Washington International Law Journal

Volume 28 | Number 2

4-1-2019

Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations

Colin Patrick

DEBUGGING THE TALLINN MANUAL 2.0'S APPLICATION OF THE DUE DILIGENCE PRINCIPLE TO CYBER OPERATIONS

Colin Patrick*

Abstract: As global cyber connectivity increases, so does opportunities for large-scale nefarious cyber operations. These novel circumstances have necessitated the application of old-world customs to an increasingly complex world. To meet this challenge, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations was created. The Manual provides 154 black letter rules detailing how international law applies to cyber operations during peacetime. Of particular import is the Manual's interpretation of the due diligence principle. This principle, which defines the contours of a state's obligation to prevent their territory to inflict extraterritorial harm, is increasingly significant in light of the above-mentioned increase in global network connectivity. It is with regards to this principal where the Manual's application is flawed. However, because of the principle's inherent flexibility, and the unique nature of the cyber risks, there are patches that are consistent with international law and would better serve global peace and security.

Cite as: Colin Patrick, *Debugging the Tallinn Manual 2.0's Application of the Due Diligence Principle to Cyber Operations*, 28 WASH. INT'L L.J. 581 (2019).

I. INTRODUCTION

Rapid development of the world's cyber infrastructure is bringing enormous change to the geopolitical order and requiring new applications of international customary law.[1] As global network connectivity increases, new pathways open up for transboundary interactions. But so do pathways for inflicting transboundary harm. States, terrorist organizations, hacktivists, and other actors are exploiting this risk, causing varying levels of damage from across the world.[2] One international custom aimed at reducing these harms is the due diligence principle—the "obligation of states to take measures to ensure their territories are not used to the detriment of other states."[3] However, the diffused nature of certain malicious cyber operations problematizes states' due diligence expectations and increases the likelihood and impact of

* J.D. Candidate at the University of Washington School of Law, Class of 2019. I want to express to my deepest thanks to Professor Melissa Durkee whose guidance and feedback was invaluable.

1 Riham Alkousaa, *German Companies See Threefold Rise in Cyber Attacks, Study Finds*, REUTERS (Oct. 5, 2017, 8:25 AM), https://www.reuters.com/article/us-cyber-attack-germany/german-companies-see-threefold-rise-in-cyber-attacks-study-finds-idUSKBN1CA1WX.

2 *Id.*

3 Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68, 69 (2015), http://www.yalelawjournal.org/forum/in-defense-of-due-diligence-in-cyberspace.

transboundary harms. Malicious operations, like the Mirai Botnet,[4] are often decentralized and utilize networks in numerous jurisdictions, creating a collective action problem that results in uncertainty over how the due diligence principle is applied to cyber operations. Uncertainty which manifests gaps for nefarious entities to exploit.

To stabilize state expectations, international law experts put forth their application of due diligence required by states to prevent harmful cyber operations.[5] Released in 2017, the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereafter, "The Manual") is the work of twenty international law experts to restate the application of international law to the realm of cyber operations.[6] While the first version of the Manual focused solely on applying the precepts of *jus in bello* and *jus ad bellum* to cyber operations, the second version gave particular attention to "fully develop[ing] the peacetime law of cyber operations."[7] This included an application of the due diligence principle to cyber operations.[8]

The Manual makes a strong case for why the due diligence principle is applicable to cyber operations, and why states should abide by its mandates. And the Manual's application of the principle has been lauded by scholars for its normative pronouncements.[9] However, as other scholars have stated, the Manual is just the beginning of a "long-term conversation" about due diligence in the world of cyber operations.[10] This work aims to add to that conversation.

Drawing from the abundance of different applications of the principle, this work argues that certain interpretations of how the principle applies may be counter-productive to maintaining international peace and security by underappreciating the threat of botnets and giving too much leeway to malicious states. Rather, because of the inherent uncertainty and variability of

---

[4] Nicky Woolf, *DDoS Attack that Disrupted Internet was Largest of its Kind in History, Experts Say*, THE GUARDIAN (Oct. 26, 2016, 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[5] TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 33, cmt. 21 (Michael N. Schmitt ed., Cambridge Univ. Press, 2017) [hereinafter, TALLINN MANUAL 2.0].

[6] *See id.* at 2.

[7] Schmitt, *supra* note 3, at 69.

[8] TALLINN MANUAL 2.0, *supra* note 5, at 30–50.

[9] Ian Yuying Liu, *The Due Diligence Doctrine Under Tallinn Manual 2.0*, 33 COMPUTER L. & SEC. REV. 390, 395 (2017) (praising the work of the experts as a "positive step led by scholars to delineate the framework of international law in cyberspace").

[10] Michael J. Adams, *A Warning About Tallinn 2.0… Whatever it Says*, LAWFARE BLOG (Jan. 4, 2017, 8:30 AM), https://www.lawfareblog.com/warning-about-tallinn-20-%E2%80%A6-whatever-it-says.

the cyber risks, different frames of analytical application are necessary. This paper provides those different frames and explains how they are consistent with the principal and international law.

Parts II & III provide an overview of due diligence, its development into custom, and its modern applications. Parts IV & V describe the Manual's application of the principle, detail flaws with the application, provide solutions to those flaws, and explain why those solutions are consistent with the tenets of the due diligence principle. Part VI concludes and identifies areas for future scholarship.

II. OVERVIEW OF THE DUE DILIGENCE PRINCIPLE

Due diligence is customary international law.[11] It requires that states take measures to prevent their territory from being used in activities meant to inflict extraterritorial harm.[12] Failure to take such measures may result in the state violating international law or even being found responsible for the harm, regardless of its relative intent in carrying out the precipitating act.[13] This responsibility for the harm may potentially expose a state to countermeasures.[14] Furthermore, if the harm rises to the level of an armed attack, it may justify a victim state's use of force against an offending state's territory.[15] Therefore, states have an incentive to be vigilant and minimize the risk of harm originating from their territory.[16]

Due diligence, while eminently flexible in application,[17] still contains two essential elements. First, responsibility for a harm only attaches if the state knew its territory was being used in activities to harm other states[18] and that harm crosses a severity threshold.[19] Second, if knowledge exists, a state

---

[11] *See, e.g.*, United States v. Arjona, 120 U.S. 479, 484 (1887); U.N. Secretary-General, *Survey of International Law in Relation to the Work of Codification of International Law Commission*, ¶ 57, U.N. Doc. A/CN.4/1/Rev.1 (Feb. 1, 1949).

[12] *See* Schmitt, *supra* note 3, at 69.

[13] *See* Robert P. Barnidge, Jr., *The Due Diligence Principle under International Law*, 8 INT'L COMMUNITY L. REV. 81, 91 (2006).

[14] *See* G.A. Res. 56/83, Responsibility of States for Internationally Wrongful Acts, at 11–12 (Jan. 28, 2002).

[15] *See id.* at 12.

[16] JOANNA KULESZA, DUE DILIGENCE IN INTERNATIONAL LAW 1 (2016).

[17] *See* 1 MAX PLANCK INST. FOR COMP. PUBLIC & INT'L L., ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 1114 (Rudolf Bernhardt ed., 1992).

[18] *See* F.V. García Amador, *State Responsibility*, U.N. Doc. A/CN.4/134 & ADD.1 (Jan. 26, 1961), http://legal.un.org/ilc/publications/yearbooks/english/ilc_1961_v2.pdf.

[19] TALLINN MANUAL 2.0, *supra* note 5, at 32, cmt 7.

must take all feasible measures to prevent the harm.[20] Keeping in line with the central conceit of due diligence, these elements inform one another and are applied flexibly based on the context.[21] International legal bodies consistently grapple with these issues and have produced extensive jurisprudence and writings to clarify states' obligations under the principle. Moreover, states take it upon themselves to define due diligence obligations in several situations.[22]

As noted above, flexible application is a defining characteristic of due diligence.[23] The various situations where due diligence applies evinces this fact. For example, international adjudicative bodies have found that due diligence may require a state to warn others of threats in their territory,[24] protect foreign nationals during insurrections,[25] or prevent transboundary environmental harm.[26] Likely because of this flexibility, due diligence is subject to a wide range of interpretation.[27] International adjudicative bodies apply the principle narrowly in some contexts, only requiring minimal measures to discharge the obligation.[28] Others interpret the principle expansively and expect significant efforts by states,[29] including precautionary duties.[30] Ultimately, and because of its malleability, the extent of a state's due diligence obligation will require a fact-specific determination.[31]

A state's due diligence obligations can also manifest through the precautionary principle.[32] In the context of environmental protection, traditional due diligence obligations were ineffective in preventing transboundary harm because those obligations only triggered if the harm was

---

[20] *See* Garcia Amador, *supra* note 18, at addendum.

[21] *See* ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 17, at 1114.

[22] *See* Convention on the Law of the Sea, 1833 U.N.T.S. 397 (Dec. 10, 1982).

[23] *See* ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 17, at 1114.

[24] Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 12 (Apr. 9).

[25] Youmans (U.S. v. Mex.), 4 R.I.A.A. 110, 112 (Gen. Claims Comm'n. 1926).

[26] Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963-65 (Arbitral Trib. 1941).

[27] Jonathan Bonnitcha & Robert McCorquodale, *The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights*, 28 EUR. J. OF INT'L L. 899, 900 (2017).

[28] *See* TIM STEPHENS & DUNCAN FRENCH, ILA STUDY GROUP ON DUE DILIGENCE IN INTERNATIONAL LAW SECOND REPORT 2 (2016).

[29] *See* Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the International Seabed Area, Case No. 17, Advisory Opinion of Feb. 1, 2011, ITLOS Rep. 1, ¶ 122 (noting adherence to precautionary principle is part of a state's due diligence obligation in this context).

[30] *See id.*; Trail Smelter, 3 R.I.A.A at 1963–65; Ling Chen, *Realizing the Precautionary Principle in Due Diligence*, 25 DALHOUSIE J. LEGAL STUD. 1, 4 (2016).

[31] ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW, *supra* note 17, at 1114.

[32] *See id.*; Trail Smelter, 3 R.I.A.A. at 1963-65; Chen, *supra* note 30, at 4

"reasonably foreseeable."[33] Since the nature of such harm was often unforeseeable, likely because of a lack of scientific evidence, a state would have no obligation to prevent harm that only later would be found severe.[34] To fill this gap in enforcement, a precautionary obligation emerged.[35] This obligation of prevention meant states must "ensure that activities within their jurisdiction do not harm an extraterritorial environment."[36] While a precautionary approach has usually been confined to environmental issues, its application has expanded to other contexts, specifically those that carry risks similar in certainty and scope to those in international environmental law,[37] including the European Union explicitly finding that due diligence obligations includes a more general protection against threats to human health.[38]

III. THE RISE AND REFINEMENT OF THE DUE DILIGENCE PRINCIPLE

Originally outlined by Dutch scholar Hugo Grotius in the seventeenth century,[39] the principle of due diligence entered international law in the nineteenth century.[40] Technological developments and increased global awareness brought the international community closer together,[41] increasing the possibility of both states and non-state actors inflicting transboundary damage.[42] This gave rise to expanded obligations on state conduct, including the due diligence principle.

From the tail end of the nineteenth century through World War II (WWII), states increasingly invoked the principle when seeking redress against one another.[43] Post-WWII, the space between states continued to decrease as the world experienced rapid technological, cultural, and geopolitical changes.[44] Unsurprisingly, states subsequently increased their

---

[33] *See* Chen, *supra* note 30, at 4.

[34] *Id*.

[35] *Id*.

[36] *Id*.

[37] *See* Arie Trouwborst, *Prevention, Precaution, Logic and Law: The Relationship between the Precautionary Principle and the Preventative Principle in International Law and Associated Questions*, 2 ERASMUS L. REV. 105, 115 (2009).

[38] *Communication from the Commission on the Precautionary Principle*, at 4, COM (2000) 1 final (Feb. 2, 2000).

[39] DUNCAN FRENCH & TIM STEPHENS, ILA STUDY GROUP ON DUE DILIGENCE IN INTERNATIONAL LAW FIRST REPORT 2 (2014).

[40] *See* Barnidge, *supra* note 13, at 92.

[41] *See* FRENCH & STEPHENS, *supra* note 39, at 2.

[42] *See id.*

[43] *See* Barnidge, *supra* note 13, at 92.

[44] *See id.*

due diligence claims against one another.[45] Several international instruments and legal decisions arose out these claims, producing an analytical framework of the principle's constitutive elements.

A. Scope of the Due Diligence Principle

Due diligence obligations only attach to a state when third-parties act within its territory to harm another state and that harm crosses a specific threshold.[46] Rephrased, a triggering actor and harm are required before any due diligence responsibility may attach. If either a triggering actor or harm is not present, then a state bears no due diligence obligation, even if it was aware of the harm.[47]

International law has steadfastly held that third-party state action satisfies the triggering actor condition.[48] Although at one time there was an unsettled question whether the same held true for non-state actors,[49] this question was answered affirmatively by the mid-twentieth century, and its development is traceable through a series of international arbitrations.

The *Alabama Claims Arbitration* arose from United States' claims against the United Kingdom for violating its promise of neutrality during the American Civil War when it allowed the Confederate Navy to construct warships within their ports.[50] To resolve these claims, the United States and the United Kingdom brokered the *Treaty of Washington*.[51] The *Treaty of Washington* established a tribunal to adjudicate the claims and set the public international law governing the proceedings.[52] Article VI of the treaty defined the due diligence obligation of a neutral state as rules meant to prevent its territory from being used to cause harm by belligerents.[53] The belligerent in question, while claiming to be a sovereign state, was an insurrectionary force

---

[45] *See id*.

[46] TALLINN MANUAL 2.0, *supra* note 5, at 32, cmt 7.

[47] *See id.*

[48] *See* Corfu Channel, 1949 I.C.J. at 20–23 (finding that even another state had laid the mines, Albania still bore a due diligence obligation to warn).

[49] *See* Barnidge, *supra* note 13, at 91–92.

[50] Tom Bingham, *The* Alabama *Claims Arbitration*, 54 INT'L & COMP. L.Q. 1, 2–9 (2005).

[51] *Id.* at 14.

[52] *Id.* at 15.

[53] *See* Bingham, *supra* note 50, at 15–16.

and not a state under international law.[54] Thus, when the Tribunal determined the United Kingdom failed to meet its due diligence obligations, it recognized that an entity other than a state could qualify as a triggering actor. [55]

The litigation on the issue of non-state actors continued, especially in cases involving a state's due diligence responsibility for actions of its nationals.[56] In *Youmans*, a tribunal found Mexico liable for harm done to an American by Mexican nationals during a mob uprising.[57] Whereas in *Sambiaggio*, a commission decided whether Venezuela could be liable for harm to an Italian national by insurrectionist revolutionaries.[58] The Commission ultimately agreed with Venezuela's defense that they lacked access to effective feasible measures to incur liability for the specific alleged harms.[59] However, the Tribunal did note that under other circumstances, a state may bear responsibility if it "failed to use promptly and with appropriate force its constituted authority" to prevent or end a harm.[60]

The well-known *Trail Smelter Arbitration* finally settled the question of non-state actor applicability. During WWII, smoke from a privately-owned smelter operating in Trail, British Columbia, caused extensive damage to forests and agricultural land across the U.S.-Canadian Border.[61] When farmers and landowners objected to the pollution, the United States decided to raise their claims with Canada.[62] To resolve these disputes and calm tensions, an arbitral tribunal was established.[63] Relying on scholarly works and cases from several domestic jurisdictions, the Tribunal determined that "under the principles of international law . . . no state has the right to use or permit the use of its territory in such a manner as to cause injury . . . to the territory of another."[64] Therefore, by holding Canada responsible for the pollution caused by the privately-owned smelter, the Tribunal explicitly held that under

---

[54] OFFICE OF THE HISTORIAN, *Preventing Diplomatic Recognition of the Confederacy, 1861–1865*, U.S. DEPT. OF STATE, https://web.archive.org/web/20130828005906/http://history.state.gov/milestones/1861-1865/Confederacy.

[55] Alabama Claims of the United States of America against Great Britain, 29 R.I.A.A. 125, 130–31 (1871).

[56] *See* Barnidge, *supra* note 13, at 95–98.

[57] *See id.* at 95–96

[58] *See id.* at 97.

[59] *Id.* at 97–98.

[60] *Id.* at 98.

[61] Trail Smelter, 3 R.I.A.A at 1915–16.

[62] *Id.* at 1912

[63] *Id.*

[64] *Id.* at 1963–65.

customary international law the due diligence principle is applicable to a state's responsibility for the actions of non-state actors within its territory.[65] As of today, there is no question that non-state actors may be a triggering actor and that several adjudicatory bodies have held states liable for failing to prevent non-state actors from causing harms.

Unlike the triggering actor condition, what constitutes a triggering harm is an amorphous standard and necessarily circumstance-specific.[66] Generally, actions resulting in "serious adverse consequences" will justify the principal,[67] while minimal injuries will not.[68] Noticeably however, there is a wide chasm between those two poles, especially considering "severe adverse consequences" is a "fairly high threshold."[69] This high standard is reasonable in situations where the harm's impact is reasonably foreseeable.[70]

Of course, there are myriad contexts where the degree of a harm, or even its existence, is unknown to the state. Thus to effectuate the purpose and intent of the principle, states expanded the concept of the triggering harm beyond just its foreseeable consequences and considered whether there is a risk of serious or irreversible damage from the uncertain harm.[71] This expansion was born out of a recognition that even though a harm's impact was uncertain, the risk of that harm, when reasonably foreseeable that it will occur, ought to trigger due diligence obligations.[72]

However, in certain circumstances, where a harm's impact is unknowable or imprecisely understood, but may be so severe or irreversible, it attaches due diligence obligations on a state even if the eventual totality of that harm would not otherwise trigger the principle.[73] Consequently, these harms attach their own form of obligation.[74] This distinction between harms

---

[65] *Id.* at 1965–66.

[66] *See id.* at 1963–65.

[67] *Id.* at 1965.

[68] *See id.* at 1963 (discussing the Federal Court of Switzerland's decision involving a shooting range near the border of two cantons).

[69] KULESZA, *supra* note 16, at 244.

[70] NICOLAS DE SADELEER, ENVIRONMENTAL PRINCIPLES: FROM POLITICAL SLOGANS TO LEGAL RULES 74–75 (2002).

[71] *See id.*; Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 151–52 (2001).

[72] Int'l Law Comm'n., *supra* note 71, at 152.

[73] Int'l Law Comm'n., *supra* note 71, at 155 (recognizing the flexibility inherent in the due diligence principle may require states take "abundant caution").

[74] *See* Trouwborst, *supra* note 37, at 116.

triggering preventative measures and those triggering precautionary ones is discussed later in this piece.

The scope of the due diligence principle, in terms of whose actions it covers, is broad and settled. Regardless of the actor, states are expected to conduct due diligence to ensure those actions do not harm other states. However, what can be a triggering harm is more often narrowly defined, and traditionally requires "serious adverse consequences" before responsibility attaches to the territorial state. Although, when the context involves unique harms, the flexibility of the principle may justify a lower threshold to uphold the purpose of due diligence.

B. The Knowledge Element

A state violates its due diligence obligations only if it has knowledge that its territory is being used for activities that harm other states.[75] However, international courts interpret this knowledge requirement broadly, finding either actual or constructive knowledge can constitute a state's awareness of harmful actions.[76] In 1949, the International Court of Justice (ICJ) decided the *Corfu Channel Case*. This case arose after British warships struck mines while passing through the Corfu Strait off the coast of Albania.[77] The British, after examining several mines pulled from the strait, believed Albania mined the strait prior to the warships passing.[78] Albania rejected this accusation, contending the mines "may have been floating mines, coming from old minefields in the vicinity, or magnetic ground mines, magnetic moored mines, or German GR mines."[79] After determining that the British passage was innocent, the ICJ held Albania liable for the damage done to the British ships.[80] While Albania's actual knowledge of the mines may have been in doubt, the totality of circumstances led the ICJ to find that Albania must have, or at least should have, known mines were laid in the strait.[81] Reasoning that a victim state may be incapable of establishing iron-clad proof of actual knowledge of the offending state, the majority opinion determined that the use of indirect facts and evidence, combined with the offending state's exclusive control of the territory, can be sufficient to satisfy the knowledge requirement

---

[75] *See* Amador, *supra* note 18, at addendum.
[76] Corfu Channel, 1949 I.C.J. at 20.
[77] *Id.* at 12.
[78] *Id.* at 13.
[79] *Id.*
[80] *Id.* at 22–23.
[81] *Id.* at 20.

of due diligence.[82] Consequently, due diligence obligations could attach if the state knew or should have known their territory was being used in activities to harm other states.[83]

C. The Feasible Measures Element

The feasible measures required from a state are dependent on both the nature of the harm and the ability of the state to combat it.[84] Weaker states may have access to fewer feasible measure than their stable and economically-powerful counterparts.[85] Moreover, whether the harm requires a preventative or precautionary approach informs what actions must be taken.[86] Ultimately, what feasible measures a state is required to perform is a context-driven analysis, specifically considering the capacity of a state and the specifics of the harm occurring. These concepts are explored in a set of ICJ decisions and scholarly works.

In the *Tehran Hostages Case*, the ICJ delineated between a state's negligence and lack of resources.[87] The ICJ determined Iran's failure to take "appropriate steps" to protect the United States embassy and staff was not due to lack of ability or access to appropriate means, but rather constituted negligence on behalf of the government because there were reasonable measures which could have been undertaken.[88] While finding Iran failed to take feasible measures, the *Tehran Hostages* judgment intimated that a lack of resources capable of addressing the specific harm may render a state unable to take feasible measures.

The *Paramilitary Activities* judgment confirmed this proposition. In that case, the ICJ found Nicaragua did not breach its due diligence obligation by failing to prevent the flow of arms into El Salvador.[89] The court noted "the geographical obstacles . . . and the intrinsic character of any clandestine arms traffic" indicated the arms trafficking could be "carried on successfully without any complicity from governmental authorities, and even when they

---

[82] *Id.* at 18.

[83] *See* Barnidge, *supra* note 13, at 105–06.

[84] FRENCH & STEPHENS, *supra* note 28, at 3.

[85] *Id.*

[86] *See* Trouwborst, *supra* note 37, at 116.

[87] United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), Judgment, 1980 I.C.J. Rep. 3, ¶ 63 (May 24).

[88] *See id.* at ¶ 63, 66.

[89] Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 157 (June 27).

seek to put a stop to it."[90] They reasoned that Nicaragua, a developing nation experiencing civil unrest, was not capable of carrying out measures to end the trafficking of arms through their territory.[91] Combined, these cases stand for the proposition that what is feasibly required from a state is determined by the capacity of that state to enact those measures within specific circumstances.

Beyond a state's capabilities, the measures they must take to discharge their due diligence obligations are dependent on the nature of the harm. As noted in the above section, triggering harms can be conceived as those necessitating prevention and those mandating precaution.[92] When the exact consequences of a harm are known, it triggers preventative measures.[93] Whereas if the consequences are uncertain, but potentially severe or irreversible, the measures required are classified as precautionary.[94] Professor Nicolas de Sadeleer identifies the key distinction between the two as the "degree of uncertainty surrounding the probability of risk,"[95] and notes that "the lower the margin of uncertainty, the greater the justification for intervention as a means of prevention rather than in the name of precaution. By contrast, precaution is used when scientific research has not yet reached a stage that allows the veil of uncertainty to be lifted."[96] While the concept of precaution originated in the international environmental law context, the underlying logic of threat uncertainty and its effect on state obligations is transferable to other contexts.[97] The question of uncertainty evolved away from one that is purely focused on scientifically ascertainable risks, such as pollution or overfishing, to one that focuses on the uncertainty of known risk whose contours are not easily ascertainable,[98] such as the effects of nuclear weapons testing[99] and dam building[100] on human health. Thus, in determining the extent and character of the measures required from the state, the certainty of a particularized risk is an essential part of the calculus.

When a state bears due diligence obligations, the nature of those obligations and the capacity of the state informs what measures are feasible

---

[90] *Id.*

[91] *See id.* at ¶ 157–58 (comparing the abilities of the Central American nation to that of the United States and concluding it is unreasonable to expect Nicaragua be able to know and deter the flow of arms.).

[92] *See* Trouwborst, *supra* note 37, at 116.

[93] *Id.*

[94] *Id.*

[95] DE SADELEER, *supra* note 70, at 74–75.

[96] *Id.*

[97] *See* Trouwborst, *supra* note 37, at 117.

[98] *Id.*

[99] Nuclear Weapons (N.Z. v. Fr.), Order, 1995 I.C.J. 288 (Sept. 22).

[100] Gabcikovo-Nagymoros (Hung. v. Slovk.), Judgment, 1997 I.C.J. 7 (Sept. 25).

and thus necessary. One must analyze the situation holistically to understand what should be required of a state.

IV. THE TALLINN MANUAL 2.0'S APPLICATION OF THE DUE DILIGENCE PRINCIPLE TO CYBER OPERATIONS

Due diligence came in the second iteration of the Manual. The first version of the Manual focused almost exclusively on the rules of war regarding cyber operations.[101] This left out several key peacetime rules for cyber operations, including the due diligence principle.[102]

Chapter Two of the Manual lays out the application of the due diligence principle to cyber operations. Consisting of two rules, this chapter explains why the due diligence principle applies to cyber operations, under what circumstances the principle applies, and the measures needed to discharge the obligations of the principle.[103]

A. Rule 6 of the Tallinn Manual 2.0

Rule 6 sets out the general principle for due diligence obligations over cyber operations.[104] It states that "[a] state must exercise due diligence in not allowing its territory . . . to be used for cyber operations that might affect the rights of, and produce serious adverse consequences for, other states."[105] The commentary to this rule notes the principle's application to cyber operations is *lex lata*.[106] The Manual found that, as the principle is custom, it applies to new contexts and technologies "absent a legal exclusion therefrom."[107] The Manual could not find such a legal exclusion, and therefore the principle applies to cyber operations.[108]

The commentary of Rule 6 details the principle's application to the cyber operations of non-state actors. Only cyber operations attributable to a state can violate another state's sovereignty or contravene the prohibition on

---

[101] Schmitt, *supra* note 3, at 70.

[102] *Id.*

[103] TALLINN MANUAL 2.0, *supra* note 5, at 30–50.

[104] *Id.* at 30.

[105] *Id.* (The rule also encompasses territory or cyber infrastructure under a state's control.).

[106] *Id.* at 31, cmt. 3–4 (acknowledging, but rejecting, a view that the due diligence is not customary international law).

[107] *Id.* at 31, cmt. 4.

[108] *Id.*

use of force[109] and such operations are only attributable to a state if they "result in serious adverse consequence and . . . affect a right of the target state."[110] If a non-state actor launched a cyber operation that violated the sovereignty of another state, to the level of serious adverse consequences, the territorial state would bear a due diligence obligation, regardless of whether the operation would be a *per se* violation of international law.[111]

Concerning the triggering harm, the Manual adopts the standard of "serious adverse consequences."[112] While recognizing the harm threshold is an open question, the Manual notes this standard was adopted by analogy from the "context of international environmental law."[113] The Manual declined to adopt the minority viewpoint that a lower harm threshold, such as "significant" or "substantial" adverse consequences, was appropriate.[114] Furthermore, the Manual rejected the idea that an aggregation of cyber incidents, such as those caused by Botnets, can constitute serious adverse consequences.[115] Thus, even if a state's territory is used as part of a larger attack that, in totality, would cross threshold of serious adverse consequences, no due diligence obligation will attach unless the amount of harm specifically attributable to a state is sufficient to cross that threshold.[116]

Beyond establishing the general scope of the principle, Rule 6 outlines the due diligence knowledge requirement for cyber operations. In line with *Corfu Channel*, the Manual states the Rule encompasses both actual and constructive knowledge.[117] The Manual does, however, recognize that advances in malware and other cyber capabilities may render proving constructive knowledge extremely difficult.[118] Regardless of this difficulty, the Manual states the constructive knowledge standard does not mandate any obligation to monitor the state's cyber infrastructure.[119] Instead, a state is only required to act as some hypothetical "reasonable state" based on the circumstances, and therefore constructive knowledge may be imputed to a

---

[109] *Id.* at 35, cmt. 20.
[110] *Id.* at 35, cmt. 21.
[111] *Id.* at 35–36, cmt. 21.
[112] *Id.* at 35, cmt. 21.
[113] *Id.* at 37, cmt. 25 (citing Trail Smelter, 3 R.I.A.A. at 1965.).
[114] *Id.*
[115] *Id.* at 38–39, cmt. 31.
[116] *Id.* at 38–39, cmts. 31, 32.
[117] *Id.* at 40–41, cmts. 37, 39.
[118] *Id.* at 41, cmt. 41.
[119] *Id.* at 41–42, cmts. 41, 42.

state only when, if under the circumstances, the state should have discovered the operation.[120]

In sum, Rule 6 of the Manual finds that there is no legal exclusion of the due diligence principle with regards to cyber operations and, as customary international law, is therefore applicable to this context. Borrowing from international environmental law, the Manual adopts sets a standard for the triggering harm and does not consider aggregation when calculating the extent of the harm attributable to a state. However, as discussed below, the Manual declined to adopt international environmental law's precautionary approach to threats. Finally, while the Manual recognizes the difficulty of establishing constructive knowledge, it does not modify the contours of the triggering harm with the respect to the certainty needed to attach obligations.

B. Rule 7 of the Tallinn Manual 2.0

Rule 7 lays out the feasible measures element of the principle. The Rule "requires a state to use all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other states."[121] Consistent with the reasoning in *Tehran Hostages* and *Paramilitary Activities*, the Manual recognizes that feasible measures are coextensive with the "readily available measures" of the territorial state.[122] Further, failure to take readily available measures encompasses both the failure to exhaust available measures and state inaction, such as ignoring an identified non-state actor cyber operation harming the sovereignty of another state.[123]

The Manual states that what constitutes readily available measures will differ based on the stage of the operation.[124] Specifically, the Manual distinguishes between cyber operations underway and those not yet launched. With regards to operations underway, the Manual is unequivocal. Once the territorial state has knowledge of the operation, it must "exhaust all feasible measures to terminate it."[125] Conversely, when dealing with an unlaunched attack, a state need only take feasible measures when they are reasonably sure

---

[120] *Id.* at 42, cmt. 42.
[121] *Id.* at 43.
[122] *Id.*, cmt. 1.
[123] *Id.*, cmt. 2.
[124] *Id.*, cmt. 1.
[125] *Id.*, cmt. 2.

that material steps have been taken to carry out the attack.[126] Accordingly, if a state is aware of an unlaunched attack, such as a plan to steal sensitive data, its obligations are focused on whether the attack is possible and imminent. However, if the attack is underway, its obligations shift to ending the attack. In either case, the attack must also rise to the triggering harm threshold outlined in Rule 6 before feasible measures are required.[127]

While the due diligence principle requires termination of known cyber operations, the Manual recognizes that states have significant discretion in how to terminate such operations.[128] For example, a state may choose to terminate the operation and apprehend those responsible, or inform the targeted state of the operation.[129] Either way, the state would have discharged its due diligence obligations.[130] However, the principle does recognize that the qualities of a state may affect its capacity to enact feasible measures. A weak state will assuredly have less capacity than a strong state.[131] Although, a weak state may be required to hire a private entity to terminate the operation.[132] Finally, the principle may allow a state to delay termination of an operation, if that delay would result in a more effective and definitive termination.[133]

Under the Manual's interpretation, states are never required to enact general preventative measures to discharge a due diligence obligation.[134] Following the reasoning employed in the *Nuclear Weapons* Advisory Opinion, the Manual determined states are not required to generally prevent cyber operations launched from their territory, but rather combat specific instances of such cyber operations.[135] As the Manual puts it, "the term 'prevent' in this context means 'stop.'"[136] Therefore, a state's due diligence obligations do not include any requirement to remove legal barriers on enacting feasible measures,[137] strengthen the security of its

[126] *Id.*, cmt. 3.
[127] *See id.* at 46, cmt. 12.
[128] *Id.* at 44, cmt. 6.
[129] *Id.*
[130] *Id.*
[131] *Id.* at 47, cmt. 16.
[132] *Id.*, cmt. 17.
[133] *Id.* at 47–48, cmt. 18.
[134] *Id.* at 44–45, cmt. 7.
[135] *Id.* at 45, cmt. 7.
[136] *Id.*
[137] *Id.* at 48, cmt. 21.

cyberinfrastructure,[138] or improve its knowledge capacity.[139] Even if a state is aware that its network is vulnerable to being conscripted by cyber threats or has been used by malicious entities in the past, unless there is a known threat, a state does not bear any due diligence obligations.

Further, the Manual, building from its rejection of general preventative measures, also rejects the idea that general precautionary measures, such as monitoring one's cyber infrastructure, may be mandated by the principle.[140] Oddly, the Manual characterizes this measure as preventative,[141] despite the measure having more in common with precautionary logic.[142] The Manual does state, however, that if a state monitors its cyber infrastructure for threats, it would "bear on whether it has knowledge of any cyber operations directed at another state within its territory."[143]

According to the Manual, what feasible measures are needed for a state to discharge its due diligence obligation is context dependent. The type and stage of the operation, the state's capacity, any exercise of discretion by the state, and other factors will determine the extent of a state's readily available measures. However, general preventative measures are not required as a state is only responsible for specific and perceivable cyber operations. This blanket rejection includes any general precautionary measures, including those that may reduce a state's uncertainty over the existence of a specific cyber operation.

V. FLAWS WITH THE TALLINN MANUAL 2.0'S APPLICATION OF THE DUE DILIGENCE PRINCIPLE TO NON-STATE ACTOR CYBER OPERATIONS

There are flaws with the application of the Manual which may threaten international peace and security. Two flaws are notable and the focus of this section. First, rejecting the theory of aggregation when determining the character of the triggering harm fails to cover Botnet operations. Second, the wholesale rejection of general precautionary measures as an obligation creates perverse incentives for states. These flaws, in tandem, deteriorate the principle's effectiveness and threaten global security. Fortunately, there are

---

[138] *Id*. at 44, cmt. 7.

[139] *Id*.

[140] *Id*. at 45, cmt. 10.

[141] *Id*.

[142] *See* Trouwborst, *supra* note 37, at 113–14 (identifying measures based on precautionary logic when they are "roughly correspond[ing] to erring on the safe side").

[143] TALLINN MANUAL 2.0, *supra* note 5, at 45, cmt. 10.

potential fixes to these flaws that are consistent with the *corpus* of due diligence jurisprudence.

A. Flaw One: Failure to Incorporate Aggregation when Calculating the Triggering Harm

The Manual declined to adopt the theory of aggregation when determining the character of the triggering harm.[144] Thus, even if a state's territory is used in committing an operation that, if aggregated, would create "severe adverse consequences," that state has not violated its due diligence obligations unless the impact attributable to its territory alone led to "severe adverse consequences."[145] While it is undoubtedly true that some attacks will cross the requisite triggering threshold without the need for aggregation,[146] this interpretation, as the Manual implicitly admits, would exclude any state responsibility for Botnet operations.[147]

A Botnet operation is when a malicious party takes control of Internet of Things (IoT) devices[148]—which can be anything from a washing machine to a lamp to a jet engine[149]—and uses them to launch large-scale Distributed Denial of Service (DDoS) attacks.[150] Botnet operations can originate from more than one state[151] and take over IoT devices in even more.[152] Thus, the use of Botnets diffuses the means of attack across a multitude of states, and thereby diffusing the individual responsibility of each states. As such, the harm attributable to any given state would likely not reach the high threshold of serious adverse consequences. With no responsibility attached, no obligations manifest.[153] This creates a situation where a targeted state is

---

[144] TALLINN MANUAL 2.0, *supra* note 5, at 38–39, cmt.31.

[145] *Id.*

[146] *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014, 6:30 AM), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

[147] *See* TALLINN MANUAL 2.0, *supra* note 5, at 38–39, cmt. 31.

[148] Neena Kapur, *The Rise of IoT Botnets*, AM. SECURITY PROJECT (Jan. 13, 2017), https://www.americansecurityproject.org/the-rise-of-iot-botnets/.

[149] Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#41fd11f11d09.

[150] Bernard Marr, *Botnets: The Dangerous Side of the Internet of Things*, FORBES (Mar. 7, 2017, 2:18 AM), https://www.forbes.com/sites/bernardmarr/2017/03/07/botnets-the-dangerous-side-effects-of-the-internet-of-things/#49e9c3b73304.

[151] *Id.*

[152] Mary-Ann Russon, *New DDoS Attack Technique Could Unleash Devastating Internet Meltdown Warns Experts*, YAHOO NEWS (Oct. 26, 2016), https://in.news.yahoo.com/ddos-attack-technique-could-unleash-120733762.html.

[153] *See* TALLINN MANUAL 2.0, *supra* note 5, at 37, cmt. 26.

subjected to enormous harm but possesses no peaceful means sufficient to redress its grievance. It either must endure the damage or resort to legally unjustifiable means. Both scenarios are untenable and threaten international peace and security.

This is not some metaphysical threat, but rather an impending catastrophe for the international community. During October 2016, the Mirai Botnet shutdown cyber infrastructure giant Dyn in what was likely the largest DDoS attack in history.[154] The attack caused millions in economic damage and violated the sovereignty of multiple states.[155] All the more worrisome is that the mastermind behind the Mirai malware was not the director of a state's cyber organ or a terrorist organization, but instead a group of college-aged kids trying to scam Minecraft servers.[156] This disturbing trend has continued with the Reaper botnet.[157] Building off Mirai, the Reaper operation has infected IoT devices around the world, and while it has yet to be used in any DDoS attacks, there are predictions that it could eclipse the scope and damage of the Mirai attack against Dyn.[158]

At the heart of the Botnet problems is a collective action issue.[159] States may believe protecting their cyber infrastructure against Botnets is the right thing to do,[160] but know that successful prevention requires collective action.[161] Therefore, states who act alone may suffer some negative externality and so would be otherwise unwilling to act without some assurance of reciprocity.[162]

---

[154] *See* Woolf, *supra* note 4.

[155] *Id.*

[156] Garrett M. Graff, *How a Dorm Room Minecraft Scam Brought Down the Internet*, WIRED (Dec. 13, 2017, 3:55 PM) https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

[157] Andy Greenberg, *The Reaper IoT Botnet Has Already Infected a Million Networks*, WIRED (Oct. 20, 2017, 5:45 PM) https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

[158] *Id.*

[159] *See* ROBERT H. SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND SECURITY 242 (2014).

[160] *See, e.g.*, THE SECRETARY OF COMM. & THE SECRETARY OF HOMELAND SECURITY: A REPORT TO THE PRESIDENT ON ENHANCING THE RESILIENCE INTERNET AND COMMUNICATIONS ECOSYSTEM AGAINST BOTNETS AND OTHER AUTOMATED, DISTRIBUTED THREATS 3 (2018), https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/05/30/enhancing-resilience-against-botnets--report-to-the-president/final/documents/eo_13800_botnet_report_-_finalv2.pdf; Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. (2017).

[161] THE SECRETARY OF COMM. & THE SECRETARY OF HOMELAND SECURITY, *supra* note 160, at 3.

[162] *Id.*

Aggregation resolves this problem. Under aggregation, a state would bear responsibility for the part of the triggering harm attributable to it.[163] Thus, responsibility and potential punishments for non-compliance are attached to each culpable state. This increases the incentives for states to act, and, in combination with the inherent benefit of Botnet prevention, may outweigh any negative externality associated with such an action. Furthermore, initial state action would function as the assurance of reciprocity needed by skeptical states.[164] This could portend cooperation amongst the states and lead to the collective solutions necessary for effective Botnet prevention.[165]

Admittedly, whether aggregation is consistent with due diligence is an open question. As noted earlier, there was a minority view among the experts that aggregation is appropriate.[166] They analogize that composite cyber operations, such as using Botnets, are sufficiently similar to composite armed attacks.[167] This is when a set of individual operations, if treated as composite, rises to the level of armed attack, and may be attributable to a single originator or multiple originators if they are acting in concert.[168] Admittedly, armed attacks require intent to harm by the originators,[169] and therefore the two concepts are not perfect analogs. However, the hallmarks of due diligence are flexibility and reasonableness,[170] and the failure of the principle to cover Botnet operations because of a rigid application seems eminently unreasonable.

In addition to the analogy to composite armed attacks, adopting aggregation is justified by the uncertainty of the harm created by Botnets. As discussed above, when a harm poses an uncertain risk that may incur severe or irreversible damage, the concept of what constitutes a triggering harm may be adjusted to meet that context.[171] With Botnets, uncertainty exists both in the extent of impact and the extent of the compromised IoT device network.

---

[163] TALLINN MANUAL 2.0, *supra* note 5, at 38, cmt. 30.

[164] *See* Morgan R. Frank et al., *Detecting Reciprocity at a Global Scale*, 4 SCI. ADV. 1, 4–5 (2018).

[165] *Id.*; SLOAN & WARNER, *supra* note 159, at 243 (arguing collective solutions are necessary to address the common problem of malware).

[166] TALLINN MANUAL 2.0, *supra* note 5, at 38, cmt. 30 (noting some acceptance amongst experts that the "accumulation of effects" theory, as applied in determining an armed attack, would be consistent under international law).

[167] *Id.*

[168] *Id.*

[169] Oil Platforms (Iran v. U.S.), Judgment, 2003 I.C.J. 161, ¶ 64 (Nov. 6).

[170] *See* MAX PLANCK INST. FOR COMP. PUBLIC & INT'L L., supra note 15, at 1114.

[171] *See* DE SADELEER, *supra* note 70, at 74–75; Int'l Law Comm'n., *supra* note 71, at 152, ¶ 4–5.

In several environmental contexts, such an abundance of uncertainty justifies a precautionary approach in conceptualizing the triggering harm.[172]

While this context is obviously not within the environmental gambit, the Manual's adoption by analogy of "severe adverse consequences" from international environmental law[173] provides further reasoning for adopting aggregation. By failing to adopt aggregation—which, as discussed above, is the precautionary approach in this context—the Manual selectively adopts "severe adverse consequences." This selective adoption is inconsistent with international environmental law because it would exclude the precautionary logic embedded in the constitution of that context's triggering harm.[174] Thus, adopting the triggering harm standard from international environmental harm not only legitimizes incorporating aggregation, but in fact, seems to demand it.

B. Flaw Two: Failure to Require Precautionary Knowledge Building Measures

The Manual contends preventative measures are not required under the principle.[175] This includes precautionary knowledge building measures, like monitoring and "other steps designed to alert authorities to misuse of cyber infrastructure located on the state's territory."[176] Furthermore, the Manual also recognizes that a state's knowledge, or constructive knowledge, of a harmful cyber operation in its territory may be impossible to prove if they lack capacity or the operation is highly complex.[177] However, the difficulty in determining constructive knowledge, combined with the lack of knowledge building measures, undermines the effectiveness of the principle. Malintent states could capitalize on this opening by implementing a policy of plausible deniability when it comes to cyber operations in their territory. Without an obligation of precautionary knowledge building measures, these states are free to exploit this loophole, fully aware that any alleged violations of their obligations are extraordinarily difficult to prove. And without some diplomatic framework, the harmed state is likely constrained to responses that

---

[172] *See, e.g.*, Request for Advisory Opinion Submitted to the Seabed Disputes Chamber, Case No. 17, Opinion of Feb. 1, 2011, 17 ITLOS Rep. 38, 40; Southern Blue Fin Tuna Cases (Nos. 3 & 4) (N.Z. v. Japan; Austl. v. Japan). Case Nos. 3 & 4, Order of Aug. 27, 1999, 3 & 4 ITLOS Rep. 280, 296.

[173] TALLINN MANUAL 2.0, *supra* note 5, at 37, cmt. 25.

[174] *See* Trouwborst, *supra* note 37, at 113–16.

[175] TALLINN MANUAL 2.0, *supra* note 5, at 44–45, cmt. 7.

[176] *Id.* at 42, cmt. 42.

[177] *Id.* at 41, cmt. 41.

escalate the situation and threaten global peace—such as retaliatory hacks or "hackbacks"[178]—or that are wholly insufficient because they cannot leverage an external source of pressure.[179]

An imposition of precautionary knowledge building measures rectifies this problem. By requiring states to undertake such measures, there are now opportunities for harmed states to hold accountable those states that either conducted the attack through a covert cyber organ or allowed a third-party to conduct the attack.[180] For example, if a state is harmed by a cyber operation it may allege that another state failed to perform the expected knowledge building measures to prevent its territory from being used in the operation. If the accused state cannot establish that it undertook those measures, then it has failed its due diligence obligations and the international legal system may be used to resolve the problem before it escalates. Moreover, if the accused state proclaims that they executed such measures, then the harmed state has much stronger argument for constructive knowledge. Even the Manual implies that when a state undertakes knowledge building measures it is more likely to be found to have constructive knowledge of harmful operations.[181] Therefore, under either scenario, a malicious state is no longer capable of exploiting a due diligence obligation gap that allows its territory to be a launch pad for cyber operations.

Requiring knowledge building measures is consistent with the object and purpose of the due diligence principle. The flexibility inherent in due diligence allows for the imposition of precautionary duties if the context requires.[182] A prime example is the precautionary principle in international environmental law. Environmental harms are often as uncertain as they are severe.[183] Therefore, not obligating states to adopt a risk averse stance could

---

[178] Benjamin Jenson, Brandon Valeriano, & Ryan C. Maness, *Cyberwarfare has taken a New Turn. Yes, it's time to Worry*, WASH. POST (July 13, 2017) https://www.washingtonpost.com/news/monkey-cage/wp/2017/07/13/cyber-warfare-has-taken-a-new-turn-yes-its-time-to-worry/.

[179] Jenna McLaughlin, *NSA Official says US Doesn't have 'Political Fortitude' to challenge Russia in Cyberspace*, CNN (Apr. 9, 2018, 2:46 PM), https://www.cnn.com/2018/04/09/politics/nsa-laing-russia-cyberspace/index.html.

[180] WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY, 115th Cong. 1–2 (2017) (report of Daniel R. Coats, Director of National Intelligence) (detailing the list and type of cyber threats).

[181] TALLINN MANUAL 2.0, *supra* note 5, at 45, cmt. 10.

[182] *See* Trouwborst, *supra* note 37, at 113–16.

[183] *See* U.N. Conference on Environment and Development, *Rio Declaration on Environment and Development*, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. I), annex I (Aug. 12, 1992) (describing the nature of the harms covered by the precautionary principle).

result in irreversible damage.[184] Adherence to the precautionary principle is thus necessary to make a state's environmental due diligence responsibilities meaningful.[185] As such, there is precedent for requiring precautionary measures as part of a state's due diligence obligations when the failure to do so could reasonably defeat the object and purpose of the principle.

Furthermore, the way the triggering harm should be understood strengthens the case of a knowledge building expectation. Under aggregation, a state bears responsibility for the portion of a qualifying cyber operation attributable to it.[186] However, unless knowledge is also attributable to the state, it likely will not incur any obligations.[187] Therefore, without knowledge building measures, even under a theory of aggregation, a state may avoid any due diligence obligations.

Precautionary measures are likely necessary to ensure states cannot shirk their due diligence responsibilities with impunity when it suits them. Specifically, the lack of precautionary knowledge building expectations allows states to maintain plausible deniability in perpetuity without repercussions. Certainly, this would defeat the object and purpose of the due diligence principle. Moreover, precautionary knowledge building measures are necessary to ensure that severe or irreversible harms are put in check.

Undoubtedly, a state's capacity will dictate the extent of the required precautionary measures. Both the strength of the state and its commitments to internet privacy may constrain what feasible measures are readily available. If a state lacks the technical expertise, or the ability to acquire it, to conduct precautionary measures, then it may have a legitimate reason for having no due diligence obligations. However, with the rapid growth of global technological acumen, the larger concern is how states with commitments to internet privacy are able to balance that interest with the need for precautionary measures. No doubt the context will be determinative, but there are some avenues already available to states. States are free to inspect their government-run and critical cyber infrastructure systems for malware. By scanning their own systems, states can, at the very least, get an idea of whether their IoT devices, and thus potentially others, are being used in a Botnet

[184] *See id.*
[185] Chen, *supra* note 30, at 3.
[186] TALLINN MANUAL 2.0, *supra* note 5, at 38, cmt. 30.
[187] *See id.* at 37, cmt. 26.

operation. This idea has already been discussed by the United States.[188] Furthermore, software industry groups have offered up a number of possible approaches to improve knowledge building precautionary measures that aim to balance privacy with the need for secure cyber infrastructure.[189] As such, there are opportunities for states to cooperate with private business, which would allow them to carry out knowledge building measures in a way that does not run afoul of their internet privacy commitments. Ultimately, a state's capability to perform knowledge building measures may be difficult to ascertain, but that cannot be a reason to avoid expecting such an obligation in the first place.

Either of the above flaws may render any due diligence principle for cyber operations ineffective in maintaining international peace and security. Further, if the principle is ineffectual, then states may not implement it in practice, which vitiates any benefits the principle could accrue.[190] By modifying the principle in the ways explained above, due diligence obligations can be effective in preserving global order while being consistent with international law.

VI. CONCLUSION AND NEXT STEPS

The Manual's interpretation of the due diligence principle is a great opening salvo to what must be a long-term conversation about state responsibility in the cyber world. However, there are flaws in the Manual's interpretation of due diligence that could open the door to threats to global stability. Fortunately, any "bugs" in the Manual's application can be fixed. Through the adoption of aggregation and precautionary knowledge building measures, the due diligence principle for cyber operations would be an indispensable tool in maintaining international peace and security.

Moving forward with this research requires an examination of state practices to see how states are responding to the scenarios at the core of the problems with the Manual's application. The litany of Botnet attacks and other malicious cyber operations are creating a bevy of state actions. Delving

---

[188] Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. (2017-2018).

[189] Letter from Tommy Ross, Senior Director, The Software Alliance, to Evelyn Remaley, Deputy Associate Admin., Nat'l Telecomm. and Info. Admin., regarding Promoting Stakeholder Action Against Botnets and Other Automated Threats 2–4 (July 28, 2017).

[190] *See* David P. Filder, *Cyberspace, Terrorism and International Law*, 21 J. CONFLICT & SECURITY L. 475–78 (2016) (arguing international law has failed to check cyber operations causing state to fail to implement international instruments to prevent the problem).

into that will be essential in determining the full extent of the due diligence principle for cyber operations.