**Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm**

Russell Buchan*

Abstract

That states are subject to an obligation to prevent their cyber infrastructure from being used in a manner injurious to the international legal rights of other states is well established in customary international law. This obligation imposes a dual duty upon states. The first duty is an obligation of result insofar as it requires states to implement the laws and institutions necessary to prevent and punish malicious cyber conduct emanating from their territory, although international law confers upon states a wide margin of appreciation in deciding the design and content of such measures. The second duty is an obligation of conduct in the sense that where a threat emanates from their cyber infrastructure and states have (actual or constructive) knowledge of that threat they must act reasonably in utilising their capacity and resources to suppress it. What is reasonable in the circumstances will depend upon various factors operating at the time such as the resources available to the state and the risks involved in the particular activity. Taken together, these duties construct an international legal obligation which offers states a certain degree of protection from malicious transboundary cyber conduct committed by non-state actors. However, the conclusion of an international treaty or several international treaties dealing with specific cyber threats will be crucial to achieving a secure cyberspace.

Keywords: cyber security; cyber conflict; transboundary harm; cyber due diligence; cyber space

## 1. Introduction

The presence of non-state actors on the international stage has grown steadily in recent years. The unique features of cyberspace, including its borderless character, its inherent interconnectedness, the anonymity it affords and its accessibility, has provided a thriving environment for non-state actors and cyberspace has thus further empowered non-state actors to act independently from states in the international arena. Indeed, it is likely that malicious transboundary cyber conduct

* Senior Lecturer in Law, University of Sheffield. Contact: r.j.buchan@sheffield.ac.uk.

committed by non-state actors now exceeds that committed by states.[1] In an international community based upon the sovereignty equality of its member states,[2] international law demands the existence of effective international legal rules that provide states with protection from non-state actors that commit malicious cyber conduct from the territory of other states.

Whilst steps have been taken towards making non-state actors responsible for their conduct under international law developments in this area have been slow and piecemeal and states remain the principal subjects and objects of international law.[3] States are not generally responsible for the conduct of non-state actors that causes detriment to other states simply because of a territorial link; that is, state responsibility on the basis that the non-state actor committed such conduct whilst within the territory of that state. There are however essentially two ways in which states can be held responsible in such circumstances, both of which could potentially be utilised to provide states with international legal protection.

First, a state is responsible for the actions of a non-state actor where those actions constitute an internationally wrongful conduct and can be attributed to the state;[4] namely, where the state exercised 'effective control' over the unlawful conduct in question.[5] However, the use of the attribution doctrine to hold states responsible for malicious cyber conduct committed by non-state

[1] LR Blank, 'International Law and Cyber Threats from Non-State Actors' (2013) 89 *International Law Studies* 406.
[2] Article 2(1), UN Charter 1945.
[3] Although on the international legal responsibility of non-state actors that commit malicious cyber operations from the territory of failed states or ungoverned spaces see in this volume N Tsagourias, 'International Responsibility for Malicious Cyber Activities by Non-State Actors Operating from Failed States or Ungoverned Spaces'.
[4] Article 2, International Law Commission's Draft Articles on State Responsibility 2001.
[5] *Application of the Convention on the Protection and Punishment of the Crime of Genocide* (Bosnia v Serbia) (2007) ICJ Rep 1, para 400.

actors is problematic and unlikely to occur.[6] The reason for this is because to establish the requisite factual link between a state and a non-state actor technical attribution must be necessarily achieved - the actor that perpetrated the internationally wrongful act must be accurately identified. This is difficult in cyberspace because although devices connected to the internet are assigned internet protocol (IP) addresses these do not reveal the specific identity of the device to other users but only their general geographic location. Moreover, the use of anonymizing techniques like Botnets and anonymising software such as Virtual Private Networks (VPNs) or The Onion Router (Tor) has made it even more improbable that the authors of malicious cyber conduct can be identified. In essence, these anonymizing techniques and software significantly hinder technical attribution because they reroute malicious cyber conduct through the cyber infrastructure of other states and in the process are assigned different IP addresses, indicating to the victim that the damaging conduct was launched from a computer in a geographical location different from its original source.[7] Whilst recent technological developments have meant that accurate cyber tracing is now possible it is still extremely difficult.[8] Yet, even if the author of malicious cyber conduct can be identified, satisfying the international legal criteria for attribution is nevertheless difficult because the test for attribution is that of effective control or, in the words of the International Law Commission (ILC), the state must have 'instructed', 'directed' or 'controlled' the unlawful conduct.[9] As has been well documented in the literature, this requires an 'exceptionally high' degree of factual control to be exercised in order for legal attribution to be established.[10]

[6] On the difficulties of attribution in cyberspace see N Tsagourias, 'Cyber Attack, Self-Defence and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229.
[7] On the potential to anonymise cyber operations see S Shaffiq, P Kavita, A Monica, '"Spoofing"……. Headache to IT world' (2012) 1 *International Journal of Advanced Research in Computer Engineering and Technology* 86.
[8] Z Fryer-Biggs, 'DoD's New Cyber Doctrine: Panetta Defines Deterrence, Preemption Strategy' (13 October 2012) *DefenseNews* http://archive.defensenews.com/article/20121013/DEFREG02/310130001/DoD-8217-s-New-Cyber-Doctrine
[9] Draft Articles on State Responsibility (n 4) Article 8.
[10] M Milanovic, 'State Responsibility for Genocide' (2006) 17 *EJIL* 553, 576.

Second, a state can incur responsibility where it fails to satisfy a primary obligation, whether conventional or customary, to take positive action in relation to the conduct of a non-state actor operating within its territory or, more broadly, subject to its jurisdiction. Importantly, there is a positive obligation contained in customary international law which requires states to prevent their territory from being used in a manner contrary to the international legal rights of other states.[11] In evaluating the effectiveness of international law in suppressing malicious transboundary cyber conduct committed by non-state actors the utility of this customary obligation is twofold.[12] First, unlike attribution, the obligation to prevent doctrine obviates the need to specifically identity the author of the cyber conduct (technical attribution) because it applies where harmful conduct emanates from cyber infrastructure located on a state's territory. As we know, IP addresses reveal the general geo-location of the computer used to launch the cyber operation. Significantly, this customary obligation applies regardless of whether the harmful conduct originated in that territory or is instead transiting through it, as would be the case where a non-state actor reroutes malicious cyber conduct through cyber infrastructure located on the territory of another state using a Botnet or IP spoofing software such as a VPN or Tor. Second, whereas attribution requires the state to have exercised effective control over the individual committing the unlawful conduct, the obligation to prevent doctrine exhibits the 'less burdensome'[13] requirement that the state knew or ought to have known that harmful conduct was emanating from its territory and failed to take all reasonable measures to terminate that conduct or mitigate the extent of its harmful effects.

[11] *Corfu Channel* (United Kingdom of Great Britain and Northern Ireland v Albania) [1949] ICJ Rep 1.
[12] 'Due diligence obligations to prevent and punish private misconduct can play a key role in establishing state responsibility in cases where the misconduct cannot be attributed to a state'; H Tonkin, *State Control over Private Military and Security Companies in Armed Conflict* (CUP, 2011) 63.
[13] S Shackelford, S Russell and A Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) *Chicago Journal of International Law* 10.

Whilst much academic energy has been dedicated to examining the attribution doctrine in the context of cyberspace,[14] academic investigation into the customary obligation upon states to prevent transboundary harm as a legal mechanism to protect state sovereignty from malicious cyber operations has received significantly less attention.[15] In light of this, the objective of this article is to assess the application of the obligation to prevent doctrine to states whose cyber infrastructure is being used by non-state actors to commit malicious transboundary cyber conduct and, more specifically, to determine the nature, scope and content of this legal obligation.

In pursuit of this objective this article is structured as follows. Section 2 identifies the obligation to prevent transboundary harm as a general obligation under customary international law. Section 3 argues that this obligation actually contains two distinct duties, one requiring states to possess a minimum legal and administrative apparatus capable of preventing non-state actors from using their cyber infrastructure to commit injurious transboundary conduct and, the other, requiring states to utilise this apparatus diligently to suppress threats emanating from their territory. Section 4 argues that the first duty integrated into the obligation to prevent principle is an obligation of result and explores the legislative and administrative features that a state must exhibit in order suppress malicious cyber conduct. Section 5 argues that second duty built into the obligation to prevent is an obligation of conduct and identifies the factors that are used to inform the standard of due diligence to which a state will be held when utilising its resources to address cyber threats emanating from its cyber infrastructure. Section 6 offers some concluding remarks on the utility of the obligation to

[14] MN Schmitt and L Vihul, 'Proxy Wars in Cyberspace: The Evolving International Law of Attribution' (2014) *Fletcher Security Review* 53; N Tsagourias, 'Cyber Attacks, Self-Defense and the Problem of Attribution' (2012) 17 *Journal of Conflict and Security Law* 229. Also on the topic of attribution in cyberspace see in this volume K Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors'.

[15] Notable exceptions include MN Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) *Yale Law Forum* 68 and C Antonopoulos, 'State Responsibility in Cyberspace', N Tsagourias and R Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar, 2015) 55.

prevent doctrine in providing states with effective international legal protection against malicious cyber conduct committed by non-state actors in foreign jurisdictions.

## 2. The Customary Obligation to Prevent Harm

The obligation upon states to prevent their territory from being used to cause harm to other states has deep roots in international law. The most famous articulation of this customary obligation can be found in the *Corfu* case in 1949.[16] In this case two British warships struck mines whilst passing through an international strait in Albanian waters. Whilst the International Court of Justice (ICJ) was unable to conclude that the mines had been laid by Albania, the ICJ determined that the Albanian government must have known of the mines' existence and therefore had a duty to warn ships utilising the international strait. In particular, the ICJ based its decision on 'certain general and well-recognized principles' namely, 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'.[17] In this context, conduct 'contrary to the rights of other states' refers to acts of non-sate actors that, if they had been committed by a state, would amount to an internationally wrongful act.

At its creation many argued that as a virtual world cyberspace was an a-territorial environment and thus immune from sovereign claims.[18] If this view is correct then the obligation upon states to

[16] *Corfu Channel* (n 11).
[17] Ibid, 22.
[18] D Johnson and D Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367.

prevent transboundary harm, which is imposed upon states in relation to activities occurring within their sovereign territory, is inapplicable to malicious conduct emanating from cyberspace.

Recent state practice however illustrates that states do in fact exercise territorial sovereignty over those aspects of cyberspace which are supported by physical infrastructure located within their territory.[19] As a result, states have recognised the applicability of the customary international law obligation to prevent transboundary harm to threats that emerge from their cyber infrastructure. The US, for example, has explained that states 'should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse'.[20] Indeed, the applicability of this obligation to cyberspace is confirmed by Rule 5 of the Tallinn Manual, which explains that '[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States'.[21] Importantly, this obligation applies to harmful conduct emanating from a state's territory, which includes host states but also transiting states. For example, in the *Nicaragua* case the ICJ held that Nicaragua was under an obligation to prevent its territory from being used as a trafficking route for military equipment intended for insurgents in El Salvador.[22] By analogy, in cyberspace the customary obligation to prevent transboundary harm applies not only to states whose cyber infrastructure is being used by non-state actors as a launch pad for malicious cyber conduct but also extends to those states whose cyber infrastructure is being used as a conduit for

[19] 'State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty'; WH von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace' (2013) 89 *International Law Studies* 123, 126. See also Rule 1 of the Tallinn Manual; MN Schmitt (General Editor), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, 2013).
[20] The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (2011) 10 https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[21] *Tallinn Manual* (n 19) Rule 5.
[22] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14, para 157.

malicious cyber operations which were concocted and perpetrated by non-state actors in another state and are making their way to their final destination elsewhere.

## 3. Scope and Nature of the Obligation to Prevent Transboundary Harm

Where international law imposes upon a state an obligation to take positive action it is necessary to categorise that international legal duty either as an obligation of result or an obligation of conduct.[23] Obligations of result impose an 'absolute'[24] obligation upon states to 'guarantee'[25] that a precise result is attained. Failure by a state to meet this obligation will constitute an internationally wrongful act regardless of whether the state was at fault in failing to achieve the result. In contrast, obligations of conduct are 'non-absolute'[26] and do not require specific results to be achieved but instead require that states 'deploy adequate means, to exercise best possible efforts, to do the utmost, to obtain [the] result'.[27] Transgression of an obligation of conduct therefore only occurs where it can be proved that the state is at fault; responsibility hinges upon a state's failure to exercise adequate vigilance, care or prudence or, to utilise the current international law terminology, the state fails to exercise due diligence. In the *Genocide* case the ICJ provided a useful explanation of the nature of obligations of conduct

[23] On the difference between these types of obligations see P-M Depuy, 'Reviewing the Difficulties of Codification: On Ago's Classification of Obligations of Means and Obligations of Result in Relation to State Responsibility' (1999) 10 *EJIL* 371.
[24] R Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of International State Responsibility' (1993) 35 *German Yearbook of International Law* 9, 35.
[25] Ibid, 26.
[26] J Kulesza, 'Due Diligence in Cyberspace', in IM Portela and F Almeida, *Organizational, Legal, and Technological Doimeisons of Information System Administration* (Information Science, 2014) 76, 79.
[27] *Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, Seabed Disputes Chamber of the International Tribunal for the Law of the Sea, Advisory Opinion (2011) para 110.

> it is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide as far as possible.[28]

Thus, the dispositive factor in evaluating whether a state acted with due diligence is whether the state acted as any other reasonable state would have done in those circumstances. To put the matter differently, it will concluded that a state failed to act with due diligence where it can be shown that there was 'an insufficiency of governmental actions so far short of international standards that every reasonable and impartial man would readily recognize its insufficiency'.[29] Note that where a state fails to conduct itself reasonably and violates an obligation of conduct the state is liable for the failure to prevent the unlawful conduct and not for the act that produces the resulting harm,[30] which is significant from the perspective of the adequacy of compensation/reparations owed to the victim and, for example, the nature and extent of countermeasures that the victim state can adopt.

It is the language of a particular obligation that provides the clues as to whether it is to be interpreted as an obligation of result or an obligation of conduct. The ILC has explained that where international law imposes upon a state an obligation that requires it to *prevent* certain types of

[28] *Bosnian Genocide* (n 5) para 430.

[29] *USA (L.F. Neer) v. United Mexican States* (1926) RIAA iv 60, 61-2.

[30] '[T]he state is never responsible for the act of an individual as such: the act of the individual merely occasions the responsibility of the state by revealing the state in an illegality of its own – an omission to prevent or punish, or positive encouragement of, the act of the individual'; C Eagleton, *The Responsibility of States in International Law* (New York, New York Press 1928) 77.

activity then that obligation usually takes the form of an obligation of conduct: '[o]bligations of prevention are usually construed as best efforts obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur'.[31] The implication, then, is that the customary international law obligation upon states to prevent their territory from being used to cause detriment to other states is an obligation of conduct. Importantly, however, in his seminal work on the topic of state responsibility Pisillo-Mazzeschi argues that the position is rather more complex. In particular, he argues that a

> careful examination of [state] practice reveals that the obligation to prevent has a twofold content; that is, it includes *two distinct obligations* of the State. The first is that of *possessing*, on a permanent basis, a legal and administrative apparatus normally able to guarantee respect for the international norm on prevention. The second obligation, instead, is that of *using* such apparatus with the diligence that the circumstances require.[32]

As we shall see below, the first duty imposed by the obligation to prevent is characterised as an obligation of result whereas the second duty is an obligation of conduct.

## 4. Developing State Capacity: an Obligation of Result

[31] Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries (2001), 62.
[32] Pisillo-Mazzeschi (n 24) 26.

The obligation of prevention imposes a duty upon states to engage in capacity building in the sense that they must equip themselves with the means to detect, prevent, mitigate and punish conduct by non-state actors within their territory that is contrary to the international legal rights of other states. Developing state capacity capable of preventing such conduct will invariably require 'the enacting of legislation and regulations and the establishment of an effective administrative and judicial apparatus'.[33]

As an obligation of result[34] the important question becomes what specific legislative measures and administrative apparatus a state must implement in order to discharge its duty to prevent its territory from being used in a manner injurious to the international legal rights of other states. Generally speaking, this would include those laws and institutions that are 'the natural attribute of any Government' that exercises effective control over its territory,[35] which as we know is a key criterion for a political community to be recognised as a state under international law.[36] But the question still remains as to what are the specific legal and institutional features necessary for a state to be regarded as being in effective control of its territory. In particular, and in relation to the legislative and administrative measures necessary for a state to be regarded as being in effective control of its cyber infrastructure, does international law require the implementation of regulatory frameworks that incentivize or even cajole providers of information and communication technology (ICT) such as search engines, Internet Service Providers (ISPs), software providers etc to suppress

[33] Tonkin (n 12) 70.
[34] 'Having established the dual content of the obligation to prevent, we should note that, in the practice, the duty of the State to possess a minimum legal and administrative apparatus is not in any way conditioned by the due diligence rule [i.e. it is an obligation of result]'; Pisillo-Mazzeschi (n 24) 27.
[35] '[States] should possess a legal system and sufficient resources to maintain an adequate administrative apparatus to control and monitor the activities. It is however understood that the degree of care expected of a State with a well-developed economy and human and material resources and with highly evolved systems and structures of government is different from States which are not so well-placed. Even in the latter case, vigilance, employment of infrastructure and monitoring of hazardous activities in the territory of the State, which is a natural attribute of any Government, are expected'; International Law Commission, *Commentary to the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities* 2001, 155.
[36] Article 1, Montevideo Convention on the Rights and Duties of States 1933.

malicious cyber conduct? Does this duty require states to criminalise certain types of malicious cyber conduct, perhaps even accompanied by specific forms of punishment (such as incarceration, for example)? In order to meet their international law obligation must states also create institutions specifically dedicated to providing cyber security, such as Computer Emergency Response Teams (CERTs), which are specialised entities that can detect, suppress and mitigate malicious cyber operations? Does this duty require states to devise policies and develop processes that can facilitate the sharing of information amongst the various ICT stakeholders, both public and private?

When international law requires states to take positive action and achieve a particular result but the primary obligation does not specify the exact measures that a state must deploy so as to achieve that result international tribunals have accorded states a wide margin of appreciation in choosing which specific measures to adopt.[37] With regard to the customary obligation upon states to prevent their territory from being used in a manner injurious to the legal rights of other states Lauterpacht has noted

> International law is not concerned with the manner in which states elect to meet this particular duty of theirs … So long as these laws are reasonably sufficient to prevent hostile acts or to punish them after they have occurred, the state has performed its duty. But should it visit such offences by small fines, or, with regard to foreigners, by expulsion only, or should its laws be of such nature that, notwithstanding their theoretical comprehensiveness, they are in fact incapable of enforcement, then again it will find it difficult to escape liability for hostile acts

[37] *Request for Interpretation of the Judgment of 31 March 2004 in the Case concerning Avena and other Mexican Nationals* (Mexico v USA) (2009) ICJ Rep 3, para 44.

> rendered more probable as a result of the leniency or technical shortcomings of its laws.[38]

Where international law wishes to impose obligations upon states that require them to implement specific measures (such as regulatory frameworks and institutions) a treaty will usually be necessary. In the context of malicious transboundary cyber conduct committed by non-state actors the Council of Europe's Convention on Cybercrime requires states parties to adopt 'legislative and other measures' to ensure that the offenses listed in the Convention are 'punishable by effective, proportionate and dissuasive sanctions'.[39] In particular, the Convention requires states parties to criminalise conduct that falls into one of four categories: offences against the confidentiality, integrity and availability of computer systems; computer related offences (forgery, fraud); content-related offences (child pornography); and offences related to infringement of copyright and related rights.[40] The Convention requires states to adopt measures to establish procedures for the purpose of criminal investigations into, and criminal proceedings for, these offences.[41] In addition, the Convention contains a number of provisions on mutual assistance and extradition which are designed to ensure that states parties 'cooperate with each other … to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'.[42] As an example, Article 35 requires that states 'designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of

[38] H Lauterpacht, 'Revolutionary Activities by Private Persons against Foreign States' (1928) 22 *AJIL* 105, 128.
[39] Article 13, Convention on Cybercrime (Council of Europe), CETS No 185, 23 November 2001. See generally P Kastner and F Mégret, 'International Legal Dimension of Cybercrime', Tsagourias and Buchan, *Research Handbook on International Law and Cyberspace* (n 15) 190.
[40] In 2003 an Additional Protocol to the Convention was adopted which requires signatory states to criminalise conduct relating to the dissemination of racist and xenophobic material on the internet; Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems (Council of Europe), CETS No 189, 28 January 2003.
[41] Convention on Cybercrime (n 34), Article 14(1).
[42] Ibid, Article 23.

investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence'.[43]

Since the early 1960s states have adopted various multilateral and regional treaties relating to terrorism. As many of these conventions pre-dated the cyber era they do not refer to cyber terrorism specifically but their definition of terrorist-related activities is sufficiently broad to encompass acts of terrorism perpetrated through cyber means.[44] More recent instruments do refer specifically to cyber terrorism.[45] The gist of these conventions is to define conduct as terrorist-related and to impose obligations upon states parties to criminalise such conduct and exercise their jurisdiction when these offences are committed. Moreover, under Chapter VII UN Charter the Security Council has adopted resolutions imposing binding obligations upon UN member states to adopt specific counter-terrorism measures.[46] Again, whilst these resolutions do not refer to cyber terrorism specifically, their definition of terrorist-related activity is sufficiently broad to include such conduct. *Inter alia*, these resolutions impose obligations upon member states to designate as serious criminal offences the financing, planning, preparation or perpetration of terrorist acts or in support of terrorist acts and to provide other states with warnings and information where they are at threat of terrorist activities.

[43] The African Union's Convention on Cyber Security and Personal Data Protection is a regional arrangement designed to promote cyber security. Whilst the treaty has been adopted it is not yet in force. This notwithstanding, if/when it comes into force it will require member states to, *inter alia*, adopt 'legislative and/or regulatory measures as it deems effective by considering as substantive criminal offences acts which affect the confidentiality, integrity, availability and survival of information and communication technology systems, the data they process and the underlying network infrastructure, as well as effective procedural measures to pursue and prosecute offenders' (Article 25(1)); African Union's Convention on Cyber Security and Personal Data Protection 2014.

[44] For a good discussion of how these instruments apply to cyber terrorism see in this volume D Fidler, 'Cyberspace, Terrorism, and International Law'.

[45] See for example ASEAN Convention on Counter Terrorism 2007. The Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation 2010 and the Protocol Supplemental to the Convention for the Suppression of Unlawful Seizure of Aircraft 2010 also refer specifically to acts of cyber terrorism but these agreements have yet to enter into force.

[46] SC Res 1373 (2001); SC Res 2178 (2014).

From the perspective of this article it is important to note that the Convention on Cybercrime only concerns malicious cyber conduct that the treaty classifies as criminal and the relevant anti-terrorist conventions and Security Council resolutions encompass only that type of cyber conduct which falls within their definition of terrorism. Thus, these international legal regimes do not comprehensively address all forms of malicious cyber conduct that violate the international legal rights of other states and consequently there will be many instances where states continue to look to the customary international law obligation upon states to prevent transboundary harm for protection.

## 5. Utilising State Capacity: an Obligation of Conduct

Where a state is to found to be in possession of the requisite laws and institutions the obligation of prevention requires it to utilise this apparatus in order to address known threats. As an obligation of conduct this is an obligation conditioned by the due diligence standard. In many fields of international law primary obligations have appeared which have been interpreted as requiring states to exercise due diligence in the pursuit of particular results, such as in the fields of international environmental law, international diplomatic law and international human rights law.[47]

Although these due diligence obligations are located within specific international legal frameworks and thus their content is defined by reference to the primary norm within which they are contained, the way in which these due diligence standards have been interpreted within different international legal contexts can be nevertheless used as an aid to interpret due diligence standards found in other

[47] See generally International Law Association, *Study Group on Due Diligence in International Law*, First Report (7 March 2014) http://www.ila-hq.org/en/committees/study_groups.cfm/cid/1045.

primary obligations of international law.[48] In this sense, whilst due diligence obligations may not possess a unified content they do contain core features and thus exhibit a 'common standard'.[49] It is the objective of this section to identify the core features of the due diligence standard and, more specifically, to define the material contents of the obligation of due diligence with particular reference to the customary obligation upon states to use their capacity to prevent their cyber infrastructure from being used by non-state actors as a platform to commit malicious transboundary conduct.

### 5.1 *Knowledge*

Knowledge is the 'decisive element of due diligence'[50] and it is only where a state has knowledge of a threat that the obligation upon it to use its capacity to suppress that threat is triggered.[51] Note however that just because a threat emanates from within a state's territory does not mean that it is automatically assumed to have known of the threat. In the *Corfu* case it was held that 'it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known' what was happening.[52]

[48] R Barnidge Jr, 'The Due Diligence Principle under International Law' (2006) 8 *International Community Law Review* 81, 92.
[49] A O'Donoghue, 'The Exercise of Governance Authority by International Organizations: The Role of Due Diligence Obligations after Conflict', M Saul and J Sweeney (eds), *International Law and Post-Conflict Reconstruction Policy* (Routledge, 2015) 48.
[50] K Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations' (2014) 14 *Baltic Yearbook of International Law* 23, 28.
[51] '[A] State's obligation to prevent, and the corresponding duty to act, arise at the instant that the State learns of, or should normally have learned of, the existence of a serious risk that genocide will be committed'; *Bosnian Genocide* (n 5) para 431.
[52] *Corfu Channel* (n 11) 18.

Where the state has actual knowledge of the threat the duty of due diligence is obviously activated. Interestingly, in the *Corfu* case the ICJ concluded that Albania was subject to a duty to prevent because the evidence indicated that it 'must have known'[53] of the mines and the threat that they represented. This conclusion was based on the fact that; Albania kept 'a jealous watch over its territorial waters'[54] and that the mines were laid so close to Albania's coastline that '[t]he laying of a minefield in these waters could hardly fail to have been observed by the Albanian coastal defences';[55] Alabama frequently used military force within the strait;[56] Albania demanded that foreign vessels request 'permission' before they entered the strait.[57] The preparedness of the Court to presume knowledge derives from the fact that one cannot deny knowledge of facts that are widely known, such as where facts are reported through official government channels or even in the media generally.[58] In the context of cyber, for example, a state may be presumed to have knowledge of a threat where it intensively guards and patrols its cyber infrastructure, where it is widely reported that a state's cyber infrastructure is infected with particular malware and where a state has become a well-known sanctuary for those wishing to organise and launch malicious cyber operations.

An important question concerns the adequacy of constructive knowledge. The International Group of Experts that drafted the Tallinn Manual were unable to reach a consensus on whether the obligation of prevention applies where the state ought to have known of the threat.[59] Case law however seems to support an interpretation in favour of the adequacy of constructive knowledge because 'it would appear incongruous if a state could avoid responsibility by claiming its lack of

[53] Ibid, 20.
[54] Ibid, 19.
[55] Ibid.
[56] Ibid.
[57] Ibid.
[58] *Re Yamashita* No. 61, Misc. Supreme Court of the United States 327 US 1; 66 S. Ct. 340; 90 L. Ed. 499; 1946 U.S. LEXIS 3090.
[59] Tallinn Manual (n 19) 28.

knowledge if it could have discovered the prohibited activity through diligent detection'.[60] In *Corfu* it was explained that

> It is true, as international practice shows, that a State on whose territory or in whose waters an act contrary to international law has occurred, may be called upon to give an explanation. It is also true that that State cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and its authors.[61]

Similarly, in the *Genocide* case the ICJ explained that 'to incur responsibility … it is enough that the State was aware, or should normally have been aware, of the serious danger that acts of genocide would be committed.'[62]

In light of the adequacy of constructive knowledge the question becomes whether it is reasonable to expect the state to have known of the threat in light of the circumstances prevailing at that time. Relevant circumstances include the technical capacity of the state in question. Thus, it is not reasonable to expect a state with under-developed technical capacity to detect highly sophisticated malicious cyber operations in the same way as a technologically advanced state. Similarly, in an instantaneous environment like cyberspace cyber operations occur at an 'unbelievable speed' and this also needs to be factored into the equation when determining whether the state should have

[60] Tonkin (n 12) 67.
[61] *Corfu Channel* (n 11) 18.
[62] *Bosnian Genocide* (n 5) para 432.

reasonably known of the threat's existence.[63] This is especially the case where a malicious cyber operation is transiting through a state's cyber infrastructure.

As knowledge can be constructed international law imposes a monitoring obligation upon states in the sense that states must keep themselves informed of threats emanating from their territory.[64] There is a legitimate concern here that the duty upon states to actively monitor their cyber infrastructure in search of threats could be exploited by malevolent states to encroach upon the fundamental human rights of its citizens, especially the right to privacy. However, our fears should not be overstated because, as was explained in the *Genocide* case, when discharging a due diligence obligation to prevent (in this case genocide) 'it is clear that every State may only act within the limits permitted by international law'.[65] Indeed, that states must respect the right to privacy when operating in cyberspace has been affirmed by the UN General Assembly,[66] UN Human Rights Officials[67] and the UN Special Rapporteur on the right to privacy.[68] Thus, the obligation upon states to detect threats in cyberspace 'cannot legitimise violations of international human rights law or other rules'.[69]

[63] B Gates, EdX Course CS50x3 (Computer Science 50) (2015) Week 1 Harvard College.
[64] In *Pulp Mills* it was held that the due diligence principle requires 'the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators'; *Pulp Mills on the River Uruguay* (Argentina v Uruguay) (2010) ICR Rep 14, para 197. *Cf* Schmitt (n 15) 75 ['There appears to be an emerging consensus among scholars and state legal advisers against the existence of obligations either to monitor cyber activities on one's territory or prevent malicious use of cyber infrastructure within one's borders'].
[65] *Bosnian Genocide* (n 5) para 430.
[66] UN General Assembly, *Resolution 68/167—The Right to Privacy in the Digital Age*, UN Doc. A/RES/68/167, 18 December 2013.
[67] *The Right to Privacy in the Digital Age: Report of the Office of the UN High Commissioner for Human Rights*, UN Doc. A/HRC/27/37, 30 June 2014; *Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism*, UN Doc. A/69/397, 23 September 2014.
[68] Human Rights Council, *The Right to Privacy in the Digital Age*, UN Doc. A/HRC/28L.27, 24 March 2015.
[69] Bannelier-Christakis (n 50) 31.

5.2 *The Duty to Prevent*

Where a threat is known, or should be reasonably known in the circumstances, the crucial question is '[w]hat exactly does the 'due diligence' standard require and how much positive action can reasonably be expected of a state in a particular case?'[70] Broadly speaking, the obligation to prevent requires states to use their legislative framework and institutional apparatus to address threats which either originate within their territory or are transiting through it and, if harm occurs, to mitigate its effects. States must also use their capacity to investigate and punish harmful activities where they occur.[71]

It is important to underscore that the obligation to prevent encompasses a duty to investigate and, where appropriate, punish those responsible because such conduct serves 'a critical preventative function by reinforcing the state's prohibitory measures and deterring other potential wrongdoers'.[72] 'The duty to investigate, like the duty to prevent, is not breached merely because the investigation does not produce a satisfactory result. Nevertheless, it must be undertaken in a serious manner and not as mere formality preordained to be effective'.[73] Depending upon the nature of the harmful activity, this may require a criminal investigation and prosecution. In the *Janes* case, for example, the Tribunal explained that Mexican authorities failed in their duty of due diligence to protect from harm an American citizen in Mexico because 'the Mexican authorities took no proper steps to apprehend and punish Carbajal [the individual responsible for killing the American national]

[70] Tonkin (n 12) 69.
[71] In the *Pulp Mills* decision the ICJ explained that the obligation to prevent 'is an obligation which entails not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement'; *Pulp Mills* (n 64), para 197.

[72] Ibid, 158.
[73] *Velásquez -Rodriguez Case*, Inter-American Court of Human Rights Decisions and Judgments 91 (ser C) No 4 (1988) para 177.

[and] that such efforts as were made were lax and inadequate'.[74] The Tribunal concluded that '[t]he culprit is liable for having killed or murdered an American national; the Government is liable for not having measured up to its duty of diligently prosecuting and properly punishing the offender'.[75]

In other instances investigations of a non-criminal nature may be considered appropriate, such as the use of public inquiries or fact-finding commissions, and the use of non-criminal sanctions, such as fines or rescinding operating licenses. In the *Corfu* case the ICJ chastised Albania for not setting up a commission to investigate the mining of the strait (as the Greek government had) 'nor did it proceed to the judicial investigation incumbent, in such a case, on the territorial sovereign'.[76]

Fundamentally, ascertaining the precise demands of due diligence in any given situation is determined according to what is reasonable in the circumstances.[77] The question is whether a reasonable state in those circumstances would have acted as the state under examination did. Given such a test it is clear that '[v]arious parameters operate when assessing whether a State has duly discharged the [DD] obligation concerned'.[78] Due diligence obligations therefore have 'an elastic and relative nature'[79] and embody a 'flexible reasonableness standard adaptable to the particular facts and circumstances'.[80] As a result, '[t]he content of "due diligence" obligations may not easily be described in precise terms … "due diligence" is a variable concept'.[81] This being said, determining whether a state acted reasonably in addressing a threat will require consideration of a number of key factors, primarily the *capacity* of the state in question and *risks* involved in the particular activity.

[74] *Janes* (US v Mexico) 4 RIAA 82 (1926) para 4.
[75] Ibid, para 20.
[76] *Corfu Channel* (11) 20.
[77] 'The test in such circumstances is one of reasonableness'; *Tallinn Manual* (n 19) 27.
[78] *Bosnian Genocide* (n 5) para 429.
[79] Pisillo-Mazzeschi (n 24) 44.
[80] R Barnidge Jr, *Non-State Actors and Terrorism: Applying the Law of State responsibility and the Due Diligence Principle* (TMC Asser Press, 2007) 138.
[81] *Activities in the Area* (n 27) para 117.

### 5.2.1 State Capacity

As an obligation of conduct rather than result determining how a reasonable state would have reacted to a threat is subject to an 'available means' analysis, which requires identification of the financial, technical and human resources of the state. The crux of the matter is that a '[due diligence] obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities'.[82] This was central to the ICJ's analysis in the *Genocide* case where it held that in order to discharge its due diligence obligation to prevent genocide a state is required to take only those measures that are 'reasonably available' and 'within its power'.[83]

The consequence of this available means test is that '[t]he due diligence standard ... varies in many contexts on the basis of common but differentiated responsibilities'.[84] For example, in the *Armed Activities* case the ICJ determined that Congo did not violate its obligation of due diligence by failing to prevent dissident armed groups located within its territory from using armed force against Uganda because of the inimical geographical terrain from where the armed group operated and also the material inability of the government to control that part of its territory.[85]

[82] *Osman v UK* (App No 23452/94), ECtHR 28 October 1988, para 116.
[83] *Bosnian Genocide* (n 5) para 430. As Trapp says, '[i]nternational jurisprudence has generally been sympathetic to the resource incapacity argument as a basis for finding no lack of diligence, and states often invoke limited resources to justify their failures to prevent'; K Trapp, *State Responsibility for International Terrorism* (OUP, 2011) 71 (footnotes omitted).
[84] Study Group on Due Diligence in International Law (n 47) 27.
[85] *Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v Uganda) (Merits) (2005) ICJ Rep 168, para 301.

The notion of differentiated responsibilities is particularly important in the context of cyberspace because the technical capabilities of states differ so drastically. As we have already seen, one of primary reasons for why cyberspace is such a difficult environment to regulate is because actors can easily obfuscate their identity. Another reason is because actors can easily conceal malware within ostensibly legitimate computer operations. Technologically advanced states will possess sophisticated cyber tracing techniques that enable authorities to accurately identify those responsible for committing malicious cyber operations and thus take enforcement action against them and will also be able to better decipher computer codes in order to ascertain whether they contain malware. International law requires these states to do more to counter cyber threats emanating from their territory than those possessing less technical capacity. Note however that the standard of due diligence owed in any particular case can become more demanding if a state's capacity changes

> [Due diligence] may change over time as measures considered sufficiently diligent at a certain moment may become not diligent enough in light, for instance, of new scientific or technological knowledge.[86]

Thus, if over time a state's capabilities develop and improve, or perhaps diminish as the case may be, then the standard of due diligence owed will be elevated or reduced. This is important in relation to cyberspace because it means that as states engage in knowledge transfer and capacity building – which can occur rapidly and dramatically in terms of a state's cyber capabilities – there will be a correlative increase in the intensity of the duty they owe in terms of policing their cyber infrastructure and addressing threats that emanate from within it.

[86] *Activities in the Area* (n 27) para 117.

If the capacity of a state indicates that suppressing a cyber threat is 'technically impractical, the state that fails to do so is not in breach of its due diligence obligation; the diligence that is due under the legal standard cannot exceed the state's capabilities'.[87] It is important to stress however that where a state is unable to prevent harmful conduct emanating from its territory it must nevertheless do all that is reasonable in light of its capacity to mitigate the effects of the damaging conduct. At a very minimum, a state that lacks the technical means to suppress a cyber threat should notify and warn those states that are likely to be the victim of the attack and, where reasonable, cooperate with likely victim states so as to help prevent or mitigate the attack, such as providing details as to whom is perpetrating the attack, when the attack will occur, the nature of the attack and which infrastructure is likely to be targeted. In the *Corfu* case the ICJ explained that in light of Albania's knowledge of the mines in its territorial sea it should have notified/warned approaching vessels about the risk and its failure to do so amounted to a violation of its customary obligation to prevent harm.[88]

Related to this, where a state is a victim or likely victim of damaging conduct and the source of the threat emanates from different actors operating from cyber infrastructure located within different states each host state must do its part to help prevent the threat or alleviate it effects. In the *Genocide* case the ICJ opined that

> it is irrelevant whether the State whose responsibility is in issue claims, or even proves, that even if it had employed all means reasonably at its disposal, they would not have sufficed to prevent the commission of genocide. As well as being generally

[87] Schmitt (n 15) 74.
[88] *Corfu Channel* (n 11) 22.

> difficult to prove, this is irrelevant to the breach of the obligation of conduct in question, the more so since the possibility remains that the combined efforts of several States, each complying with its obligation to prevent, might have achieved the result — averting the commission of genocide — which the efforts of only one State were insufficient to produce.[89]

The key issue here is that a state cannot 'do nothing'[90] when its territory is being used as a platform to launch injurious conduct. Take for example a DDOS attack that emanates from many hundreds or even thousands of zombied computers located in different states across the globe. One state acting alone is unlikely to be able to prevent the attack. States cannot remain inert however. Instead, international law requires each state to take all reasonable measures to contribute to preventing the threat or dampening its effects.

The standard of due diligence owed in any given situation is not only affected by the resources available to the state but also by the degree of influence that the state exercises over the actor that is the source of the threat. In the *Genocide* case the ICJ explained that when determining the degree of diligence required it is important to consider the state's

> capacity to influence effectively the action of persons likely to commit, or already committing, genocide. This capacity itself depends, among other things, on the geographical distance of the State concerned from the scene of the events, and on

[89] *Bosnia Genocide* (n 5) para 430.
[90] Ibid, para 438.

> the strength of the political links, as well as links of all other kinds, between the authorities of that State and the main actors in the events.[91]

In this case it was held that 'FRY was in a position of influence over the Bosnian Serbs who devised and implemented the genocide'[92] and that its failure to do so engaged its international responsibility.

In recent years there has been a rise in so-called patriotic hackers that commit cyber attacks against other states in defence of the (perceived) interests of their nation state.[93] In 2007 Estonia was subject to widespread and systematic DDOS attacks after it decided to relocate a statute commemorating Russian soldiers that were killed during World Word II. Reports into the incident revealed that the origins of the cyber attacks were from computer networks located within Russia[94] and Estonia quickly alleged that the Russian government was responsible.[95] Definitive attribution however could not be established. But even if Russia did not commit the DDOS attacks and they were instead committed by Russian nationals disgruntled by Estonia's decision to relocate the statute, Russia was nevertheless subject to an obligation under customary international law to prevent its cyber infrastructure from being used to interfere with Estonia's sovereignty and this required the Russian government to exercise its influence over those individuals which sought to act in defence of Russian interests so as to discourage the attacks and bring them to an end.

[91] Ibid, para 430.
[92] Ibid, para 434.
[93] A Segal, *The Rise of Asia's Cyber Militias*, The Atlantic, 23 February 2012 http://www.theatlantic.com/international/archive/2012/02/the-rise-of-asias-cyber-militias/253487/.
[94] G Evron, 'Bating Bonets and Online Mobs' (2008) Winter/Spring, *Georgetown Journal of International Affairs* 121, 125
[95] I Traynor, 'Russia Accused of Unleashing Cyberwar to Disable Estonia', *The Guardian*, 17 May 2007 http://www.theguardian.com/world/2007/may/17/topstories3.russia.

### 5.2.2 Degree of Risk

The Seabed Disputes Chamber has explained that the demands of the due diligence obligation 'may also change in relation to the risks involved in the activity'.[96] In this context risk can take two forms.

First, the due diligence standard can become more or less demanding depending upon the likelihood of the threat occurring. Where there is a greater likelihood of a threat occurring a state will be required to dedicate more of its resources to addressing the threat in order to be considered to have acted with reasonable diligence. Conversely, the action required by a state will be less demanding where the probability of harm occurring is tenuous and remote. For example, the ILC has stated that when fixing the standard of due diligence to assess the legality of state conduct it must be 'appropriate and proportional to the degree of risk of transboundary harm in the particular instance'.[97]

In the *Genocide* case the ICJ held that FRY knew that the Bosnian Serbs embraced a 'deep-seated hatred' of the Muslims and so it was 'clear that there was a serious risk of genocide in Srebrenica',[98] thus demanding that FRY prioritise the threat and dedicate more resources to its suppression. Similarly, in the context of preventing transboundary terrorism the obligation to prevent terrorist groups operating within one's territory is more demanding where there is a 'real and immediate' risk of transboundary harm

[96] *Activities in the Area* (n 27) para 117.
[97] Commentary to the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities (n 35) 154.
[98] *Bosnian Genocide* (n 5) para 438.

> The fact that a state possessed information as to terrorist threats and failed to act on it could conceivably be sufficient to render the state responsible if the threats are realised, although this would depend on there being clear information indicating a 'real and immediate risk' in circumstances where the state was in a position reasonably to prevent deaths and failed to do so.[99]

This is important in the context of cyberspace because it is an instantaneous domain where threats can mature quickly and unexpectedly. At one moment a cyber threat may be nascent and remote yet, within a matter of seconds and the press of a button, malware can be downloaded and launched and the threat can become reality. These factors need to be taken into account when assessing whether a state faced with such a rapidly developing cyber threat acted with due diligence in its attempt to suppress it.

Second, where the likely consequences of a threat becoming reality are grave and severe a state will be required to do more in order to prevent its occurrence and mitigate its effects (and, in the aftermath of the incident, punish those responsible). According to the Seabed Disputes Chamber, the due diligence standard may

> change in relation to the risks involved in the activity. As regards activity in the Area it seems reasonable to state that prospecting is, generally speaking, less risky than exploration activities which, in turn entail less risk than exploitation. Moreover, activities in the Area concerning different kinds of minerals, for example, polymetallic nodules on the one hand and polymetallic sulphides or

[99] H Duffy, *The 'War on Terror' and the Framework of International Law* (CUP, 2005) 308.

> cobalt rich ferromanganese crusts on the other, may require different standards of diligence. The standard of due diligence has to be more severe for the riskier activities.[100]

In relation to cyber, if the likely consequences of a cyber attack are that the critical national infrastructure of the molested state will be disabled or seriously affected and that this will pose a risk to life (and especially if this risk extends to a large number of people), in such an extreme scenario the territorial state could be required to shut down its computer networks entirely. Note however that when deciding whether it is reasonable for a state to adopt a particular course of action this assessment must also take into account harm caused to the territorial state. 'It would be incongruent to impose the obligation in situations in which the burden levied on the territorial state far outweigh the harm being imposed on the target state'.[101] Thus, calculating reasonableness requires that the 'nature, scale, and scope of the (potential) harm to both states must be assessed',[102] an exercise which is far from straightforward in cyberspace where, not least because of its interconnectedness, the exact ramifications of cyber operations are often hard to gauge.

5.3 Damage

[100] *Activities in the Area* (n 27) para 117.
[101] Schmitt (n 15) 75.
[102] Tallinn Manual (n 19) 27.

It is a general principle of international law that where a state violates an international legal norm responsibility attaches regardless of whether damage is caused;[103] it is the breach of the international legal obligation itself that provides sufficient grounds for invoking state responsibility. However, and as Crawford has noted, there are caveats to this general principle and in certain instances a primary obligation may stipulate that damage is required in order for state responsibility to occur.[104] Indeed, it some instances it may be the case that a *de minimis* threshold is built into the primary obligation, with responsibility attaching only where serious damage is occasioned.

With regard to the customary obligation to prevent, whether state practice requires damage or even serious damage to occur in order to establish state responsibility is especially important when it comes to malicious transboundary cyber operations committed by non-state actors. This is because whilst such operations will likely violate international law, for example the entitlement of states to have their territorial sovereignty preserved, many such operations will often cause no damage to the victim state or at most cause minor irritation or inconvenience, such as website defacement or the temporary denial of non-critical services. Whether damage is required hinges upon the state practice that constitutes this customary obligation.

In the *Corfu* case the ICJ interpreted state practice as encompassing conduct 'contrary to the rights of other states', without seeming to require that additional damage be caused. Similarly, in the *Nuclear Weapons Advisory Opinion* the ICJ concluded that customary international law imposes an obligation upon states to 'respect the environment of other states', the implication again being that

[103] Draft Articles on State Responsibility (n 4) 36.
[104] 'If the primary rules require fault (of a particular character) or damage (of a particular kind) then they do; if not, then not'; J Crawford, 'Revisiting the Draft Articles on State Responsibility' (1999) 10 *European journal of International Law* 435, 438.

it is the violation of the international legal rights of other states that gives rise to responsibility, regardless of whether damage is caused.[105]

In the *Trail Smelter* case however the Tribunal explained that state responsibility arises only where an injury is caused that is of 'serious consequence' to the victim state.[106] The Tallinn Manual adopts a similar position, explaining that the due diligence obligation only extends to 'activities that inflict *serious damage*, or have the potential to inflict such damage, on persons and objects protected by the territorial sovereignty of the target State'.[107] Damage here does not refer exclusively to physical damage but includes damage to computer systems or networks that produce serious consequences such as where networks that sustain critical national infrastructure are disabled.[108]

Whilst it is correct that the rationale for the customary obligation to prevent transboundary harm is to ensure that the territory of a state is not used in a manner incompatible with the sovereign rights of another state,[109] in the context of malicious transboundary cyber operations Schmitt accurately notes that to date 'there has been no suggestion from any quarter that the duty extends to mere irritation or inconvenience … Rather, harm must rise to such a level that it becomes a legitimate concern in intra-state relations and, thus, an appropriate subject of international law right and obligations'.[110] The predominant view, then, is that in order to establish a violation of the customary obligation of prevention an infringement of the victim state's international legal rights must occur and, in addition, this must produce serious (physical or non-physical) damage.

---

[105] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion (1996) ICR Rep 226, para 29.
[106] *Trail Smelter Case* (United States v Canada) (1941) 3 *Reports of International Arbitral Awards* 1905, 1965.
[107] Tallinn Manual (n 19) 26 (my emphasis).
[108] Ibid, 27 ('[t]here is no requirement that the cyber operation in question result in physical damage to objects or injuries to individuals; it need only provide a negative effect').
[109] In the Island of Palmas case it was explained that as sovereign equals states must 'protect within the[ir] territory the rights of other states, in particular their right to integrity and inviolability in peace and war'; *Island of Palmas*, 2 RIAA (Perm. Ct. Arb. 1928) 829, 839.
[110] Schmitt (n 15) 76.

If serious damage occurs the next question is whether it is the occurrence of such damage that gives rise to state responsibility or whether there must be a casual nexus between the state's failure to take preventative steps and the subsequent occurrence of serious damage.

The answer to this question depends on the content of the primary norm and not upon secondary rules of state responsibility. This being said, in relation to international obligations that are conditioned by the due diligence standard, the emerging approach is that responsibility will be incurred only where it can be shown that the state failed to take measures that were reasonably available to it and that such action might have contributed to avoiding the damage. In the *Genocide* case for example the ICJ explained that state responsibility for a failure to prevent genocide is incurred 'if the State manifestly failed to take all measures to prevent genocide which were within its power, and which *might have contributed* to preventing the genocide'.[111] Similarly, in the *Keenan* decision of the European Court of Human Rights, which was addressing Article 2 of the European Convention on Human Rights which requires member states not only to refrain from depriving individuals within its jurisdiction of their right to life but also obligates states to take appropriate steps to safeguard the lives of such individuals, it was explained

> For a positive obligation to arise, it must be established … that the authorities knew or ought to have known at the time of the existence of a real and immediate risk to the life of an identified individual from the criminal acts of a third party and that they failed to take measures within the scope of their

[111] *Bosnian Genocide* (n 5) para 430 (my emphasis).

> powers which, judged reasonably, might have been expected to avoid that risk.[112]

## 6. Concluding Remarks

This article has revealed that customary international law imposes an obligation upon states to prevent cyber infrastructure located upon their territory from being used in a manner injurious to the rights of other states. This obligation contains two distinct duties. The first duty is an obligation of result and imposes an absolute obligation upon states to implement laws and institutions that are capable of preventing their territory from being used in such a way as to violate the international legal rights of other states. Where states possess such capacity the second duty imposed upon them is an obligation of conduct in the sense that where a threat emerges and states have (actual or constructive) knowledge of that threat they must act reasonably in utilising their capacity and resources to suppress it. What is reasonable in the circumstances will depend upon the various factors operating at the time but, in particular, the extent of the resources available to the state and the risks associated with the threat will be of crucial consideration.

This article has demonstrated that the obligation to prevent doctrine does offer states a certain degree of legal protection from malicious transboundary cyber conduct committed by non-state actors and that the utility of this doctrine should not be overlooked, which is currently the case in international legal literature. This being said, the effectiveness of this customary obligation is limited. In relation to the first duty contained within the obligation of prevention, international law confers

[112] *Keenan v UK* (App No 27229/95), ECHR, 3 April 2011, para 89 (quoting *Osman v UK* (App No 23452/94), ECHR, 28 October 1998, para 116).

upon states a wide margin of appreciation as to what minimum legislative and institutional measures are necessary to discharge this international legal duty. This duty therefore lacks the specificity that is needed in order to create those laws and institutions that are necessary to enable states to effectively address the various threats emerging from cyberspace. In relation to the second duty, it imposes differentiated responsibilities upon states relative to their capacity and the concern is that in a heavily interconnected domain like cyberspace non-state actors will forum-shop and reroute their malicious cyber operations through the cyber infrastructure of less technologically capable states in order to minimise the possibility of the host state being able to suppress the activity.[113]

For these reasons, and especially as cyberspace becomes increasingly sophisticated with the emergence of the 'internet of things' and thus the threats associated with cyberspace continue to develop and evolve, it will be necessary to devise an international treaty (or even several international treaties) to regulate how states address threats emerging from cyberspace. The use of treaty law offers two main benefits.

First, an international treaty can 'upgrade'[114] state obligations by requiring states to adopt those specific laws and institutions that are considered necessary to suppress cyber threats. This could require, for example, states to criminalise certain forms of conduct, impose detailed regulatory frameworks upon providers of ICT and create CERTS that have expertise in detecting cyber threats and vulnerabilities and responding to incidents once they occur.

[113] In 2015 the Seabed Disputes Chamber explained that due diligence must be applied to states 'according to their capabilities'. Interestingly, the Chamber expressed concern that the differentiated responsibilities approach could 'jeopardize uniform application of the highest standards of protection of the marine environments' and that there was a need to ensure the '[e]quality of treatment between developing and developed States'; *Activities in the Area* (n 27) para 159.

[114] Bannelier-Christakis (n 50) 35.

Second, an international treaty can require states to proactively cooperate over issues of cyber security. As I have shown, the obligation to prevent transboundary harm requires states to cooperate with other states over cyber threats that emanate from their cyber infrastructure. Indeed, more generally Peters accurately notes that the corollary of the customary international law obligation upon states to resolve disputes peacefully is 'a general, customary law-based duty to cooperate with a view to a settlement'.[115] However, both of these international legal duties to cooperate are *reactive* in the sense that they only apply to known cyber threats or a where a cyber threat endangers international peace and security. In order to create a secure cyberspace what is needed is *prospective* cooperation and collaboration between the relevant stakeholders (including international organisations, states, software providers, cyber security companies etc) over issues of cyber security and internet governance.[116] A commitment encompassing such diverse actors to this type of dense, future-orientated cooperation can only be achieved through an international treaty. In addition, in order to ensure effective cooperation between stakeholders detailed procedural obligations would need to be imposed. These may include, for example, the requirement that states create domestic authorities that can act as 24/7 points of contact and which can liaise and interact with similar authorities in other states over cyber vulnerabilities and cyber threats and even the creation of supranational institutions that provide a forum for states and other stakeholders to meet to discuss threats connected with cyberspace, debate potential solutions, share information, set agendas, take collective decisions, exchange best practices and assist less developed states with enhancing their cyber capacity. Such detailed procedural obligations cannot be imposed by the

[115] A Peters, 'International Dispute Settlement: A Network of Cooperational Duties' (2003) 14 *European Journal of International Law* 1, 9.

[116] That a vibrant and secure cyberspace can only be achieved where states and other stakeholders actively cooperate over cyber threats was the gist of the Group of Government Expert's 2015 report; *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (22 July 215) UN Doc A/70/174.

duties to cooperate that currently exist under customary international law[117] but would need to be specifically crafted and implemented by a treaty.

There have been soft law attempts to create procedures and institutions to forge this type of cooperation. For example, the Global Forum for Cyber Expertise (GFCE) was launched in April 2015 and contains 50 members including states, international organisations and representatives from the private sector such as Microsoft and Symantec. The objective of GFCE is to facilitate the 'exchange best practices and expertise on cyber capacity building. The aim is to identify successful policies, practices and ideas and multiply these on a global level. Together with partners from NGOs, the tech community and academia GFCE members develop practical initiatives to build cyber capacity'.[118] Entities such as these should be encouraged and represent a step in the right direction towards securing closer cooperation over cyber security. Fundamentally, however, such soft law mechanisms cannot be the substitute for effective international legal regimes that compel states to adopt cyber-specific laws and institutions that are sufficient to address threats that emerge from cyberspace and to work with supranational agencies and authorities that facilitate and encourage close cooperation and capacity building between the relevant stakeholders.

[117] See V Lowe, *International Law* (OUP, 2007) 111.
[118] Global Forum for Cyber Expertise http://www.thegfce.com/about.