The European Journal of International Law Vol. 33 no. 3

Back to the Roots: The Laws of Neutrality and the Future of Due Diligence in Cyberspace

Jan Martin Lemnitzer*

Abstract

The question of whether the due diligence rule applies in cyberspace has become a key issue in the cyber norms debate. Yet there is no consensus whether the rule is binding, and states lack clear guidance on what the norm requires them to do. This is not just unfortunate but also dangerous since a crisis caused by a cyber attack routed through a third state where the victim state and the third state have fundamentally different views as to which duties apply carries a serious escalation risk. While scholars have suggested adapting legal approaches from other successful due diligence regimes, these rules are not a good match for the crucial issue in cyber due diligence: what do states need to do to ensure that no state is attacked using their networks? This article suggests going back to the roots and implementing principles derived from the laws of neutrality, the field that originally brought the due diligence principle into international law. Designed to manage escalation risk at the fringes of international conflict, it is our best guide through the grey zone of due diligence in cyberspace. The classic cases such as Alabama *and* Corfu Channel *were disputes related to armed conflicts but between states that were at peace with each other. Read closely, they offer clear guidance on how to develop a flexible, but reliable, due diligence standard for cyberspace that will help states manage expectations of responsible behaviour and thereby defuse future potential conflicts before they arise, while avoiding the need to formally attribute the original attack. The final section will seek to consolidate the historical, legal as well as technological developments discussed here to lay out what the due diligence rule in cyberspace is likely to look like soon.*

1 Introduction: Due Diligence in Cyberspace

Within the fast-growing debate over the scope and application of international law in cyberspace, the question whether states have cyber-specific due diligence duties

* Department of Digitalization, Copenhagen Business School, Copenhagen, Denmark. Email: jl.digi@cbs.dk.

and what they might look like has emerged as a key issue. Cyber attacks can have devastating consequences for the civilian population of victim states, especially if directed at critical infrastructure. Crucially, both state and private actors conducting cyber attacks routinely use the networks of third states to facilitate offensive cyber operations or criminal activities and to hide their tracks.[1] The question concerning which duties third states have to prevent harm from others if their networks are used to conduct destructive cyber operations is therefore extremely serious. The status and scope of the due diligence norm in cyberspace is not an academic problem but already a political issue. For example, part of the European Union's (EU) response to the COVID-19 pandemic was a declaration by the EU's High Representative Josep Borrell invoking a due diligence duty to stop cyber criminals from attacking hospitals in other countries.[2]

Unfortunately, there is considerable uncertainty about the existence of a binding due diligence duty for cyberspace and what exactly it might compel states to do. This is not just unfortunate but also dangerous: states that are the victims of a serious cyber attack using the networks of a third state, while the original attacker remains unknown, are unlikely to show much patience if that third state is slow to act or fails to stop the attack. Instead, they might conduct cyber operations of their own, although the legality of such robust responses is doubtful, certainly in peacetime. Therefore, the disagreement over the duties that third states have to prevent or stop their networks from being exploited for harmful cyber attacks poses a serious escalation risk. This article argues that the best guidelines for navigating this legal minefield and developing universally agreed rules and principles for the due diligence duty in cyberspace can be found in the ancient laws of neutrality. This is because they were designed with the reduction of conflict escalation risk between belligerents and third states as their main purpose. It is law created for the grey zone at the fringes of, or just below, armed conflict: due diligence in the laws of neutrality regulates the relationship between belligerents and neutrals who might have a dispute related to a conflict but are at peace with each other. In fact, due diligence was first introduced to international law to fulfil this specific function in the laws of neutrality. Therefore, we should go back to these roots to develop a flexible, but reliable, due diligence standard for cyberspace that will help states manage expectations of responsible behaviour and thereby defuse future potential conflicts before they arise.

[1] This technique is not limited to criminals or rogue states: the use of third countries' networks to hide the tracks of its own offensive cyber operations is official US strategy. See Smeets, 'US Cyber Strategy of Persistent Engagement and Defend Forward: Implications for the Alliance and Intelligence Collection', 35(3) *Intelligence and National Security* (2020) 444, available at https://doi.org/10.1080/02684527.2020.1729316.

[2] See Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic, 30 April 2020, available at www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

While attempts to explore these parallels have been made,[3] this article is the first to systematically link the classic laws of neutrality to the current state of debate on cyber due diligence as well as the current cyber-security capabilities of small and large states alike. After presenting the status and scope of due diligence in cyberspace and why it is so problematic, the article will lay out the main principles applied in the laws of neutrality to limit escalation risks at the fringes of international conflicts. While the failed efforts to protect global trade and communication networks from the ravages of war have contributed to neutrality law's mixed reputation, neutrality law has been remarkably successful in protecting neutral territory. The due diligence standard was a key element of this success, and three case studies will show how it was developed, how it was meant to work in practice, and how the principles and dynamics could be applied to cyberspace. The final section will seek to consolidate the historical, legal as well as technological developments discussed here to lay out what the due diligence rule in cyberspace is likely to look like soon.

2 The Status and Scope of Due Diligence in Cyberspace

A *The Status of the Due Diligence Norm in Cyberspace*

While there is an ongoing debate whether due diligence is a general principle, a rule of international law or, perhaps, a framework of legal and non-legal norms, it clearly exists as a duty that states must respect. Numerous courts and arbitration tribunals have applied it to establish that a state has acted unlawfully and awarded compensation payments.[4] What is also undisputed is that there is a general due diligence rule and more detailed due diligence regimes in specific domains such as environmental or investment law, setting out the duties of states in more detail.[5] Therefore, we must ask, first, whether the general (and binding) due diligence duty applies as a specific rule in cyberspace and, second, whether we have already seen the emergence of a specialized due diligence regime for cyberspace. Curiously, the answer seems to be 'no' to the first question and 'yes' to the second.

There is currently no consensus that due diligence is a binding norm in cyberspace: a report compiled by Duncan Hollis in 2020 for the Organization of American States discovered that most, but not all, Latin American states see due diligence as binding

[3] See S. Cordey and K. Kohler, 'The Law of Neutrality in Cyberspace', December 2021, available at https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/t/h/e/l/the_law_of_neutrality_in_cyberspace (who sketch out the broader relationship between neutrality and cyberspace, stressing that this discussion is still in its infancy); see also Reinisch and Beham, 'Mitigating Risks: Inter-State Due Diligence Obligations in Case of Harmful Cyber-Incidents and Malicious Cyber-Activity – Obligations of the Transit State', 58 *German Yearbook of International Law* (*GYIL*) (2015) 101.

[4] McDonald, 'The Role of Due Diligence in International Law', 68(4) *International and Comparative Law Quarterly* (*ICLQ*) (2019) 1041, available at https://doi.org/10.1017/S0020589319000344.

[5] For a recent overview, see the contributions in H. Krieger, A. Peters and L. Kreuzer (eds), *Due Diligence in the International Legal Order* (2021).

in cyberspace.[6] New Zealand recently declared itself 'not yet convinced that a cyber-specific "due diligence" obligation has crystallised in international law'.[7] A recent overview of the views of the USA and six European states on the law of cyberspace found that, while five of the states agreed, the USA and the United Kingdom (UK) refused to publicly commit to that position.[8] As Eric Talbot Jensen and Sean Watts argue, given the USA's unique combination of global political and technological clout, an endorsement by the US government would transform the debate, but Washington has so far proved unwilling.[9] A paper published in November 2021 by the United Nations' (UN) Institute for Disarmament Research (UNIDIR) dryly summarizes the *status quo* by saying that 'states have divergent positions on whether it is a voluntary norm, a rule or a principle of international law imposing certain obligations'.[10] Most states accept a binding due diligence norm in cyberspace, but many influential ones do not.

Interestingly, in multilateral documents, the community of states seems unanimous in its desire to create a specialized due diligence regime for cyberspace while, at the same time, denying the binding nature of the norm. The influential 2015 UN Group of Governmental Experts' (GGE) report that has been endorsed by the Group of Seven and the Group of Twenty organizations says that 'states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs [information and communication technologies]', a wording that deliberately evokes the classic formulation of due diligence duties in the 1949 *Corfu Channel* case that it is 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.'[11] At the same time, the drafters used 'should' instead of 'must', indicating it is a recommendation rather than binding law. The latest GGE report from 2021 still uses the same wording.[12] The states seem to assume that it is possible to take existing legal duties and declare them 'voluntary and non-binding' as part of a norm-building effort in a new field. This position has been criticized by leading international lawyers such as Dapo Akande and Francois Delerue who have argued that, while some

6 D. Hollis, 'Improving Transparency: International Law and State Cyber Operations', 5 March 2020, at 20–21, available at www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf.

7 Statement on the Application of International Law to State Activity in Cyberspace, 1 December 2020, at 3, para. 17, available at www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf.

8 P. Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', Hague Program for Cyber Norms Policy Brief, March 2020, available at https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf?sequence=1&isAllowed=y.

9 E. Jensen and S. Watts, 'Due Diligence and the U.S. Defend Forward Cyber Strategy', BYU Law Research Paper no. 20-24, 16 September 2020, available at https://ssrn.com/abstract=3694056.

10 A. Kastelic, 'Due Diligence in Cyberspace: Normative Expectations of Reciprocal Protection of International Legal Rights', November 2021, at 21, available at www.unidir.org/publication/due-diligence-cyberspace-normative-expectations-reciprocal-protection-international.

11 United Nations (UN) Group of Governmental Experts' (GGE) Report 2015, Doc. A/70/174 (2015), paras 13(c), 28(e); *Corfu Channel (United Kingdom v. Albania)*, Merits, 15 December 1949, ICJ Reports (1949) 4, at 22.

12 Report of the UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security, 28 May 2021, available at https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

new, specific rules reflecting the governance needs of a new technology need to be created, there is no reason to assume that a new field of international law begins as a blank slate.[13] Yet that is exactly what the community of states has done with the due diligence norm in cyberspace.

For some states, the opposition to due diligence in cyberspace goes further. When the Open-Ended Working Group (OEWG) established by the UN General Assembly to define rules of responsible state behaviour in cyberspace presented its final report in March 2021, the section on due diligence was removed and relegated to the 'President's letter' outlining issues too controversial for the main text.[14] Diplomats involved in the drafting confirm that, although a clear majority of states support due diligence, it was sacrificed to ensure that all states would sign up to the final document, although the group had further weakened the due diligence wording by stating that states 'should seek to ensure' (instead of 'should') that their territory is not used to commit internationally wrongful acts using ICT.

B *The Scope of the Due Diligence Duty in Cyberspace*

The reason why some powers are apprehensive regarding the due diligence norm in cyberspace is that they fear it might burden them with detailed requirements in the future. Therefore, there is also little interest in precisely defining the present scope of the norm in multilateral documents. The UNIDIR paper cited earlier concludes that 'states are yet to reach an agreement on the scope of the norm, knowledge conditions, standards, and thresholds of the norm'.[15] Even the five states surveyed earlier that believed a binding due diligence norm existed all resorted to the same vague language, asserting that states were required to take 'reasonable measures' after being informed about a cyber attack using its networks but without offering any further details.[16]

The best available guide is the *Tallinn Manual 2.0*, compiled by a group of experts in 2017, and we will refer to it throughout this article.[17] It is not a ratified treaty like the 1907 Hague Conventions but, rather, more comparable to the 1880 *Oxford Manual on the Laws of War*, an important and authoritative steppingstone towards a codification,

[13] Akande, Coco and de Souza Dias, 'Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond', *EJIL:Talk!* (5 January 2021), available at www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/; F. Delerue, *Cyber Operations and International Law* (2020), at 9–10.

[14] Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), Draft Report, Doc. A/AC.290/2021/CRP.2, 11 March 2021, available at https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf. The section was still included in the Draft Dubstantive Report (zero draft), Doc. A/AC.290/2021/L.2, 19 January 2021, para. 30, available at https://undocs.org/A/AC.290/2021/L.2.

[15] Kastelic, *supra* note 10, at 21.

[16] Roguski, *supra* note 8; see also German Foreign Office, 'Position Paper on the Application of International Law in Cyberspace', March 2021, at 3, available at www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf.

[17] M. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017).

but still the work of academics rather than states.[18] Unfortunately, the *Tallinn Manual 2.0* concludes that 'the precise scope of action required by the due diligence principle is unsettled'.[19] While insisting that it is every state's duty to take 'all reasonably available measures' to prevent their networks being used to harm others and discussing a great variety of actions states could reasonably take to fulfil their due diligence duty, it rejects the idea of any of them being accepted by states as binding requirements.[20] Interestingly, it deviates from the UN-sponsored texts in saying that 'a State *must* exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States'.[21] This may explain why concerned states approached the expert group during the drafting process to ensure that all obligations remain hortatory rather than binding.[22] After due diligence was dropped in the final version of the OEWG's report, the fact that it was featured again in the GGE report published shortly afterwards in June 2021 is significant in itself. Yet the expression of the norm remained vague, simply stating that 'the norm raises the expectation that a State will take reasonable steps within its capacity to end the ongoing activity in its territory'.[23]

Because of the diplomatic hand-wringing, states lack guidance on how they are supposed to fulfil their due diligence obligations. What 'reasonable efforts' is a state expected to take, and which demands by the victim state can it safely reject as excessive? The lack of clarity of what due diligence in cyberspace requires not only undermines what would otherwise be a very good argument to support cyber capacity building. What is worse is that the gap between what different states think is required by the due diligence duty creates an obvious escalation risk in future cyber conflicts.[24] The rules of responsible state behaviour matter most when one state acts irresponsibly and others call it out. The less clarity there is regarding what responsible state behaviour in cyber space might look like, the more fraught with tension this process is going to be. Without agreed legal foundations, a crisis involving cyber attacks routed through third states will pose a much higher risk of escalation.

[18] Note that the current edition will be replaced by a Tallinn Manual 3.0 expected in 2025, available at https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/. The text of the *Oxford Manual on the Laws of War on Land*, adopted by the Institute of International Law on 9 September 1880, is printed in D.Schindler and J.Toman, *The Laws of Armed Conflicts* (1988), 36–48.

[19] *Tallinn Manual 2.0*, *supra* note 17, at 41, para. 1.

[20] For this reason, Eric Talbot Jensen argues that the *Tallinn Manual* will not encourage states to show heightened diligence. See Jensen, 'Due Diligence in Cyber Activities', in H. Krieger, A. Peters and L. Kreuzer (eds), *Due Diligence in the International Legal Order* (2021) 252, at 262.

[21] *Tallinn Manual 2.0*, *supra* note 17, Rule 6 (emphasis added). Note that the project director of the *Tallinn Manual* process had criticized the use of 'should' in 2015. See Schmitt, 'In Defense of Due Diligence in Cyberspace', 125 *Yale Law Journal Forum* (2015) 68, at 73, available at www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace.

[22] Schmitt, 'Grey Zones in the International Law of Cyberspace', 42(3) *Yale Journal of International Law* (2017) 2, at 12–13.

[23] GGE, *supra* note 12, para. 30.

[24] For a similar view, see Kastelic, *supra* note 10, at 19.

C *Possible Pathways for the Future Development of the Due Diligence Norm in Cyberspace*

Some scholars have recommended settling this problem though a treaty.[25] Unfortunately, codification seems a distant prospect as the UN must first unite the two parallel working groups working on cyber norms.[26] Moreover, given the current controversy surrounding it, due diligence is an unlikely candidate for early codification. Historically, due diligence rules were forged by fire, not calmly negotiated at conference tables. States are loath to create new duties for themselves, and the due diligence standard is the result of norm development through diplomatic crisis. But are there ways to develop the norm without international conflict?

Given the prominent role of due diligence as a driver of legal innovation in other fields, scholars have looked for analogies that might be transferred into a cyber context, particularly from the successful due diligence regime in environmental law. Peter Stockburger has proposed the adoption of the precautionary principle in cyber law.[27] However, the key logic behind it is that harm done to nature and wildlife is usually irreversible, which is not the case in cyberspace (with the important exception of some data loss). Joanna Kulesza has suggested viewing the Internet as a global commons like the high seas or the ocean floor and assigning specific safeguarding duties to Internet service providers.[28] Yet the use of the global commons concept for a man-made and privately owned structure is inherently problematic. Other environmental due diligence rules like the duty to conduct potentially harmful projects according to the best available technical standards are also unlikely to be transferred; given that cyber security is about protecting a large number of networks rather than managing a single building project, due diligence is more likely to require the use of commonly used technology to defend networks. On the other hand, the *Tallinn Manual*'s idea of introducing a threshold of a cyber attack needing to cause 'serious adverse consequences' in the victim state before triggering a due diligence duty was directly adapted from the due diligence regime in environmental law.[29] In conclusion, while some ideas lend

[25] Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', 21(3) *Journal of Conflict and Security Law* (2016) 429; Couzigou, 'Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations', 32(1) *International Review of Law, Computers and Technology* (2018) 37.

[26] Even this will be 'an uphill struggle'. See Moynihan, 'The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace', *Journal of Cyber Policy* (29 October 2020), available at www.tandfonline.com/doi/full/10.1080/23738871.2020.1832550.

[27] Stockburger, 'From Grey Zone to Customary International Law: How Adopting the Precautionary Principle May Help Crystallize the Due Diligence Principle in Cyberspace', in T. Minárik, R. Jakschis and L. Lindström (eds), *CyCon X: 10th International Conference on Cyber Conflict* (2018) 245, available at https://ccdcoe.org/uploads/2018/10/Art-13-From-Grey-Zone-to-Customary-International-Law.-How-Adopting-the-Precautionary-Principle-May-Help-Crystallize-the-Due-Diligence-Principle-in-Cyberspace.pdf.

[28] Kulesza,'Due Diligence in Cyberspace', in J. Kulesza (ed.), *Organizational, Legal, and Technological Dimensions of Information System Administration* (2014) 76; Brunée and Meshel, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance', 58 *GYIL* (2015) 129.

[29] *Tallinn Manual 2.0*, *supra* note 17, at 37, para. 25.

themselves to adaptation, environmental due diligence cannot solve the problems faced by due diligence in cyberspace.

The due diligence norm has also taken root in the field of international humanitarian law, and it is easy to see how concepts such as the need to take due care in targeting decisions or avoiding indiscriminate damage can be transferred into cyberspace.[30] However, this is law that is designed to constrain belligerents, and international humanitarian law (IHL) takes limited interest in the role of third states. Therefore, attempts to translate IHL norms requiring non-parties to conflicts to protect civilians into a cyber context have only resulted in vague commitments to 'protecting critical civilian infrastructure and services' from cyber threats.[31] Obviously, this is not the detailed guidance that states require on due diligence in cyberspace. Other scholars suggest adopting the procedures of private sector due diligence, particularly from US practices regarding mergers and acquisitions. However, these practices are still being developed, lack conformity and are not yet widely implemented.[32] Moreover, while cooperation between private and state actors is an absolute necessity in the world of cyber security, many due diligence business practices have no close parallel to international disputes related to cyber conflict.

Given the lack of exact parallels in other due diligence regimes and the dispute over the binding nature of the norm, Antonio Coco and Talita de Souza Dias have recently proposed a 'patchwork approach', creating a cyber due diligence regime through an eclectic mix of existing obligations from other fields without making any firm statement about the legal nature of due diligence in cyberspace. They define due diligence as a subset of a large number of provisions where states are required to show a reasonable amount of care.[33] Yet IHL rules are not written for third states, and most of the rules they take inspiration from were created for peace, not conflict. As they themselves admit, their approach means trying to create a due diligence regime for cyberspace by assembling rules from a wider corpus of norms that, in their vast majority, were not designed with the scenario of a state's territory being used to do significant harm to another in mind.[34]

Yet this is precisely what cyber due diligence is about: how can and must third states act to prevent the use of their networks in cyber attacks that either happen at the fringes of an armed conflict or are deliberately set just below the threshold of an armed attack? This article argues that, to find guidance for the 'grey zone' of modern

[30] See Longobardo, 'The Relevance of the Concept of Due Diligence for International Humanitarian Law', 37 *Wisconsin International Law Journal* (2020) 44; Kelsey, 'Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare', 106 *Michigan Law Review* (2008) 1427.

[31] Coco and de Souza Dias, '"Cyber Due Diligence": A Patchwork of Protective Obligations in International Law', 32 *European Journal of International Law* (*EJIL*) (2021) 771, at 804.

[32] Shackelford, Russell and Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors', 17(1) *Chicago Journal of International Law* (2016) 1, available at https://chicagounbound.uchicago.edu/cjil/vol17/iss1/1.

[33] Coco and de Souza Dias, *supra* note 31, at 775, 777.

[34] *Ibid.*, at 778.

cyber conflict, we must go back to the roots of the due diligence rule in international law and consult the laws of neutrality. By looking at the precedents and state practice of a field that for centuries has guided states on how to manage international conflicts in their vicinity and prevent their further escalation, we can distil useful lessons and approaches for managing due diligence in cyberspace.

3 The Laws of Neutrality and the Due Diligence Rule

The laws of neutrality were developed because interstate conflict is not a duel, and military activity between states always touches upon the territories or interests of third states. While they can be traced back to the Middle Ages, their importance grew in the early modern period with the increasing entanglement of trade and transport and Europe's global expansion.[35] Their main purpose was to prevent the escalation of existing military conflicts by creating a balance between the interests of belligerents and neutrals. For the purposes of this article, we can distinguish two main aspects of the laws of neutrality: (i) the use of neutral territory and (ii) the protection of international networks. As for neutral territory, the fundamental principle is that belligerents must respect it and may not use it to gain a military advantage. Troops entering neutral territory must disarm, and neutrals are expected to defend their neutrality: as the Hague Conventions make clear, the use of force to expel troops from neutral territory cannot be regarded as a hostile act.[36] When this norm was broken with the German invasion of Belgium in 1914, the violation of neutrality was a key reason why Britain entered World War I. At the same time, neutrals must treat all belligerents equally and not allow their territory to be used in a way that grants one belligerent a military advantage or causes another belligerent serious harm. As we shall see, the due diligence principle turned out to be an extremely valuable tool in defining and calibrating the scope of this neutral duty over time and in vastly different political, geographical and technological contexts. However, the key questions have always been about what extent of monitoring is required by neutral states to ensure that they can detect a violation of the neutrality of their territory early on and about how fast they need to respond once they are notified by others.

The principles of neutrality law regarding the protection of international trade and communication networks from belligerent interference should offer tempting analogies for the laws of cyberspace, but their historical record is less than promising. As maritime trade became increasingly important for states towards the end of the early modern period, states argued whether the principle that protected neutral territory from interference should be extended to neutral trade routes: were neutrals free to trade with both sides as naval war waged around them, or were belligerents entitled to confiscate neutral vessels carrying enemy cargo and harass them off the enemy's

[35] S. Neff, *The Rights and Duties of Neutrals: A General History* (2000); L. Muller, *Neutrality in World History* (2019).

[36] Hague Convention (V) on the Rights and Duties of Neutrals in Land Warfare 1907, 205 CTS 299, Arts 2, 10.

coastline? Britain traditionally took a hard line and tried to use its naval power to limit its enemies' capabilities to benefit from trade with neutral nations – for example, during the Seven Years War.[37] Neutral nations disagreed and experimented with so-called 'armed neutralities' to defend the rights of their ships as a united bloc, but, in the end, the targeting of trade networks tended to lead to the escalation of wars as neutral nations either joined the conflict or began a separate war against one of the belligerents (as the USA did against Britain in 1812). The Napoleonic Wars marked the culmination of this process as the belligerent focus on economic warfare ultimately (involved) almost every European neutral in the fighting.[38]

This scarring experience weighed heavily on the minds of the next generation of statesmen as they tried to ensure that the next European great power conflict did not lead to a global conflagration.[39] This is why Britain and France promised at the beginning of the Crimean War in 1854 to protect neutral rights in wartime.[40] The gamble paid off as maritime trade continued as normal, and neutral nations eventually aligned around Britain and France rather than Russia. In the Declaration of Paris, which was signed just after the war in 1856, the new guarantees for neutral trade became permanent rights for all signatories.[41] The preamble makes it explicit that the main goal was to prevent the escalation of neutrality disputes into military conflicts. The signatories were so determined to achieve this goal that they invited all nations to sign up to its principles to secure their instant global recognition, inventing the modern multilateral law-making treaty in the process.[42] Yet the Declaration of Paris was only meant to be the beginning of a framework for the laws of maritime war and neutrality. This full codification came in two steps in 1907 and 1909: first with the Hague Conventions in 1899 and 1907 and then with the Declaration of London, which tried to finally solve the vexed problems regarding neutrality and maritime war.[43]

Yet it was never ratified, and when the unfinished legal edifice was put to the test in World War I, the rules for protecting neutral trade that had been painstakingly created unravelled within months. By 1915, neutral merchant vessels faced minefields, compulsory British controls and German torpedoes.[44] The law protecting global communications networks had not fared any better as belligerents used a 'military necessity' exception in the Hague Conventions to cut many of the privately owned submarine telegraph cables right at the beginning of the war.[45] This collapse and the failure of

37 C. Kulsrud, *Maritime Neutrality to 1780* (1936).

38 Marzagalli and Muller, '"In Apparent Disagreement with All Law of Nations in the World": Negotiating Neutrality for Shipping and Trade during the French Revolutionary and Napoleonic Wars', 28 *International Journal of Maritime History* (2016) 108.

39 M. Abbenhuis, *An Age of Neutrals: Great Power Politics 1815–1914* (2014).

40 Declaration of 28 March 1854, reprinted in 46 *British and Foreign State Papers* (1865) 36.

41 Declaration Respecting Maritime Law. Paris, 16 April 1856, printed in 15 Martens NRG (1890) 791.

42 See J. Lemnitzer, *Power, Law and the End of Privateering* (2014), at 57–75.

43 Declaration concerning the Laws of Naval War. London, 26 February 1909, printed in D. Schindler and J. Toman, *The Laws of Armed Conflicts* (1988), 845.

44 J. Coogan, *The End of Neutrality: The United States, Britain, and Maritime Rights, 1899–1915* (1981); J. den Hertog and S. Kruizinga (eds), *Caught in the Middle: Neutrals, Neutrality, and the First World War* (2011).

45 Hague Convention (IV) Respecting the Laws and Customs of War on Land (1907), 187 CTS 227, Art. 54.

several subsequent attempts to rebuild the network protection aspects of neutrality law in the interwar period contributed to the idea that the laws of neutrality were ineffective and outdated, although some states successfully defended the neutrality of their territory for the entirety of World War II.[46]

In 1945, the UN Charter envisioned the UN Security Council as the final arbiter in military disputes, deciding whose side member states should support. Therefore, the very idea of neutrality seemed superfluous, which is why the International Law Commission singled out the laws of neutrality as the one field of international law unworthy of further development in 1949.[47] More than 70 years later, it has become abundantly clear that the assumption behind that decision has proven overconfident, but the laws of neutrality never regained their earlier prominence and remain the preserve of a tiny field of specialists.[48] None of the earlier legal protections for neutral maritime traffic were resurrected, and there is little to suggest that future belligerents will refrain from targeting the privately owned submarine cables that transport the bulk of Internet traffic today.[49] The only treaties in this field that are undoubtedly in force and generally recognized as customary international law are the Hague Conventions of 1899 and 1907 regarding the rights and duties of neutral states, written just after the invention of wireless radio. Still, Ukraine joined both the 1899 and the 1907 versions of the convention regulating land warfare in May 2015, showing the continuing legal relevance of these ancient documents.[50]

However, the principle that belligerents must respect neutral territory has held firm through the centuries, not least because of the corresponding duty for neutrals not to allow their territory to be used to interfere in military conflicts. The due diligence

[46] The failure of the League of Nation's Disarmament Conference undermined attempts at codification in the early 1930s, and the Harvard project trying to fill this gap suffered from inauspicious timing when it presented its draft version of a new rulebook in late August 1939. See Harvard Research in International Law, Draft Convention on Rights and Duties of Neutral States in Naval and Aerial War, reprinted in 33 *American Journal of International Law* (*AJIL*), Supplement (1939) 204; see also N. Ørvik, *The Decline of Neutrality, 1914–1941* (1953); N. Wylie (ed.), *European Neutrals and Non-belligerents during the Second World War* (2002).

[47] See *Yearbook of the International Law Commission* (1949), at 281.

[48] A typical modern document relating to neutrality is the *San Remo Manual*, assembled by a group of scholars concerned about the lack of modern laws to regulate maritime conflict at sea. L. Doswald-Beck (ed.), *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (1995).

[49] See Kraska, 'The Law of Maritime Neutrality and Submarine Cables', *EJIL Talk!* (29 July 2020), available at www.ejiltalk.org/the-law-of-maritime-neutrality-and-submarine-cables/. This highlights the urgency and relevance of the work done by scholars seeking to establish a specific norm protecting the public core of the Internet. See D. Broeders, *The Public Core of the Internet: An international Agenda for Internet Governance* (2016); Broeders, 'Aligning the International Protection of "The Public Core of the Internet" with State Sovereignty and National Security', 2 *Journal of Cyber Policy* (2017) 366.

[50] The list of states parties for the 1899 Convention with Respect to the Laws and Customs of War on Land and the 1907 Convention Respecting the Laws and Customs of War on Land show that Ukraine joined both treaties on 29 May 2015, see https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=150 and https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=195. For a discussion of the status of these norms and subsequent state practice, see J. Upcher, *Neutrality in Contemporary International Law* (2020).

rule was brought into international law more than 150 years ago to help interpret this precise duty, and we shall now look at three cases roughly 50 years apart from each other to explore how the principle adapted to extensive geopolitical and technological change. The implications of these legal approaches for cyber due diligence will be briefly discussed at the end of each case.

4 Case Studies on Due Diligence and the Laws of Neutrality

The *Alabama* arbitration was the case that established the term 'due diligence' to precisely describe the duties of a neutral state. It also demonstrates that norms do not have to be long established to be the basis for huge compensation payments. The second example on the neutral control of radio broadcasting shows that, even when existing codification is relatively undemanding, states might decide to over-implement due diligence rules to avoid disputes. Finally, the *Corfu Channel* case is often cited as the classic definition of due diligence, but a closer look at the judgment will reveal that it has much more to offer to the laws of cyberspace.

A *The* Alabama *Arbitration*

Arms exports by private companies are a classic flashpoint between belligerents and neutrals. When private companies in Belgium and Prussia sold large amounts of advanced rifles to Russia during the Crimean War, they correctly argued that there was nothing illegal about these sales. Unimpressed, Britain threatened to blockade the Dutch and Belgian coastlines and declare war on the Prussians if the exports were not stopped.[51] During the American Civil War, the USA considered war on Britain after British-built ships had given the Confederates a navy. Confederate agents had tried to exploit a loophole in Britain's neutrality legislation: the 1819 Foreign Enlistment Act did not explicitly ban the building of a vessel that was only equipped as a warship after leaving British jurisdiction.[52] US spies quickly spotted the suspicious activities at the John Laird & Sons shipbuilding company in Liverpool, and the US government demanded that these vessels should be seized. Yet London proved slow to respond, and the buyers took one of the vessels on a 'trial run' and fitted it out as a warship upon reaching the Azores. Named CSS *Alabama*, it captured and burned 64 Union merchant vessels and one US navy steamer before a huge search effort by the US navy led to her being sunk just outside of Cherbourg, France, in June 1864. One reason why the *Alabama* evaded her pursuers was that she was able to access British ports in the Caribbean and Southern Africa where she was treated as an official Confederate vessel rather than a British lawbreaker. During this time, the US government and Congress seriously considered war on Britain and only thought again after London became

[51] Lemnitzer, *supra* note 42, at 32–34.

[52] Bingham, 'The Alabama Claims Arbitration', 54(1) *ICLQ* (2005) 1, at 9; Foreign Enlistment Act 1819, 59 Geo. 3, c. 69.

much swifter in seizing other vessels built for Confederate agents – for example, the *Alexandra* in April 1863.[53]

After the war had ended, a royal commission was set up in 1867 to review the 1819 law. Following their recommendations, the 1870 Foreign Enlistment Act made the building of warships for use in foreign wars illegal, regardless of where they were fitted out.[54] The US government understood this to be an admission of guilt and suggested settling the dispute through arbitration. The UK was reluctant to agree because US politicians openly discussed the idea of compensation in the form of British territories such as Canada and because the idea of having the adequacy of British domestic laws reviewed by international arbitrators was then radically new.[55] However, by 1871, the common interest of the two governments in a better strategic relationship persuaded both to sign an agreement setting up an arbitration tribunal in Geneva.[56] The Treaty of Washington also defined the applicable law, stating in Article 7 that (i) neutrals must exercise due diligence in preventing the fitting out of armaments in their jurisdiction; (ii) that any vessels fitted out in this way must not be admitted into the nation's ports; and (iii) that neutrals have a separate due diligence duty to actively monitor their ports and waters, and, in regard to any persons within its jurisdiction, to prevent any violation of the abovementioned duties.[57]

Interestingly in the context of cyber due diligence, Britain argued that its actions should be purely measured by what was 'reasonable', claiming that a lack of due diligence meant 'a failure to use… such care as governments ordinarily employ in their domestic concerns, and may reasonably be expected to exert in matters of international interest and obligation'.[58] However, the tribunal sided with the US contention that a due diligence standard requires a neutral government to act in exact proportion to the risks to which belligerents may be exposed from any failure to fulfil obligations of neutrality. Due diligence, therefore, was a flexible concept but one that demanded swift and effective action. The tribunal also rejected the British defence that it had no legislation covering this precise activity at the time and explicitly ruled that not having relevant legislation in place does not relieve a state from fulfilling its due diligence duties. Instead, Britain had failed to act after having been informed of the ships' construction and failed to mitigate the damage as it only took inadequate

[53] Charles Francis Adams to William Seward, 7 April 1863, reprinted in 1 *Papers Relating to the Foreign Relations of the United States* (*FRUS*) (1863) 228; Bingham, *supra* note 52, at 10.

[54] Foreign Enlistment Act 1870, 33 & 34 Vict., c. 90. The act is still in force and is available at www.legislation.gov.uk/ukpga/Vict/33-34/90.

[55] Dashew, 'The Story of an Illusion: The Plan to Trade Alabama Claims for Canada', 15(4) *Civil War History* (1969) 332.

[56] Britain wanted a better relationship after Germany's win over France in January 1871, and the USA wanted access to London's financial markets. See Sexton, 'The Funded Loan and the Alabama Claims', 27(4) *Diplomatic History* (2003) 449.

[57] Treaty of Washington 1871, Papers Relating to Foreign Relations of the United States,1873, at 410, available at https://history.state.gov/historicaldocuments/frus1873p2v3/d84.

[58] See *Case Presented on the Part of the Government of Her Britannic Majesty in Papers Relating to Foreign Relations of the United States*, part 2, vol. 1 (1872), at 412.

measures to pursue them once they had escaped.[59] The compensation awarded to the USA amounted to an astonishing $15.5 million, an enormous sum at the time.

The due diligence duties for preventing the fitting out of warships and the proactive monitoring of ports and territorial waters were both codified at the Second Hague Peace Conference in 1907.[60] Moreover, the *Alabama* decision has several additional features that have direct relevance for the future due diligence regime in cyberspace. First, it established the general principle that states have a responsibility for arms exported by private companies from their territory and that a higher level of due diligence is required for high-risk technologies. Here, 'reasonable' efforts are insufficient. Second, if a state is too slow to act after being notified to prevent harm being done to another state, it is liable for compensation. Third, a state cannot absolve itself of due diligence duties by failing to create domestic legislation. The *Alabama* tribunal's interpretation of due diligence is much stricter than what states currently accept for cyberspace. Still, passing on hacking tools to a rebel group in an armed conflict is considered an internationally wrongful act.[61] Therefore, a modern tribunal might easily conclude that negligence leading to a failure to prevent this export by a private company is a due diligence failure, making the state liable for the damage caused by subsequent cyber attacks using these tools.

B *The Neutral State's Due Diligence Duty to Monitor Telegraph and Radio Stations*

Like arms exports, the question concerning what neutral nations must do to prevent abuse of telecommunications equipment on their territory by belligerent states has been part of international law for more than 150 years. The consistent theme is that the practice of states indicates a much stricter approach to monitoring duties than the written law they codified. In the Franco-Prussian War of 1870–1871, the French navy used telegraph stations along the Brazilian and Argentinian coasts to alert their squadron to movements of German merchant vessels that they wished to capture. Prompted by daily Prussian protests, Argentina and Brazil both decided that the only way to protect their neutrality was to ban belligerents from using their telegraph networks for military purposes.[62] When long-range radio technology emerged, belligerents immediately tried to deploy it on neutral territory: during the 1904–1905 Russo-Japanese War, the Russian military used a purpose-built wireless station in Chefoo (modern Yantai) in neutral China to relay messages from the besieged Port Arthur to the Russian mainland. Observers at the time wondered whether China had violated its duties as a neutral by tolerating this structure.[63] In 1907, the Hague

[59] *Arbitration Award*, done at Geneva, 14 September 1872, available at https://legal.un.org/riaa/cases/vol_XXIX/125-134.pdf.

[60] Hague Convention (XIII) on the Rights and Duties of Neutrals in Naval War 1907, 205 CTS 299, Arts 8, 9.

[61] *Tallinn Manual 2.0*, *supra* note 17, at 100, para. 19.

[62] Lemnitzer, *supra* note 42, at 161.

[63] Woolsey, 'Wireless Telegraphy in War', 14(5) *Yale Law Journal* (*YLJ*) (1905) 247, available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1762&context=ylj.

Conventions explicitly banned the erection of wireless broadcasting equipment for military purposes on neutral territory.[64]

Interestingly, it chose not to follow the state practice set by Argentina and Brazil to prevent the use of their public telegraph networks for military means. Instead, the Hague rules specify that states are not required to restrict the use of their commercial or state telegraph, telephone or wireless networks by belligerents if they are open to the public.[65] This rule is important because the drafters of the *Tallinn Manual* transferred it to cyberspace and created a distinction between non-commercial government information technology (IT) infrastructure and 'the Internet' when it comes to their use for military purposes.[66] The clear implication is that states have no monitoring duty to prevent the military use of any network infrastructure that is not under direct government control.

However, they only considered the codified law of 1907 when crafting these rules and ignored subsequent state practice. As Francis Colt de Wolf noted in the 1930s, 'during the last world war most neutral states adopted stringent regulations regarding electronic communications which went beyond the obligations assumed by them in the Hague convention'.[67] The danger of getting involved in disputes with belligerents led neutrals to act as if the due diligence rule required active monitoring of wireless broadcasting. In the USA, President Woodrow Wilson required all broadcasters to prevent military use of their installations and took direct control over stations capable of broadcasting across the Atlantic.[68] Every encoded message had to be sent through the government-manned stations Sayville and Tuckerton, with written copies provided to navy specialists.[69] This approach was mirrored by small nations far removed from the European battlefields – for example, Colombia decided in 1914 that its neutrality required it to take control of all radio stations, and eventually shut down a German-owned one to prevent the sending of secret messages.[70] The key concern here was that these radio stations might be used to direct naval vessels on the high seas to their targets, which would make the neutral state a base of military operations and expose it to recriminations by belligerents. In many cases (such as that of the Sayville station), concerns were compounded because the ultimate owners were leading German technology companies. Immediately after the sinking of the *Lusitania*, there were

[64] Hague Convention (XIII), *supra* note 60, Art. 5; Hague Convention (V), *supra* note 36, Art. 3.

[65] Hague Convention (V), *supra* note 36, Art. 8.

[66] This distinction was developed in the first version of the *Tallinn Manual* (M. Schmitt (ed.) Tallinn Manual on the International Law Applicable to Cyber Warfare (2013)), Rule 92, at 251, and copied verbatim into the *Tallinn Manual 2.0*, *supra* note 17, at 558, para. 3.

[67] De Wolf, 'Telecommunications and Neutrality', 30(1) *AJIL* (1936) 117, at 119.

[68] 'Executive Order of 5 August 1914 Regarding Unneutral Radio Messages', reprinted in *FRUS* (Supplement: The World War) (1914) 668; 'Executive Order of 5 September 1914 Regarding Government Control over High-Powered Radio Stations', reprinted in *FRUS* (Supplement: The World War) (1914) 678.

[69] 'Regulations Concerning Radio Stations', 7 November 1914, reprinted in *FRUS* (Supplement: The World War) (1914) 680.

[70] Rausch, 'Colombia's Neutrality during 1914–1918: An Overlooked Dimension of World War 1', 14(53) *Iberoamericana* (2014) 103, at 107, available at https://journals.iai.spk-berlin.de/index.php/iberoamericana/article/view/280.

suspicions that messages from Sayville had enabled the location of the ocean liner.[71] Radio amateur Charles Emory Apgar's recordings on a homebuilt device proved that secret messages were being sent each night, prompting the swift seizure of the station.[72] This highly publicized story brought the importance of monitoring wireless communications for protecting neutrality to the attention of a wide audience. After the war, a working group tasked with updating the laws of neutrality as part of the 1922 Washington Conference codified the duty that neutrals should prevent the transmission of information relating to military operations through radio stations on their territory, but, as we have seen, no new rule on neutrality created after 1907 has found universal recognition.[73]

So how does the existing 1907 law and subsequent state practice on radio monitoring relate to modern scenarios of cyber warfare? With respect to the Hague rule banning the erection of new broadcasting equipment on neutral territory, the *Tallinn Manual* acknowledges that applying the rule to newly erected cyber infrastructure is possible, but it does not elaborate further.[74] We could easily imagine a state or state-linked hacker group establishing a cloud server in a third state and using this infrastructure for cyber attacks against another state. The question, then, is whether the victim state could successfully argue that there were sufficient indications for the third state to conclude that this was not a normal commercial cloud server. It would certainly have a duty to swiftly shut down new malevolent infrastructure once notified.

As for the malevolent use of existing radio infrastructure, we can now see that the *Tallinn Manual*'s approach of simply copying the Hague Convention's distinction between public and closed communication infrastructure ignores relevant state practice from before and after World War I where states decided to pre-empt trouble by closing public communication infrastructure to belligerents or closely monitor their use. The recent case of the Rohingya people suing Facebook for £150 billion over its negligent failure to prevent its platform from being used to facilitate genocide in Myanmar shows that web-based services can have direct consequences on a battlefield.[75] The state where the company offering the service is registered might have a hard time in court explaining why ignoring its role in genocide or conflict abroad was appropriate or reasonable.

[71] 'Fear Wireless Trap Caught Lusitania: Close Scrutiny of All Messages at Two German Stations Called For', *New York Times* (10 May 1915), at 7.

[72] 'Plant under Suspicion: Officers Think German Station May Send Messages to Submarines', *New York Times* (1 July 1915), at 1–2; J. Reed Winkler, *Nexus: Strategic Communications and American Security in World War I* (2009), at 51–53.

[73] Hague Rules Concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, reprinted in 17 *AJIL* (1923) 242, Art. 3, 4, 5.

[74] *Tallinn Manual 2.0*, *supra* note 17, at 558.

[75] Milmo, 'Rohingya Sue Facebook for £150bn over Myanmar Genocide', *The Guardian* (6 December 2021), available at www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence.

C *The* Corfu Channel *Case*

Although the founding of the UN was supposed to have superseded the ancient institution of neutrality, the very first dispute that a gridlocked Security Council passed on to the new International Court of Justice (ICJ) was a dispute over military operations by neutrals at the fringes of a military conflict. The dispute emerged in the context of the Greek civil war in which the UK and Albania were formally neutral. However, the UK was the main supporter of the Greek government (until the USA took over that role in 1947), and Albania sympathized with the communist side.[76] When British cruisers passed through the Corfu Channel separating the Greek island of Corfu from the Albanian coastline in May 1946, Albanian shore batteries opened fire but without hitting a vessel. While Britain insisted that it had a right of innocent passage through the channel, Albania claimed that entering Albanian territorial waters without permission was a hostile act. In October 1946, a British flotilla passed through the channel again, but this time the destroyer *Saumarez* hit a mine and was heavily damaged, with 36 sailors killed. The destroyer *Volage* took her in tow only to hit another mine, with a further eight sailors killed. While the shore batteries remained silent, the mines had killed 44 people and injured 42, and the *Saumarez* was damaged beyond repair. Three weeks later, the Royal Navy conducted a mine-clearing operation in the channel without requesting Albanian permission, and the government formally complained to the UN about this incursion into its territory. The UK, on the other hand, demanded reparations from Albania and blamed it for laying the mines. Albania blamed Greece instead.

The UK brought a suit against Albania in May 1947, and the ICJ issued its first ever merits judgment in April 1949.[77] It supported the British argument that the vessels entering the channel in October 1946 were conducting an innocent passage through an international strait, clarifying the rules for such channels. However, it rejected the British claim that Albania had laid the mines and found no compelling evidence to decide who had done so. Instead, the judges developed a highly interesting due diligence argument: the channel formed part of Albanian territorial waters, and Albania was known to be on a heightened state of alert due to the military conflict in its vicinity. Therefore, the Court argued that it did need to determine who had laid the mines but found that Albania should have known that mine laying was going on and therefore had a duty to warn others of the danger. Although Albania withdrew from the proceedings at this point, the Court moved to the compensation stage and ultimately awarded £843,947 in compensation for the mine damage to the two vessels and the casualties caused. Thus, the ICJ used its interpretation of due diligence duties as the legal basis for a huge compensation payment and held Albania responsible for the damage and deaths caused, even though the Court agreed that there was no evidence that it had laid the mines. Therefore, cyber lawyers citing the judgment as the classic definition of the due diligence principle need to be aware that the ICJ laid down

[76] Constantinidis, 'The Corfu Channel Case in Perspective: The Factual and Political Background', 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* (2012) 41.

[77] *Corfu Channel*, *supra* note 11.

a much tougher duty to monitor state territory and warn others or be held responsible than states would currently accept for digital networks.

Applied to a cyber scenario, the *Corfu Channel* approach to due diligence means that a victim state of a cyber attack under certain conditions can sue a third state through whose network the attack was executed for compensation for a due diligence failure without ever attributing the cyber attack to a specific state or group. The conditions described by the ICJ amount to a 'should have known' standard composed of (i) geopolitical risk factors (in this case, the war in a neighbouring country); (ii) geographical proximity and government control (it happened in Albanian waters); and (iii) state capability (Albania could at least have detected, if perhaps not cleared, the mines). We will discuss below how this standard could be used to outline a due diligence monitoring duty for cyberspace.

5 The Future Due Diligence Regime in Cyberspace

As the previous section has shown, scholars only need to scratch the surface of the classic due diligence cases in neutrality law to find principles, approaches and dynamics that can be easily applied or transferred to a cyber context. Based on these historical precedents and current trends, this section attempts fill some of the gaps identified in the introduction. In trying to outline how the due diligence norm in cyber space is likely to develop, the guiding question is which practices are most likely to be considered to be something that a reasonable state would do and which practices should be considered due diligence duties that bind rich and poor states alike.

A *States Will Sue for Compensation for Due Diligence Failures Relating to Cyber Attacks*

Lawyers exploring the options of states facing a third state that is unwilling to fulfil its cyber due diligence obligations almost exclusively focus on the countermeasures available to compel them to put an end to an ongoing cyber attack routed through their networks.[78] Yet both the *Tallinn Manual 2.0* and the University of Exeter's *Cyber Law Toolkit* highlight the numerous legal conditions that countermeasures against a recalcitrant, non-cooperative third state must fulfil, even if it is clearly the source of a cyber attack committed by another state or non-state actor. Both sources agree that most countermeasures such as a hack back to take out the servers spreading or controlling the malware would be a violation of sovereignty.[79]

[78] *Tallinn Manual 2.0*, *supra* note 17, at 50, para. 28.

[79] *Ibid.*, at 130, para. 11; 139, para. 17 (only allowing an exemption for counter-hacking when critical infrastructure is under attack, at 138, para. 11). University of Exeter, *Cyber Law Toolkit*, scenario 6, available at https://cyberlaw.ccdcoe.org/wiki/Scenario_06:_Cyber_countermeasures_against_an_enabling_State. Nevertheless, scholars already warn that strengthening due diligence in cyberspace might lead to a 'proliferation of self-help', see Jensen and Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer', 95 *Texas Law Review* (2016–2017) 1555. Note that Jensen is more positive towards the idea of strengthened due diligence in his latest publication. See Jensen, *supra* note 20, at 268.

Yet it is striking that cyber lawyers rarely mention the one route that has been driving the development of due diligence standards for centuries: holding a state to account before an arbitration tribunal or court of law and demanding compensation.[80] States have used the compulsory dispute settlement or arbitration clauses in friendship treaties or multilateral treaties, special agreements and a variety of other means to establish a legal forum for their compensation claims.[81] Moreover, there is a clear line from the *Alabama* arbitration to recent ICJ decisions that omissions to act can be violations of due diligence duties.[82] The cases presented here show that the law does not need to be settled: all it takes is for the claimant to prove that the respondent acted unreasonably when being notified of a cyber incident involving its networks in order to win compensation for the damages caused. This means that there is no need to prove that the cyber attack crossed the threshold of an armed attack, and it neatly sidesteps the attribution problem. As the *Corfu Channel* case has shown, a victim state can win compensation for a due diligence failure even if the perpetrators of an attack remain forever shrouded in mystery.[83] Given the tremendous technical and political difficulties involved in legally attributing cyber attacks to a specific actor, this will be an important consideration for victim states.[84]

B *States Will Have to Prepare for Fulfilling Their Due Diligence Duties*

The drafters of the *Tallinn Manual 2.0* rejected any requirement for states to prepare for the exercise of their due diligence duties in cyberspace. Citing the ICJ's 2007 *Genocide* decision, they argue that a duty to prevent only arises once a state learns of a specific

[80] The one exception is Walton, 'Duties Owed: Low-intensity Cyberattacks and Liability for Transboundary Torts in International Law', 126 *YLJ* (2017) 1460, available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=5798&context=ylj.

[81] For example, Iran used a compulsory dispute settlement clause in a 1955 friendship treaty to launch a compensation claim against the USA in the *Oil Platforms Case (Iran v. United States)*, preliminary objections, 12 December 1996, ICJ Reports (1996) 803, at 821.

[82] See 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* (2012) 295, at 309–312 (who discusses the implications of the ICJ's *Genocide* decision).

[83] Heathcote, *supra* note 80, at 295. The point that due diligence duties of third states may be a way of getting around the attribution problem is also made by Jensen and Watts, *supra* note 79, but they only look at states using countermeasures for due diligence violations rather than the more likely route of compensation claims. There has even been a proposal to apply due diligence in cyberspace primarily as a standard of attribution. See Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', 67(3) *ICLQ* (2018) 643.

[84] Tsagourias and Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', 31 *EJIL* (2020) 941, available at https://doi.org/10.1093/ejil/chaa057; Egloff, 'Public Attribution of Cyber Intrusions', 6(1) *Journal of Cybersecurity* (2020), available at https://doi.org/10.1093/cybsec/tyaa012; Lindsay, 'Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack', 1(1) *Journal of Cybersecurity* (2015) 53, available at https://doi.org/10.1093/cybsec/tyv003.

act being committed.[85] Yet cyber attacks are vastly more common than attempts at genocide and are a known risk that every state can be affected by at any moment. For the *Tallinn Manual* drafters, this was a further argument against a duty to prevent – as it is impossible for any state to prevent all known cyber threats from materializing, defending against them should not be a due diligence duty.[86] Only if a specific part of a state's IT infrastructure has already been used for a cyber attack against another state, and there are concrete indications that the same vulnerability will be used again, will a duty to act be accepted since the threat is no longer 'purely speculative'.[87] This legal position on prevention not only promotes a dubious understanding of what might be a 'reasonable' or 'appropriate' state response to current cyber threats, but it also actively sets perverse incentives: as the *Tallinn Manual* acknowledges, even taking part in capacity-building exercises might have the effect of extending the scope of a state's due diligence duties since that scope is tied to a state's cyber capability.[88] In other words, this interpretation of due diligence puts a state doing nothing into a more favourable legal position than one that chooses to prepare for a well-known threat.[89]

However, states should also consider that the legal situation as a third state changes significantly in case of an armed conflict: the old rule allowing belligerents to take swift action against neutrals failing to stop the military use of their territory was transferred wholesale into both versions of the *Tallinn Manual*. Belligerents have the right to take any necessary measures in case a neutral state is unable to put an end to the use of its networks for hostile purposes, even if the neutral state applied its best efforts to end a cyber attack but was unsuccessful. The manual suggests that a hack back against servers located in neutral countries is a likely remedy.[90] Thus, according to the *Tallinn Manual*, states have no duty to prepare for responding to a cyber attack using their networks, but if a belligerent anywhere in the world abuses them for a cyber attack and the neutral state fails to stop it swiftly, the victim state is entitled to turn the neutral state's networks into a battlefield.

The argument that states have a due diligence duty but are not required to make any preparations for fulfilling it is inherently unsound and unlikely to be the dominant legal stance much longer.[91] Instead, states will seek to improve their cyber capabilities out of their own self-interest and will show increasingly less understanding for states that have chosen not to do so and then find themselves incapable of responding to a cyber attack exploiting their networks. Once recognized, a duty to prepare will most

[85] *Tallinn Manual 2.0*, *supra* note 17, at 44, para. 7. *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, ICJ Reports 2007, 43, at paras 430–432.

[86] *Ibid.*, at 44, para. 8.

[87] *Ibid.*, at 46, paras 14, 15.

[88] *Ibid.*, at 45, para. 10.

[89] This position is still supported by some states such as Australia or Ecuador. See Kastelic, *supra* note 10, at 9–10.

[90] *Tallinn Manual*, *supra* note 66, at 255; *Tallinn Manual 2.0*, *supra* note 17, at 561, para. 6.

[91] Note that a duty to prevent has already been endorsed by Canada, Chile, Croatia, Finland, France and the Group of Seven. See Kastelic, *supra* note 10, at 9.

likely require states to pass relevant legislation, build up incident response capabilities and embed themselves in networks that they can use to request additional state or private sector support.

1 States Must Have Passed Legislation Allowing Them to Act in Cyberspace

The lack of relevant legislation can cause problems as state organs trying to take quick action in the digital sphere must improvise to establish the legal foundations for their efforts or find themselves challenged by other constitutional organs. At the point of formal notification of a cyber attack being routed through a state's networks, it will most likely be unclear whether it is being committed by a private or state actor, so legal uncertainty whether and which crimes can be committed in the digital sphere can hold up a response even against a state actor. Victim states are highly unlikely to show great patience until these questions are resolved under national law.

According to the UN Conference on Trade and Development, 79 per cent of states have already enacted relevant legislation, and a recent report by the Council of Europe concludes that, as of March 2020, 92 per cent of UN member states had either enacted cybercrime legislation or had such efforts underway. Fast progress is being made in Africa, and 106 (or 55 per cent of) UN members had cybercrime legislation in place that the Council perceives to be 'broadly in line' with the standards of the 2001 Budapest Convention against Cybercrime.[92] While the *Tallinn Manual* rejects any duty to legislate, it nevertheless urges states to consider 'pass[ing] legislation empowering it to require Internet service providers to take down botnet command and control servers in the event such servers are set up on its territory'.[93] The way in which the judges of the *Alabama* tribunal swiftly dismissed the 'no national legislation' defence for due diligence duties more than 150 years ago should provide food for thought for those states that still have no relevant legislation to cover cyber attacks or cybercrime, especially given that the UN first called upon states to pass such legislation more than 20 years ago.[94]

2 States Must Have Incident Response Capabilities and Procedures in Place

The argument that states have no duty whatsoever to prepare for a known threat that might harm others using their territory is out of line with the historical development of due diligence duties. It is a duty to prevent harm, not only to respond to harm and mitigate it once it materializes. For example, states need not only to protect an embassy

[92] Budapest Convention against Cybercrime 2001, ETS N. 185, available at https://unctad.org/page/cybercrime-legislation-worldwide; Council of Europe, 'The Global State of Cybercrime Legislation 2013 –2020: A Cursory Overview', 20 March 2020, available at https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9. Buchan argues that a duty to legislate already exists and that the Budapest Convention should be the yardstick. Buchan, *supra* note 25, at 439; see also Kshetri, 'Cybercrime and Cybersecurity in Africa', 22(2) *Journal of Global Information Technology Management* (2019) 77.

[93] *Tallinn Manual 2.0*, *supra* note 17, at 49, para. 23.

[94] See GA Res. 55/63, 4 December 2000, para. 1(a).

once it comes under attack but also to take 'all appropriate steps' to ensure its protection.[95] States do not have to mirror the capabilities of the most advanced cyber powers or the leading private tech companies, but they should acquire affordable, readily available and effective means to protect their networks.

Today, even most developing countries such as Laos,[96] Papua New Guinea[97] and Uganda[98] have an official Cyber Emergency Response Team (CERT) that is embedded into the relevant global networks for information sharing and assistance.[99] Both international organizations and private cyber security companies engage in capacity-building activities: states wishing to set up a team or even a security operations centre will easily find detailed guidance or free training resources for their prospective staff members and team leaders.[100] For a very modest outlay, establishing a CERT will enable a country to adequately respond to all but the most sophisticated cyber threats. Yet there are still states that do not have a single skilled incident response team. As Enenu Okwori points out, due diligence duties apply to rich and developing countries alike, and all states should build the necessary capacities to respond to cyber threats, if necessary with support from others.[101] Recently, Guatemala became the first country to demand that all states should be required to have a CERT established and in regular exchange with the international CERT community.[102] The *Tallinn Manual* agrees that, if a duty to prepare were assumed to exist, then setting up a CERT team would be a very good idea.[103] Even today, a state lacking any incident response capability will struggle to argue that this is an 'appropriate' state of affairs once notified of cyber attacks emanating from its networks. At the very least, it will face firm demands by victim states to procure or allow outside assistance.

3 States Will Be Expected to Request or Allow Technological Support If They Are Incapable of Ending a Cyber Attack Using Their Networks

A further advantage of having a CERT in place is that it not only provides a state with sophisticated technological capabilities in incident response, but it also embeds it in a global network that can provide additional technological support through trusted channels. If the cyber attackers' activities in a state's network are too large in scale or

[95] Vienna Convention on Diplomatic Relations 1961, 500 UNTS 95, Art. 22(2).

[96] See their website at https://laocert.gov.la/Home for more information.

[97] See their website at www.pngcert.org.pg/ for more information.

[98] See their website at www.cert.ug/ for more information.

[99] The term 'computer emergency response team' has been in use since the 1980s; other comparable teams use different terms such as computer security incident response team (CSIRT). The Forum of Incident Response and Security Teams is the global association of CSIRTs. See their website at www.first.org/ for more information.

[100] A recent example is the guide 'How to Set up CSIRT and SOC', *European Union's Agency for Cybersecurity*, 10 December 2020, available at www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc.

[101] Okwori, 'The Obligation of Due Diligence and Cyber-Attacks: Bridging the Gap between Universal and Differential Approaches for States', *Ethiopian Yearbook of International Law* (2018) 205, at 235–236.

[102] See Hollis, 'Improving Transparency: International Law and State Cyber Operations', 5 March 2020, at 20, available at www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf.

[103] *Tallinn Manual 2.0*, *supra* note 17, at 10, para. 12.

too sophisticated to be dealt with in this way, the general duty to prevent harm emanating from one's territory would compel a state to make reasonable efforts to bring in further assistance.[104] This could mean hiring a private cyber security company or bringing in teams from a friendly state with more advanced cyber capabilities. Looking at their submissions for the UN OEWG's report, private cyber security companies are already preparing for this eventuality and demanding that a clear framework for incident response cooperation between public and private entities should be established in advance.[105] This is a sensible suggestion since a state that is facing a cyber intrusion beyond its own technological capabilities will also find managing and coordinating the private incident response to an acute crisis challenging.

The legal position becomes more complicated when the victim state demands access for its own teams or the attack abuses the most vulnerable and important networks of a third state to coordinate a cyber attack. At what point does an unwillingness to allow foreigners access to some of its most sensitive networks mean the violation of a due diligence duty towards another state, resulting in legal liability for some of the damages caused by the ongoing cyber attack? The 2015 UN GGE report acknowledges these tensions and says that states in this situation are entitled to 'due regard for sovereignty'.[106] Yet there is no guidance on how 'due regard' for state sovereignty is to be balanced with the victim state's right not to be harmed. At what point does demanding respect for sovereignty stop being reasonable if it undermines any efforts to expel the attackers from the networks? This question is important since it also marks the precise threshold when the victim state would be entitled to take legal steps of its own because the third state whose networks are being abused is unwilling to exercise its due diligence duty. The *Tallinn Manual* comes down on the side of sovereignty and rejects any duty to obtain outside assistance.[107] But can the requirement to find ways of ending an attack emanating from one's territory that causes serious harm in other states really be sidestepped completely with a simple reference to sovereignty? A court or tribunal might well discover the little reference in the *Tallinn Manual 2.0* stating that, if ending an attack using its networks is beyond a state's technical capabilities, hiring a private company might be a 'reasonably feasible' measure.[108] From there, it only requires a small logical leap to conclude that what could have easily been done should have been done in a specific case, and the refusal to do so marks a due diligence failure.

C *Network Monitoring as a Due Diligence Duty*

So far, the measures discussed refer to preparations that a state should take to be able to respond effectively if it is notified about a cyber attack emanating from networks

[104] See GGE, *supra* note 11, para. 30b.

[105] See, e.g., the submission by the cyber-security company Kaspersky. Private Sector Technical Perspective to Best Practice Implementation of 2015 UN GGE Norms, September 2020, available at https://front.un-arm.org/wp-content/uploads/2020/10/kaspersky-submission-to-oewg.pdf.

[106] UN GGE Report 2015, Doc. A/70/174 (2015), para. 13(h).

[107] *Tallinn Manual 2.0*, *supra* note 17, at 50, para 26.

[108] *Ibid.*, at 47, para. 17.

located in its territory. But, as we have seen in the case studies, due diligence as required by the laws of neutrality also includes certain monitoring duties. So will states have to actively monitor networks for cyber threats that might harm others as part of their due diligence duties in cyberspace? This article argues that, for certain networks and certain forms of cyber threats, this will indeed be the case. Today, this is not a position endorsed by a majority of states. For example, New Zealand recently affirmed that 'it is clear that states are not obliged to monitor all cyber activities on their territories or to prevent all malicious use of cyber infrastructure within their borders'.[109] For the drafters of the *Tallinn Manual*, this was not quite as clear, and there was a lively discussion whether the legal principle that 'a neutral Power is bound to exercise such surveillance as the means at its disposal allow' implied that network monitoring was expected if at all feasible. The phrase is found in the Hague rules relating to a state's 'ports or roadsteads or in its waters' as a direct codification from the *Alabama* decision, but it has also been used in near identical wording in texts such as the 1928 Inter-American Convention on Maritime Neutrality, the 1994 *San Remo Manual on Maritime War* and the 2009 *Berne Manual on Air and Missile Warfare*.[110] The majority rejected this idea and decided that there is no duty to acquire the necessary means to observe or monitor network data flows.[111]

Yet the drafters only considered the relatively permissive Hague rules on radio monitoring but ignored the subsequent state practice from 1914 onwards described in the second case study. The reason why states suddenly adopted a much more stringent interpretation of their neutral radio monitoring duties at the outbreak of World War I is that the Hague Conventions give extensive rights to belligerents to take swift and forceful action if a neutral country allows itself to become a base for enemy operations. Rather than relying on their ability to swiftly respond to any belligerent complaint, states decided it was safer to monitor for such threats proactively. Once developments in international relations force states to think seriously about the implications of the legal situation, then they are likely to stop relying on lenient codified rules and start monitoring their networks. But, unlike in 1914, just sending government agents into the offices of ISP providers will not be enough. Monitoring networks for intrusions and suspicious data packages requires sophisticated technology that must be set up in each network and then calibrated over several months. States might decide that it makes sense to build up this capability before it is urgently needed, even though

[109] Statement on the Application of International Law to State Activity in Cyberspace, 1 December 2020, available at https://www.mfat.govt.nz/en/media-and-resources/the-application-of-international-law-to-state-activity-in-cyberspace/.

[110] See Hague Convention (XIII), *supra* note 60, Art. 25; Inter-American Convention on Maritime Neutrality 1928, 135 L.N.T.S. 187, Articles 4b and 26, available at https://ihl-databases.icrc.org/ihl/INTRO/290; *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (1995), Art. 15; *Manual on International Law Applicable to Air and Missile Warfare*, 15 May 2009, Rule 170b, available at https://reliefweb.int/sites/reliefweb.int/files/resources/8B2E79FC145BFB3D492576E00021ED34-HPCR-may2009.pdf.

[111] *Tallinn Manual 2.0*, *supra* note 17, at 559, para. 5. Note that network monitoring is about detecting malware or suspicious network activity and is different from the content monitoring for harmful or illegal content that many countries legally require of social media providers.

according to the logic of the *Tallinn Manual* this will extend the scope of their due diligence duties in peace time. In addition, by introducing network monitoring, states can improve their own security: many government or private organizations already use network monitoring for their own protection to detect intrusions that might indicate a cyber attack, regardless of whether it is aimed at themselves or at others.

This leaves the question about which networks states should be required to monitor as part of their due diligence duty. The *Tallinn Manual* mentions submarine cables in this regard, but, given their enormous flows of largely encrypted data, this is unrealistic.[112] Likewise, we cannot expect any government to ensure intrusion monitoring of every privately owned network in the country. Instead, the logic developed in the *Corfu Channel* case regarding Albania's duty to monitor its coastal waters and warn others of dangers can be used to develop a parallel argument for cyberspace: by replacing the court's points on geographical proximity with different degrees of government responsibility for a network, it could be argued that state should have a due diligence duty to monitor at least their own IT infrastructure. The *Tallin Manual 2.0* goes surprisingly far in developing this precise argument by claiming that a 'State breaches its due diligence obligation if it is in fact unaware of the cyber operations in question, but objectively should have known that its territory was being used for the operation'.[113] In a second step, the manual notes that this is particularly relevant for government IT infrastructure.

Things are more complicated with the networks of critical infrastructure companies, which are running vital services but are privately owned and managed. There are specific cyber norms granting special protection to such networks, but since there is no universally recognized definition of the term 'critical infrastructure', each state is free to assign it to whatever industries it sees fit.[114] Therefore, a state's national legislation would be an appropriate starting point – for example, if a state has set up a centralized monitoring system for critical infrastructure (like Denmark is doing)[115] or if specific industries are covered by a monitoring system arranged by the state with a private provider (the IT security company BitSight claims that it is doing this for 20 per cent of the world's nations).[116] If such an arrangement is in place, the expectation under the due diligence norm would be that it is being used.[117]

[112] See Kraska, *supra* note 49.

[113] *Tallinn Manual 2.0*, *supra* note 17, at 41, paras 39, 40. This 'constructive knowledge' approach is supported by states such as Finland, the Netherlands, Norway, Romania and Switzerland. See Kastelic, *supra* note 10, at 13.

[114] UN GGE Report 2015, *supra* note 11, Norm 13(f), (g).

[115] For example, the Danish Centre for Cyber Security runs a sensor network intended to monitor dozens of public and private institutions deemed to be critically important. For more information on the sensor network and its legal foundations, see the website at https://cfcs.dk/da/om-os/netsikkerhedstjenesten/sensornetvarket/.

[116] See BitSight, 20% of the World's Countries Now Use BitSight to Protect National Security, 1 October 2020, available at https://www.bitsight.com/press-releases/20-percent-of-the-worlds-countries-now-use-bitsight-to-protect-national-security.

[117] Coco and de Souza Dias, *supra* note 31, 788.

Regarding the question about what kind of cyber attack we could expect these systems to detect, the *Tallinn Manual* correctly argues that it is unreasonable to expect a state's monitoring system to identify highly advanced, unknown malware (for example, fileless malware that only assembles itself in the victim's networks).[118] However, it accepts that such an assumption of knowledge might be 'more appropriate' if the malware in question is a known sample (for example, one that has been uploaded on VirusTotal, a widely used malware database).[119] Likewise, if parts of the monitored network start to connect to servers known to be used as command and control units for hacking groups and begin an observable intrusion into networks in a different country, a duty to warn should apply. Therefore, by combining *Corfu Channel*'s stricter due diligence standard, its 'should have known' approach and the *Tallinn Manual*'s technical observations, it is already possible to construct the outlines of a future network monitoring duty for government networks and critical infrastructure.

D *States Will Be Expected to Control the Export of Cyber Weapons*

As we have seen with the Belgian and Prussian arms traders in the Crimean war, the argument that selling arms across the world is just a private business activity has a long tradition. Indeed, some rarely cited provisions of the 1907 Hague Conventions still echo this view.[120] Yet it is not just historians studying the international arms trade in the late 19th century who have claimed that it was a contributing factor for the global arms race that preceded World War I.[121] Many states had come to the same conclusion, and when the efforts to control arms exports related to the League of Nations' work on global disarmament failed, they introduced their own measures. As historian Jonathan Grant writes, 'by the end of the 1930s, Belgium, Sweden, France, Britain, and the United States had established the peacetime licensing of arms exports as normal practice'.[122] Today, no private company will expect to export tanks or artillery without government interference.

Initially, the trade in exploits and hacking tools did not involve much government oversight and worked through middlemen connecting hackers and their customers, often intelligence agencies. Yet many countries that saw a private cyber-security industry emerge soon began to take a closer look. The Wassenaar Arrangement (a non-binding, but influential, arms control regime) has included surveillance software as a dual use good since 2013.[123] The arrangement is primarily a European regime, but

[118] *Tallinn Manual 2.0*, *supra* note 17, at 41.

[119] *Ibid.*, at 41, para. 40.

[120] See Hague Convention (IV), *supra* note 18, Art. 7.

[121] J.A. Grant, *Rulers, Guns, and Money: The Global Arms Trade in the Age of Imperialism* (2007).

[122] Grant, '"Merchants of Death": The International Traffic in Arms', *Origins: Current Events in Historical Perspective*, November 2012, https://origins.osu.edu/article/merchants-death-international-traffic-arms?language_content_entity=en; see also J.A. Grant, *Between Depression and Disarmament: The International Armaments Business, 1919–1939* (2018).

[123] Granick and Fiedler, 'Changes to Export Control Arrangement Apply to Computer Exploits and More', *Just Security*, 15 January 2014, available at www.justsecurity.org/5703/export-control-arrangement-apply-computer-exploits/.

the fact that countries like India and South Africa have formally joined in recent years highlights its potential to become the core of a universal set of rules on arms control.[124] Yet this is highly unlikely to take the form of a comprehensive arms control or anti-proliferation treaty for cyber weapons. First, there are tremendous legal and technical difficulties in providing definitions of controlled or banned versus permitted technologies in a field that is marked by a frantic pace of technological development. Second, the hacking tools developed by private security companies for penetration testing by their red teams would almost certainly end up being classified as cyber weapons. For countries with a significant private cyber-security industry such as the USA, this is an important concern.

To see the beginnings of an alternative route to norm development involving the due diligence principle, it is instructive to look at the case of the Israeli cyber-security industry. When this author asked the ministry of foreign affairs in May 2020 how Israel ensures that its large and highly capable cyber-security industry does not sell cyber weapons into conflict regions or to regimes that might abuse them, its answer highlighted Israel's associate status with the Wassenaar Arrangement and its own arms exports legislation, which also refers to the arrangement.[125] Once the French government asked essentially the same question in the wake of the NSO scandal in November 2021 (which involved the revelation that a French government minister had been spied on by NSO state clients and led to the NSO Group being put on a US sanctions list), the answer was very different. Israel promised urgent improvements of the sector's government oversight and began to review the granting of export licences for cyber-security companies.[126]

These export licenses are key features in the legal review of private cyber-security exports: it is no coincidence that Amnesty International has targeted them for years in Israeli courts.[127] When the Italian company Hacking Team responded to criticism about its dealings with Sudan by a UN panel exploring sanctions violations by arguing that its product was not controlled as a weapon and, therefore, outside the scope of the panel's inquiry, an embarrassed Italian government swiftly withdrew Hacking Team's general export licence.[128] Providing a meaningful supervision of private cyber-security companies and a reliable process for granting and, if necessary, revoking export licenses is highly likely to become a recognized due diligence duty for states.[129] For

[124] For the most recent information on which countries are engaging with the Wassenaar Arrangement, see their website at www.wassenaar.org/about-us/.

[125] Email communication to the author via the Israeli embassy in Denmark, 6 May 2020.

[126] See Beaumont and Oltermann, 'Israel to Examine Whether Spyware Export Rules Should Be Tightened', *The Guardian* (22 July 2021), available at www.theguardian.com/news/2021/jul/22/israel-examine-spyware-export-rules-should-be-tightened-nso-group-pegasus.

[127] See 'Israeli Court Dismisses Amnesty's Petition against Spyware Firm NSO', *Reuters* (13 July 2020), available at www.reuters.com/article/us-cyber-nso-group-amnesty/israeli-court-dismisses-amnestys-petition-against-spyware-firm-nso-idUSKCN24E1GP.

[128] See Currier and Marquis-Boire, 'A Detailed Look at Hacking Team's Emails About Its Repressive Clients', *The Intercept* (7 July 2015), available at https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/.

[129] Cordey and Kohler, *supra* note 3, at 58, argue there is a particularly strong case for this duty for permanently neutral countries.

example, the recent revision of the EU Dual-Use Regulation introduced new licensing rules for cyber-surveillance items, requiring businesses to conduct their own due diligence to demonstrate to member states that they are not intended to be used in ways that violate human rights or international humanitarian law.[130]

So far, the public debate has focused on the use of surveillance software against human rights activists or opposition politicians, but the world's largest tech companies have warned in rare unity that the military use of private hacking tools poses even greater risks. When the NSO Group was sued by WhatsApp for the hacking of US servers in a Californian court and tried to claim state immunity from prosecution because its usual clients were states, Microsoft, Google, Cisco and others filed a joint *amicus* letter to the appeals court.[131] Their main contention was that private cyber-security companies produce not only surveillance tools but also powerful cyber weapons for their hacking teams and customers, so awarding them state immunity posed grave risks to global cyber security. Instead, they argued, states must control their activities or face enormous proliferation risks.[132] Given the fast-moving nature of technology, the more flexible due diligence approach is clearly preferable to a cyber-weapons export control agreement that would require years of negotiations and complex oversight mechanisms. The standard suggested by the *Alabama* arbitration, which tied the supervision requirements to the potential risk posed by a private company's export activities, could provide a sensible yardstick. The dispute between the French and Israeli governments demonstrates how such confrontations can promote the development of due diligence rules and establish the principle that states having a private cyber-security industry are expected to provide meaningful oversight and control.

6 Conclusion

In conclusion, we have a problem with due diligence in cyberspace. States cannot agree whether the norm is a binding duty or what exactly the special due diligence regime for cyberspace that they are committed to building should require states to do. This lack of clarity regarding what behaviour states expect from each other in a crisis involving a cyber attack using a third state's networks poses evident escalation risks. After all, the due diligence duty is supposed to help states deal with major cyber attacks routed through unsuspecting third states that, once unleashed, can hit multiple organizations at the same time and disable critical infrastructure, while

[130] Council Regulation 2021/821, OJ 2021 L 206.

[131] Kirchgaessner, 'NSO Group Points Finger at State Clients in Whatsapp Spying Case', *The Guardian* (7 April 2020), available at www.theguardian.com/world/2020/apr/07/nso-group-points-finger-at-state-clients-in-whatsapp-spying-case.

[132] The letter of 21 December 2020 is available at https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v.-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf; see also DeSombre *et al.*, 'Countering Cyber Proliferation: Zeroing in on Access-as-a-Service', 1 March 2021, available at www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/.

politicians scramble to control the situation. We also know that state and non-state actors routinely use third state networks to hide their activity when conducting offensive cyber operations. It is only a matter of time until this constellation emerges in an international crisis, either as a stand-alone cyber attack or with cyber operations conducted as part of an armed conflict. Then, the lack of clear guidance about what states whose networks are used should do will compound a dangerous situation.

Clearer guidance could come from multiple sources, but they are all fraught with difficulties. With the cyber-norms process at the UN facing its own troubles and due diligence having been dropped from the OEWG's report as being too controversial, we cannot hope for a multilateral agreement to solve this issue. The transfer of legal principles and ideas from other successful due diligence regimes cannot solve the main problem that is unique to due diligence in cyberspace: what does a state have to do to prevent, detect, stop or mitigate an attack on another state using its ICT networks, most likely in a fast-moving crisis situation where the identity of the attackers remains unclear?

This article has argued that the laws of neutrality and the way in which due diligence has been used in this field in the last 150 years offer an almost perfect parallel, as the duties of neutral states to defend and monitor their territory have been defined ever more precisely and adapted to technological and political change. These are rules for the grey zone, with explosive disputes occurring at the fringes of a conflict but between states that are still at peace with each other. In fact, the main difficulty is the lack of familiarity with the classic cases of neutrality due diligence among modern international lawyers. Section 3 has shown how the failure of the legal edifice built to protect global trade and communication networks in the age of the World Wars led to the field's marginalization by the UN and the International Law Commission, but the case studies in section 4 have demonstrated that the use of a due diligence approach to clarify a state's monitoring and response duties in preventing the abuse of their territory by belligerents is highly effective. Moreover, these cases include highly relevant legal principles and approaches that can be used to develop the due diligence regime in cyberspace and create the necessary balance between flexibility and effectiveness.

The *Alabama* case introduced the due diligence duty into international law and was cited in the influential *Trail Smelter* decision of 1941 as the origin of its principle that states have 'a duty to protect other States against injurious acts by individuals from within its jurisdiction'.[133] For a cyber context, its most important principles are that (i) a lack of relevant national legislation is no legal defence for the failure to meet due diligence duties; (ii) states must monitor the arms export activities by private companies active on their territory; and (iii) states have a raised diligence duty if the technology poses a high risk of causing harm to others, especially in the wrong hands. Once being notified, a state must respond swiftly and effectively to prevent or mitigate harm to another or face being liable for compensation.

The *Corfu Channel* case points to a way for victim states to obtain compensation for due diligence failures without ever attributing the attack they suffered to a specific

[133] *Trail Smelter (United States v. Canada)* (1941), reprinted in UNRIAA, vol. 3, 1963, at 1965.

perpetrator. It also confirms that rich and poor states alike have a clear responsibility for what is happening on their territory, especially if there are reasons for heightened vigilance such as a nearby military conflict. The 'should have known' standard that was used to define Albania's due diligence failure can be applied to create the outlines of a duty for network monitoring of government networks or critical infrastructure. The case study looking at the military use of telegraph and radio networks in neutral countries shows that states tend to reinterpret their due diligence duties in much stricter ways if they fear becoming embroiled in a major military conflict. In other words, state practice in due diligence tends to be driven by international disputes and usually develops much faster than the codified rules, as was the case with radio monitoring.

By linking the lessons and principles from the precedents in the neutrality case studies to current debates regarding the legal and technical requirements for due diligence in cyberspace, section 5 has identified specific duties that are highly likely to become expected of third states (and, thus, binding in a legal sense) soon. Most importantly, states will come to accept a duty to prepare for meeting their due diligence duties in cyberspace as, otherwise, the norm will remain a hollow shell. This will involve duties to pass relevant legislation as well as to set up and maintain CERT teams and embed them in international cyber-security cooperation frameworks and to procure external assistance if necessary, but this list could and probably will be extended by the international community. All of these measures should be actively supported by cyber capacity-building programmes so that a lack of material wealth is no excuse for a state not to have them.

Funding will be a commonly raised objection for establishing network-monitoring solutions as a duty, but, at least for government networks, a strong case can be made already. The technology will also become more common in the protection of critical infrastructure for the simple reason that it helps protect these vital networks from cyber threats. At some point, the fact that it also allows states to stop or contain an attack against others conducted through their networks will be seen as an added bonus rather than as an onerous duty. Finally, those states having a cyber-security industry selling sophisticated intrusion and surveillance tools will be required to control it by establishing an export control and licensing system. Taken together, adopting these measures would enable every state to consider a binding due diligence duty in cyberspace with confidence.

Overall, international law is not as unprepared for cyberspace as some states seem to believe: after all, global telegraph networks and transatlantic radio messaging were common technologies a century ago. State practice and case law to support the development of due diligence in cyberspace exist, but international lawyers must act today to lay the necessary groundwork that will assist states in responding effectively and reliably in crisis situations. Fortunately, only a small number of the legal issues with due diligence in cyberspace are conceptually new and have no comparable precedents in international law, such as defining the outlines of responsible vulnerabilities management or the legal difficulties created by cyber attacks conducted through the

aggregation of a botnet spread out over dozens of jurisdictions.[134] For most others, we should look at the roots of the due diligence norm in international law and the state practice and precedents of neutrality law. Designed to manage escalation risk at the fringes of international conflict, they are our best guide through the grey zone of due diligence in cyberspace.

[134] The Group of Experts was split whether attacks by a botnet can be aggregated to trigger self-defence rights in the victim state, with the majority rejecting this view. See *Tallinn Manual 2.0*, *supra* note 17, at 38, paras 30–31. For an opposing view, see Patrick, 'Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations', 28 *Washington International Law Journal* (2019) 581, at 597.