British Institute of International and Comparative Law

# A DUE DILIGENCE STANDARD OF ATTRIBUTION IN CYBERSPACE

LUKE CHIRCOP*

**Abstract** The technical and legal challenges of attribution in cyberspace prevent the meaningful operation of the international law framework of State responsibility. Despite the anticipation surrounding its publication, the *Tallinn Manual 2.0* went no further than its predecessor in offering a cogent legal solution to this problem. Instead, the Manual confined its analysis of attribution to the well-known provisions of the International Law Commission's Articles on State Responsibility. This article departs from the *Tallinn Manual 2.0* in arguing that the due diligence principle offers a preferable and appropriate standard of attribution in cyberspace.

**Keywords**: Public international law, attribution, cyber, due diligence, State responsibility, *Tallinn Manual 2.0*.

## I. INTRODUCTION

The attribution to States of cyber operations[1] presents unique technical and legal challenges that international law has so far inadequately addressed. As a result, for all its virtues, cyberspace remains a domain in which the actions of unscrupulous States and opportunistic hackers can threaten peace and security internationally. In the absence of an effective State responsibility regime, a strong commitment to existing international law and respect for the rule of law can wane. But as Toomas Hendrik Ilves, former President of Estonia, stated in his foreword to the *Tallinn Manual 2.0*, it is misleading to dismiss international law as 'window-dressing on realpolitik'.[2] This article contends that adopting a due diligence standard of attribution in cyberspace would be an effective means of ensuring that cyber operations are appropriately governed by the international law framework of State responsibility. While the attention of some has moved to 'second generation'

* Juris Doctor, Melbourne Law School, University of Melbourne, lchircop93@gmail.com. The author would like to thank Rain Liivoja for his guidance and support in the preparation of this article.

[1] 'Cyber operation', as used in this article, refers to all conduct which, if attributed to a State, would constitute an internationally wrongful act.

[2] TH Ilves, 'Foreword' in MN Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) xxiii.

[*ICLQ* vol 67, July 2018 pp 643–668] doi:10.1017/S0020589318000015

cyberspace issues, such as the operation and enforcement of obligations,[3] attribution continues to be an unresolved precondition of legal responsibility.[4] Furthermore, those who have dealt with attribution in cyberspace have often done so in a perfunctory way.

This article seeks to offer a comprehensive account of the due diligence principle and its relevance to State responsibility in the cyber context. The general applicability of due diligence to the cyber domain is not disputed. On the contrary, it has been widely accepted that States must not allow their territory to be used for cyber operations which produce serious adverse consequences for other States.[5] However, it is generally assumed that when a State fails to act with due diligence, it is merely responsible for a procedural failing. This is the view adopted by the International Group of Experts (IGE) who prepared the *Tallinn Manual 2.0*, the most recent and notable attempt at an 'objective restatement of the *lex lata*' pertaining to cyber operations.[6] Specifically, the Experts were 'careful to distinguish application of the due diligence principle from the international wrongfulness of the particular cyber operation that has been mounted from … the State's territory'.[7] They did so because they considered that the question of attribution was dealt with exhaustively by the *Articles on the Responsibility of States for Internationally Wrongful Acts* (Articles on State Responsibility).[8] In the lexicon of the International Law Commission (ILC), the IGE treated the due diligence principle as a primary rule of international law, which gave content to an international obligation.[9] This article departs from the conclusion of the *Tallinn Manual 2.0* in this regard. Instead, it is argued that due diligence

[3] B Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace' in K Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO Cooperative Cyber Defence Centre of Excellence 2013) 189, 194.

[4] J Crawford, *State Responsibility: The General Part* (Cambridge University Press 2013) 113.

[5] MN Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) 30 (Rule 6) (*Tallinn Manual 2.0*); *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 (24 June 2013) [23] (GGE Report 2013); *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/70/174 (22 July 2015) [13](c), [13](f) (GGE Report 2015); MN Schmitt, 'In Defence of Due Diligence in Cyberspace' (2015) 125 YaleLJ Forum 68, 69–71.

[6] Schmitt, *Tallinn Manual 2.0* (n 5) 3.

[7] ibid 42 (Rule 6, [44]).

[8] ibid 79, 87–104 (Rule 15–18).

[9] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, UN Doc A/56/10 (2001) 31 (General Commentary, [1]) (Articles on State Responsibility Commentaries). See also MN Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017) 42 Yale Journal of International Law Online 1, 11 <https://campuspress.yale.edu/yjil/files/2017/08/Schmitt_Grey-Areas-in-the-International-Law-of-Cyberspace-1cab8kj.pdf>.

should operate as a secondary rule of international law, setting out a general condition for State responsibility in the context of cyberspace.[10]

A due diligence failure occurs when a State has knowledge of a cyber operation being carried out from within its territory, contrary to the rights of another State, and fails to take reasonable measures to prevent it.[11] In such cases, the unlawful cyber operation should be attributable to the State, which would then incur responsibility for any resulting violation of international law. The purpose of formulating due diligence as a secondary rule in this way is the promotion of peace and security in the international system.[12] Making the attribution of cyber operations to States less difficult increases the potential accountability of States for nefarious cyber activities that they might tolerate within their territory, or carry out themselves. Were due diligence to operate as a primary rule of international law, as contemplated by the IGE, this could not be as effectively achieved. In particular, the regime of countermeasures provided for in international law could not be fully relied upon by States seeking to resolve cyber-related disputes.[13] The remainder of Part I identifies the limitations of applying the existing attribution framework to cyber operations and addresses alternative scholarly responses to this problem. The following three parts then consider in more detail the content (Part II), the rationale (Part III), and the source (Part IV) of the due diligence principle as a standard of attribution in cyberspace.

### *A. Bridging the 'Gap': Shortcomings of the Existing Attribution Framework*

The law of State responsibility has a clear framework in customary international law, codified by the ILC in their Articles on State Responsibility.[14] Conduct will be attributed to a State if there is a sufficient nexus between the actor who carried out the conduct, and the State. That nexus is satisfied when the actor is a State organ,[15] a person exercising government authority,[16] or is under the direction or control of the State.[17] However, this framework is frustrated in the context of cyber operations. In particular, there is a 'three-level problem of attribution in cyberspace' which inhibits back-tracing the harmful effects of a cyber operation to a responsible State.[18]

[10] Despite this departure, this article accepts the *content* given to the due diligence principle in *Tallinn Manual 2.0*: see below Pt II. [11] See below Pt II. [12] See below Pt III(A).
[13] See below Pt III(B).
[14] *Responsibility of States for Internationally Wrongful Acts*, GA Res 56/83, UN Doc A/RES/56/83 (28 January 2002, adopted 12 December 2001) annex (Articles on State Responsibility).
[15] ibid art 4; *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights (Advisory Opinion)* [1999] ICJ Rep 62, 87 [62].
[16] Articles on State Responsibility (n 14) art 5. [17] ibid art 8.
[18] Pirker (n 3) 211. See also SJ Shackelford and RB Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 GeoJIntlL 971, 984–5.

First, there is the challenge of identifying which computer or computers were used to carry out a cyber operation.[19] Computer identification is only possible because a computer's IP address is unique, and in some cases this can be traced to reveal its precise location.[20] However, it is possible for an actor to mask their IP address when carrying out harmful cyber operations.[21] Moreover, actors can use network modification techniques to 'spoof' their identify, feigning the IP address of a computer in a location different to that where it actually is.[22] The internet, as has been observed, is 'one big masquerade ball', where actors 'hide behind aliases … [and] can surreptitiously enslave other computers'.[23]

Second, even if the computer used to carry out a cyber operation can be identified, this is of limited utility for the purposes of attribution. As attribution is predicated on the nexus between an actor and a State, attribution cannot be made out unless the person who was operating the computer can also be identified.[24] Naturally, the 'location of a computer rarely allows for definite conclusions regarding the identity of the individual operating the machine'.[25] This difficulty has been termed the 'human machine gap'.[26] It is for this reason that the mere fact that a cyber operation is carried out on a State's territory, or from a State's governmental cyber infrastructure, is insufficient to attribute the operation to that State.[27]

Third, even if an actor responsible for a cyber operation were identified, attribution would only occur in those cases where there was a sufficient legal nexus between that actor and the State. Problems of attribution at this third level of analysis[28] are not peculiar to the cyber context. Similar difficulties

[19] ET Jensen and S Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer' (2017) 95 TexLRev 1555, 1557–8; Z Huang, 'The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations' (2014) 14 Baltic Yearbook of International Law 41, 43; K Macak, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors' (2016) 21 JC&SL 405, 407–8; P Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 Melbourne Journal of International Law 496, 503.

[20] C Antonopoulos, 'State Responsibility in Cyber Space' in N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015) 55, 62; M Pihelgas, 'Back-Tracing and Anonymity in Cyberspace' in Ziolkowski, *Peacetime Regime for State Activities in Cyberspace* (n 3) 31, 33.

[21] N Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 JC&SL 229, 233; Shackelford and Andres (n 18) 981–2.

[22] Pirker (n 3) 212.

[23] M Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations' (2015) 50 TexIntlLJ 233, 234.

[24] Huang (n 19) 42.

[25] R Geiβ and H Lahmann, 'Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention' in Ziolkowski, *Peacetime Regime for State Activities in Cyberspace* (n 3) 621, 625. See also J Kulesza, 'State Responsibility for Cyber-Attacks on International Peace and Security' (2009) 29 PolishYBIntlL 139, 147–8.

[26] Geiβ and Lahmann (n 25) 625.

[27] MN Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 34 (Rule 7) (*Tallinn Manual 1.0*). There is no equivalent rule replicated in *Tallinn Manual 2.0*. See also Antonopoulos (n 20) 62; MN Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasure Response Option and International Law' (2014) 54 VaJIntlL 697, 708.

[28] See, eg, Crawford, *State Responsibility* (n 4) 147–56.

arise whenever it is asserted that the State is responsible for the conduct of an individual actor, and the Articles on State Responsibility are designed to address them. It is, therefore, the unique challenges presented by the first two levels of analysis—locating and identifying the computer and actor responsible for a harmful cyber operation—which cause the shortcomings of the existing State responsibility framework in the cyber context.

A further complicating factor for the attribution of conduct in cyberspace is the presence of active and sophisticated non-State actors.[29] These actors largely sit outside the scope of the framework of the Articles on State Responsibility, and so enjoy a relative degree of impunity for the harmful consequences of their conduct. Additionally, they will often act 'in varying degrees of support for particular [S]tates and their policy objectives'.[30] Therefore, great caution is needed when drawing inferences from surrounding political and contextual circumstances concerning the source of a particular cyber operation.[31] This is especially the case given that States are presumed to act in accordance with their international legal obligations.[32] What might, at first glance, appear to be a State-sponsored cyber operation could in fact be the work of a patriotic (but non-State) hacker.[33] In this way, an adequate legal response to the challenges of attribution in cyberspace must address two problems: first, when *States* carry out harmful cyber operations for strategic purposes they should be held responsible for their conduct despite the difficulties outlined above; and second, when *non-State actors* carry out harmful cyber operations, targeted States should, in appropriate circumstances, be able to have recourse to international law mechanisms for remedy and dispute resolution.

State-based efforts to address this problem have been met with limited success. The chief vehicle for the codification, by States, of international law pertaining to cyberspace was the work of the United Nations' Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security. The GGE produced three reports between 2010 and 2015, which represented the unanimous views of State-participants in the GGE process.[34] The two most

[29] Schmitt, 'Grey Zones in the International Law of Cyberspace' (n 9) 9.

[30] MN Schmitt and L Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution' (2014) 1 Fletcher Security Review 55, 55.

[31] JK Canfil, 'Honing Cyber Attribution: A Framework for Assessing Foreign State Complicity' (2016) 70 JIntlAff 217, 218–19.

[32] CE Foster, 'Burden of Proof in International Courts and Tribunal' (2010) 29 AustYBIL 27, 36; CF Amerasinghe, *Evidence in International Litigation* (Martinus Nijhoff Publishers 2005) 215.

[33] Canfil (n 31) 218. Uncertainty over Russian involvement in the 2007 cyber attacks against Estonia, North Korean involvement in the 2014 Sony Hack, and Russian involvement in the 2016 hack of the DNC, was caused by the prominence of patriotic hacker groups in each instance: T Payne, 'Teaching Old Law New Tricks: Applying and Adapting State Responsibility to Cyber Operations' (2016) 20 Lewis and Clark Law Review 683, 706.

[34] *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/65/201 (30 July 2010) (GGE Report 2010); GGE Report 2013 (n 5); GGE Report 2015 (n 5).

recent reports articulated non-binding norms, 'derived from existing international law',[35] which should apply to and govern State conduct in cyberspace.[36] Thus, the early work of the GGE held promise for the future crystallization of cyber-specific customary international law principles, or at best a comprehensive multilateral cyber treaty. A new GGE formed and was due to report to the United Nations General Assembly in 2017. However, the group was unable to reach consensus during its final session.[37] The group fragmented over controversial areas of international law, including the self-defence doctrine, countermeasures, and international humanitarian law.[38] While the previous GGE reports remain valid and applicable, the future of the GGE's work is uncertain.[39] Bilateral or regional efforts might now be required to propel the emergence of new or novel legal rules to adequately address the difficulties of attribution in cyberspace.

### *B. Evidence-Based Alternatives for Addressing Cyber Attribution*

Before proceeding, it should be noted that some scholars have suggested alternative means of addressing the unique difficulties presented by anonymity in the cyber context. In particular, it has been argued that rules of evidence are the most suitable vehicle through which attribution issues can be resolved. Proponents of these arguments observe that the shortcomings of attribution are of a 'technical and policy nature', pertaining to questions of fact, not law.[40] They submit that the Articles on State Responsibility offer a cogent legal framework for attribution provided there is sufficient evidence to identify the actor responsible for a cyber operation.[41] This reasoning has given rise to two distinct evidence-based 'solutions' to cyber attribution. First, it has been suggested that once it is clear that a cyber operation emanates from within a State's territory, there should be a 'presumption of [that State's] responsibility' for the operation, rebuttable by contrary evidence.[42] This amounts to a reversal of the burden of proof which ordinarily operates at international law.[43]

[35] GGE Report 2013 (n 5) [16]. [36] ibid [16]–[25]; GGE Report 2015 (n 5) [13].

[37] Geneva Internet Platform, *Digital Watch Newsletter: Issue 22* (30 June 2017) 1, 6 <https://dig.watch/sites/default/files/DWnewsletter22.pdf>.

[38] AM Sukumar, 'The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?' *Lawfare* (4 July 2017) <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>; E Korzak, 'UN GGE on Cybersecurity: The End of an Era?' *The Diplomat* (31 July 2017) <https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe>.

[39] Geneva Internet Platform (n 37); Sukumar (n 38); Korzak (n 38).

[40] Comment, 'Use of Force and Arms Control: State Department Legal Adviser Addresses International Law in Cyberspace' (2013) 107 AJIL 243, 247; Geiβ and Lahmann (n 25) 623.

[41] Geiβ and Lahmann (n 25) 623.

[42] Antonopoulos (n 20) 64. See also Margulies (n 19) 501, 515.

[43] *Pulp Mills on the River Uruguay (Argentina v Uruguay) (Judgment)* [2010] ICJ Rep 14, 71 [162] (*Pulp Mills*); Articles on State Responsibility Commentaries (n 9) 72 (Circumstances Precluding Wrongfulness, [8]); Roscini, 'Evidentiary Issues in International Disputes' (n 23) 243.

Arguments of this kind have, however, been strongly criticized. Given the possibility of routing cyber operations through transit States,[44] reversing the burden of proof might 'lead to wrong and even absurd results … and to the denouncing of wholly uninvolved and innocent States'.[45] For instance, the Stuxnet attack against Iran in 2010 emanated from computers in Denmark and Malaysia, two States who were 'clearly unaware' of the operation.[46]

Second, some have advocated for a relaxed standard of proof to accommodate the exigencies of the cyber context.[47] This argument can also be rejected. Standards of proof exist 'not to disadvantage' States harmed by cyber operations, 'but to protect … against false attribution'.[48] As such, there is no reason 'why the standard of proof should be lower simply because it is more difficult to reach'.[49] Furthermore, international courts have adopted increasingly consistent standards of proof when dealing with the same internationally wrongful acts.[50] On this basis, it is unlikely that a lower standard of proof would be adopted in the case of a cyber attack amounting to a use of force than would be adopted in the case of a kinetic attack violating the same principle. In contrast to evidential standards, the laws of State responsibility are flexible and responsive to different practical contexts.[51] As such, they offer the best vehicle for addressing the limitations of attribution in the cyberspace.

## II. CONTENT OF THE DUE DILIGENCE PRINCIPLE

Due diligence reflects a general principle of international law best articulated by the International Court of Justice (ICJ) in its *Corfu Channel* judgment: 'it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[52] Since *Corfu Channel*, due diligence has been particularized in various specialized regimes of

[44] Schmitt, *Tallinn Manual 1.0* (n 27) 36 (Rule 8, [1]).

[45] Geiβ and Lahmann (n 25) 628; Roscini, 'Evidentiary Issues in International Disputes' (n 23) 248.

[46] Geiβ and Lahmann (n 25) 628 n 43. Similarly, the DDoS attacks against Estonia in 2007 emanated from computers in Russia, as well as the United States, Canada, Europe, Brazil, Vietnam, and other countries: Roscini, 'Evidentiary Issues in International Disputes' (n 23) 248.

[47] Roscini, 'Evidentiary Issues in International Disputes' (n 23) 251. See also MC Waxman, 'The Use of Force against States that Might Have Weapons of Mass Destruction' (2009) 31 MichJIntlL 1, 62.

[48] Roscini, 'Evidentiary Issues in International Disputes' (n 23) 251.

[49] ibid.

[50] R Teitelbaum, 'Recent Fact-Finding Developments at the International Court of Justice' (2007) 6 The Law and Practice of International Courts and Tribunals 119, 125–6; Roscini, 'Evidentiary Issues in International Disputes' (n 23) 250; J Crawford, *Brownlie's Principles of Public International Law* (8th edn, Oxford University Press 2012) 38, 41.

[51] See below Pt IV(A)(2).

[52] *Corfu Channel (United Kingdom v Albania) (Judgment)* [1949] ICJ Rep 4, 22 (*Corfu Channel*).

international law.[53] This does not, however, preclude application of the principle in new or novel contexts. On the contrary, as due diligence is a general principle, 'the presumption is that it applies unless State practice or *opinio juris* excludes it'.[54] The *Tallinn Manual 2.0* contains a detailed and helpful analysis of how due diligence should be applied in cyberspace.[55] It is worthwhile briefly mapping out the principle's content, given that a natural concern with accepting a due diligence standard of attribution is that it would lead to indeterminate liability for States. As the following analysis will demonstrate, a State will only breach its obligation of due diligence in narrowly defined circumstances. In a sense, each element of the principle acts as a reasonable limitation on potential State responsibility. Specifically, a State will only fail to exercise due diligence when it has (1) knowledge of a cyber operation being carried out from within its territory, which is (2) contrary to the rights of another State, and it (3) fails to take feasible measures to prevent it.

The first element, knowledge, can be satisfied by both actual and constructive knowledge.[56] Whilst it might be difficult to ascertain evidence of a State's actual knowledge of a given cyber operation, a constructive knowledge standard ensures that the due diligence approach is not rendered all but redundant.[57] Pursuant to this standard, a State is taken to have knowledge of all things 'a similarly situated and equipped State in the normal course of events would have discovered'.[58] For instance, State knowledge is more likely to be ascribed for publicly known or easily detected uses of malware.[59] Furthermore, a State is more likely to have knowledge of the use of its governmental cyber infrastructure than it is of the use of private infrastructure in its territory.[60] If assuming knowledge is unreasonable in the circumstances, a State's due diligence obligation will not be engaged.

The second element, that the cyber operation be contrary to the rights of another State, is the least settled at international law.[61] It is sufficient to say for the purposes of this article that only cyber operations of a certain level of

[53] International Law Association, 'ILA Study Group on Due Diligence in International Law' (First Report, ILA, 7 March 2014).

[54] Schmitt, 'In Defence of Due Diligence in Cyberspace' (n 5) 73.

[55] This article departs from the treatment of due diligence in the *Tallinn Manual 2.0* only insofar as the Manual overlooks or rejects that attribution is an appropriate consequence of the principle's violation: Schmitt, *Tallinn Manual 2.0* (n 5) 42 (Rule 6, [44]).

[56] ibid 40 (Rule 6, [37]), 41 (Rule 6, [39]).

[57] See, eg, *Corfu Channel* (n 52) 22.

[58] Schmitt, *Tallinn Manual 2.0* (n 5) 42 (Rule 6, [42]). See also K Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?' (2014) 14 Baltic Yearbook of International Law 23, 30.

[59] Schmitt, *Tallinn Manual 2.0* (n 5) 41 (Rule 6, [40]).

[60] ibid.

[61] ibid 36 (Rule 6, [25]). See also Schmitt, 'Grey Zones in the International Law of Cyberspace' (n 9) 11–12. This mirrors ambiguity under international environmental law concerning the threshold of harm that will enliven a State's due diligence obligation in that context: International Law Commission, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with Commentaries*, UN Doc A/56/10 (2001) 152–3 (art 2, [4]–[7]); J Bunnée, 'Sic Utere Tuo Ut Alienum Non Laedas', *Max Planck Encyclopaedia of Public International Law* (Oxford University Press, March 2010) [12].

gravity will engage a State's obligation of due diligence. Specifically, the principle deals with cyber operations that amount to an internationally wrongful act,[62] and which result in serious adverse consequences for the target State.[63] This appropriately limits potential liability under the due diligence standard by excluding from its scope the vast number of minor cyber operations that are not regulated by international law.[64]

The third element, concerning feasible measures, provides that States are only required to intervene in a cyber operation when they have the capacity to do so, and when doing so is reasonable in the circumstances. This element offers the greatest protection to States against the imposition of indeterminate liability.[65] The 'feasibility' of measures for a State will vary based on the technical, intellectual and financial resources at its disposal.[66] As such, States will not violate international law for failing to prevent highly complex cyber operations that they lack the ability to control.[67] Furthermore, even in instances where States have the capacity to prevent harmful cyber operations carried out in their territory, they are under no obligation to do so when it would be unreasonable in the circumstances.[68] For instance, a State would very rarely, if ever, be required under a due diligence standard to act in a way that resulted in the self-denial of essential networks or important cyber infrastructure.[69]

In this way, the due diligence principle can operate as a standard of attribution in a clearly proscribed set of circumstances. While a fear of expanding State responsibility is understandable, it should be tempered by the limited scope of the doctrine. States will only ever be responsible for cyber operations with serious adverse consequences, which they have the capacity to identify and respond to. In such instances, if a State knowingly fails to curtail the harm inflicted upon a neighbouring State, why should international responsibility not follow?

## III. RATIONALE OF THE DUE DILIGENCE PRINCIPLE

### *A. Peace, Security and the Rule of Law*

An important rationale for adopting the due diligence principle as a standard of attribution is the contribution this would make to the maintenance of international peace and security. Despite early pronouncements that the internet would remain independent of the 'tyrannies' of elected government

[62] Schmitt, *Tallinn Manual 2.0* (n 5) 34–6 (Rule 6, [15]–[24]).
[63] ibid 36–9 (Rule 6, [25]–[31]). The IGE of the *Tallinn Manual 2.0* were unable to identify a 'bright line threshold' for the identification of such consequences.
[64] ibid 37 (Rule 6, [26]–[27]), 168 (Rule 32).
[65] See Schmitt, 'In Defence of Due Diligence in Cyberspace' (n 5) 74–5.
[66] Schmitt, *Tallinn Manual 2.0* (n 5) 47 (Rule 7, [16]).
[67] ibid 47 (Rule 7, [17]).
[68] ibid 49 (Rule 7, [24]). See also Bannelier-Christakis (n 58) 32–4.
[69] Schmitt, *Tallinn Manual 2.0* (n 5) 49–50 (Rule 7, [25]).

and sovereignty,[70] it is now generally accepted that cyberspace is governed by international law.[71] Were this not the case, cyber operations would occur in 'lacunae or "law-free zones" carrying the implication that lack of normative regulation may lead to any or unrestricted behaviour'.[72] The threat that an unregulated cyberspace could pose to the maintenance of international peace is clear. Cyber operations have the capacity to harm the security, economy and infrastructure of States on an equivalent scale to kinetic attacks. The main State participants in cyberspace are some of the world's most influential powers, including the United States, China and Russia. As these States are each equipped with a nuclear arsenal, the potential threat to the global community that might follow from escalating cyber conflict is apparent.[73] Furthermore, as noted earlier, the general accessibility of the cyber domain 'leaves the potential for mass destruction within the grasp of far less sophisticated [non-State] actors'.[74]

Even putting peace and security to one side, there are principled reasons why the application of international law is important in all spheres of State conduct. As then US Department of State Legal Advisor Harold Koh stated in 2012:

> International law … frees us and empowers us to do things we could never do without law's legitimacy. If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we do take will earn enhanced legitimacy worldwide for their adherence to the rule of law.[75]

Cultivating a culture of compliance with international law in the cyber realm is of intrinsic value to States, because it stands to legitimize their actions and demonstrate their status as good global citizens. This being said, the *effective* operation of international law in cyberspace is not a given. Considerable State-based[76] and scholarly[77] efforts to apply international law principles to the cyber context have not yielded encouraging practical outcomes. Despite the occurrence of more than ten serious publicly reported peacetime cyber operations in the past decade,[78] no cyber dispute has yet been brought before

[70] JP Barlow, *A Declaration of the Independence of Cyberspace* (8 February 1996) Electronic Frontier Foundation <https://www.eff.org/cyberspace-independence>.

[71] GGE Report 2013 (n 5) [16]; GGE Report 2015 (n 5) [1]; Schmitt, *Tallinn Manual 2.0* (n 5) 11 (Rule 1, [1]); Macak (n 19) 406; Margulies (n 19) 505; Pirker (n 3) 193–4; WH von Heinegg, 'Legal Implications of Territorial Sovereignty in Cyberspace' in C Czosseck, R Ottis and K Ziolkowski (eds), *4th International Conference on Cyber Conflict* (NATO Cooperative Cyber Defence Centre of Excellence 2012) 7.

[72] Antonopoulos (n 20) 57.

[73] Kulesza (n 25) 142.

[74] Payne (n 33) 685.

[75] Comment (n 40) 247.

[76] GGE Report 2010 (n 34); GGE Report 2013 (n 5); GGE Report 2015 (n 5).

[77] Schmitt, *Tallinn Manual 1.0* (n 27); Schmitt, *Tallinn Manual 2.0* (n 5).

[78] See, eg, Antonopoulos (n 20) 56 (Estonia 2007); Schmitt and Vihul (n 30) 55 (Agent.btz 2008); JE Messerschmidt, 'Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm' (2013) 52 ColumJTransnatlL 275, 276 (DDoS attacks against the US and South Korea 2009); G Brown and K Poellet, 'The Customary International Law of Cyberspace' (2012) 6(3) Strategic Studies Quarterly 126, 131 (Stuxnet 2010 and Google Hack 2010); M Roscini, 'Cyber Operations as a Use of Force' in N

an international court or tribunal. Perhaps more notably, no State has sought reparation from another State for harm caused by cyber operations, nor has any State responded to a cyber operation explicitly justifying their conduct as a countermeasure, or an act of self-defence or necessity.

The most likely explanation for this is that the challenges of attribution in the cyber context deter States from having recourse to traditional international systems of dispute resolution. This, in turn, limits the capacity of international law to mitigate conflict and facilitate peace and security between States and non-State actors. It also undermines the legitimacy and adherence to the rule of law that follows from a culture of compliance with international law. In fact, without an operative State responsibility framework, cyberspace is not so far from the lawless lacuna some hoped it would become. For this reason, a standard of attribution that more actively engages cyber operations with the existing international law paradigm is necessary.

### *B. Giving Effect to the Countermeasures Regime in Cyberspace*

A further (and related) rationale for a due diligence standard of attribution in cyberspace is that its current status as a primary rule of international law precludes meaningful engagement with the regime of countermeasures. It was assumed by the IGE of the *Tallinn Manual 2.0* that States targeted by the hostile cyber operations of other States could respond in kind with countermeasures.[79] It was further assumed that countermeasures would be similarly available to targeted States when another State failed to exercise due diligence.[80] However, where due diligence operates as a primary obligation of reasonable efforts, States harmed as a result of another's due diligence failure can only have recourse to a limited range of countermeasures by way of response. In particular, they cannot respond with measures of an equivalent scale or severity as the cyber operation they have fallen victim to. It is in this regard that the distinction between the status of due diligence as a primary rule and secondary rule becomes important. As stated, this article argues that the principle should operate as a secondary rule, pursuant to which States can incur direct responsibility. Only if this

Tsagourias and R Buchnan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015) 233, 244 (Saudi Aramco Hack 2012); Geiβ and Lahmann (n 25) 637 (US Department of Defense Hack 2012); Payne (n 33) 684 (Sony Hack 2014); E Nakashima, 'Chinese Breach Data of 4 Million Federal Workers' *The Washington Post* (4 June 2015) <https://www.washingtonpost.com> (US Office of Personnel Management Hack 2014); D Hollis, 'Russia and the DNC Hack: What Future for a Duty of Non-Intervention' *Opinio Juris* (25 June 2016) <http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention> (DNC Hack 2016).

[79] Schmitt, *Tallinn Manual 2.0* (n 5) 111 (Rule 20), 116 (Rule 21), 122–3 (Rule 22), 127 (Rule 23).

[80] ibid 50 (Rule 7, [28]).

https://doi.org/10.1017/S0020589318000015 Published online by Cambridge University Press

thesis is accepted will due diligence give holistic effect to the informal dispute resolution mechanisms envisaged by international law.[81]

Countermeasures are actions taken by a State that would otherwise violate international law, but which are permissible insofar as they respond to a breach of an international legal obligation owed to it by another State.[82] Given the difficulties of establishing State responsibility in the cyber context, the principle of due diligence has received particular attention in discussions of the self-help conduct that countermeasures enable.[83] As countermeasures permit States to carry out otherwise internationally wrongful conduct, they are subject to considerable limitations. Two of these limitations will be expanded on here: first, countermeasures must be directed towards inducing a State to comply with its international obligations (the purpose requirement);[84] and second, countermeasures must be proportionate to the gravity of the internationally wrongful conduct it is responding to (the proportionality requirement).[85] Were the due diligence principle to operate merely as a primary rule, the purpose and proportionality requirements would render ineffective the countermeasures available to harmed States.

The purpose requirement reflects the overarching objective of the countermeasure regime; that is, to induce States to cease internationally wrongful conduct.[86] As a corollary, countermeasures cannot be taken against non-State actors.[87] Furthermore, not only must they be taken 'in response to' another State's prior wrongful conduct,[88] but the countermeasure must be intimately related to the obligation breached. This requires careful examination of the legal character of the rights involved.[89] For instance, consider the countermeasures available to a State (State B) harmed by a cyber operation that another State (State A) failed to address in contravention of the due diligence principle. Further, presume that the due diligence principle

[81] This article assumes that countermeasures are an effective means for promoting peace and security. For a contrary view, that increased recourse to countermeasures might have a destabilizing effect on the international community, see Jensen and Watts (n 19) 1568–75.

[82] Articles on State Responsibility Commentaries (n 9) 75 (art 22, [1]); Schmitt, *Tallinn Manual 2.0* (n 5) 111 (Rule 20, [1]); *Gabcíkovo-Nagymaros Project (Hungary v Slovakia) (Judgment)* [1997] ICJ Rep 7, 55 [83] (*Gabcíkovo-Nagymaros*).

[83] See, eg, Schmitt, '"Below the Threshold" Cyber Operations' (n 27); N Tsagourias, 'The Law Applicable to Countermeasures against Low-Intensity Cyber Operations' (2014) 14 Baltic Yearbook of International Law 105.

[84] Articles on State Responsibility (n 14) art 49(1); Schmitt, *Tallinn Manual 2.0* (n 5) 116 (Rule 21).

[85] Articles on State Responsibility (n 14) art 51; Schmitt, *Tallinn Manual 2.0* (n 5) 127 (Rule 23); *Gabcíkovo-Nagymaros* (n 82) 56 [85].

[86] Articles on State Responsibility Commentaries (n 9) 130 (art 49, [1]).

[87] ibid 130 (art 49, [3]); Schmitt, *Tallinn Manual 2.0* (n 5) 113 (Rule 20, [6]–[7]). Countermeasures may, however, 'incidentally affect' non-State actors: Articles on State Responsibility Commentaries (n 9) 130 (art 49, [5]).

[88] *Gabcíkovo-Nagymaros* (n 82) 55 [83].

[89] MN Schmitt and MC Pitts, 'Cyber Countermeasures and Effects on Third Parties: The International Legal Regime' (2014) 14 Baltic Yearbook of International Law 1, 8.

operates as merely a primary rule of international law. Due diligence imposes an obligation of *conduct*, not of result.[90] Accordingly, State A's violation of international law might be the result of its failing to reasonably monitor its cyber infrastructure, or by failing to take reasonable steps to terminate the cyber operation. The only lawful countermeasures available to State B are those directed towards inducing State A to conduct itself more diligently. Importantly, State B would be unable to directly terminate the cyber operation itself. To do so would infringe the purpose requirement. It would be directed towards achieving a particular *result* (ending the cyber operation), which is not the touchstone of the international obligation breached (exercising diligent conduct). Proponents of the utility of due diligence in the cyber context have repeatedly misunderstood or overlooked this nuance.[91]

Now consider the same countermeasures scenario where due diligence operates as a secondary rule. State A's due diligence failure results in its international responsibility for the cyber operation harming State B. The relevant internationally wrongful conduct is not a failure of diligence in this case, but a direct violation of State B's sovereignty.[92] In this instance, State B could lawfully terminate the cyber operation itself, because in doing so it would 'directly achieve compliance' by State A with its obligation not to interfere with State B's sovereignty.[93] This is important because cyber operations can cause significant and irreversible harm. As such, an expedient and direct response by a targeted State will often be the most efficacious way to end or deescalate potential hostilities. If such a response to a harmful cyber operation is not directed to achieving compliance with international law, it will be inconsistent with the purpose requirement.

The proportionality requirement further demonstrates the virtues of due diligence as an attribution standard. Pursuant to this requirement, countermeasures must be 'commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act'.[94] Proportionality is concerned with 'the relationship between the internationally wrongful act and the countermeasure'.[95] This means that less grave violations of international law will result in more limited recourse to countermeasures by harmed States. As such, States injured by cyber operations who take countermeasures based on another State's due diligence failure (in the primary rule sense) must exercise great caution. The proportionality of their countermeasure will be assessed against the procedural failure to take reasonable preventive measures, not

[90] Schmitt, *Tallinn Manual 2.0* (n 5) 49 (Rule 7, [24]).

[91] Schmitt, 'In Defence of Due Diligence in Cyberspace' (n 5) 79; M Schmitt, 'Cyber Responses "By the Numbers" in International Law' EJIL: *Talk!* (4 August 2015) <https://www.ejiltalk.org/cyber-responses-by-the-numbers-in-international-law>; M Schmitt, 'International Law and Cyber Attacks: Sony v North Korea' *Just Security* (17 December 2014) <https://perma.cc/NE6S-NMH8>.

[92] See, eg, Schmitt, *Tallinn Manual 2.0* (n 5) 17 (Rule 4), 312 (Rule 66), 329 (Rule 68).

[93] ibid 117 (Rule 21, [3]).

[94] Articles on State Responsibility (n 14) art 51; Schmitt, *Tallinn Manual 2.0* (n 5) 127 (Rule 23).

[95] Articles on State Responsibility Commentaries (n 9) 135 (art 51, [7]).

against the severity or the consequences of the cyber operation itself.[96] This could curtail the effective operation of the countermeasures regime in cyberspace if it has a chilling effect on the willingness of harmed States to respond to cyber operations. Again, this is a concern overcome if the due diligence principle operates as secondary rule. Were this the case, the proportionality of a countermeasure would be measured against a direct violation of international law, as the cyber operation would itself be the internationally wrongful act. Accordingly, the harmed State could respond more appropriately to protect their interests.

The countermeasures regime is not the only means of international dispute resolution relevant to the cyber context, but it is a particularly important one. This is because, as noted already, States have been reluctant to bring disputes involving cyber operations before international courts or tribunals for adjudication. Furthermore, the two other notable self-help measures available to States harmed by cyber operations, self-defence and necessity, are only available in a far more limited range of circumstances. A State's inherent right of self-defence is engaged whenever they are targeted by a cyber operation that constitutes an armed attack.[97] While much ink has been spilled debating the precise content of 'armed attack' in the cyber context,[98] it is sufficient to note here that a cyber operation justifying self-defence would have to be of the scale and have an effect of the 'most grave forms of the use of force'.[99] The plea of necessity is similarly available to States when responding to certain harmful cyber operations. Necessity, it must be accepted, has some notable practical benefits given the difficulties of attribution in the cyber context;[100] actions taken based on the plea need not be a response to an internationally wrongful act,[101] and may be taken directly against non-State actors (or in cases where the originator of the precipitating

[96] Schmitt, *Tallinn Manual 2.0* (n 5) 130 (Rule 23, [11]); Schmitt, '"Below the Threshold" Cyber Operations' (n 27) 709.

[97] *Charter of the United Nations* art 51; Articles on State Responsibility (n 14) art 21; Schmitt, *Tallinn Manual 2.0* (n 5) 339 (Rule 71).

[98] The first edition of the *Tallinn Manual* was entirely directed towards articulating the international law regulating the conduct of armed conflict, encompassing both the *jus ad bellum* and *jus in bello*: Schmitt, *Tallinn Manual 1.0* (n 27) 4. See also Tsagourias, 'The Law Applicable to Countermeasures' (n 83) 114–15; Geiβ and Lahmann (n 25) 621–3.

[99] *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Judgment)* [1986] ICJ Rep 14, 103–4 [195] (*Nicaragua*); Schmitt, *Tallinn Manual 2.0* (n 5) 341 (Rule 71, [7]).

[100] See generally, on the application of the plea of necessity in cyberspace, C Schaller, 'Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity' (2017) 95 TexLRev 1619; MN Schmitt, 'Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum' (2017) 8 Harvard National Security Journal 239, 251–3; A Henriksen, 'Lawful State Responses to Low-Level Cyber-Attacks' (2015) 84 NordicJIntlL 323, 348–50; Schmitt, '"Below the Threshold" Cyber Operations' (n 27) 702–3.

[101] Articles on State Responsibility Commentaries (n 9) 80 (art 25, [2]); Schmitt, *Tallinn Manual 2.0* (n 5) 137 (Rule 26, [9]).

attack is altogether unknown).[102] However, like self-defence, necessity is only available in exceptional circumstances. Specifically, the plea will only preclude the otherwise wrongful conduct of a State if it is the only way to safeguard an 'essential interest' against a 'grave and imminent peril'.[103]

Importantly, preoccupation with cyber operations that would justify responsive action based on self-defence or necessity is 'counter-experiential'.[104] Few (if any) known cyber operations have crossed the armed attack threshold, or have been deemed sufficiently exceptional to justify a plea of necessity.[105] By contrast, cyber operations below that level are commonplace, and have been labelled 'the most pressing and potentially dangerous' threat to national and international security in recent times.[106] For this reason, the effective functioning of the countermeasures regime is essential to promoting international peace and security. It is the most appropriately designed mechanism for dealing with low-gravity cyber operations. Furthermore, it will be engaged most effectively if the due diligence principle is accepted as an attribution standard, rather than merely as a primary obligation of conduct.

## IV. SOURCE OF THE DUE DILIGENCE PRINCIPLE

The previous two parts have addressed the content of the due diligence principle, and the normative and legal rationales for its adoption. This part addresses the current status of the principle in international law. It does not go so far as to posit that the principle, as outlined, constitutes custom. Rather, it suggests that due diligence as a standard of attribution is reconcilable with existing regimes of international law, and that it could and should emerge as a customary norm in future. It proceeds in two parts: first, addressing the Articles on State Responsibility; and second, canvassing State practice and *opinio juris* that supports the emergence of the principle.

### *A. Articles on State Responsibility*

Since their completion in 2001, the Articles on State Responsibility have widely been accepted as an authoritative codification of well-established customary rules of international law relating to State responsibility.[107] Because of their pervasiveness, they are the starting point, and often the end point, of any discussion on the means of attribution. Articles 4–11 set out the laws of attribution, and do not provide for a standard of due diligence. Consistently with the prevailing understanding of the principle in international law, due

[102] Articles on State Responsibility Commentaries (n 9) 80 (art 25, [2]); Schmitt, *Tallinn Manual 2.0* (n 5) 137–8 (Rule 26, [10]–[11]).
[103] Articles on State Responsibility (n 14) art 25; Schmitt, *Tallinn Manual 2.0* (n 5) 135 (Rule 26). See also Articles on State Responsibility Commentaries (n 9) 81 (art 25, [5]).
[104] Schmitt, '"Below the Threshold" Cyber Operations' (n 27) 698.
[105] ibid.
[106] Bannelier-Christakis (n 58) 23.
[107] Antonopoulos (n 20) 58.

https://doi.org/10.1017/S0020589318000015 Published online by Cambridge University Press

diligence was contemplated by the ILC as a primary rule of international law.[108] As such, the future development of the due diligence principle as a secondary rule faces the challenge of having been considered, but ultimately overlooked, by the ILC when drafting their State responsibility framework. Thus, before discussing State practice and *opinio juris*, it is worth considering the extent to which the development of such a principle can be accommodated by the Articles on State Responsibility.

### *1. The ILC's drafting process*

The final formulation of the Articles' text was considerably shaped by the need for expediency and compromise. Due diligence played a 'significant role' in the earlier drafting efforts of the ILC.[109] However, controversy developed over whether an internationally wrongful act necessarily required the presence of an additional element of fault.[110] As such, in an attempt to find common ground, due diligence was shifted to the level of a primary rule,[111] and eventually, primary rules were altogether removed from the scope of the ILC's work.[112] The attribution standards that *were* included in the Articles were shaped by the historical context in which they were drafted. Specifically, they implicitly contemplate 'proxy wars fought by non-[s]tate actors' using 'conventional weapons' provided to them by States.[113] This is evidenced by the fact that the most relaxed attribution standard codified, that of 'direction or control',[114] derives its content from the ICJ's *Nicaragua* decision.[115] A key issue in that case was whether the United States should be held responsible for the 'planning, direction and support' it offered to the contras, an organized group who were fighting against the Nicaraguan government at the time.[116] In the cyber context however, non-State actors are less dependent on the support of State actors, and cyber weapons are far easier than conventional weapons to acquire and deploy. This is not to say, of course, that the Articles on State Responsibility are superfluous to the cyber context. However, the rejection of due diligence as an attribution standard in the Articles should be seen as a reflection of 'the exigencies of codification',

[108] Articles on State Responsibility Commentaries (n 9) 34 (art 2, [3]).
[109] T Koivurova, 'Due Diligence' *Max Planck Encyclopaedia of Public International Law* (Oxford University Press, February 2010) [4].
[110] ibid [5]; S Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility' in K Bannelier, T Christakis and S Heathcote (eds), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (Routledge 2012) 295, 302.
[111] Koivurova (n 109) [5].
[112] Ibid [6]; Heathcote (n 110) 303–4. See also Articles on State Responsibility Commentaries (n 9) 31 (General Commentary, [1], [4]), 34–5 (art 2, [3]).
[113] British Institute of International and Comparative Law, 'State Responsibility for Cyber Operations: International Law Issues' (Event Report, London, 9 October 2014) 4.
[114] Articles on State Responsibility (n 14) art 8.
[115] Articles on State Responsibility Commentaries (n 9) 47 (art 8, [4]).
[116] *Nicaragua* (n 99) 50 [86].

rather than any principled opposition to the doctrine operating as a secondary rule of international law.[117]

### 2. *Text, object and purpose*

Furthermore, the notion of *flexibility* is inherent in the nature of the Articles on State Responsibility. They are not a treaty. While it has been extensively cited by international courts and tribunals, the provisions contained within it merely reflect customary international law on State responsibility as it existed at the time of their drafting.[118] It is trite to recite that customary international law is created when general State practice is accompanied by the requisite *opinio juris*. However, the constituent elements of custom demonstrate its malleability. For as long as States are conducting their affairs in new contexts and novel ways, international law will continue to develop accordingly.[119] Although the Articles on State Responsibility were designed to set out general rules applicable to all fields of international law,[120] their comprehensive scope and authoritative tone may have triggered more deference than is warranted; it would be absurd to maintain that the laws of attribution were exhaustively settled in 2001.[121] On the contrary, for instance, the content of the 'direction or control' standard contained in Article 8 appeared to be in flux at least until the ICJ's 2007 *Bosnian Genocide* decision.[122] Moreover, the attention paid by international law to non-State actors following the September 11 attacks is in stark contrast to the Articles' State-centric approach to attribution.[123] It is not difficult to comprehend how the idiosyncratic characteristics of cyberspace might also challenge the assumptions underpinning the State responsibility framework, and in doing so prompt the development of new customary rules.

The flexibility of the Articles on State Responsibility is also acknowledged explicitly in its text. In particular, Article 55 provides that the ordinary rules of State responsibility 'do not apply where and to the extent that … responsibility of a [s]tate [is] governed by special rules of international law'.[124] This is a codification of the *lex specialis* maxim, a generally accepted technique for reconciling conflicting norms that deal with the same subject matter at international law.[125] Importantly, an entire regime of law is not required to

[117] Koivurova (n 109) [27].
[118] Antonopoulos (n 20) 58.
[119] MN Shaw, *International Law* (7th edn, Cambridge University Press 2014) 52.
[120] Articles on State Responsibility Commentaries (n 9) 31 (General Commentaries, [1]); Huang (n 19) 44.
[121] Margulies (n 19) 509; DD Caron, 'The ILC Articles on State Responsibility: The Paradoxical Relationship between Form and Authority' (2002) 96 AJIL 857, 861.
[122] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment)* [2007] ICJ Rep 43, 206–11 [396]–[407].
[123] Margulies (n 19) 509.
[124] Articles on State Responsibility (n 14) art 55.
[125] International Law Commission, *Conclusions of the Work of the Study Group on Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*, UN Doc A/61/10 (2006) [5].

displace operation of the ordinary rules of attribution. One aspect of general law 'may be modified, leaving other aspects still applicable'.[126] This would be the effect of introducing a previously unrecognized standard of attribution, like due diligence, but leaving applicable other attribution standards codified in the Articles.[127] In substance, applicability of the *lex specialis* doctrine turns on whether a new legal standard of attribution in the cyber context constitutes a 'special rule' within the meaning of Article 55. This inquiry prompts two related questions: are the existing attribution rules, established long before the formation of cyberspace, general enough to accommodate the peculiarities of cyber operations; and further, is the uniqueness of the cyber context 'special' enough to warrant the formulation of tailored rules of State responsibility?[128] This article has already addressed some of the novel challenges posed to existing attribution frameworks in cyberspace.[129] Of particular note is the evidential uncertainty that follows from a domain that is readily accessible to non-State actors, and in which technical anonymity continues to permeate.[130] It is unnecessary here to determine conclusively whether a due diligence standard of attribution could constitute a 'special rule' of international law within the meaning of Article 55. It is sufficient to note that the Articles on State Responsibility explicitly contemplate the formulation of additional rules to account for new contexts.

### 3. *Attribution in the International Court of Justice*

Finally, international courts have repeatedly engaged with novel arguments concerning the State responsibility framework. While judicial decisions are a 'subsidiary' source of international law,[131] pronouncements on issues of substance by the ICJ are generally considered to be of 'great weight'.[132] As such, the Court's willingness to accept new standards of attribution in appropriate circumstances is particularly instructive. It has done so on at least two occasions, in its *Corfu Channel* and *Armed Activities* decisions.

[126] Articles on State Responsibility Commentaries (n 9) 140 (art 55, [3]). The ILC provide the example of a treaty excluding a State from relying on *force majeure* or necessity, but leaving unchanged other circumstances precluding wrongfulness. Another example is art 91 of Additional Protocol I to the Geneva Conventions, which regulates State responsibility for acts committed during armed conflict but not peacetime: *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978) art 91.

[127] The norm 'inconsistency' for *lex specialis* to resolve, in such a case, would be between a due diligence standard of attribution (which clearly contemplates responsibility for the conduct of non-State actors), and the general principle that the only conduct attributable to States is that of its organs or agents: Articles on State Responsibility Commentaries (n 9) 38 (Attribution of Conduct to a State, [2]).

[128] Huang (n 19) 45.

[129] See above Pt I(A).

[130] Huang (n 19) 45.

[131] *Statute of the International Court of Justice* arts 38(1)(d), 59.

[132] Crawford, *Brownlie's Principles of Public International Law* (n 50) 78.

https://doi.org/10.1017/S0020589318000015 Published online by Cambridge University Press

While *Corfu Channel* preceded the completion of the Articles on State Responsibility, it nonetheless provided the seminal articulation of the due diligence principle as a primary rule of international law.[133] The dispute concerned Albania's responsibility for damage caused to two British warships by mine explosions in Albanian territorial waters.[134] Although Albania was not responsible for laying the mines,[135] its failure to warn incoming warships of imminent danger constituted a due diligence violation.[136] Submissions during the course of proceedings directed the ICJ to consider alternative attribution standards. In particular, the United Kingdom invoked the notions of 'complicity' and 'connivance' in attempting to impute Albania with responsibility for the creation of the minefield.[137] Complicity and connivance were formulated to more closely resemble a standard of attribution than a primary rule.[138] This submission was ultimately disregarded by the Court because of evidential uncertainty,[139] but the ICJ did not reject the formulation as a matter of principle.

In the *Armed Activities* case, the ICJ again took the opportunity to consider novel submissions concerning attribution. In this instance, the Court seemed to endorse a 'toleration' or 'acquiescence' standard for attributing uses of force to States. Specifically, it observed that two paragraphs of the *Friendly Relations Declaration*, which prohibited 'tolerat[ing]' or 'acquiescing in' acts constituting the use of force or civil strife, were 'declaratory of customary international law'.[140] This standard was then employed by the Court when assessing whether Congolese authorities had committed a use of force in supporting anti-Ugandan insurgents.[141] The ICJ concluded that, on the available evidence, it could not consider the Congo to have tolerated or acquiesced in the insurgent's activities.[142] In the alternative, it observed that Uganda had carried out an illegal use of force against the Congo on 7 August 1998, and any subsequent military action by Congolese authorities was justified

[133] *Corfu Channel* (n 52) 22. [134] ibid 15. [135] ibid 15–16. [136] ibid 22–3.

[137] 'Memorial Submitted by the Government of the United Kingdom of Great Britain and Northern Ireland', *Corfu Channel (United Kingdom v Albania)* [1947] ICJ Pleadings 19, 21 [4], 48 [94].

[138] Some scholars have likened 'complicity' to the 'aid or assistance' standard of attribution codified in art 16 of the Articles on State Responsibility: O Corten and P Klein, 'The Limits of Complicity as a Ground for Responsibility: Lessons Learned from the *Corfu Channel* Case' in K Bannelier, T Christakis and S Heathcote (eds), *The ICJ and the Evolution of International Law: The Enduring Impact of the* Corfu Channel *Case* (Routledge 2012) 315, 315, 332. However, in expanding upon the article's scope, the ILC at no point drew upon the *Corfu Channel* decision, nor made reference to 'complicity' or 'connivance': Articles on State Responsibility Commentaries (n 9) 65–7 (art 16, [1]–[11]).

[139] *Corfu Channel* (n 52) 16–17.

[140] *Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations*, UN Doc A/RES/25/2625 (24 October 1970) annex, [1] (*Friendly Relations Declaration*); *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Judgment)* [2005] ICJ Rep 168, 226–7 [162] (*Armed Activities*).

[141] *Armed Activities* (n 140) 262 [277], 268 [300].

[142] ibid 268 [301].

as action taken in self-defence.[143] In either case, the ICJ seems to have prima facie accepted the operation of a toleration or acquiescence standard for attributing uses of force.[144]

While the Court limited the toleration or acquiescence standard of attribution to uses of force in *Armed Activities*, it need not have done so. The *Friendly Relations Declaration* similarly requires States to act with vigilance to avoid intervention in another State's domestic affairs, territorial integrity, or sovereignty.[145] Furthermore, because *Armed Activities* was decided in 2005, four years after the completion of the Articles on State Responsibility, the decision lends support to the view that the Articles are inherently flexible. Given changes to the nature of interstate conflict as contemplated by the ILC during the drafting process, it is comprehensible that the cyber context might demand the application of new legal rules. If this is the case, a due diligence standard of attribution in cyberspace would not be antithetical to the Articles on State Responsibility. On the contrary, it would be entirely consistent with its text and historical treatment by international courts.

### B. *State Practice and* Opinio Juris

A due diligence attribution standard will develop in the cyber context if it is supported by generally uniform State practice and accompanying *opinio juris*.[146] While available evidence of such a customary rule does not meet this threshold, it has manifested to some degree in at least two ways. First, there has been an increasingly accepted recourse by States to self-defence in response to the conduct of terrorist organizations. While this does not directly implicate cyber operations, on one view, it does demonstrate a willingness to regulate non-State actors by altering the State responsibility framework. Second, through a number of multilateral agreements and resolutions, States have supported a due diligence standard of attribution as a means of addressing the unique vulnerabilities and threats arising in cyberspace.

#### 1. *Self-defence against non-State actors*

States have an inherent right to resort to force in self-defence when they are the victim of an armed attack.[147] Traditionally, this right was only thought to arise

[143] ibid 269 [304].

[144] Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (n 21) 243; Tsagourias, 'The Law Applicable to Countermeasures' (n 83) 113–14; C Focarelli, 'Self-Defence in Cyberspace' in N Tsagourias and R Buchnan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015) 255, 278.

[145] *Friendly Relations Declaration* (n 140) [1].

[146] *Statute of the International Court of Justice* art 38(1)(b); *North Sea Continental Shelf (Federal Republic of Germany v Denmark) (Merits)* [1969] ICJ Rep 3, 43 [74] (*North Sea Continental Shelf*); *Nicaragua* (n 99) 97–8 [184], 98 [186].

[147] *Charter of the United Nations* art 51; *Nicaragua* (n 99) 94 [176].

when the actor responsible for the armed attack was another State.[148] However, this assumption has been challenged by the invocation of the self-defence doctrine by States to justify their hostile responses to terrorist activities. The most commonly cited example of this trend is the United States' use of force against Afghanistan following September 11.[149] While the US was ostensibly responding to the conduct of Al-Qaeda, no distinction was made between the terrorist organization and the Taliban regime governing Afghanistan.[150] This example of State practice is particularly significant because it was followed by two Security Council resolutions affirming the legality of the United States' conduct.[151] However, it has also been reinforced by subsequent instances of States similarly responding to terrorist activity on the basis of self-defence. In 2002, Russia declared a right of self-defence against Georgia in response to the conduct of Chechen rebels.[152] In 2006, Israel relied on self-defence against Lebanon to counteract the conduct of Hezbollah.[153] Since 2014, the United States has justified its actions in Iraq and Syria as self-defence against the Islamic State.[154] And finally, a series of surgical strikes in 2016 by India against military launch pads used by terrorists in Pakistan have been justified on the basis of self-defence.[155]

The consistency of this practice, repeatedly endorsed by the United Nations,[156] has led some to suggest that the traditional understanding of the self-defence doctrine should no longer be maintained. Instead, support has emerged for a so-called 'unwilling or unable' doctrine.[157] While not always made explicit, the 'doctrine is split into two conceptually different subsets'.[158] The first, more prevalent view, is that there is now a discrete right of self-defence against terrorist organizations that arises when a territorial State is unwilling or unable to curb the organization's conduct.[159]

[148] Shaw (n 119) 823; Crawford, *Brownlie's Principles of Public International Law* (n 50) 771.

[149] See, eg, Focarelli (n 144) 276–7; Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (n 21) 243; Tsagourias, 'The Law Applicable to Countermeasures' (n 83) 113; Margulies (n 19) 509.

[150] Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (n 21) 242–3.

[151] SC Res 1368, UN Doc S/RES/1386 (12 September 2001) (SC Res 1368); SC Res 1373, UN Doc S/RES/1373 (28 September 2001) (SC Res 1373). But see Huang (n 19) 51–3; N Jupillat, 'Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Law of State Responsibility' (2015) 92 UDetMercyLRev 115, 122–4.

[152] Focarelli (n 144) 277–8 nn 152–3. [153] ibid 276–7.

[154] J Brunnée and SJ Toope, 'Self-Defense against Non-State Actors: Are Powerful States Willing but Unable to Change International Law?' (2018) ICLQ (forthcoming) 8–10; British Institute of International and Comparative Law (n 113) 5.

[155] A Banerjee, 'Indian Surgical Strikes: Accelerating the Emergence of Nascent Norms of Use of Force against Non-State Actors' Cambridge International Law Journal Blog (6 September 2017) <http://cilj.co.uk/2017/09/06/indian-surgical-strikes-accelerating-the-emergence-of-nascent-norms-of-use-of-force-against-non-state-actors>.

[156] See especially *Measures to Eliminate International Terrorism*, GA Res 49/60, UN Doc A/RES/49/60 (9 December 1994); SC Res 1267, UN Doc S/RES/1267 (15 October 1999); SC Res 1333, UN Doc S/RES/1333 (19 December 2000); SC Res 1368 (n 151); SC Res 1373 (n 151).

[157] Support for this doctrine is not uncontroversial though: see generally Brunnée and Toope (n 154). [158] Geiβ and Lahmann (n 25) 639. [159] ibid.

https://doi.org/10.1017/S0020589318000015 Published online by Cambridge University Press

This view, however, does not explain why tacit States must simply accept encroachments on their sovereignty as self-defence measures against non-State actors.[160] Furthermore, it considerably departs from the State-centric conceptualization of the use of force doctrine in Articles 2(4) and 51 of the *Charter of the United Nations*.

The alternative view, more akin to the approach taken in this article, is that a State's unwillingness or inability to repress terrorist activity within its territory results in the attribution of that activity to the territorial State.[161] As a result, because its direct responsibility has been engaged, responsive self-defence measures can lawfully be taken against the territorial State. This view should be preferred because it preserves the traditional conception of the self-defence doctrine, as applicable only in cases of an armed attack 'by one State against another State'.[162] Additionally, it is generally consistent with State practice. That is, States invoking self-defence have made concerted efforts to identify *a* nexus between a territorial State and the terrorist organization; this nexus is just one which falls below the 'direction or control' standard of attribution contained in the Articles on State Responsibility.[163] It is a nexus that can be seen as equivalent, in substance, to a due diligence standard of attribution. Such an attribution standard would not lead to unreasonable or excessive interference with a territorial State's sovereignty in this context because self-defence measures remain, as ever, strictly constrained by the requirements of necessity and proportionality.[164]

The acceptance of a due diligence standard of attribution in the terrorism context is important for the development of an equivalent standard in cyberspace. This is because the rationale for the acceptance of a tailored principle of State responsibility is identical in each case. Terrorist groups operate on a sub-national level, without a defined or consistent territory.[165] They utilize unconventional 'weapons' in their operations, and are not necessarily reliant on State support or training for their survival. Non-State actors in the cyber context similarly defy territorial conceptions of international relations, and the general accessibility of cyberspace has already been noted. Most importantly, the significant impact of both terrorist organizations and non-State hacker groups on international security was not

[160] ibid; CJ Tams, 'The Use of Force against Terrorists' (2009) 20 EJIL 359, 384.

[161] Geiβ and Lahmann (n 25) 639; Tams (n 160) 385; 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 MilLRev 1, 12–13, 38–9; Tsagourias, 'The Law Applicable to Countermeasures' (n 83) 113–14; Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (n 21) 243.

[162] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion)* [2004] ICJ Rep 136, 194 [139]. See also *Nicaragua* (n 99) 105 [200]; Tams (n 160) 363–4.

[163] Tams (n 160) 385.

[164] *Nicaragua* (n 99) 103 [194]; *Oil Platforms (Iran v United States of America) (Judgment)* [2003] ICJ Rep 61, 183 [43]; *Armed Activities* (n 140) 223 [147].

[165] SC Res 1373 (n 151) [2](g).

contemplated in the Articles on State Responsibility. As such, in both contexts, the need for recourse to self-defence against non-State actors is particularly compelling.[166] Such recourse only becomes practically possible, however, upon acceptance of a suitable due diligence standard of attribution.

### 2. Due diligence in cyberspace

State practice and *opinio juris* supporting a due diligence standard of attribution in cyberspace has arisen in three different ways. First, and most notably, a large number of States have assumed international obligations in the cyber context pursuant to the *Convention on Cybercrime* (*Cybercrime Convention*).[167] While treaties are a source of law in their own right,[168] they can also be a powerful expression by ratifying States of the legal obligations applicable in a particular field.[169] The *Cybercrime Convention* creates an obligation on States to domestically criminalize data interference and system interference,[170] and to enforce sanctions for non-compliance.[171] A duty to domestically criminalize nefarious cyber operations necessarily complements a more general duty of diligence.[172] As the ICJ observed in *Pulp Mills*, a due diligence obligation 'entails not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement'.[173] The *Cybercrime Convention* has been ratified by 55 States and signed, without ratification, by a further four States.[174] The Convention's obligations have also been echoed by the United Nations General Assembly, which has called on States to 'ensure their laws … eliminate safe havens for those who criminally misuse information technologies'.[175]

Second, a series of 'soft law' instruments have been produced, which endorse the taking of due diligence measures to prevent harmful cyber operations. Foremost among these are the United Nations' GGE reports, discussed above.[176] The 2013 GGE report prohibits the use, by States, of 'proxies to commit internationally wrongful acts' in cyberspace.[177] It further requires States to 'ensure that their territories are not used by non-[s]tate actors' for unlawful cyber purposes.[178] The 2015 GGE report acknowledges 'the challenges of attribution' in cyberspace.[179] Relatedly, it provides that States

[166] Focarelli (n 144) 280.
[167] *Convention on Cybercrime*, opened for signature 23 November 2001, ETS No 185 (entered into force 1 July 2004) (*Cybercrime Convention*).
[168] *Statute of the International Court of Justice* art 38(1)(a).
[169] Shaw (n 119) 58; Crawford, *Brownlie's Principles of Public International Law* (n 50) 24.
[170] *Cybercrime Convention* (n 167) arts 4–5. [171] ibid art 13.
[172] Geiß and Lahmann (n 25) 654. [173] *Pulp Mills* (n 43) 79 [197].
[174] Council of Europe Treaty Office, *Chart of Signatures and Ratifications of Treaty No 185: Convention on Cybercrime* (11 June 2017) <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures>.
[175] *Combatting the Criminal Misuse of Information Technologies*, GA Res 55/63, UN Doc A/RES/55/63 (22 January 2001) [1](a). [176] See above Pt I(A).
[177] GGE Report 2013 (n 5) [23]. [178] ibid. [179] GGE Report 2015 (n 5) [13](b).

https://doi.org/10.1017/S0020589318000015 Published online by Cambridge University Press

must not 'conduct',[180] 'support',[181] or 'knowingly allow'[182] their territory to be used for unlawful cyber operations. Notwithstanding the uncertain future of the GGE, both these reports substantively affirm a responsibility of due diligence for States in cyberspace. The norms and principles set out in each report are non-binding.[183] However, they are of weight as a codification effort achieved by government agents, in their official capacity, representing an 'equitable geographic distribution' of States.[184] Furthermore, each report has been unanimously adopted and affirmed by the United Nations General Assembly.[185] The sentiment of the 2013 and 2015 GGE reports is echoed by the works of the North Atlantic Treaty Organization (NATO). For instance, in terms more prescriptive than those adopted by the GGE, the NATO Cyber Defense Policy recognizes the 'responsibility' of States to protect their national networks, and in doing so to facilitate the 'detection' and 'prevention' of international cyber security threats.[186] Finally, the *Tallinn Manual 2.0* cannot be altogether ignored as a reflection of the practice and *opinio juris* of States.[187] It was drafted with the 'unofficial' assistance of over 50 States and international organizations, and the text was settled by the consensus of legal, academic, and technical experts.[188] It was intended as a 'reflection of the law as it existed' at the time of drafting,[189] and it extensively codifies a due diligence obligation.[190]

The third, and final, manifestation of State practice and *opinio juris* is the response of States to publicly known cyber incidents. Historically, even widely reported cyber operations have proved a limited source of evidence to support the formation of customary norms. For obvious reasons, States who have carried out hostile cyber operations rarely comment on their occurrence. States have also been reticent to officially comment on cyber operations they have been targeted by, even when they believe to have identified the perpetrator.[191] For instance, despite the extensive damage caused to the Natanz nuclear facility by the high-profile Stuxnet virus,[192] Iran resisted

[180] ibid [13](f). [181] ibid. [182] ibid [13](c).
[183] ibid [13]. See also GGE Report 2013 (n 5) [16].
[184] *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 66/24, UN Doc A/RES/66/24 (2 December 2011) [4] (GA Res 66/24); *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 68/243, UN Doc A/RES/68/243 (27 December 2013) [4] (GA Res 68/243). The 2013 GGE included representatives from 15 States. The 2015 GGE included representatives from 20 States (10 of which were not represented in 2013). On the impact of codification efforts on customary law generally: T Treves, 'Customary International Law', *Max Planck Encyclopaedia of Public International Law* (Oxford University Press, November 2006) [68]–[71].
[185] GA Res 66/24 (n 184); GA Res 68/243 (n 184); *Developments in the Field of Information and Telecommunications in the Context of International Security*, GA Res 70/273, UN Doc A/RES/70/237 (23 December 2015).
[186] North Atlantic Treaty Organisation, *World Summit Declaration* (5 September 2014) [72].
[187] Treves (n 184) [62]. [188] Schmitt, *Tallinn Manual 2.0* (n 5) 5–6. [189] ibid 2–3.
[190] ibid 30–50 (Rule 6–7). But see above Pt I(A) for the extent to which the principle discussed in this article departs from the one formulated in *Tallinn Manual 2.0*.
[191] Shackelford and Andres (n 18) 985. [192] Messerschmidt (n 78) 288–9.

https://doi.org/10.1017/S0020589318000015 Published online by Cambridge University Press

claims it had fallen victim to a cyber attack.[193] State responses of this kind are likely motivated by a desire to save face, and avoid alerting other States or non-State actors to particular cyber vulnerabilities. In recent years, however, there has been a gradual departure from this trend. In 2014, US President Barack Obama blamed North Korea for the hacking of Sony, and declared an intention to respond.[194] Shortly thereafter, North Korea experienced widespread unexplainable internet outages, which were assumed to be caused by a United States cyber operation.[195] In 2016, following the hack of the DNC's servers, three private cybersecurity firms concluded the responsibility of two Russian hacker groups with government connections.[196] A protracted official investigation confirmed the involvement of the Russian government in the hack, following which the United States responded with a number of lawful diplomatic sanctions.[197] While the Sony and DNC hacks are somewhat unique in this regard, they signal a greater willingness of States to openly attribute and respond to hostile cyber operations. The uncertainty and anonymity of the cyber sphere still hinders the extraction of particularly prescient State practice or *opinio juris* from these cases. In time though, similar events might provide explicit support for the emergence of a due diligence standard of attribution in cyberspace.

### 3. *An emerging customary norm*

While extensive and uniform practice is required to deduce the existence of new legal rules, the conduct of States 'whose interests are specially affected' is of notable weight.[198] In this regard, despite the accessibility of the domain, there are relatively few parties actively engaging in hostile cyber operations.[199] Nearly all publicly known cyber operations that have occurred since the Estonia attacks in 2007 have involved, either as the alleged perpetrator or victim, the United States, Russia or China.[200] As such, the

[193] Brown and Poellet (n 78) 131–2.

[194] 'North Korean Website Back Online after Shutdown' *The Times* (22 December 2014) <http://www.nola.com/science/index.ssf/2014/12/north_korean_websites_back_onl.html>.

[195] Payne (n 33) 684.

[196] D Alperovitch, 'Bears in the Midst: Intrusion into the Democratic National Committee', *CrowdStrike* (15 June 2016) <https://www.crowdstrike.com/blog>; 'Rebooting Watergate: Tapping Into the Democratic National Committee', *ThreatConnect* (17 June 2016) <https://www.threatconnect.com/blog/tapping-into-democratic-national-committee>; M Buratowski, 'Findings From Analysis of DNC Intrusion Malware', *Fidelis Cybersecurity* (20 June 2016) <https://www.fidelissecurity.com/threatgeek>. See generally JD Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law' (2017) 95 TexLRev 1579.

[197] W Banks, 'State Responsibility and Attribution of Cyber Intrusions after Tallinn 2.0' (2017) 95 TexLRev 1487, 1488–91.

[198] *North Sea Continental Shelf* (n 146) 43 [74].

[199] See K Geer *et al.*, *World War C: Understanding Nation-State Motives behind Today's Advanced Cyber Attacks* (Fire Eye, 2014).

[200] See, eg, Estonia 2007 (Russia); Georgia 2007 (Russia); Agent.btz 2008 (Unites States and Russia); DDoS attacks against the US and South Korea 2009 (United States); Stuxnet 2010 (United States); Google Hack 2010 (China); US Department of Defense Hack 2012 (United

participation of these States in norm building efforts is of particular importance. Importantly, all three were among the States who produced the 2013 and 2015 GGE reports. The United States has additionally ratified the *Cybercrime Convention*, and is bound by NATO's Cyber Defense Policy.

The development of new customary norms in cyberspace is further facilitated by the uniqueness of the domain. While the applicability of international law to the cyber context is now settled, the urgency of coping with new technologies enables customary law to come into existence very rapidly.[201] In the same way that novel principles concerning sovereignty in outer space developed 'instantly' after the first satellites were launched,[202] a due diligence standard of attribution might quickly develop with respect to cyberspace. On balance, instances of supportive State practice lack the quantum and uniformity to establish a crystallized or emerging customary norm. If, however, the United States' response to the Sony and DNC hacks signals a newfound willingness to allege State responsibility following cyber operations, a due diligence standards of attribution might soon follow.

## V. CONCLUSION

'At a time when the actions of unscrupulous [s]tates and violent extremist groups continue to threaten peace and security internationally, it is even more important that such actions are countered with a strong commitment to existing international law'.[203] However, the anonymity and accessibility of the cyber domain has thus far frustrated the effective operation of the existing State responsibility framework. This article has contended that due diligence offers a suitable standard of attribution that can rectify its limitations. The principle overcomes concerns of indeterminate liability because of its clearly and carefully defined scope: States assume responsibility only for unlawful conduct carried out from within their territory that they have knowledge of and the capacity to respond to. While due diligence has traditionally been thought of as a primary rule of international law, its utility in the cyber context is dependent on its characterization as a general condition of responsibility. Its status as such is supported, to some degree, by a series of multilateral agreements and resolutions, reflecting the views of the most prolific users of cyberspace. Given the rapid rate at which norms can emerge in new technological domains, due diligence might well crystallize into a customary attribution standard in the future. If and when it does so, international law will no longer be dismissed as 'window-dressing' on the realpolitik of cyberspace.

States); Sony Hack 2014 (United States); US Office of Personnel Management Hack 2014 (United States and China); DNC Hack 2016 (United States and Russia).

[201] Shaw (n 119) 55–6; Crawford, *Brownlie's Principles of Public International Law* (n 50) 24; Treves (n 184) [24].

[202] B Cheng, *Studies in International Space* (Oxford University Press 1997) 125–49.

[203] Ilves (n 2) xxiv.

https://doi.org/10.1017/S0020589318000015 Published online by Cambridge University Press