THE FUTURE OF DUE DILIGENCE IN CYBERSPACE

YIRONG SUN*

I. INTRODUCTION

Empowered by technical innovations, malicious cyber operations by non-state actors are becoming more effective in achieving their goals and more difficult for states to detect and mitigate. The concept of due diligence has thus become a promising tool in international law for imposing upon states positive duties to prevent, halt, and/or redress online harms.[1] In July 2021, the United Nations Group of Governmental Experts (UN GGE) Report reaffirmed that the due diligence principle is applicable in cyberspace, meaning "[s]tates should not knowingly allow their territory to be used for internationally wrongful acts using ICTs [informational and communications technologies]."[2] The 2021 official compendium of voluntary national contributions (the 2021 compendium), which are comments by states on the Report, add to the understanding of how it applies.[3]

Unlike other norms in the UN GGE report that primarily regulate state behavior, the due diligence principle aims to

* LL.M. candidate in International Legal Studies, New York University School of Law; LL.B., 2021, Tsinghua University. I am grateful to Maria Ciacci for her significant assistance. Additional thanks to Professor Angelina Fisher and Professor Thomas Streinz for instructing me about the role of infrastructure in regulation in the 2021 Global Data Law class, and to Professor Xinjun Zhang for his teachings and scholarship in state responsibility. Any and all errors are my own.

1. Antonio Coco & Talita de Souza Dias, *Cyber Due Diligence: A Patchwork of Protective Obligations in International Law*, 20 EUR. J. INT'L L. 1, 2 (2021).

2. Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of Int'l Sec., U.N. Doc. A/76/135, at 10 (July 14, 2021) [hereinafter GGE Report].

3. Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of Int'l Sec. Established Pursuant to General Assembly Resolution 73/266, at 26, 48–49, 59, 71–72, 76, U.N. Doc. A/76/136, (July 13, 2021) [hereinafter Compendium].

regulate the conduct of non-state actors.[4] Its success depends on states' control over individual acts.[5] This comment considers the applicability of due diligence in cyberspace. Section II introduces the mechanism of due diligence in the traditional context and examines the current understanding of its application in cyberspace. Section III explores how the technical attributes of cyber operations affect the applicability of due diligence and discusses the potential benefits of establishing cyber due diligence.

II. Due Diligence in Cyberspace

A. *The Mechanism of Due Diligence: A Two-Step Process*

Due diligence is a standard of conduct measuring whether a state has employed reasonable diligence to address certain harm by non-state actors.[6] It consists of a two-step process. First, states have a general duty of vigilance as a corollary of their territorial sovereignty or as a result of their overwhelming control over areas abroad.[7] It is noteworthy that the existence of a general duty of vigilance itself does not necessarily lead to a duty to act upon any specific non-state actors' activities within this area. Second, when states, through vigilance, know or should have known of harmful activities, the general duty of vigilance transforms into a specific duty to act, namely taking reasonable steps to prevent, halt, and/or redress.[8]

---

4. *But cf.* Tallinn Manuel 2.0 on the International Law Applicable to Cyber Operations 32 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter Tallinn Manual 2.0] (stating that due diligence "applies to any third party cyber operation, irrespective of whether it is carried out by a private person, corporation, non-State group, or State").

5. Int'l L. Ass'n, *Second Report of the ILA Study Group on Due Diligence in International Law*, at 12 (July 2016).

6. Antonio Coco & Talita de Souza Dias, *Due Diligence and COVID-19: States' Duties to Prevent and Halt the Coronavirus Outbreak*, EJIL:Talk! (March 24, 2020) https://www.ejiltalk.org/part-i-due-diligence-and-covid-19-states-duties-to-prevent-and-halt-the-coronavirus-outbreak/.

7. *See e.g.*, Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), Judgment, 2005 I.C.J. 168, ¶ 179 (Dec. 19) (attributing responsibility to Uganda for human rights and international humanitarian law violations in Ituri on the basis of Uganda's control as an occupying power).

8. *See* Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro),

Due diligence does not have a common standard of conduct in general,[9] and is by nature flexible.[10] The substance of the vigilance duty is usually determined by the threshold of *de facto* control exercised by a state towards the territory in question.[11] And in practice, the extent of vigilance is a prime indicator to prove a state's knowledge (usually constructive).[12] Therefore, the concept of due diligence depends on a state's control,[13] which has critical implications in assessing the applicability of due diligence in cyberspace and will be further discussed in Section III.

B. *Current Approaches of Applying Due Diligence in Cyberspace*

The 2021 UN GGE Report's norm 13(c) does not provide much insight into how due diligence applies in cyberspace. It merely replicates the *Corfu Channel* definition, i.e., "obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[14] In its commentary to norm 13(c), the term "territory" is mentioned seven times with no explanation on how "territory" will function in cyberspace.[15] Its last paragraph—"[a]n ICT incident emanating from the territory or the infrastructure of a third State"—might allude to the infrastructure approach in the *Tallinn Manuel*,[16] where the International Group of Experts (IGE) try to mirror the

---

Judgment, 2007 I.C.J. 222, ¶ 431 (Feb. 26) (holding that a state's obligation to act appears when the state learns of or should have normally learned of the severe risk of genocide).

9. Int'l L. Ass'n, First Report of the ILA Study Group on Due Diligence in International Law 31–32 (2014).

10. Tallinn Manuel 2.0, *supra* note 4, at 39.

11. Dem. Rep. Congo v. Uganda, 2005 I.C.J. ¶¶ 300–304 (holding that the Congo's central government had almost no control in the area in question due to its remote and mountainous geographic features, and thus, the Congo had no obligation to act).

12. Corfu Channel Case (Gt. Brit. & N. Ir. v. Alb.), Judgment, 1949 I.C.J. 4, 58, at 66 (Apr. 9) (dissenting opinion by Badawi, J.).

13. *See* Tallinn Manuel 2.0, *supra* note 4, at 33.

14. Corfu Channel Case, 1949 I.C.J. at 22.

15. GGE Report, *supra* note 2, at 10.

16. The Tallinn Manuel defines cyber infrastructure as "the communications, storage, and computing resources upon which information systems operate." Tallinn Manuel on the International Law Application to Cyber Warfare 15 (Michael N. Schmitt ed., 2012) [hereinafter Tallinn Manual 1.0].

physical world in cyberspace by regulating cyber infrastructures.[17]

In the 2021 compendium, nine out of fifteen states made comments about how due diligence shall apply in cyberspace. Except for the United States and the United Kingdom,[18] they all agreed upon the nature of cyber due diligence as a custom or general principle, meaning it imposes an obligation on states regardless of their adherence to a formal treaty.[19] The scope of application in the traditional context is activities in areas under the state's control (i.e., activities plus territory/extra-territory). However, in the cyberspace context, the state comments take various approaches regarding the scope of application. I categorize them into the following groups:

Territory

1. Infrastructure: Norway took a pure infrastructure approach and extended the traditional understanding of territorial sovereignty to cyber infrastructures by stating that "[a]s a consequence of the right to exercise sovereignty over cyber infrastructure located on its territory, [s]tates also have a corresponding obligation . . . ."[20]

2. Actor: Instead of infrastructure, Japan focused on the actors, i.e., "a person or group of persons located in its territory."[21]

3. Activity: Estonia alluded to activities on one's territory as a critical element by saying, "[w]ithout this obligation, international law would leave injured states defenseless in the face of malicious cyber activity that emanates from other states' territories."[22]

4. Mixed: Germany's description was "cyber activities, persons engaging therein as well as cyber infrastructures in the terri-

17. *Id.* at 26.

18. Compendium, *supra* note 3, at 117, 141.

19. Still, due diligence in cyberspace has not achieved *lex lata* status. TALLINN MANUEL 2.0, *supra* note 4, at 31; *see also* Eric Talbot Jensen, *Due Diligence in Cyber Activities*, *in* DUE DILIGENCE IN THE INTERNATIONAL LEGAL ORDER 252, 258 (Heike Krieger et al. eds., 2020). *But cf.*, Coco & Dias, *supra* note 1, at 8–13.

20. Compendium, *supra* note 3, at 71.

21. *Id.* at 48–49.

22. *Id.* at 26.

tory of a [s]tate,"[23] which seems to include activities, actors, and infrastructures. The Netherlands took a similar approach.[24] Notably, Tallinn Manuel 2.0 also takes the mixed approach: a state has a due diligence obligation vis-à-vis both cyber infrastructure and activities therein,[25] but does not mention actors in its territory.

Extra-territory

Norway, Japan, Estonia, and Germany did not mention the extraterritorial application of due diligence in their submissions. The states that accept extraterritorial application, i.e., Romania, the Netherlands, and Switzerland, all took the activity approach, but they differ on the extent of "extra-territory."

In Tallinn Manuel 2.0, the International Group of Experts (IGE) contends that due diligence extends extraterritorially in two cases: (i) territory abroad controlled by the state (through annexation or military occupation); (ii) cyber infrastructure controlled by the state. Romania[26] and the Netherlands[27] took the same approach as the IGE, while Switzerland only accepted the first scenario.[28]

III. Assessing the Applicability of Due Diligence in Cyberspace

The core function of due diligence is the allocation of risk posed by non-state actors.[29] Such distribution is initially based on territorial sovereignty,[30] which aligns with the classical understanding that with states' exclusive rights comes a duty to protect the rights of other states within their respective territo-

23. *Id.* at 33.

24. *Id.* at 59.

25. Tallinn Manuel 2.0, *supra* note 4, at 33.

26. Compendium, *supra* note 3, at 76.

27. *Id.* at 59.

28. *Id.* at 91.

29. Federica Violi, *The Function of the Triad 'Territory', 'Jurisdiction', and 'Control' in Due Diligence Obligations*, *in* Due Diligence in the International Legal Order 75, 76 (Heike Krieger et al. eds., 2020).

30. Maria L. Banda, *Regime Congruence: Rethinking the Scope of State Responsibility for Transboundary Environmental Harm*, 103 Minn. L. Rev. 1879, 1941 (2019).

ries.[31] The transboundary harm jurisprudence extends the scope of application from "territory" to a more flexible concept—"jurisdiction or control."[32] The Inter-American Court of Human Rights (IACHR) observed that the state is presumed to have "effective control" over the activities that happened in the area under their jurisdiction or control.[33] The rationale behind due diligence thus slightly shifts from an implied duty of exclusive territorial rights into a reasonable allocation of risk between states based on "proximity."[34]

This understanding is essential in determining whether and how to apply the due diligence principle in cyberspace. The ideas of "territory," "jurisdiction," and "control" are imperative in non-state actor governance. But their application in cyberspace is still under ongoing debate.[35] In the following parts, I will introduce two distinct technical attributes of cyberspace that complicates the applicability of due diligence by disturbing the function of "territory," "jurisdiction," and "control": separability and convert communication.

---

31. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 839 (Perm. Ct. Arb. 1928).

32. *See, e.g.*, U.N. Conference on the Human Environment, *Stockholm Declaration on the Human Environment*, Principle 21, U.N. Doc. A/CONF.48/14/Rev.1 (June 5–16, 1972) (stating that states have a responsibility with respect to activities "within their jurisdiction or control"); *see also* U.N. Conference on Environment and Development, *Rio Declaration on Environment and Development*, Principle 2, U.N. Doc. A/CONF.151/26/Rev.1 (Vol. 1) (Aug. 12, 1992) (declaring states' responsibilities over activities within their "jurisdiction"); United Nations Framework Convention on Climate Change, May 9, 1992, 1771 U.N.T.S. 107 (referring to states' responsibilities over activities within their "jurisdiction").

33. Environment and Human Rights (State Obligations in Relation to the Environment in the Context of the Protection and Guarantee of the Rights to Life and to Personal Integrity: Interpretation and Scope of Article 4(1) and 5(1) in Relation to Articles 1(2) and 2 of the American Convention on Human Rights), Advisory Opinion OC-23/17, Inter-Am. Ct. H.R. (ser. A) No. 23, ¶ 102 (Nov. 15, 2017).

34. Violi, *supra* note 29, at 76.

35. *See, e.g.*, Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention* 8 (Chatham House, Research Paper, Dec. 2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/2-application-sovereignty-cyberspace.

A. *Separability*

The UN GGE and the IGE approaches both focus on the physical location of either cyber infrastructure or activities. Nonetheless, territory may not serve as the best tool to divide between nations the "cyberspace" through which human activities are conducted. The global interconnectedness of cyberspace breaks the physical constraints of territorial boundaries.[36] The ICTs have a multi-layer structure and enable the separation of the geographical location of cyber infrastructure and cyber activities.[37] Although states retain jurisdiction and control over their territory, the jurisdiction over a physical infrastructure does not necessarily lead to their jurisdiction over cyber activities.

The separability creates a complicated jurisdiction issue. As exemplified by the globalized data centers providing cloud service, most cyber activities are conducted with data stored or computed extraterritorially. In 2018, the *Microsoft Ireland* case before the Second Circuit Court in the United States raised the issue of whether a U.S. warrant can reach emails and other communications content run by a U.S. company but stored in an overseas data server.[38]

Technologies not only can separate storage and access into two known geographical locations, but can also enable the distributive storage into multiple locations around the globe without the users' control. Early in 2017, the *Google Pennsylvania* case before the Eastern District of Pennsylvania presented the issue of whether the government could access a local company's information distributed in its global net-

---

36. Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207, 207 (2017).

37. Roxana Vatanparast, *The Infrastructures of the Global Data Economy: Undersea Cables and International Law*, 61 HARV. INT'L L. J. FRONTIERS (2020), https://harvardilj.org/wp-content/uploads/sites/15/Vatanparast-PDF-format.pdf.

38. *In re* Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014), *rev'd*, 829 F.3d 197 (2d Cir. 2016) (the Second Circuit refused to grant the warrant under the Stored Communications Act, while the Supreme Court ultimately declared that the enactment of the CLOUD Act would obligate Microsoft to give the government that information due to the CLOUD Act's extraterritorial reach).

work.[39] Google contended that it currently has no capability to determine the location of data because its algorithm takes a dynamic approach by distributing data to domestic and international servers to achieve operational efficiencies.[40] The Eastern District of Pennsylvania observed that "Google user data . . . is not stored as one single, cohesive digital file; instead, Google stores individual data files in multiple data shards, each separate shard being stored in different locations around the world."[41]

The above example illustrates the separability problem in the context when cyberspace is used to conduct malicious activities in the physical world, e.g., terrorism correspondence. A pure cyber-attack can make the situation worse. Take hackers using botnet malware as an example.[42] In a recent distributed denial of service (DDoS) attack, "[t]he attacks traffic originated from more than 20,000 bots in 125 countries around the world."[43] No centralized infrastructure is required to conduct a DDoS attack. The concept of a centralized ICT infrastructure for states to exercise control over is even further from reality in this situation than the data center example. Therefore, jurisdiction over the physical server does not equal effective control over activities mentioned by the IACHR. Thus, it is unreasonable to let states shoulder due diligence obligations over cyber activities emanating from or through infrastructures in their territory if states cannot even ensure access to the data in question.

B. *Covert Communication*

The covert nature of certain ICTs allows non-state actors to circumvent state supervision, while the function of due dili-

---

39. *In re* Search Warrant No. 16-960-M-01, 232 F. Supp. 3d 708 (E.D. Pa. 2017).

40. *Id.* at 712–713.

41. *Id.* at 724.

42. "Botnet" means a network of private computers each of which is infected with malware and is remotely controlled as a group by a hacker (or Botmaster).

43. Jonathan Greig, *Cloudflare Says It Stopped the Largest DDoS Attack ever Reported*, ZDNET (Aug. 27, 2021), https://www.zdnet.com/article/cloudflare-says-it-stopped-the-largest-ddos-attack-ever-reported/.

gence highly relies upon the state's ability to control.[44] For example, the increasingly prominent end-to-end encryption (E2EE) used by platforms and operating systems renders the communication only available and readable to particular users. The design of E2EE is aimed at achieving greater cyber security and user privacy protection, but the flip side is that illegal activities are also more insulated from law enforcement agencies. The paradigmatic case occurred following the 2015 terrorist attack in California, when Apple refused to help the Federal Bureau of Investigation unlock the perpetrators' encrypted iPhones.[45]

One solution is to regulate covert communication by its design, which falls within each state's prescriptive jurisdiction. Some states adopt strict regulation by requiring licenses,[46] requiring telecommunication companies to retain copies of user content,[47] creating a centralized networking system,[48] etc. However, such laws face strong pushback in the human rights area, as evidenced by a 2015 report of the U.N. Special Rapporteur on the right to freedom of opinion and expression: "[s]tates should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows."[49]

---

44. *See* Corfu Channel Case, 1949 I.C.J., at 44 (separate opinion by Alvarez, J.) (stating the vigilance duty varies with the means of a state); *see also* Dem. Rep. Congo v. Uganda, 2005 I.C.J., ¶ 179 (assigning responsibility due to control).

45. *In re* Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

46. *E.g.*, Federal'nyi Zakon ot 8 avgusta 2001 g. No. 128-FZ o Licenzirovanii Otdel'nyh Vidov Dejatel'nosti [Federal Law No. 128-FZ of August 8, 2001 on Licensing Specific Types of Activity], Sobranie Zakonodatel'stva Rossiiskoi Federatsii [SZ RF] [Russian Federation Collection of Legislation] 2001, No. 128-FZ.

47. *E.g.*, *Russia: 'Big Brother' Law Harms Security, Rights*, HUM. RTS. WATCH (July 12, 2016), https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights.

48. *E.g.*, Joint Statement on Russia's "Sovereign Internet Bill," HUM. RTS. WATCH (Apr. 24, 2019), https://www.hrw.org/news/2019/04/24/joint-statement-russias-sovereign-internet-bill#.

49. David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, at 20, U.N. Doc. A/HRC/29/32 (2015).

Furthermore, sometimes states have no power to regulate the design when the construction of new infrastructure unavoidably depends on the existing one. A prominent example is coronavirus contact-tracing apps. The development of apps relies upon the application programming interface (API) provided by operating systems. In 2020, the British government tried to develop a contact-tracing app in a centralized way so the government could know who tested positive and where he or she went.[50] But Google and Apple disagreed and only provided API for decentralized solutions,[51] where the aforementioned personal information would be inaccessible. Because of the indispensable reliance on prior infrastructure (in this case, the API), the British government finally gave up and accepted the decentralized model. This example underscores the difficulty of regulating infrastructure by design when the pre-existing infrastructure's impact is dominant.

C. *Is Cyber Due Diligence Still Promising?*

Despite the difficulties mentioned above, many still advocate for cyber due diligence. One of the alleged benefits is to fill the gap in the case of states using non-state actors as proxies.[52] Through the rule of attribution, state A has to prove the activity in question is attributable to (usually this means proving it is under the effective control of) state B,[53] whereas through due diligence, state A only needs to prove state B has actual or constructive knowledge of the activity to hold state B responsible. Such a complementary role of due diligence is alluded to by the IGE in its commentary as well.[54] Due diligence is also described to potentially simplify the attribution issue when facing anonymizing and rerouting techniques such as

---

50. Luciano Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, 33 PHIL. & TECH. 369, 369 (2020).

51. Michael Veale, *Sovereignty, Privacy and Contact Tracing Protocols*, *in* DATA JUSTICE AND COVID-19: GLOBAL PERSPECTIVES 34, 37 (Linnet Taylor et al eds., 2020) ("[D]ecentralized apps only transmit information upon diagnosis that an individual's device emitted.").

52. Nori Katagiri, *Why International law and Norms Do Little in Preventing Non-State Cyber Attacks*, 7 J. CYBERSECURITY 1, 4 (2021).

53. Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 47–49 (2001).

54. TALLINN MANUEL 2.0, *supra* note 4, at 42.

virtual private networks and other international protocol spoofing software.[55]

However, to prove constructive knowledge is not necessarily easier than to prove attribution, as acknowledged by the IGE itself.[56] Besides, there are discussions among states and academics about the feasibility of creating an international mechanism to tackle the attribution of state-sponsored cyber operations.[57] Considering the collateral impact on non-proxy actors and corresponding diligence shouldered by states, the application of due diligence to include non-state actors acting as proxies for states is not as beneficial as it looks.

Another potential benefit is that due diligence may incentivize[58] or even obligate[59] states to take feasible measures to prevent their territory from being used to conduct malicious cyber operations. Under due diligence, states will set up a minimal national legal framework tackling the misuse of ICTs. And for those that do not, violation of the due diligence principle opens the door of legitimate countermeasures towards the territorial state.

Nevertheless, the incentivization might be moot, and states have equal possibility to be counter incentivized. To trigger the duty to act upon a specific malicious activity, the territorial state must have actual or constructive knowledge of it. The extent of vigilance determines the knowledge. In other words, a state with a more comprehensive preventive system is more likely to know the existence of such cyber operations, and therefore, the state will shoulder a greater obligation to police cyberspace and bear a higher risk of being attacked by the victim state through legitimate countermeasures.

Moreover, the flexible due diligence standard of conduct leaves little guidance for states on how to conduct mitigating operations. For example, to mitigate a DDoS attack, "an unspecified number of devices can be investigated and innocent

55. Coco & Dias, *supra* note 1, at 2.

56. TALLINN MANUEL 2.0, *supra* note 4, at 40.

57. Moynihan, *supra* note 35, at 4.

58. Michael Schmitt, *Three International Law Rules for Responding Effectively to Hostile Cyber Operations*, JUST SEC. (July 13, 2021), https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/.

59. Coco & Dias, *supra* note 1, at 18.

users may be impacted,"[60] which exemplifies the tension between international security and human rights protection. But no answer can be found in due diligence due to its flexible and case-by-case nature. Thus, due diligence becomes an empty promise to secure better cyberspace.

IV. Conclusion

Despite the UN GGE report and some states' and academia's continuing faith, due diligence may not be an appropriate tool to govern non-state actors' behavior in cyberspace. Because separability and covert communication of cyber operations weaken the link between cyberspace and the physical world, they render the concept of "territory or jurisdiction" insufficient for presuming control. Meanwhile, cyber due diligence hardly brings benefits either by filling the gaps of attribution or by incentivizing states to take feasible measures in advance.

Indeed, projecting the due diligence principle in the physical world to cyberspace limits the legal imagination to govern non-state actors. Unlike transboundary harm, where the source of harm can only be handled by the territorial state, the mitigating operation in cyberspace does not need to be conducted in the territorial state where the attack emanates. Therefore, instead of using due diligence as a gap-filler, it is more reasonable to create a more adaptive framework of attribution and alleviation of potential legal risks for victim states to self-help.

---

60. Policy Department C: Citizens' Rights and Constitutional Affairs, European Parliament, *Legal Framework for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* 24 (2017), https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf.