Disasters Caused in Cyberspace

James A Green

1. Introduction

The advent of cyberspace[1] can be seen as something of a double-edged sword when it comes to global disasters. It is clear that disaster response and post-disaster rebuilding can be, and in many instances has been, significantly improved by the use of cyberspace. The Internet, of course, facilitates the fast and widespread dissemination of information, which can help to more effectively unite victims of disasters, galvanise and coordinate efforts to respond (including internationally) and provide valuable support to those in areas effected by disasters.[2]

At the same time, 'cyberspace has also become a repository for various threats, vulnerabilities and insecurities.'[3] The threat of significant global harm being inflicted through cyberspace is now a primary concern in international relations, and has become deeply rooted in the psyche of governments. To give just one example, at the time of writing Chancellor George Osborne has announced – in a speech made at GCHQ on 17 November 2015, in the wake of the horrific terrorist attacks that took place in Paris four days earlier – that agents of the so-called 'Islamic State' are attempting to develop the ability to launch deadly cyber-attacks

[1] Cyberspace has been defined, in a much repeated formulation by the US Department of Defence, as '[a] global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'. *Department of Defense Dictionary of Military and Associated Terms*, (Joint Publication 1-02, 8 November 2010) (as amended through 15 June 2015) 58 <http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf> accessed 22 October 2015.

[2] See M Laituri, 'Geospatial Responses to Disasters: The Role of Cyberspace' (2010) 32 ArcNews <http://www.esri.com/news/arcnews/summer10articles/files/arcnews32_2/arcnews-summer10.pdf> accessed 1 October 2015.

[3] MN Schmitt, 'Introduction' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) 1.

on targets in the United Kingdom (UK), and that the UK is to roughly double its cyber security budget to guard against this and other such cyber threats.[4]

This chapter examines international law in relation to 'cyber disasters'. That is, it considers disasters – broadly defined as 'calamitous events'[5] – that are caused by, or through, cyberspace. Admittedly, the notion of a cyber disaster remains, at least to an extent, potential. It would be something of a stretch to conclude that cyber activity has, as yet, resulted in harm or damage rising to the level of what might be considered 'a disaster'. Indeed, some commentators have played down the likelihood of cyber disasters occurring in the future, viewing as hyperbolic the commonly repeated claim that actions in cyberspace are likely to cause large-scale harm.[6]

It is true that there are 'very few single cyber-events with the capacity to provoke a global shock',[7] in the true sense of a *disaster*. One must be careful not to overestimate the likelihood of cyber disasters occurring. On the other hand, there is little question that in the modern, cyber-reliant and interconnected world, the potential for disasters to be caused in cyberspace is now very real.[8] Various 'cyber doomsday scenarios' have been envisaged in the literature with increasing regularity. For example, scholars have noted the possibility of the use of computers to melt down a nuclear power plant, turn a state's unmanned military drones

[4] 'Chancellor's Speech to GCHQ on Cyber Security' (original script, 17 November 2015) <https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security> accessed 19 November 2015.
[5] See International Law Commission, *Draft Articles on the Protection of Persons in the Event of Disasters* UN Doc. A/CN.4/L.831 (15 May 2014) art 3.
[6] See, e.g., MJ Ranum, *The Myth of Homeland Security* (Wiley Publishing, 2004); C Farivar, 'A Brief Examination of Media Coverage of Cyber-Attacks (2007 – Present)' in C Czosseck and K Geers (eds), *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, 2009); T Rid, *Cyber War Will Not Take Place* (Hurst, 2013).
[7] P Sommer and I Brown, *Reducing Systemic Cybersecurity Risk* (Multi-Disciplinary Issues International Futures Programme, OECD/IFP Project on 'Future Global Shocks' 3 IFP/WKP/FGS, 14 January 2011) 10.
[8] Committee on Private-Public Sector Collaboration to Enhance Community Disaster Resilience, Geographical Science Committee, Board on Earth Sciences and Resources, Division on Earth and Life Studies, and National Research Council, *Building Community Disaster Resilience through Private-Public Collaboration* (The National Academies Press, 2011) 20-2; R Stiennon, *There Will Be Cyberwar: How the Move to Network-Centric War Fighting has Set the Stage for Cyberwar* (IT-Harvest Press, 2015).

against it, and drop its planes from the sky (to name just a few of the plethora of contemplated cyber-caused catastrophes).[9]

The scale and likely transboundary nature of cyber disasters mean that the threat that they pose is inherently 'international' in nature, and thus requires an international legal response.[10] In the late 2000s, the need for international law to engage with the issue of large-scale cyber threats was brought sharply into focus, following the various Distributed Denial of Service (DDoS) attacks directed against Estonia in 2007. Those attacks – which caused widespread disruption to Estonia's banking, telecom and government infrastructure – were of a notably greater scale than the cyber-attacks that had occurred previously. They were also allegedly the first major acts of cyber aggression to be perpetrated by a state, albeit that state responsibility was never conclusively established for the cyber-attacks against Estonia, either factually or legally.[11] In 2010, the infamous Stuxnet virus attack on Iran represented a further escalation, in that it was the first cyber-attack to directly cause significant physical harm. The virus affected the centrifuges at Iran's Natanz nuclear power plant, causing notable 'real world' damage.[12] At the time of writing, Stuxnet represents the 'high-water mark' for harm caused by a cyber-attack,[13] but the very fact of its occurrence suggests that the water will continue to rise.

Despite the escalation of harmful cyber activity, international law has still not caught up with the threat that cyberspace poses. At present there are extremely few specific rules of international law that govern the sorts of activities that would likely lead to cyber disasters (such as inter-state cyber-attacks, large-scale cyber-attacks by non-state actors or regulation of

[9] See, e.g., RA Clarke and R Knake, *Cyber War: The Next Threat to National Security and What to do About It* (Harper Collins, 2010) 64-8; DB Garrie, 'Cyber Warfare, What are the Rules?' (2012) 1 Journal of Law and Cyber Warfare 1, 5.
[10] TA Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 Case Western Reserve Journal of International Law 567, 581; Sommer and Brown (n 7) 10.
[11] See L Hansen, 'Digital Disaster, Cyber Security, and the Copenhagen School' (2009) 53 International Studies Quarterly 1155, 1168-71.
[12] See R Stiennon 'A Short History of Cyber Warfare' in JA Green (ed.), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015) 20-2.
[13] ibid 22.

action that could lead to unintentional cyber catastrophe). Indeed, the only international treaty regulating cyberspace *per se* remains the 2001 Budapest Convention on Cybercrime,[14] which, by its nature, largely does not relate to the sorts of threats considered in this chapter.

Against this backdrop, this chapter assesses the extent to which international law is (or may be) able to reduce the likelihood of cyber disasters occurring. It briefly considers the possibility of new bespoke international law provisions being created to govern cyberspace, before turning to the most common approach taken in the literature with regard to large-scale cyber threats: the application of the *jus ad bellum* and, particularly, the prohibition of the use of force. It is argued herein that this approach has a number of major flaws. Instead, focusing on a different existing rule of international law that has been largely-overlooked in the cyber context – the duty of due diligence – is significantly preferable as a means of trying to prevent cyber disaster.

2. The creation of new international law governing cyber security and the applicability of existing international law

Given that there is a seeming vacuum in international law when it comes to large-scale threats stemming from cyberspace, the most intuitively appealing response is simply to create bespoke law to tackle the issue. On this basis, a number of writers have argued that there is a need for a new cyber security treaty, dealing with the most egregious cyber threats.[15] Perhaps

[14] Convention on Cybercrime (adopted 23 November 2001). At the regional level, it is worth also noting the African Union (AU) Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014), although this treaty explicitly only acts to reaffirm existing obligations incumbent on AU member states, and is, in any event, not focussed on large-scale security threats.

[15] See, e.g., D Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47 Harvard International Law Journal 179; OA Hathaway, R Crootof, P Levitz, H Nix, A Nowlan, W Perdue and J Spiegel, 'The Law of Cyber-Attack' (2012) 100 California Law Review 817, 880-4; S Moore, 'Cyber Attacks and the Beginning of an International Cyber Treaty' (2013) 39 North Carolina Journal of International Law and Commercial Regulation 223.

more importantly, some states have also produced proposals for the development of new law.[16] Russia, in particular, has been calling for a cyber security treaty since the late 1990s,[17] and, in 2011, drew up a full draft treaty on the subject.[18]

However, while a cyber security treaty is appealing in theory (because it would, one might hope, provide clear and explicit rules aimed at lessening the likelihood of large-scale cyber threats materialising), in practice any such treaty is extremely unlikely to emerge, at least any time soon.[19] There exist deep rooted differences of opinion among states as to what form any future treaty should take. For example, Russia has essentially sought a cyber arms control agreement, which would be broadly regulatory in nature. In contrast, the United States favours a very different approach, focussed on a law-enforcement paradigm and prohibition rather than regulation.[20] These fundamental disagreements mean that the emergence of a treaty specifically governing large-scale cyber threats – or, at least, a treaty of this kind that would have widespread state support, and thus have any realistic chance of being at all effective – is quite simply a political impossibility at present.

The lack of existing bespoke international law on cyber security, coupled with the unlikelihood of any new law on the subject emerging, has led some commentators to argue that threats posed by cyberspace exist 'in a legal netherworld'.[21] This is, in fact, incorrect. The majority view in the literature is that the rules of international law that existed prior to the

[16] See, e.g., the proposal made to the UN collectively by Russia, China, Tajikistan and Uzbekistan in 2011: *International Code of Conduct for Information Security*, annexed to *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN Doc. A/66/359 (14 September 2011).
[17] See *Role of Science and Technology in the Context of Security, Disarmament and Other Related Fields*, UN Doc. A/53/576 (General Assembly, Report of the First Committee, 53rd sess., 18 November 1998).
[18] Draft Convention on International Information Security (Concept) (24 September 2011) <http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/7b17ead7244e2064c3257925003bcbcc!OpenDocument> accessed 27 October 2015.
[19] MC Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 YJIL 421, 426; R Nguyen, 'Navigating *Jus ad Bellum* in the Age of Cyber Warfare' (2013) 101 California Law Review 1079, 1111.
[20] See CA Ford, 'The Trouble with Cyber Arms Control' (2010) 29 The New Atlantis – A Journal of Technology and Society 5.
[21] M Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to The Right of Self-Defense' (2009) 32 Boston College International and Comparative Law Review 439, 440.

emergence of cyberspace are applicable to large-scale cyber threats, and can act to limit the possibilities of them materialising.[22] While the widespread adoption of this position is probably, at least to an extent, a pragmatic academic response to the fact that a cyber security treaty is clearly on the legal backburner, this does not mean that it is inaccurate. New security threats have emerged in various guises throughout the United Nations (UN) era, and there is nothing so inherently unique about cyberspace that means that existing legal provisions are necessarily inapplicable to it.[23]

Equally, the application of rules of international law created prior to the advent of cyberspace to modern cyber threats will obviously be somewhat anachronistic.[24] While it must be correct that existing international law is (or can be) *applicable* to cyber threats, the actual *application* of 'old' law to such threats is neither self-evident nor straightforward. This is amplified by the fact that there remains relatively little guidance from states as to how the law is to be applied to cyberspace, either in the form of practice or *opinio juris*: it is worth keeping in mind that much of the discussion over how best to mobilise existing legal provisions to guard against cyber threats has been left to academics.[25]

The academic focus in relation to large-scale cyber threats has predominantly been on the existing provisions of international law that govern military action. Particularly, much ink has been spilt over the application to cyber threats of the two branches of international law that relate to military force and warfare: the *jus ad bellum* and the *jus in bello*. The former of these

[22] See, e.g., MN Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Prepared by the International Group of Experts at the Invitation of the North Atlantic Treat Organization (NATO) Cooperative Cyber Defence Centre of Excellence, CUP 2013) 5; M Benatar, 'The Use of Cyber Force: Need for a Legal Justification?' (2009) 3 Goettingen Journal of International Law 375, 395; MN Schmitt, 'Cyberspace and International Law: The Penumbral Mist of Uncertainty' (2013) 126 Harvard Law Review Forum 176, 176-7; N Tsagourias, 'The Legal Status of Cyberspace' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015).
[23] W Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 International Legal Studies 123, 123-4; C Waters, 'New Hacktivists and the Old Concept of *Levée en Masse*' (2014) 37 Dalhouse Law Journal 771, 773-5.
[24] R Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions' (2012) 17 JCSL 212, 212-13.
[25] MN Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 Yale Law Journal Forum 68, 69.

concerns the general prohibition of military force and its exceptions, and thus relates to deterrence/prevention; the latter is a regulatory area of international law governing the conduct of hostilities, which accepts that military action is already underway and looks to minimise its impact. As such, the application of the *jus in bello* to cyberspace is beyond the scope of this chapter, which focuses on the law's potential to restrict the likelihood of cyber disasters occurring *per se*. Consideration in this chapter of the common academic approach of focusing on the *jus ad bellum* and *jus in bello* provisions will thus be restricted to the former.[26]

It is argued herein that the widespread focus on these two branches of international law has led to a general lack of consideration of the role that the law may be able to play in relation to cyber threats that do not emanate from the armed forces of a state,[27] and – more generally – has overly 'militarised' the legal approach to cyber security.[28] These are concerns to which we will return throughout this chapter.

3. The prohibition of the use of force and cyberspace: Problems of application and scope

3.1. The prohibition of the use of force under article 2(4) of the UN Charter

In the context of the *jus ad bellum*, scholars have commonly focused[29] on the question of whether state acts of cyber aggression constitute violations of the prohibition of the use of force, under article 2(4) of the UN Charter:

[26] See HA Harrison Dinniss, 'The Regulation of Cyber Warfare under the *Jus in Bello*' in JA Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015) (providing an excellent summary of the applicability of the *jus in bello* to cyberspace).
[27] Schmitt, 'Introduction' (n 3) 3.
[28] ME O'Connell, 'Cyber Security without Cyber War' (2012) 17 JCSL 187.
[29] See, for just a few representative examples, HA Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP, 2012) 37-74; M Roscini, *Cyber Operations and the Use of Force in International Law* (OUP, 2014) 45-67; J Maogoto, *Technology and the Law on the Use of Force: New Security Challenges in the Twenty-First Century* (Routledge, 2015) 53-68.

> 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.[30]

The prohibition contained in article 2(4) is one of the most fundamental rules of the UN system and is often referred to as a 'cornerstone' provision.[31] Indeed, it is generally seen as a non-derogable *jus cogens* norm.[32] The hallowed status of the prohibition makes it an inherently appealing legal mechanism in relation to cyber threats: quite simply, if applied to state-authored cyber-attacks, it would prohibit them outright (other than if they constitute acts of self-defence or are authorised by the UN Security Council). However, it is far from simple to apply article 2(4) to cyberspace,[33] and – as will be explored in this section – its suitability and effectiveness as the primary mechanism for dealing with cyber disasters is questionable for a number of reasons.

3.2. Categorization problems: Are cyber-attacks covered by article 2(4)?

Article 2(4) prohibits the 'threat or use of force'. As such, an initial point of inquiry when it comes to trying to apply the prohibition to cyberspace is whether cyber-attacks qualify as 'force' for the purposes of article 2(4). This question has been debated exhaustively (and exhaustingly) in the literature, and the present author has examined the precise contours of that

[30] Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) art 2(4).
[31] Y Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 International Law Studies 99, 99.
[32] See, e.g. A Orakhelashvili, *Peremptory Norms in International Law* (OUP, 2006) 50. *Contra* JA Green, 'Questioning the Peremptory Status of the Prohibition of the Use of Force' (2011) 32 Michigan Journal of International Law 215.
[33] E Kodar, 'Computer Network Attacks in the Grey Areas of *Jus ad Bellum* and *Jus in Bello*' (2009) 9 Baltic Yearbook of International Law 133, 138. *Contra* DE Graham, 'Cyber Threats and the Law of War' (2010) 4 National Security Law and Policy 87, particularly at 88 (viewing the applicability of art 2(4) to cyberspace as being self-evident).

debate in depth elsewhere.[34] As such, it is of little value to explore it in detail again here. Nonetheless it is necessary to briefly clarify the extent to which article 2(4) has been seen as covering cyber-attacks.

Although article 2(4) itself is silent on the meaning of 'force', it became evident soon after the UN Charter's adoption that states interpreted 'force' as being limited to what might be thought of as 'military force', thus excluding from the concept various other activities that could also have been viewed as being 'forcible', such as economic or political coercion.[35] In the early legal literature concerning large-scale cyber threats, therefore, writers debated whether cyber aggression should be analogised to economic or political coercion (and thus be excluded from the scope of the prohibition), on the basis that the transfer of data in cyberspace was also an inherently 'non-physical' act,[36] or whether the potential military applications and destructive possibilities of cyber aggression meant that it should be analogised to conventional uses of military force (and thus covered by article 2(4)).[37]

This debate was largely resolved by moving away from a binary approach to determining whether cyber-attacks constituted acts of 'force', to one that focussed on the *effects* of any given cyber-attack.[38] States have long accepted that the use of certain weapons – such as chemical or biological weapons – are acts of 'force' prohibited by article 2(4) because they can cause devastating physical effects, irrespective of the fact that they do not necessarily

[34] JA Green, 'The Regulation of Cyber Warfare under the *Jus ad Bellum*' in JA Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015) particularly at 98-107.
[35] This is clear from the *travaux préparatoires* of the Charter in 1945 (see Documents of the United Nations Conference on International Organisation (UNCIO), vol VI: Commission I (General Provisions) (Library of Congress 1945), 720), as well as from subsequent state practice (see, e.g., *Report of the Special Committee on Principles of International Law Concerning Friendly Relations and Co-Operation Among States*, UN Doc. A/7619 (3 October 1969) paras 86-93; *Definition of Aggression*, GA Res. 3314 (XXIX) (14 December 1974). Scholars have also adopted this understanding of 'force': for the classic academic expression of this view, see TJ Farer, 'Political and Economic Coercion in Contemporary International Law' (1985) 79 AJIL 405.
[36] See, e.g., SP Kanuck, 'Information Warfare: New Challenges for Public International Law' (1996) 37 Harvard International Law Journal 272, 289.
[37] See, e.g., Morth (n 10) 591.
[38] See MN Schmitt 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Columbia Journal of Transnational Law 885 (the classic example of this approach being adopted in the cyber context).

constitute 'kinetic actions' in themselves.[39] An 'effects-based' approach to the meaning of 'force' in article 2(4) has now similarly been widely adopted by scholars in the cyber context.[40] Under this more nuanced approach, some cyber-attacks would constitute uses of force, while others would not. Cyber-attacks that have notably injurious consequences – comparable to the effects of traditional methods of conducting warfare – are now generally seen as constituting a breach of article 2(4); inter-state cyber aggression resulting in less severe damage – more comparable to economic loss, for example – is not.

However, there remains controversy as to whether *severe but non-physical effects* are to be considered force, or whether it is only cyber-attacks that ultimately result in grave physical damage that qualify. For example, Dinstein 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*'.[41] Under this understanding, a cyber-attack that results in large-scale physical damage or violence qualifies, while all other cyber-attacks do not. The sorts of 'cyber doomsday scenarios' noted above 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.

Yet it is entirely possible that an attack that, for example, 'corrupts data on a stock exchange and which in turn causes widespread economic harm but no direct physical damage'[42] could in some cases constitute 'a disaster', irrespective of the fact that it resulted in no direct

[39] MN Schmitt, 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts' (Committee on Deterring Cyber Attacks, National Research Council, The National Academic Press, 2010) 154; M Roscini, 'World Wide Warfare – *Jus ad Bellum* and the Use of Cyber Force' (2010) 14 Max Planck YB of United Nations Law 85, 106.
[40] See, e.g., E Haslam, 'Information Warfare: Technological Changes and International Law' (2000) 5 JCSL 157, 165; DB Silver, 'Computer Network Attack as a Use of Force under Article 2(4)' (2002) 76 International Law Studies 73, 84-92; Kodar (n 33) 139; J Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24 EJIL 129, 133.
[41] Y Dinstein, *War, Aggression and Self-Defence* (5th edn, CUP, 2011) 88, emphasis added.
[42] Goldsmith (n 40) 133.

physical effects.[43] The claim that the effects of a cyber-attack must be violent or physical in nature has thus been criticised on the basis that it is 'under inclusive', excluding too many cyber threats (including some large-scale threats) from the reach of article 2(4).[44] Some commentators therefore argue that cyber-attacks that are particularly severe in spite of not leading to physical destruction should be included.[45] The counter-argument to this 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 cyber acts to be included on the basis that their (non-physical) effects were particularly devastating would be to arbitrarily ignore the fact that other potentially equally injurious non-physical actions have long been considered excluded.[46]

Overall, while there is now a broad consensus that the term 'force' in article 2(4) covers large-scale cyber-attacks where the effects of those attacks are physical in nature, there is still significant uncertainty as to whether attacks with grave but non-physical effects can also be considered to be a violation of the prohibition.

3.3. The problem of attribution

Article 2(4) is directed only at *states*; specifically, it prohibits the use of force by members of the UN against other states. This means that for a cyber-attack to constitute a breach of article 2(4) it has to be attributed to a state actor: something that is extremely problematic in the cyber context.

---

[43] See A-M Osula, *EU Solidarity Clause and "Cyber Disaster"* (NATO Cooperative Cyber Defence Centre of Excellence, 19 November 2014) <https://ccdcoe.org/EU%20Solidarity%20Clause%20and%20Cyber%20Disaster.html> accessed 3 November 2015 (extrapolating that, for the European Union (EU), the notion of a cyber disaster 'does not seem to be necessarily tied to physical or financial damage').

[44] See, e.g., VM Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) 51 Naval Law Review 132, 155; SG Handler, 'New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare' (2012) 48 Stanford Journal of International Law 209, 229.

[45] See, e.g., Waxman (n 19) 435-6.

[46] See, e.g., W Banks, 'The Role of Counterterrorism Law in Shaping *ad Bellum* Norms for Cyber Warfare' (2013) 89 International Law Studies 157, 163.

States are legally responsible for the actions of their organs.[47] Thus, cyber-attacks perpetrated by members of a state's armed forces – or, indeed, by civilian hackers or programmers working directly for the state[48] – will be considered actions of the state and, therefore, potentially a breach of article 2(4). However, the cyber-attacks that have (allegedly) been perpetrated by a state up to this point have, in practice, commonly not come from the state's organs directly, but have instead involved a non-state actor undertaking the attack on behalf of the state.[49] Attacks of this kind are still attributable under the law of state responsibility: the actions of groups or persons 'acting on the instructions of, or under the direction or control of' the state are attributable to that state.[50] This means that a cyber-attack by a non-state actor that is directed/controlled by a state could constitute a violation of article 2(4) for which the state in question would be legally responsible.

The problem is that any *legal* attribution of cyber activity is predicated upon *factual* attribution. Questions of factual (or '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.[51] There are significant technical uncertainties in tracing the origins of cyber activities so as to be able to attribute them to any particular actor.[52] Admittedly, such problems are not, from a computer science perspective, always entirely insurmountable,[53] but they are considerable. The chances of factually – and

[47] See ILC, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*, UN Doc. A/56/10 (Rep. of the ILC on the work of its fifty-third session, 2001) art 4.
[48] ibid art 4; Roscini (n 39) 98.
[49] N Bussolati, 'The Rise of Non-State Actors in Cyberwarfare' in JD Ohlin, K Govern and C Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP, 2015) particularly at 118-22.
[50] Draft Articles on State Responsibility (n 47) art 8.
[51] N Tsagourias, 'Cyber-Attacks, Self-Defence and the Problem of Attribution' (2012) 17 JCSL 229, 233.
[52] J Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (The Penguin Press, 2011) 32; PW Singer and A Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (OUP, 2014) 75.
[53] NC Rowe, 'The Attribution of Cyber Warfare' in JA Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015).

therefore *legally* – attributing cyber-attacks to a state will, in most instances in the cyber context, be extremely small.[54]

This attribution problem is fundamental to the effectiveness of article 2(4) in relation to cyber disasters.[55] It is telling that, as yet, *no* act of cyber aggression has been conclusively factually (and, as a consequence, legally) attributed to a state.[56] If an attack cannot be attributed to a state it cannot be a violation of article 2(4). Irrespective of the prohibition's centrality to the legal literature concerning cyber threats, the application of article 2(4) to cyberspace thus remains hypothetical.

3.4. Cyber-attacks by non-state actors

The fact that article 2(4) is directed only at states creates a further issue with regard to its effectiveness in the cyber context: somewhat obviously, as the article prohibits the use of force by a state, cyber-attacks perpetrated by non-state actors entirely independently of a state are not covered by article 2(4) *at all*.

It is clear that it is not states but 'non-state actors [that] conduct the vast majority of harmful cyber operations'.[57] This means that most aggressive cyber acts fall entirely beyond the scope of the usual approach to cyber security focused on article 2(4). Admittedly, at present states remain the actors that are most likely to possess the technological resources to launch large-scale cyber-attacks. Given that this book is focussed on disasters, and thus the most catastrophic security threats, it should be kept in mind that state-authored cyber-attacks remain the most capable of inflicting such harm.[58] In other words, the likelihood of suffering cyber

[54] O'Connell (n 28) 202.
[55] Goldsmith (n 40) 136.
[56] Harrison Dinniss (n 29) 53.
[57] Schmitt, 'In Defense of Due Diligence in Cyberspace' (n 25) 77.
[58] M Korolov, '10 Deadliest Differences of State-Sponsored Attacks', *CSO Online* (1 December 2014) <http://www.csoonline.com/article/2852855/advanced-persistent-threats/10-deadliest-differences-of-state-sponsored-attacks.html> accessed 11 November 2015.

harm from a non-state actor is much greater than that of suffering it at the hands of state, but where the risk materialises in the latter case, the degree of the harm inflicted is likely to be greater.

Nonetheless, while no major act of cyber terrorism has yet occurred,[59] the ubiquity of non-state orchestrated cyber-attacks, the ever-increasing reliance on cyberspace and the inexpensiveness and anonymity associated with mounting cyber-attacks[60] mean that likelihood of a cyber disaster being caused by a non-state actor is very real.[61] Yet this threat is entirely outside of article 2(4)'s reach.

3.5. The possibility of accidental cyber disasters

Similarly, the predominant article 2(4) approach side-lines the fact that a cyber disaster could be caused entirely inadvertently. Not only is the prohibition of the use of force directed just at states, it also only prohibits the *deliberate* use of force: it is therefore relevant solely in relation to cyber-*attacks*. Accidental cyber disasters are simply beyond its scope.

It is undoubtedly the case that the potential exists for disasters to occur through cyberspace that were unintended, either because of human error or technological failure.[62] Indeed, some have argued that the greatest risk to cyber security *per se* is not the deliberate infliction of harm through cyberspace at all, but simply mistake.[63] The way in which cyber damage can 'cascade' (because of the inherent interconnectedness of cyberspace) means that even 'minor' cyber accidents have the potential to inflict great harm.[64] Despite the political and

[59] CE Lentz, 'A State's Duty to Prevent and Respond to Cyberterrorist Acts' (2010) 10 Chicago Journal of International Law 799, 807.
[60] JA Green, 'Introduction' in JA Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 2.
[61] MJ Sklerov, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent' (2009) 201 Military Law Review 1, 65; Lentz (n 59) particularly at 800; Bussolati (n 49).
[62] J Migga Kizza, *Computer Network Security and Cyber Ethics* (4th edn, McFarland and Company, 2014) 83.
[63] M Heatherly, 'How Prepared are we for Cyber Attacks and Other Disasters?' (2012) 66 Washington State Bar News 31, 31 (reporting the argument to this effect made by J Addicott, director of the Center for Terrorism Law at St Mary's University, Texas).
[64] Sommer and Brown (n 7) 32.

media fixation on the threat of cyber-*attack*, from the computer science perspective, there is little meaningful distinction to be made between deliberate cyber aggression and 'cyber mistake', in terms of the harmful effects that can be caused.[65] Again, the potential for accidental cyber disaster (or, indeed, accidental cyber harm of any scale) is not covered by article 2(4) at all.

4. An alternative approach: The duty of cyber due diligence

It is submitted, based on the forgoing, that article 2(4) is not an adequate legal mechanism to try to limit the occurrence of cyber disasters (or, at least, is inadequate as the primary legal mechanism in this regard). With no new cyber law on the horizon, there is a need to explore alternative existing provisions of international law that may be better able to reduce cyber threats. In particular, the present author takes the view that emphasis should be placed on a different norm of international law that has largely been overlooked in the cyber context: the duty of due diligence. This reorientation should not be to the total exclusion of the provisions of the *jus ad bellum*, *jus in bello*, or, indeed, other relevant norms of international law.[66] However, a focus on the duty of due diligence as the primary legal mechanism in relation to cyber security would circumvent many of the problems associated with the current emphasis on article 2(4).

4.1. The origins and nature of the duty of due diligence

[65] M Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (Routledge, 2008) 20.

[66] For example, a small number of writers have focussed on the principle of non-intervention in this context (see, e.g., Buchan (n 24); S Watts, 'Low-Intensity Cyber Operations and the Principle of Non-Intervention' in JD Ohlin, K Govern and C Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP, 2015)). However, the potential of this principle to effectively restrain inter-state cyber-attacks can be brought into question (see Banks (n 46) 170; Green (n 34) 107-10). Moreover, it is beset with many of the same problems as art 2(4) in the cyber context: an attack still needs to be attributed to a state, meaning that the principle is similarly inapplicable to both cyber-attacks by non-state actors and cyber accidents.

There is no single definition of the international legal duty of due diligence (also sometimes referred to as the 'duty to prevent'). It has been expressed in a variety of forms and applied in a range of contexts.[67] Similarly, the duty cannot be traced to a single legal source as such, although in a broad sense it derives from the principle of state sovereignty: a state enjoys rights to exercise sovereignty within its territory, but this comes with corresponding obligations to protect against activity occurring on that territory detrimentally affecting the territory of other states.[68] In its simplest form, therefore, the duty can be said to require that states take reasonable steps to ensure that activities on their territory do not cause transboundary harm.[69]

The duty of due diligence has been particularly embraced in the environmental law context.[70] Famously, the duty was set out and applied in the 1941 *Trail Smelter* arbitration, in which the Tribunal awarded damages to the United States in relation to air pollution that had emanated from Canadian territory: '[a] State owes at all times a duty to protect other States against injurious acts by individuals from within its jurisdiction.'[71] At least in the international environmental law context this duty has firmly solidified into a binding general principle of customary international law, as has been confirmed by the International Court of Justice (ICJ) in both its 1996 *Nuclear Weapons* advisory opinion[72] and the *Pulp Mills* merits decision of 2010.[73] However, the duty of due diligence has also taken on a life outside of the context of transboundary environmental harm. The ICJ applied it for the first time in 1949, in the *Corfu Channel* case, but did so not in relation to environmental damage. Instead, the Court found

[67] See, generally, JA Hessbruegge, 'The Historical Development of the Doctrines of Attribution and Due Diligence in International Law' (2003-04) 36 JILP 265.
[68] Schmitt, 'In Defense of Due Diligence in Cyberspace' (n 25) 71-2.
[69] See, generally, RP Barnidge, Jr, 'The Due Diligence Principle under International Law' (2006) 8 International Community Law Review 81.
[70] See, e.g., International Law Association Study Group on Due Diligence in International Law, *First Report*, (D French (Chair) and T Stephens (Rapporteur), 7 March 2014) <http://www.ila-hq.org/en/committees/study_ groups.cfm/cid/1045> accessed 27 October 2015.
[71] *Trail Smelter Case* (*United States*, *Canada*) (*)* Intl Arb. Rep. 1905 (Arbitral Trib., 11 March 1941) 1963.
[72] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)* ICJ Rep. 1996, 226 (8 July 1996) para 29.
[73] *Case concerning Pulp Mills on the River Uruguay (Argentine v Uruguay)* ICJ Rep. 2010, 14 (20 April 2010) para 101.

Albania to be in breach of the duty by failing to warn other states that its territorial waters were mined.[74] The ICJ has since affirmed the duty, in different forms, in various other international legal contexts.[75]

In terms of its content, it is important to note that – as its name suggests – the duty is not one of strict liability, but of *due diligence*.[76] The alternative name by which it is sometimes known, the 'duty to prevent', is therefore misleading. States do not have a duty to *prevent* transboundary harm; they have a duty to *take reasonable steps to try to prevent* such harm. The mere occurrence of transboundary harm does not entail a breach of duty; rather, a failure to have taken reasonable preventative measures in relation to that harm does.[77] This means that the duty entails a common but differentiated responsibility for states.[78] The actions that constitute reasonable steps towards prevention for one state – given, for example, the resources that it possesses – may be different from what can be reasonably expected of another.[79]

4.2. The possibility of applying the duty of due diligence to cyberspace

Two objections could be raised in relation to the potential applicability of the duty of due diligence to cyber security. First, it was argued by some scholars in the mid-1990s that cyberspace was a new 'non-territorial' realm where existing rules of state jurisdiction premised on territorial sovereignty were entirely defunct.[80] A duty that is tied to a state's ability to

[74] *Corfu Channel Case* (*United Kingdom v. Albania*), (Merits) (1949) ICJ Rep. 1949, 244 (ICJ, 9 April 1949) para 22.
[75] See, e.g., *United States Diplomatic and Consular Staff in Tehran* (*United States of America v Iran*) ICJ Rep. 1980, 3 (24 May 1980) paras 61-8; *Armed Activities on the Territory of the Congo* (*Democratic Republic of the Congo v Uganda*) ICJ Rep. 2005, 168 (19 December 2005) particularly paras 300-05; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (*Bosnia and Herzegovina v Serbia and Montenegro*) ICJ Rep. 2007, 43 (26 February 2007) particularly at paras 428-30.
[76] Roscini (n 29) 87-8.
[77] ILC, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities with Commentaries*, UN Doc. A/56/10 (Rep. of the ILC on the work of its fifty-third session, 2001) draft art 3(7), 391-2.
[78] ILA Study Group on Due Diligence (n 70) 27.
[79] C Antonopoulos, 'State Responsibility in Cyberspace' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) 69.
[80] For the classic expression of this view, see DR Johnson and DG Post, 'Law and Borders – The Rise of Law in Cyberspace' (1995-96) 48 Stanford Law Review 1367.

exercise its jurisdiction within its territory – to take steps to try to prevent harm emanating from it – would thus be useless in relation to such a 'space' that had no territorial nexus. However, while cyberspace is indeed a virtual realm it is also an *infrastructure*, and at least some of that infrastructure is necessarily physical in nature (and is, thus, inherently tied to territory).[81] It is today unquestionable that – as repeated and consistent state practice and *opinio juris* have made clear – states possess an inherent jurisdiction over cyber activities occurring on or emanating from their territory.[82]

Secondly, it could potentially be argued that states have not yet accepted the extension of the duty of due diligence to issues cyber security and that, as such, the duty is simply inapplicable in the cyber context.[83] It is true that states have been cautious in accepting the duty's applicability in cyberspace.[84] In 2013, for example, the UN General Assembly's 'Group of Governmental Experts', which was created as a state forum to consider issues of international cyber security, asserted that that states 'should' comply with the duty of due diligence in the context of cyber activity.[85] This is admittedly rather a tentative affirmation, given the use of the word 'should' as opposed to more obligatory language. Similarly, a number of states have expressed their individual view that the duty extends to cyberspace, but again, in most cases, they have used self-consciously equivocal language in so doing.[86]

---

[81] PW Franzese, 'Sovereignty in Cyberspace: Can it Exist?' (2009) 64 Air Force Law Review 1, 12.
[82] Heinegg (n 23) 126, 132-3; U Kohl, 'Jurisdiction in Cyberspace' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015).
[83] Schmitt, 'In Defense of Due Diligence in Cyberspace' (n 25) 73 (noting, but not subscribing to this possible argument).
[84] ibid, 71-3.
[85] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98 (General Assembly, 68th sess, 24 June 2013) para 23.
[86] See, e.g., the United States' *International Strategy for Cyberspace*: *Prosperity, Security, and Openness in a Networked World* (May 2011) 10 <https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf> accessed 6 November 2011 (also using the word 'should' in relation to the duty's application in cyberspace); SP Kanuck, 'Sovereign Discourse on Cyber Conflict under International Law' (2010) 88 Texas Law Review 1571, 1591, both in the main text and in note 88 (quoting the statements by India, China and Russia, taking similar positions).

Nonetheless, these cautious references to due diligence obligations evidence a growing acceptance by states that the duty does have implications for cyber security. Perhaps more importantly, no states have explicitly *opposed* its relevance to cyberspace. The duty itself clearly already exists as a binding legal principle and, in international law, 'it is unnecessary to identify a distinct reason to apply a general principle in a particular context. On the contrary, since [the duty] is a general principle, *the presumption is that the principle applies* unless state practice or *opinio juris* excludes it'.[87]

The application of the duty of due diligence to cyberspace has been largely overlooked in the literature, but a small number of writers have begun noting its relevance over the last few years: academic support for it as an alternative to article 2(4) is growing.[88] It is also telling that the hugely influential *Tallinn Manual on the International Law Applicable to Cyber Warfare*, which was prepared by an international group of experts at the invitation of the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, affirmed the duty's applicability to cyberspace in 2013.[89] Given the *Tallinn Manual's* focus on cyber *warfare*, and thus its general alignment to the common 'militarised' legal approach, it is both encouraging that the duty was referenced in this way, but also unsurprising that this reference was rather cursory (the duty is set out as 1 of the manual's 96 listed rules, with some brief commentary). Yet work is currently underway on what has been dubbed 'Tallinn 2.0', an updated version of the manual, which is expected to be completed in 2016.[90] Interestingly, the project's director, Michael Schmitt, stated in 2015 that '[a]mong the topics the experts are examining is due

[87] Schmitt, 'In Defense of Due Diligence in Cyberspace' (n 25) 73, emphasis added.
[88] See, e.g., Heinegg (n 23) particularly at 135-8; Roscini (n 29) 40, 80-8; Green (n 34) particularly at 116-20; Schmitt (ibid); Antonopoulos (n 79) 65-70; SJ Shackelford, S Russell and A Kuehn, 'Defining Cybersecurity Due Diligence under International Law: Lessons from the Private Sector' in M Taddeo (ed), *Ethics and Policies for Cyber Warfare* (OUP, forthcoming 2016) (pre-publication SSRN version, 14 April 2015) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594323> accessed 17 November 2015.
[89] *Tallinn Manual* (n 22) rule 5, 26, emphasis added.
[90] See the NATO Cooperative Cyber Defence Centre of Excellence's official statement regarding the Tallinn Manual project and 'Tallinn 2.0' <https://ccdcoe.org/research.html> accessed 5 November 2015.

diligence, this time in a more systematic and in-depth fashion.'[91] It is therefore possible that Tallinn 2.0 might provide the first detailed guidance as to how the duty should operate in relation to cyberspace.

It is evident that recognition of the relationship between the duty of duty diligence and cyber security is snowballing, with increasing support for its application in academia and, more importantly, a growing – if admittedly as yet not overwhelming – acceptance of its applicability by *states*. There is, in the view of the present author, no legal barrier to applying the duty to cyber threats in principle.

4.3. The advantages of applying the duty of due diligence to cyberspace

There are a number of advantages to emphasising a duty of cyber due diligence. For example, reference to the duty circumvents the uncertainty as to which cyber activities constitute a breach of article 2(4). A state's failure to take reasonable steps to prevent large-scale but 'non-physical' cyber-attacks from emanating from its territory would be just as much a breach of the duty as would be a corresponding failure with regard to attacks with direct physical consequences: either way, harm would have occurred as a result of that failure. The categorisation issues that plague article 2(4)'s coverage of cyber operations are sidestepped.

Perhaps more importantly, the inherent difficulty in attributing cyber-attacks to a state actor would be significantly minimised if such attacks were considered through the prism of the duty of due diligence. This is not because, as some have incorrectly argued,[92] a state's failure to prevent cyber-attacks from emanating from its territory would mean that it is legally responsible for those attacks. As noted above, a breach of the duty would entail state responsibility not for the cyber-attack itself, but for a failure to meet a separate obligation to

[91] Schmitt, 'In Defense of Due Diligence in Cyberspace' (n 25) 71.
[92] Graham (n 33) particularly at 92-6; C Lotrionte, 'State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights' (2012) 26 Emory International Law Review 825, 853-4.

take reasonable steps to prevent it.[93] Under the duty, the perpetrator is responsible for the act, whereas the state is responsible for something else: the 'act', as it were, of not taking reasonable measures to stop the act.[94]

This means that to find the state in breach of the duty of due diligence, the *exact* entity that conducted the cyber-attack would not need to be established at all, as the duty does not relate to the primary act itself. The duty would, like article 2(4), encompass attacks where the state itself was undertaking or directing the attack, but state involvement in the attack would not need to be established, either legally or factually. States would not be able to hide behind attribution issues, because their legal duty would not rest on whether or not they were the perpetrator. Problems of attribution are thus significantly minimised, to the point that Antonopoulos has argued that the duty of due diligence will 'in most cases [be] *the only ground* for establishing [state] responsibility' for large-scale harm caused through cyberspace.[95]

For the same reason, the duty of due diligence can also (indirectly) extend states' legal responsibility to cover cyber-attacks launched entirely by non-state actors from within their territory.[96] Again, while the state would not be responsible for the non-state perpetrated attack itself, it would be responsible for any failure on its part to take reasonable steps to prevent the attack. It is worth noting that, in the twenty-first century, the duty of due diligence has clearly been viewed as being applicable in relation to international terrorism in general, and has been significantly emphasised in that context.[97] It has been convincingly argued that the responsibility of states to take measures to prevent their territory from being the source of

[93] Roscini (n 29) 40.
[94] C Ryngaert, 'State Responsibility and Non-State Actors' in M Noortmann, A Reinisch and C Ryngaert (eds), *Non-State Actors in International Law* (Hart, 2015) 177 (in reference to the duty in general).
[95] Antonopoulos (n 79) 66, emphasis added.
[96] Roscini (n 29) 80-8.
[97] See, e.g., the obligations set out by the UN Security Council in Resolution 1373, UN Doc. S/RES/1373 (28 September 2001), immediately following the atrocities of 9/11 (requiring states to take preventive steps in relation to terrorist activity). For general discussion of the application of the duty to terrorist activity, see T Becker, *Terrorism and the State: Rethinking the Rules of State Responsibility* (Hart, 2006), 138-46, 341-5; RP Barnidge, Jr., *Non-State Actors and Terrorism: Applying the Law of State Responsibility and the Due Diligence Principle* (TMC Asser Press, 2008).

terrorist attacks equally applies to acts of cyber terrorism.[98] Indeed, there is no reason why this would not be the case.

As yet, commentators have not meaningfully engaged with whether the duty would also incorporate a requirement for states to take reasonable steps to protect against *accidental* cyber damage emanating from their territory being inflicted on other states.[99] However, it has long been accepted in the environmental law context that the duty extends not just to deliberate transboundary environmental harm, but also to failures of due diligence with regard to the prevention of accidental damage.[100] Despite the fact that the focus on the duty of cyber due diligence thus far in the literature (to the limited extent that there has been any focus at all) has been on the duty acting as an alternative means of governing cyber-*attacks*, it is also entirely capable of encompassing a requirement for states take reasonable precautionary measures to protect against accidental cyber disaster.[101] By analogy to the environmental context, at least, this would seem a correct understanding of the duty's scope. In relation to cyber accidents, this would require states having to adopt measures to secure their own cyber infrastructure and to promote the 'cyber good hygiene' of, for example, corporations or other major legitimate non-state actors operating on their territory.[102]

4.4. The possible limitations of applying the duty of due diligence to cyberspace

The duty of due diligence is certainly not a panacea for the threat of cyber disaster. It is worth reemphasising, for example, that where a state has taken reasonable steps to prevent

[98] Sklerov (n 61) 65-7; Lentz (n 59); B Saul and K Heath, 'Cyber Terrorism' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) particularly at 148.
[99] Although see Shackelford, Russell and Kuehn (n 88) (who at least touch on this notion, if somewhat implicitly).
[100] See G Handl, 'State Liability for Accidental Transnational Environmental Damage by Private Persons' (1980) 74 AJIL 525.
[101] R Andorno, 'The Precautionary Principle: A New Legal Standard for a Technological Age' (2004) 1 Journal of International Biotechnology Law 11 (focussing on the precautionary principle, albeit not as an element of the duty of due diligence *per se*).
[102] See, generally, O'Connell (n 28) (albeit not specifically linking these concepts to the duty of due diligence).

cyber-attacks or harmful cyber accidents from occurring from within its territory, it would not be in breach of the duty of due diligence. Where a state is entirely unable to stop the harm from materialising, despite its best efforts, the state would not be legally responsible. It was noted above that states' obligations under the duty are context specific: therefore where cyber harm emanates from a state with limited technological or intelligence resources, it would be notably less likely that a breach of the duty on the part of the state concerned could be established. It is clear that an array of cyber threats will still exist beyond the reach of the duty of due diligence. However, it is submitted that far more cyber threats will be 'caught' by the duty than by article 2(4) of the UN Charter.

Similarly, in relation to the question of attribution – which forever plagues the law's ability to deal with cyber threats – one must be clear that factual attribution would, of course, still need to be established in relation to the duty of due diligence.[103] It still has to be proven that the harmful cyber act indeed emanated from the *territory* of the state in question[104] and that the state failed to take reasonable steps, in the context of the situation, to try to prevent this.[105] As a technical matter, identifying the physical source of cyber activity – attribution to a particular computer or device located in a particular territory – is certainly significantly easier than identifying the perpetrator themselves,[106] but it still remains far from easy.[107]

Cyber-attacks can, for example, be routed through computers located on a number of territories before reaching their target, making locating the original physical 'source' all the more difficult.[108] It is worth noting that it is entirely unclear at present whether states'

[103] Heinegg (n 23) 135.
[104] M Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' in JD Ohlin, K Govern and C Finkelstein (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP, 2015) 225.
[105] See Becker (n 97) 341-5 (in relation to attribution and the duty of due diligence in general, not just in the cyber context).
[106] Rowe (n 53) 67.
[107] Sklerov (n 61) 71.
[108] EM Mudrinich, 'Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem' (2012) 68 Air Force Law Review 167, particularly at 198-200.

obligations under the duty of due diligence would extend to a requirement that they take reasonable steps to prevent not only cyber-attacks that originate on, but also those that pass *through* their territory.[109] If this were the case it would minimise the attribution problem associated with attacks 'transitioning' through a number of states, as all states that had computers on their territory through which the attack was routed would have a responsibility under the duty to take reasonable preventive steps. This would place an extremely onerous burden on states *from which the attack did not even truly originate*, however, to the extent that expecting them to take steps to guard against cyber-attacks briefly 'passing through' might not be 'reasonable' (meaning that the duty would not be breached by a failure to take such steps in any event).[110] Regardless, it is important to note that attribution problems certainly would not be overcome by applying the duty of due diligence, but they would undoubtedly be significantly lessened in comparison to the application of article 2(4).

Another concern associated with the application of the duty of due diligence to the cyber realm is that moving focus away from the *jus ad bellum* may act to dangerously limit the ability of a state to defend itself against cyber threats. A breach of article 2(4) will not necessarily, in itself, trigger the right for a state to use force in self-defence – this requires the occurrence of an 'armed attack',[111] which is an especially 'grave form' of the use of force'[112] – but the prohibition of the use of force does act as a 'gateway' to the right.[113] In other words, a violation of article 2(4) is a necessary, but not sufficient condition for states to respond in self-defence. A breach of the duty of due diligence *simpliciter* would therefore not, in itself at

[109] A Zimmermann, 'International Law and "Cyber Space"', *ESIL Reflections* (Vol 3(1), 10 January 2014) 4, <http://www.esil-sedi.eu/node/481> accessed 17 November 2015; Schmitt, 'In Defense of Due Diligence in Cyberspace' (n 25) 72-3; Shackelford, Russell and Kuehn (n 88) 10-12.
[110] Heinegg (n 23) 137-8.
[111] UN Charter, art 51.
[112] *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v United States of America*), Merits, ICJ Reports 14 (27 June 1986) para 191; *Oil Platforms* (*Islamic Republic of Iran v. United States of America*) Merits, ICJ Reports 161 (6 November 2003) para 51.
[113] Green (n 34) 110-12.

least, trigger the right of self-defence.[114] One might therefore argue 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', if it cannot take forcible measures to defend itself.[115]

This concern certainly should not be dismissed: however, it is not argued herein that the *jus ad bellum* has, or should have, *no role* in the legal regulation of cyber activity. In cases of extreme, large-scale disaster caused by a cyber-attack – a 'cyber 9/11' – it is fairly clear that not only will a *prima facie* breach of article 2(4) have occurred, but one rising to a sufficient level of gravity so as to trigger the right of self-defence.[116] This will also likely be the most appropriate response in such extreme cases: or, at least, it would be naive to expect that states would refrain from a military response having suffered a catastrophic attack (irrespective of the inherent attribution issues involved in identifying the perpetrator against which it should respond). It is also worth remembering that while a breach of the duty would not allow for self-defence in response, it can give rise to the right of the victim state to take non-forcible countermeasures.[117] It is not as though states would be left with no recourse. The *jus ad bellum*, and the right of self-defence in particular, should not be taken off the cyber table, but should nonetheless be situated at the margins of the cyber threats debate: to only be called upon where absolutely necessary and in the most extreme cases.

Finally, it is important to note that the greatest strength of the duty of due diligence is also its most significant limitation.[118] The duty's value is to be found in its flexibility: it can be (and *has been*) adapted to numerous differing areas of international concern, and can

---

[114] K Ziolkowski, '*Ius ad bellum* in Cyberspace – Some Thoughts on the "Schmitt Criteria" for Use of Force' in C Czosseck, R Ottis and K Ziolkowski (eds), *4th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2012) 306-08. *Contra* Tallinn Manual (n 22) 29 (arguing that a breach of the duty may give rise to the right to respond in self-defence).
[115] Tsagourias (n 51) 242.
[116] See, e.g., Graham (n 33) 90-2; Waxman (n 19) 111; *Tallinn Manual* (n 22) 54-61.
[117] Roscini (n 104) 225. See also, in relation to countermeasures in the cyber context more generally, O'Connell (n 28) 204-5.
[118] P Birnie, A Boyle and C Redgwell, *International Law and the Environment* (3rd edn, OUP, 2009) 149.

realistically take into account what individual states can in fact achieve, and *be expected* to achieve, in terms of securing against extra-territorial harm. However, this flexibility also means that it can be very difficult to identify exactly what actions the duty obliges a particular state to take in any given circumstance.[119] The relatively limited engagement by states with the duty's role in the cyber context means that there is as yet almost no understanding of what the duty would require. At present, it is unclear exactly what practical, 'reasonable' steps states would need to take to comply with the duty in the cyber context:

> Some of the crucial, so far largely unanswered legal questions, deriving from this generally accepted, yet quite general, concept of due diligence, relate, when it comes to 'cyber space', to the specific content of such due diligence obligations, i.e. to *the question of what level of precautions a State has to undertake*, taking into account its level of technological development.[120]

In any context, the duty of due diligence will, in effect, be comprised on a number of smaller duties.[121] In relation to cyberspace, states are yet to elucidate what these 'sub-duties' are.[122] Similarly, academics have not yet provided much guidance either, although there have been tentative suggestions that the duty might require, *inter alia*, obligations to prosecute cyber-attackers, to spend on cyber investigation, review and security technology, and to share information on cyber activity, security and governance practices with other states.[123] The

[119] ibid 149-50.
[120] Zimmermann (n 109) 4, emphasis added.
[121] Sklerov (n 61) 62.
[122] Having said this, as long ago as 2000, the UN General Assembly 'not[ed] the value of' various measures that could be taken by states in relation to cyberspace, many of which look rather like the sorts of measures one would expect to be required under a duty of due diligence (albeit that the General Assembly did not explicitly link these to the duty): *Combating the criminal misuse of information technologies*, GA Res. 55/63 (4 December 2000).
[123] See, e.g., Sklerov (n 61) 62; Shackelford, Russell and Kuehn (n 88) 7.

current pressing issue is to determine *how* the duty of due diligence should be applied to cyberspace in a practical sense.

Despite the contextual – rather than absolute – nature of the duty of due diligence, there is no question that its application will place a notable burden on states in the cyber context.[124] While they are increasingly (if rather slowly) accepting the fact that the duty applies to cyberspace, it remains to be seen – when it comes to determining what onerous requirements that translates to in practice – the extent to which states will *comply* with the duty, or at least do so effectively. This concern is amplified when it is considered that the differentiated responsibilities and 'reasonableness' criterion at the heart of the duty inevitably leave states with significant 'eye of the beholder' wiggle room as to how to apply it.

5. Conclusion

The threat of cyber-inflicted disaster looms large. However, there remain few bespoke rules of international law governing cyber threats, and there is little prospect of a new cyber security treaty emerging any time soon. The common approach to dealing with large-scale cyber threats has therefore been to apply the existing prohibition of the use of force under article 2(4) of the UN Charter. However, this is highly problematic. It is unclear exactly which cyber-attacks are covered by article 2(4), and particularly whether attacks that do not directly cause physical results will fall within its scope. More importantly, the current legal focus on article 2(4) does not sufficiently take into account the difficulties in attributing a cyber-attack to a state and covers neither cyber-attacks by non-state actors nor unintended cyber harm.

It has therefore been argued herein that focus should be reoriented to another existing international legal obligation: the duty of due diligence. This duty can act as a more effective means of trying to prevent cyber disasters. It does not require that the acts that the law is seeking

[124] Schmitt, 'In Defense of Due Diligence in Cyberspace' (n 25) 80.

to prevent are attributable to a state, but rather that states must take reasonable steps to stop such acts occurring on their territory. It therefore has the potential to limit the occurrence of attacks by non-state actors and unintentional cyber disasters. Beyond these tangible benefits, as discussed in this chapter, it is also the view of the present author that a focus on a duty that stems from notions of communitarian, environmental value and good neighbourliness is significantly preferable in terms of the cultural conception of cyber threats at the international level, than a militarised focus that inherently antagonises cyberspace *per se* and increases the likelihood of escalating cyber harm.

States are now beginning to broadly accept that the duty of due diligence can be, and should be (if, perhaps not yet that it *must* be) applied to issues of cyber security. What remains unclear is the *way* in which it will be applied and the exact obligations that it will entail: as yet, 'international law … does not spell out in detail how nations should go about enhancing their cybersecurity to account for emerging due diligence obligations'.[125] The ideal solution to this uncertainty remains that all international legal standards relevant to cyber security are crystallised in an international treaty. This could spell out how the *jus ad bellum* and *jus in bello* rules relate to the most extreme cases of cyber catastrophe, but more importantly, it could 'elaborate what [is] required of states' responsibilities in terms of due diligence.'[126] Being rather more realistic, however – given the current unlikelihood of such a treaty appearing – the hope is that the Tallinn 2.0 process can provide some clarity to the notion of cyber due diligence, which will then inform increased state engagement with the duty in this context. A shift in academic focus away from militarised legal solutions and towards the duty of due diligence can also help to change state perceptions in this regard. This change cannot come

[125] Shackelford, Russell and Kuehn (n 88) 3 and 14 (quoted at 14).
[126] ME O'Connell and L Arimatsu, 'Cyber Security and International Law', *Chatham House* (Meeting Summary (E Wilmshurst, chair), 29 May 2012) 11 <http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf> accessed 23 October 2015.

quickly enough, as the duty currently represents international law's best means of reducing the potential for cyber disasters to occur.

Selected Bibliography:

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions' (2012) 17 JCSL 212

Green JA (ed.), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge, 2015)

Harrison Dinniss HA, *Cyber Warfare and the Laws of War* (CUP, 2012)

Heintschel von Heinegg W, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 International Legal Studies 123

Lentz CE, 'A State's Duty to Prevent and Respond to Cyberterrorist Acts' (2010) 10 Chicago Journal of International Law 799

Morth TA, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 30 Case Western Reserve Journal of International Law 567

O'Connell ME, 'Cyber Security without Cyber War' (2012) 17 JCSL 187

Ohlin JD, Govern K and Finkelstein C (eds), *Cyber War: Law and Ethics for Virtual Conflicts* (OUP, 2015)

Rid T, *Cyber War Will Not Take Place* (Hurst, 2013)

Roscini M, *Cyber Operations and the Use of Force in International Law* (OUP, 2014)

Schmitt MN (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, CUP, 2013)

Schmitt MN, 'In Defense of Due Diligence in Cyberspace' (2015) 125 Yale Law Journal Forum 68

Shackelford SJ, Russell S and Kuehn A, 'Defining Cybersecurity Due Diligence under International Law: Lessons from the Private Sector' in Mariarosaria Taddeo (ed), *Ethics and Policies for Cyber Warfare* (OUP, forthcoming 2016) (pre-publication SSRN version: 14 April 2015 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594323>)

Sklerov MJ, 'Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent' (2009) 201 Military Law Review 1

Tsagourias N and Buchan R (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015)