., the views expressed by India, China and Russia, quoted in Kanuck, 2010: 1591, both in the main text and in note 88). The duty was also recently referenced in the 2013 *Tallinn Manual*:

> A state shall not knowingly allow the cyber infrastructure *located in its territory* or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other states (*Tallinn Manual*, 2013: Rule 5, 26, emphasis added).

Moving the legal focus away from the *jus ad bellum*, towards the more general duty of 'cyber due diligence' has a number of potential advantages. First, it would alleviate the need for analogy to traditional uses of force and problematic categorisation of cyber-attacks so as to 'crowbar' cyber operations into the framework of Article 2(4) and, as a result, would lessen the uncertainty and inconsistency that is so evident in the longstanding 'Article 2(4) debate'. Secondly, it may serve to somewhat conceptually 'demilitarise' interstate cyber security. This would potentially lessen the likelihood for escalation following an aggressive cyber act, at least in relation to all but the most extreme cyber-attacks.

Thirdly, and most importantly, it would help to minimise the inherent attribution problem. The focus of this book is, of course, on *interstate* cyber warfare, but it has already been noted that conclusively attributing cyber-attacks to states rather than 'independent' individuals or non-state groups is extremely problematic. The 'duty of due diligence' requirement means that the *exact* entity conducting acts of cyber aggression would not need to be established, because the rule in question does not relate to the act itself. Instead, states would be inherently responsible for failing to take reasonable steps to prevent attacks from occurring. This would, of course, encompass attacks where the state itself was undertaking or directing the attack, but *this would not necessarily need to be established*.

States themselves would not be able to hide behind attribution issues, because their legal duty does not rest on whether or not they were the perpetrator. One of the reasons that the United States has been reticent about agreeing a cyber warfare treaty with Russia applicable to *states* is that Russia, and other states such as China, are known to rely on independent actors in relation to aggressive cyber operations, the actions of which the state does not endorse but tacitly approves and takes no steps to prevent. The fear, in the United States at least, is that a cyber treaty applicable to states would hamstring the cyber capabilities of the United States while failing to catch many of the attacks emanating from Russia (or China, or elsewhere) within its legal net (Singer and Friedman, 2014: 186). A reorientation of the debate away from its primary focus on Article 2(4) and towards the application of the duty of prevention should help to avoid this lacuna.

As one might expect, relying on the duty to prevent has its own set of problems. First, factual attribution would, of course, still need to be established to the extent that it would have to be 'clearly and convincingly' shown that an act emanated from the territory of the state in question and that the state failed to take reasonable steps, in the context of the situation, to try to prevent its territory being used for cyber-attacks against other states (see Becker, 2006: 341-345). This is still no easy task. Attribution problems would therefore not be overcome, but they may perhaps be lessened.

Secondly, it is important to note that the duty is not one of strict liability, which would be overly onerous, but of *due diligence* (Roscini, 2014: 87-88). If a state has taken reasonable steps to prevent attacks from occurring from within its territory, then it would not be in breach. Thus, where a state is entirely unable to stop such actions, despite its best efforts, the duty is of little use.

Thirdly, some might question whether this approach would leave a gap in relation to available responses. It was noted above that one reason why the cyber warfare debate has been so consistently framed around Article 2(4) has been that this potentially allows for responses in self-defence (if the nature of the attack is severe enough to raise it to the level of an armed attack). Tsagourias (2012: 242) argues on this basis that 'it would not be of much consolation to the victim [of a large scale, devastating cyber-attack]…to know that it can hold the host state responsible for breaching its duty of due diligence'. Yet, for all the definitional uncertainty surrounding the *jus ad bellum*'s application to cyberspace, there is widespread agreement that cyber-attacks of the 'doomsday scenario' sort are both 'uses of force' and 'armed attacks' (see, e.g., *Tallinn Manual*, 2013: 54-61), meaning that in such cases states can respond with force. Indeed, where the defensive necessity to respond is extreme, some would argue that a state can act in self-defence even where the state is not legally responsible for the armed attack (Banks, 2013; Tsagourias, 2012: 242-243). For good or ill, this probably reflects reality, irrespective of legal questions of attribution: states will not refrain from a military response when faced with a catastrophic attack.

The acts of cyber warfare that have occurred in practice up until now have not been of this sort of catastrophic nature, however. While the threat of the 'doomsday cyber-attack' now looms large in the psyche of the developed world, it is likely that the vast majority of cyber-attacks will remain on a much smaller scale in the future. In many cases, therefore, a forcible response will not be appropriate. Instead of debating the extent to which 'non-apocalyptic' acts of cyber aggression may or may not fall within the *jus ad bellum*'s reach, then, the international community may be better served by placing the onus on legal responsibility for good cyber security and communitarian solutions to cyber aggression (see, generally,

O'Connell, 2012). This is not to suggest that the *jus ad bellum* has, or should have, no role in the legal regulation of cyber warfare, only that it should be situated at the margins – only called upon where absolutely necessary – rather than being the starting point for the debate.

It is also worth noting that various *non-forcible* countermeasures can lawfully be taken by states in response to breaches of international law (ASR, 2001: Article 22; Buchan, 2012: 226; Harrison Dinniss, 2012: 105-108; Schmitt, 2011: 581-583). There are various restrictions on such countermeasures (see *Gabčíkovo-Nagymaros* case, 1997: paras. 83-87) but, in most cases, states will in fact have the option of a response without needing to turn to military force (O'Connell, 2012: 204-205). Such non-forcible options of response should be supplemented by an increased emphasis, at the political level at least – and perhaps increasingly at the legal level (see Sofaer *et al.*, 2010) – on improved international cyber cooperation and information sharing (Hathaway *et al.*, 2012: 882-884). Prevention is, fairly obviously, preferable to response. All this can be combined with the duty for states to take reasonable steps to prevent cyber-attacks from emanating from their territory. A breach of this duty will be more easily established because of reduced issues of attribution, and the finding of such a breach – if the duty is better promoted, emphasised and clarified – may help to place political pressure on the state concerned to clean up its cyber act.

Ultimately, the present author supports a 'combination' approach to the cyber warfare problem, which *includes* resort to the *jus ad bellum*, but which centres on a duty to prevent. The ideal would be for this to all be crystallised in an international treaty, partly to spell out the *jus ad bellum* rules for the extreme cases, but more importantly to 'elaborate what [is] required of states' responsibilities in terms of due diligence' (O'Connell and Arimatsu, 2012: 11). Being rather more realistic, however – given the unlikelihood of such a treaty appearing,

at least any time soon – international lawyers would at least do well to refocus the debate away from Article 2(4) alone.

Acknowledgement

The author would like to thank Robert P. Barnidge, Jr., Lia Emanuel and Reuven (Ruvi) Ziegler for their invaluable comments on previous drafts of this chapter. He would also like to thank the University of Reading for awarding him research leave in the spring/summer of 2014, which allowed him to conduct the research underpinning it.

References

Documents, Treaties and Cases

'UNCIO vol. III, 1945': Documents of the United Nations Conference on International Organisation, Volume III: Dumbarton Oak Proposals (Comments and Proposed Amendments) (1945) New York: Library of Congress.

'UNCIO vol. VI, 1945': Documents of the United Nations Conference on International Organisation, Volume VI: Commission I (General Provisions) (1945) New York: Library of Congress.

'UN Charter, 1945': Charter of the United Nations, 1 UNTS 16, 24 October 1945.

'Statute of the ICJ, 1945': Statute of the International Court of Justice, 1945: annexed to Charter of the United Nations, 1 UNTS 16, 24 October 1945.

‘*Corfu Channel* case, 1949’: *Corfu Channel Case* (*United Kingdom v. Albania*), merits, ICJ Reports 244, 15 December 1949.

‘UN Doc. A/RES/20/2131, 1965’: Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty, GA Res. 2131 (XX), 20th sess., 21 December 1965.

‘VCLT, 1969’: Vienna Convention on the Law of Treaties 1155 UNTS 331, 23 May 1969.

‘UN Doc. A/7619, 1969’: Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States, GA Official Records, 24th sess., Suppl. No. 19.

‘UN Doc. A/RES/25/2625, 1970’: Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, GA Res. 2625 (XXV), 25th sess., 24 October 1970.

‘UN Doc. A/RES/3314, 1974’: Definition of Aggression, GA Res. 3314 (XXIX), 29th sess., 14 December 1974.

‘UN Doc. A/RES/31/91, 1976’: Declaration on Non-Interference in the Internal Affairs of States, GA Res. 31/91, 31st sess., 14 December 1976.

‘UN Doc. A/RES/36/103, 1981’: Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, GA Res. 36/103, 36th sess., 9 December 1981.

‘*Nicaragua* case, 1986’: *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), merits, ICJ Reports 14, 27 June 1986.

‘*Gabčíkovo-Nagymaros* case, 1997’: *Case Concerning the Gabčíkovo-Nagymaros Project* (*Hungary*/*Slovakia*), judgment, ICJ Reports 7, 25 September 1997.

‘UN Doc. A/53/576, 1998’: Role of Science and Technology in the Context of Security, Disarmament and Other Related Fields, General Assembly, Report of the First Committee, 53rd sess., 18 November 1998.

‘*Tadić* case, 1999’: *Prosecutor v. Dusko Tadić*, appeal judgement, IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.

‘ASR, 2001’: Draft Articles on State Responsibility, International Law Commission, 53 UN GAOR supp. 10, 43, UN Doc. A/56/10.

Convention on Cybercrime, Budapest, Hungary, 2296 UNTS 167, 23 November 2001.

‘*Oil Platforms* case, 2003’: *Case Concerning Oil Platforms* (*Islamic Republic of Iran v. United States of America*), merits, ICJ Reports 161, 6 November 2003.

Draft Convention on International Information Security (Concept), Yekaterinburg, Russia, 24 September 2011 [Online], Available: http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument [28 May 2014].

'UN Doc. A/68/98, 2013': Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly, 68th sess., 24 June 2013.

Tallinn manual on the international law applicable to cyber warfare (2013) Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (general editor: Schmitt, M.N.), Cambridge: Cambridge University Press.

'ILA Study Group, First Report, 2014': International Law Association Study Group on Due Diligence in International Law, First Report, French, D. (Chair) and Stephens, T. (Rapporteur), 7 March 2014 [Online], Available: http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1045 [28 May 2014].

Academic Works and Media Reports

Akehurst, M. (1974) 'Custom as a source of international law', *British Yearbook of International Law*, vol. 47, pp. 1-53.

Alexandrov, S.A. (1996) *Self-defence against the use of force in international law*, The Hague: Kluwer Law International.

Antolin-Jenkins, V.M. (2005) 'Defining the parameters of cyberwar operations: Looking for law in all the wrong places?', *Naval Law Review*, vol. 51, pp. 132-174.

Banks, W. (2013) 'The role of counterterrorism law in shaping *ad bellum* norms for cyber warfare', *International Law Studies*, vol. 89, pp. 157-197.

Barkham, J. (2001) 'Information warfare and international law on the use of force', *New York University Journal of International Law and Politics*, vol. 34, pp. 57-113.

Barnidge, R.P. (2006) 'The due diligence principle under international law', *International Community Law Review*, vol. 8, no. 1, pp. 81-121.

Becker, T. (2006) *Terrorism and the state: Rethinking the rules of state responsibility*, Oxford: Hart Publishing.

Benatar, M. (2009) 'The use of cyber force: Need for a legal justification?', *Goettingen Journal of International Law*, vol. 3, pp. 375-396.

Boas, G. (2012) *Public international law: Contemporary principles and perspectives*, Cheltenham: Edward Elgar.

Bothe, M. (2003) ‘Terrorism and the legality of pre-emptive force’, *European Journal of International Law*, vol. 14, pp. 227-240.

Brenner, J. (2011) *America the vulnerable: Inside the new threat matrix of digital espionage, crime, and warfare*, New York: The Penguin Press.

Brown, D. (2006) ‘A proposal for an international convention to regulate the use of information systems in armed conflict’, *Harvard International Law Journal*, vol. 47, no. 1, pp. 179-221.

Brownlie, I. (1963) *International law and the use of force by states*, Oxford: Clarendon Press.

Buchan, R. (2012) ‘Cyber attacks: Unlawful uses of force or prohibited interventions’, *Journal of Conflict and Security Law*, vol. 17, no. 2, pp. 212-227.

Clarke, R.A. and Knake, R.K. (2010) *Cyber war: The next threat to national security and what to do about it*, New York: Harper Collins.

Corten, O. (2010) *The law against war: The prohibition on the use of force in contemporary international law*, Oxford: Hart Publishing.

Dinstein, Y. (2002) ‘Computer network attacks and self-defense’, *International Law Studies*, vol. 76, pp. 99-120.

Dinstein, Y. (2011) *War, aggression and self-defence*, 5th edition, Cambridge: Cambridge University Press.

Dunlap, C.J. (2011) 'Perspectives for cyber strategists on law for cyberwar', *Strategic Studies Quarterly*, vol. 5, no. 1, pp. 81-99.

Farer, T.J. (1985) 'Political and economic coercion in contemporary international law', *American Journal of International Law*, vol. 79, pp. 405-413.

Ford, C.A (2010) 'The trouble with cyber arms control', *The New Atlantis – A Journal of Technology and Society*, vol. 29, pp. 52-67.

Franck, T.M (2002) *Recourse to force: State action against threats and armed attacks*, Cambridge: Cambridge University Press.

Goldsmith, J. (2013) 'How cyber changes the laws of war', *European Journal of International Law*, vol. 24, no. 1, pp. 129-138.

Graham, D.E. (2010) 'Cyber threats and the law of war', *National Security Law and Policy*, vol. 4, no. 1, pp. 87-102.

Gray, C. (2008) *International law and the use of force*, 3rd edition, Oxford: Oxford University Press.

Green, J.A. (2009a) *The International Court of Justice and self-defence in international law*, Oxford: Hart Publishing.

Green, J.A (2009b) 'Fluctuating evidentiary standards for self-defence in the International Court of Justice', *International and Comparative Law Quarterly*, vol. 58, pp. 163-179.

Green, J.A. (2011) 'Questioning the peremptory status of the prohibition of the use of force', *Michigan Journal of International Law*, vol. 32, no. 2, pp. 215-257.

Handler, S.G. (2012) 'New cyber face of battle: Developing a legal approach to accommodate emerging trends in warfare', *Stanford Journal of International Law*, vol. 48, no. 1, pp. 209-238.

Harrison Dinniss, H.A. (2012) *Cyber warfare and the laws of war*, Cambridge: Cambridge University Press.

Haslam, E. (2000) 'Information warfare: Technological changes and international law', *Journal of Conflict and Security Law*, vol. 5, pp. 157-175.

Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W. and Spiegel, J. (2012) 'The law of cyber-attack', *California Law Review*, vol. 100, pp. 817-885.

Henderson, C. (2013) 'The provision of arms and "non-lethal" assistance to governmental and opposition forces', *University of New South Wales Law Journal*, vol. 36, no. 2, pp.642-681.

Hoisington, M. (2009) ‘Cyberwarfare and the use of force giving rise to the right of self-defense’, *Boston College International and Comparative Law Review*, vol. 32, pp. 439-454.

Kanuk, S.P. (1996) ‘Information warfare: New challenges for public international law’, *Harvard International Law Journal*, vol. 37, pp. 272-292.

Kanuck, S.P (2010) ‘Sovereign discourse on cyber conflict under international law’, *Texas Law Review*, vol. 88, pp. 1571-1597.

Kodar, E. (2009) ‘Computer network attacks in the grey areas of *jus ad bellum* and *jus in bello*’, *Baltic Yearbook of International Law*, vol. 9, pp. 133-155.

Krasner, S.D. (1999) *Sovereignty: Organized hypocrisy*, Princeton: Princeton University Press.

Margulies, P. (2013) ‘Sovereignty and cyber attacks: Technology’s challenge to the law of state responsibility’, *Melbourne Journal of International Law*, vol. 14, no. 2, pp. 496-519.

Moore, S. (2013) ‘Cyber attacks and the beginning of an international cyber treaty’, *North Carolina Journal of International Law and Commercial Regulation*, vol. 39, pp. 223-257.

Morth, T.A. (1998) ‘Considering our position: Viewing information warfare as a use of force prohibited by article 2(4) of the U.N. Charter’, *Case Western Reserve Journal of International Law*, vol. 30, pp. 567-600.

Murphy, J.F. (2013) ‘Cyber war and international law: Does the international legal process constitute a threat to U.S. vital interests?’, *International Law Studies*, vol. 89, pp. 309-340.

Nguyen, R. (2013) ‘Navigating *jus ad bellum* in the age of cyber warfare’, *California Law Review*, vol. 101, pp. 1079-1129.

O’Connell, M.E. (2012) ‘Cyber security without cyber war’, *Journal of Conflict and Security Law*, vol. 17, no. 2, pp. 187-209.

O’Connell, M.E and Arimatsu, L. (Wilmshurst, E., chair) (2012) ‘Cyber security and international law’, 29 May, *Chatham House*, Meeting Summary [Online], Available: http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf [28 May 2014].

Orakhelashvili, A. (2006) *Peremptory norms in international law*, Oxford: Oxford University Press.

Papain, T. (2011) ‘North Korea and cyberwarfare: How North Korea’s cyber attacks violate the laws of war’, *Journal of Korean Law*, vol. 11, pp. 29-54.

Remus, T. (2013) ‘Cyber-attacks and international law of armed conflicts; a *jus ad bellum* perspective’, *Journal of International Commercial Law and Technology*, vol. 8, no. 3, pp. 179-189.

Roscini, M. (2010) ‘World wide warfare – *Jus ad bellum* and the use of cyber force’, *Max Planck Yearbook of United Nations Law*, vol. 14, pp. 85-130.

Roscini, M. (2014) *Cyber operations and the use of force in international law*, Oxford: Oxford University Press.

Schmitt, M.N. (1999) ‘Computer network attack and the use of force in international law: Thoughts on a normative framework’, *Columbia Journal of Transnational Law*, vol. 37, pp. 885-937.

Schmitt, M.N. (2010) ‘Cyber operations in international law: The use of force, collective security, self-defense and armed conflicts’, Committee on Deterring Cyber Attacks, Nations Research Council: The National Academic Press.

Schmitt, M.N. (2011) ‘Cyber operations and the *jus ad bellum* revisited’, *Villanova Law Review*, vol. 56, pp. 569-605.

Schmitt, M.N. (2013) ‘Cyberspace and international law: The penumbral mist of uncertainty’, *Harvard Law Review Forum*, vol. 126, pp. 176-180.

Schmitt, M.N. (2014) ‘Legitimacy versus legality redux: Arming the Syrian rebels’, *Journal of National Security Law and Policy*, vol. 7, pp.139-159.

Shackelford, S.J. (2009) ‘From nuclear war to net war: Analogizing cyber attacks in international law’, *Berkley Journal of International Law*, vol. 27, pp. 192-251.

Shackelford, S.J. and Andres, R.B. (2011) ‘State responsibility for cyber attacks: Competing standards for a growing problem’, *Georgetown Journal of International Law*, vol. 42, pp.971-1016.

Sharp, W.G (1999) *Cyberspace and the use of force*, Falls Church: Aegis Research Corp.

Silver, D.B. (2002) ‘Computer network attack as a use of force under Article 2(4)’, *International Law Studies*, vol. 76, pp. 73-98.

Singer, P.W. and Friedman, A. (2014) *Cybersecurity and cyberwar: What everyone needs to know*, Oxford: Oxford University Press.

Sofaer, A.D., Clark, D. and Whitfield, D. (2010) ‘Cyber security and international agreements’, *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, National Research Council, The National Academic Press [Online], Available: http://www.nap.edu/catalog/12997.html [27 May 2014].

Sudworth, J. (2009) ‘New “cyber attacks” hit S. Korea’, 9 July, *BBC* News [Online], Available: http://news.bbc.co.uk/1/hi/world/asia-pacific/8142282.stm [3 July 2014].

Sullivan, S. (2013) ‘Networking customary law’, *Kansas Law Review*, vol. 61, pp. 659-698.

Tibori Szabó, K. (2011) *Anticipatory action in self-defence: Essence and limits under international law*, The Hague: TMC Asser Press (Springer).

Tsagourias, N. (2012) ‘Cyber-attacks, self-defence and the problem of attribution’, *Journal of Conflict and Security Law*, vol. 17, no. 2, pp. 229-244.

Tubbs, D., Luzwick, P.G. and Sharp Sr., W.G. (2002) ‘Technology and law: The evolution of digital warfare’, *International Law Studies*, vol. 76, pp. 7-20.

Waters, C.P.M. and Green, J.A. (2010) ‘International law: Military force and armed conflict’, in Kassimeris, G. and Buckley, J.D. (eds.) *Ashgate research companion to modern warfare*, Farnham: Ashgate.

Waxman, M.C. (2011) ‘Cyber-attacks and the use of force: Back to the future of Article 2(4)’, *Yale Journal of International Law*, vol. 36, pp. 421-459.

Waxman, M.C. (2013) ‘Self-defensive force against cyber attacks: legal, strategic and political dimensions’, *International Legal Studies*, vol. 89, pp. 109-122.

Wu, L. (2000) ‘East Asia and the principle of non-intervention: Policies and practices’, *Maryland Series in Contemporary Asian Studies*, vol. 160, no. 5, pp. 1-39.