Ordine internazionale e diritti umani
International Legal Order and Human Rights
Ordenamiento Jurìdico Internacional y Derechos Humanos
Ordre Juridique International et Droits de l'Homme
Diretta da Claudio Zanghì, Lina Panella, Carlo Curti Gialdino
EDITORIALE SCIENTIFICA

TERESA CATALANO*

THE APPLICABILITY OF DUE DILIGENCE IN CYBERSPACE: REFLECTIONS FROM AN INTERNATIONAL LAW PERSPECTIVE**

SUMMARY: 1. The Role of Due Diligence in International Law and Cyberspace. - 2. Due Diligence in Cyberspace under International Jurisprudence - 3. The Application of Due Diligence to Cyber Activities. - 4. Conclusions and Outstanding Challenges.

1. *The Role of Due Diligence in International Law and Cyberspace*

Due diligence, as an obligation of conduct on the part of a subject of law, emerged in international law ever since its early developments. Its expansion has impacted various branches of international law and has quickly evolved into different manifestations, including the cyberspace in which is particularly relevant the nature of this principle and its applicability. More specifically, this article seeks to assess whether the principles of due diligence developed in international law should be understood as a non-binding expectation of voluntary State conduct in cyberspace, or alternatively as a binding legal obligation, the breach of which entails consequences under customary international law on State responsibility and, furthermore, if the principle is directly applicable with its specifies *sic et simpliciter* to cyberspace, or whether its application requires specific adaptations and adjustments. This also requires an examination, conducted in the course of the paragraphs, of whether the concept of due diligence, as applied in cyberspace, exhibits distinct and autonomous characteristics from those of international law.

To address this issue, it is first necessary to consider that although the advancement of information and communications technologies has conferred substantial benefits, their increasing exploitation for malicious purposes constitutes a significant challenge to the international legal rights and obligations of States. Such developments risk undermining

* Assegnista di ricerca in diritto internazionale, Università degli Studi di Bari Aldo Moro.
** This paper is part of a project that has received funding from the European Union's Horizon Europe Research and Innovation programme under grant agreement N°101168309.

international peace and security, while simultaneously heightening the potential for inter-State conflict.[1]

In order to strengthen the application of international law in the cyber era and, consequently, to cooperatively «reduce risks to international peace, security and stability», in 2015 the United Nations General Assembly endorsed the recommendations of the Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which provide guidance to States in their use of ICTs within international relations.[2]

Considering that the applicability of international law in cyberspace has been expressly recognized in the Disarmament Agenda of the United Nations Secretary-General, while the consensus report of the 2021 of GGE has provided a further layer of clarification and interpretative guidance, the issue, however, lies in determining the scope of application of the concept of due diligence.

In the panorama of international law, in the Alabama Claims Arbitration case,[3] the tribunal set to solve the dispute between Great Britain and the US elaborated the notion of due diligence in relation to the duties of neutrality incumbent upon a non-belligerent State[4]. The dispute concerned a series of claims for damages brought by the United States against the Great Britain for the attacks upon 68 ships of the Union by the Confederate cruiser Alabama, disguised as a merchant vessel and built in Britain. Following the end of the Civil War, the United States alleged that Britain had breached its neutrality obligations in maritime warfare. From the perspective advanced by the United State «a neutral State should have used active diligence, proportional to the risk and possible consequences of negligent conduct»; in contrast, Great Britain asserted that compliance with due diligence could be achieved by «such care that governments ordinarily employ in their domestic concern and may reasonably be expected to exert in matters of international interests and obligations».

The Tribunal adopted the definition proposed by the US and concluded that the standard of due diligence requires a neutral government to act in the exact proportion to the risks to which belligerents may be exposed from a failure to fulfil obligations of neutrality. Claims commissions and arbitral tribunals established in the 19th and early 20th century to determine compensation owed by States for injuries sustained by their nationals abroad, frequently relied on the concept of due diligence as the 'international standard of justice' to be evaluated against State's conduct.[5]

It is important to underline that the definitional clarification in the international context is useful for proceeding, in the next paragraph, to an examination of the main

---

[1] A. KASTELIC, *Due diligence in cyberspace, Normative expectations of reciprocal protection of international legal rights*, United Nation Institute for Disarmament Research, November 2021.

[2] See *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: note by the Secretary-General, 22 July* 2015, seventieth session, available on /digitallibrary.un.org/record/799853?v=pdf.

[3] *Alabama Claims Arbitration (United States of America v. United Kingdom)*, Final Award of 15 September 1872, in *Reports of International Arbitral Awards*, Vol. XXIX, pp.125-134.

[4] See C. BROWER II, *Alabama Arbitration*, in R. WOLFRUM (ed.), *Max Planck Encyclopedia Public International Law,* 2012; B. DE FUMICHON, W.W. PARK, *Retour sur L'Affaire de L'Alabama*, 2019*, Rev de l'Arbitrage*; J. PAULSSON, *The Alabama Arbitration: Statecraft and Stagecraft'* in U. FRANKE, A. MAGNUSSON, J. DAHLQUIST (eds.), *Arbitrating for Peace: How Arbitration Made a Difference,* 7, 2016.

[5] The International Law Commission's commentary on Article 3 of the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities refers to the *Alabama* case saying *«The required degree of care is proportional to the degree of hazard involved […]. The higher the degree of inadmissible harm, the greater would be the duty of care required to prevent it».*

international jurisprudence and of how the principles established therein are effectively applied to cyberspace, of which some can be traced to the Corfu Channel case.

2. *Due Diligence in Cyberspace under International Jurisprudence*

In the Corfu Channel case[6] the International Court of Justice (ICJ) emphasized that Albania's obligations included notifying the existence of the minefield in its waters and alerting the British warships to the imminent danger. According to the ICJ, these duties stem from "well-recognized principles" of international law, particularly the principle that every State is obliged not to knowingly allow its territory to be used for acts infringing the rights of other States. While the Court did not explicitly employ the term due diligence, it clarified that the exercise of sovereignty entails positive responsibilities to manage a State's territory in a manner that prevents harm to other States.[7]

In detail, the dispute concerned alleged violations by Albania of its duties as a neutral State, most notably its failure to provide notification of the existence of a minefield within its territorial waters.[8] In 1946, the explosion of a naval mine severely damaged four British warships while they were navigating a channel previously swept for mines in the North Corfu Strait. As the incident occurred in Albanian territorial waters, the United Kingdom held the Albanian Government responsible for the resulting damage and loss of life.

Although the ICJ found insufficient evidence to attribute the laying of the mines directly to Albania, it concluded that, given the measures taken and the vigilance exercised by the Albanian authorities over the Corfu Channel in the days preceding the incident, Albania must have had knowledge of the presence of the mines. In this regard, in cyberspace, the principle of due diligence indicates that a State whose territory is used to conduct a cyber operation that violates international rights is, at a minimum, expected to notify the affected States.

In this regard, international arbitral jurisprudence indicates that the standard of due diligence is not uniform and, therefore, with reference to cyberspace, it should be calibrated to the level of resources and cybersecurity capacities available to individual States.[9]

Considering the transversality of the principle, numerous cases resorted to concept of due diligence when grounding State responsibility on the failure of State's authorities to prevent attacks to foreigners residing in the State's territory or on the failure of the judicial apparatus to compensate the victims and punish the perpetrators of the acts.[10] In the *Wipperman* case it was maintained that a State cannot incur international responsibility for the acts of private individuals «as long as reasonable diligence is used in attempting to prevent the occurrence or recurrence of such wrongs».[11]

---

[6] ICJ, *Corfu Channel, United Kingdom of Great Britain and Northern Ireland* v. *Albania*, Judgment of 9 April 1949, in *I.C.J. Reports*, 1949, p. 4.

[7] S. J. SHACKELFORD, R. SCOTT, A. KUEHN, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, in *Chicago Journal of International Law*, 2016, pp. 1-50.

[8] A. OLLINO, *Due diligence obligations in international law*, Cambridge 2022.

[9] A. COCO, T. DIAS, *Handle with Care: Due Diligence Obligations in the Employment of AI Technologies*, in R. GEIß and H. LAHMANN (eds.), *Research Handbook on Warfare and Artificial Intelligence*, Cheltenham-Northampton, 2024.

[10] A. OLLINO, *Due diligence obligations in international law*, Cambridge, 2022.

[11] *Frederick Wipperman Arbitration (United States of America v. Venezuela)*, Final Award of 2 September 1890, Moore, in *History and Digest*, vol. 3, pp. 3039-3043.

The application of due diligence, therefore, has grown over the years due to the expansion of state responsibility in various areas of international law, where state actors are effectively required to observe a minimum standard of care.

In this sense, it is appropriate to consider that States, also in the cyberspace, are not to allow their territory to be used for internationally wrongful acts of a State. The classification of conduct as an internationally wrongful act of a State is guided by the established customary international law, collected and elaborated upon by the International Law Commission in its Articles on Responsibility of States for Internationally Wrongful Acts[12] in which a breach is considered to be internationally wrongful only when it is attributable to a State, be it directly or indirectly.

Examining another field of international law, the treatment of foreigners, for example, has been one of the areas where the development of the concept of due diligence has been observed and this can also be useful to analyze its evolution in cyberspace. In detail, in the *Youmans* case[13] due diligence was expressly articulated as the standard governing a State's obligation to protect foreign nationals residing within its territory from criminal acts perpetrated by private individuals. The standard of due diligence has served not only as a criterion for assessing State conduct in preventing harm and protecting foreign nationals from injuries inflicted by private actors, but also in evaluating the obligations incumbent upon States to investigate, apprehend, and punish those responsible for such acts. In this sense, the responsibility of the State is subject to an expansion, precisely considering the duty to adopt preventive and repressive measures. Accordingly, in the *Kennedy* case[14] instance, the arbitrators held Mexico liable on the ground that it had failed to exercise due diligence, as it did not adequately punish a Mexican citizen who had shot and seriously injured an American national.

It is appropriate, in fact, to specify that the development of due diligence as the international standard of justice for the protection of nationals abroad went hand in hand with the progressive presumption against international responsibility for acts committed by private individuals. One of the primary challenges that emerges in cyberspace concerns attribution, namely the ability to trace and legally attribute conduct in the digital domain to a State, particularly when the actors directly involved are private individuals rather than state organs, specifying that lack of due diligence in preventing and punishing illicit acts carried out by private individuals was to be regarded as a conduct of omission on the part of State' organs, and not as a form of complicity or participation of the State in the commission of the crime.[15]

In the *Sambiaggio Case*,[16] the issue of Venezuela's international responsibility for damage suffered by an Italian national as a consequence of revolutionary acts carried out by private individuals within its territory was examined. It was observed that, under the applicable principles of international law, the State could not be held responsible for acts committed by

---

[12] ILC, *Draft Articles on the Law of Treaties with commentaries*, UN Document A/CN.4/SER. A/1966/Add. 1, in *Yearbook of the International Law Commission*, vol. II, 1966, p. 187.

[13] T. YOUMANS, *United States of America* v. *United Mexican States*, Judgment of 23 November 1926, in *Reports of International Arbitral Awards*, Vol. IV, p. 110.

[14] *Usa* v. *United Mexican States,* Judgment of 14 March 1927, in *Reports of International Arbitral Awards*, Vol. IV, 199.

[15] Regarding the attribution see: ILC, *Draft Articles on the Law of Treaties with commentaries*, cit., available on legal.un.org/ilc/texts/instruments/english/commentaries/1_1_1966.

[16] *Sambiaggio case*, Mixed Claims Commission *Italy* v. *Venezuela*, 1903, in *Reports of International Arbitral Awards*, p. 499.

insurgents, insofar as such actors were neither agents of the State nor subject to its effective control.[17] Accordingly, responsibility would arise only where it could be demonstrated that the State authorities failed to exercise due diligence in preventing the harm; however, no such failure was established in the case at hand «the ordinary rules is that a government, like an individual, is only to be held responsible for the acts of its agents or for acts the responsibility for which the responsibility is expressly assumed by it»; in circumstances where international harmful acts are in fact committed by private individuals,[18] responsibility may flow exclusively from a lack of due diligence of the State in preventing damages from being inflected by revolutionists.[19]

Many arbitral awards of the first part of the 20th century show that a State would not incur international responsibility for the conduct of private individuals *per se*, but rather for its own omissions, particularly where such omissions consisted in a failure to exercise due diligence. In this regard, State responsibility was typically grounded not in attribution of private acts, but in the breach of an obligation to take reasonable preventive and protective measures. With respect to the content and meaning of the due diligence standard in the protection of aliens, it was generally understood as requiring the exercise of a "reasonable degree of care" expected of a civilized State under prevailing contemporary legal conceptions. This standard was inherently contextual and relative, assessed in light of the State's capacities and the circumstances in which protection was to be afforded.

Therefore, it is important to underline that due diligence is not considered as a general principle universally applicable to all obligations within the international legal system, but it operates as an instrument invoked in the absence of applicable treaty or customary norms in a dispute.[20] Rather, due diligence constitutes a general normative standard specifically applicable to certain primary obligations of States, demanding the exercise of utmost effort and deriving its authority from either customary international law or treaty-based obligations.[21]

On the contrary, with reference to the responsibility of companies to respect human rights and the associated duty of corporate due diligence on human rights, general principles have developed that cannot be limited to merely being a tool for filling gaps, but can also play a role in terms of regulatory production and this at the level of both national and international legal systems.[22] Conducting appropriate human rights due diligence could help companies address the risks of legal action brought against them, as it allows them to demonstrate that they have taken all reasonable measures to avoid involvement in human rights violations. However, companies that conduct such due diligence should not make the mistake of assuming that it automatically and completely absolves them from any liability for

---

[17] J.A. HESSBRUEGGE, *The Historical Developments of the Doctrine of Attribution and Due Diligence*, in *New York University Journal of International Law and Politics*, 2004, pp. 276-279.

[18] According to art. 8 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts of the International Law Commission «*The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct*».

[19] R. PISILLO-MAZZESCHI, *The Due Diligence Rule and the Nature of the International Responsibility of States* in *German Yearbook of International Law,* 1992, pp. pp. 9-51.

[20] G. BARTOLINI, *The Historical Roots of the Due Diligence Standard* in P. HEIKE KRIEGER, A. PETERS, L. KREUZER (eds.), *Due Diligence in the International Legal Order,* Oxford, 2020, pp. 23-41.

[21] S. BESSON*, Due diligence in international law*, Académie de droit international de la Haye, Hague Academy Special Edition, 2023.

[22] M. FASCIGLIONE, *Impresa e diritti umani nel diritto internazionale. Teoria e Prassi*, Torino, 2024.

causing, or contributing to, human rights violations.[23] In fact, it should be noted that the jurisprudence of human rights monitoring bodies relating to the responsibility of a State for failure to control the activities of enterprises highlights how the positive obligations to which States are addressed are not only exhausted in positive due diligence obligations but also include positive result obligations.

Understanding the nature and content of this dual type of obligation proves essential to also grasp the methods and types of measures that must be adopted.

From what has been outlined in this paragraph, it is clear that standards of compliance with international obligations and expectations arising from the principle of due diligence are inherently flexible and must be assessed considering the capabilities and competences of the States. Therefore, in cyberspace, States are expected to make every effort to ensure that their territory is not used for the commission of internationally illicit cyber operations, and its understanding was clearly reaffirmed in the 2021 GGE report. The next paragraph specifically analyses the scope of the duty of care in cyberspace and the legal implications of its application with reference to the rules articulated in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.[24]

3. *The Application of Due Diligence to Cyber Activities*

Within the increasingly prominent debate on the scope and applicability of international law in cyberspace, a central issue concerns whether States are bound by cyber-specific due diligence obligations, and, if so, how these obligations should be articulated. First, it is necessary to consider that, in absence of specific rules in cyberspace, setting out measures to be taken by States for the prevention of hazardous activities in their territories, it is difficult to determine to what extent States shall monitor or regulate potentially hazardous activities.[25] *The Tallinn Manual*,[26] which regulates the application of international law to cyber operations, initially presented a negative command of due diligence in its original

[23] Regarding corporate social responsibility see M. CASTELLANETA, F. VESSIA, *La responsabilità sociale d'impresa tra diritto societario e diritto internazionale*, Napoli, 2019.

[24] N.M. SCHMITT, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed, Cambridge, 2017*. Developed by the NATO Cooperative Cyber Defence Centre of Excellence following the cyberattacks suffered by post-Soviet countries since the mid-2000s, the volume discusses the applicability of existing principles of international law to cyberspace, both in peacetime and wartime. In the short term, the 154 norms identified by the experts should serve as a guide for policymakers and their legal advisors in responding to potential cyberattacks. In the long term, they aspire to become consolidated practice in state behaviour, assuming recognized and effective legal validity. The manual, however, warns that while cyber operations do not take place in a legal vacuum, as with other areas of international law, there will likely be significant divergence between states' different interpretations of the norms.

[25] H.S. LIN, *Offensive Cyber Operations and the Use of Force in Journal of National Security Law and Policy*, 2010, p. 4; N.M. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2013; M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; K. KITTICHAISAREE, *Public International Law of Cyberspace*, Cham, 2017; A. STIANO, *Attacchi informatici e responsabilità internazionale degli Stati*, Napoli, 2023; A. SCIACOVELLI, *Reflexions on the hostile activities in cyberspace and the international legal landscape promoted by the United Nations*, in *OSORIN*, 2024.

[26] N.M. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare,* Cambridge, 2013. Prepared by the international Group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, it consists of 95 rules, which a group of experts has arranged in a sequence addressing various areas and which partly reflects customary international law.

project as «a State shall not knowingly allow […] to be used for acts that adversely and unlawfully affect other States». Subsequently, in Rule 6 of the Manual 2.0 the prescription has become «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».

The Manual asserts that due diligence derives from the sovereign equality of States and the corresponding duty to protect each other's rights[27] and qualifies it as a general principle of specialised regimes of international law and considered that diligence obligations attach to a State through which data 'only transits', but conceded that transit State responsibility is unlikely to be carried out in practice. Malicious cyber actors frequently route cyberattacks through multiple states, compromising servers located in extraterritorial jurisdictions before inflicting harm on their ultimate target and, in this sense, the words 'only transits' is unclear. The drafters differentiated a 'transit state'[28] with a State in which «specific cyber infrastructure is set up […] for malicious purposes» but the role of a State's network in a cyberattack may not always be clear.

With reference to the effects of the cybernetic operation, it is also necessary to specify that States are not required to remedy every instance of transboundary harm, but only those that result in serious adverse consequences. It is generally assumed that certain forms or levels of harm fall below the threshold necessary to trigger the due diligence obligation.

However, it must be considered that the framework of the United Nations GGE in the context of international security States demonstrated reluctance to recognise due diligence as a binding obligation, instead accepting only that States *"should"* exercise due diligence rather than that they *"must"* do so, as suggested by the rule itself.[29] When considered alongside the principle of sovereignty, even the more cautious formulation adopted by the Experts leaves a significant gap, within which victims of cyber harm have limited avenues for redress.

The experts involved in the Tallinn Manual 2.0 clarify that for a State to incur responsibility under the standard of due diligence in preventing transboundary harm, it must possess knowledge or at least be in a position where it should reasonably have been aware, of the harmful activity. There are some common themes however that arise from the jurisprudence of the ICJ: control over territory, people or infrastructure provides prima facie evidence but does not prove knowledge without more and does not shift the burden of proof; widespread reports are not proof of knowledge of a fact. As the ICJ said in the *Nicaragua case*[30] widespread reports of a fact may prove on closer examination to derive from a single source, and such circumstances, their apparent multiplicity does not enhance their probative value, which remains equivalent to that of the original source.[31]

---

[27] The Manual cited *the Corfu Channel* judgment at 22.

[28] The example is represented by fibre optic cable located within that State.

[29] In detail, the Summary of the GGE Reports prescribes: *«States should also take appropriate measures to protect their critical infrastructure from ICT threats. States should not harm the information systems of the authorized emergency response teams of another State or use those teams to engage in malicious international activity. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions».* On the contrary, the Tallin Manual 2.0 predicts that *«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».*

[30] ICJ, *Nicaragua* v. *United States of America*, Judgment of 27 June 1986, in *I.C.J. Reports*, 1986, p. 14.

[31] N.M. SCMITT, *Attack, as a Term of Art in International Law: The Cyber Operations Context*, in C. CZOSSECK, R. OTTIS, K. ZIOLKOWSKI (eds.), *4th International Conference on Cyber Conflict. Proceedings*, Tallin, 2012, p. 288.

In practice, the establishment of proof of knowledge is inherently challenging and becomes increasingly complex within the cyber domain. While evidence may substantiate the occurrence of a harmful act, the identification of the responsible party frequently proves problematic; in the context of clandestine cyber operations, even the precise nature of the incident may remain uncertain. Consequently, establishing responsibility requires not only proof of the material elements of the act but also reliable attribution. In the cyber context, this entails demonstrating which computer or server was involved, determining its geolocation, identifying the individual or entity operating it, and establishing the nature of that actor's relationship with a State.

Standards of evidence may vary depending on whether they are invoked for political or legal purposes; however, even in the latter context, international courts frequently establish their own evidentiary rules and standards. For example, evidence cannot be presumed even where difficulties in collecting evidence exist. It cannot apply a presumption that evidence which is unavailable would, if produced, have supported a particular party's case or a presumption of the existence of evidence which has not been produced; although there is no clear standard of evidence, the ICJ has aligned the standard of evidence to the gravity of the claim.

With regard to use of force, clear and convincing evidence is needed which perhaps implies a lower standard for other operations. In the *Bosnian Genocide* Judgment, the Court also appeared to make a distinction between a violation of the prohibition of committing acts of genocide,[32] for which evidence must be 'fully conclusive', and a violation of the obligation to prevent acts of genocide, where the Court required «proof at a high level of certainty appropriate to the seriousness of the allegation».[33]

From this one may say that a lower standard is required when omissions are involved because it is difficult to establish negative facts but still there is no clear rule as to what evidence is needed to establish what should have been done; the ICJ also accepted a more liberal approach to evidence when evidence is under the opponent's control; evidence produced through espionage or surveillance even if these activities may violate international law are not inadmissible. In fact, in the Corfu Channel case, the ICJ accepted evidence collected in operations that for the Court were violations of the non-intervention rule and of sovereignty.

In a certain sense, each element of the principle operates as a reasonable limitation on potential State responsibility. Specifically, a State will only fail to exercise due diligence when it has knowledge of a cyber operation being carried out from within its territory, which contrary to the rights of another State, and it fails to take feasible measures to prevent it.[34]

Nonetheless, the drafters concluded that constructive knowledge also triggers due diligence obligations. Whilst it might be difficult to ascertain evidence of a State's actual

---

[32] On 20 March 1993, the Republic of Bosnia and Herzegovina instituted proceedings against the Federal Republic of Yugoslavia in respect of a dispute concerning alleged violations of the Convention on the Prevention and Punishment of the Crime of Genocide, adopted by the General Assembly of the United Nations on 9 December 1948, as well as various matters which Bosnia and Herzegovina claimed were connected therewith. The Application invoked Article IX of the Genocide Convention as the basis for the jurisdiction of the Court.

[33] ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment of 26 February 2007, in *I.C.J. Reports*, 2007, p. 130.

[34] K. BANNELIER, *Obligations de diligence dans le cyberespace: qui a peur de la cyberdiligence?*, in *Revue belge de droit international*, 2017, pp. 612-665.

knowledge of a given cyber operation, a constructive knowledge standard ensures that the due diligence approach is not rendered all but redundant.

Moreover, a State is more likely to possess knowledge of activities conducted through its governmental cyber infrastructure than of those occurring via private infrastructure within its territory.[35] Where attributing knowledge would be unreasonable under the circumstances, the State's obligation to exercise due diligence is not engaged.

The second element, that the cyber operation be contrary to the rights of another State, is the least settled at international law. It is sufficient to say, for the purposes of this article, that only cyber operations of a certain level of gravity will engage a State's obligation of due diligence. Specifically, the principle deals with cyber operations that amount to an internationally wrongful act, and which result in serious adverse consequences for the target State. This appropriately limits potential liability under the due diligence standard by excluding from its scope the vast number of minor cyber operations that are not regulated by international law.

The third element, concerning feasible measures, provides that States are only required to intervene in a cyber operation when they have the capacity to do so, and when doing so is reasonable in the circumstances. This element shows the greatest protection to States against the imposition of indeterminate liability. As such, States will not violate international law for failing to prevent highly complex cyber operations that they lack the ability to control.[36] Furthermore, even in instances where States have the capacity to prevent harmful cyber operations carried out in their territory, they are under no obligation to do so when it would be unreasonable in the circumstances. For instance, a State would very rarely, if ever, be required under a due diligence standard to act in a way that resulted in the self-denial of essential networks or important cyber infrastructure.

In this way, the due diligence principle can operate as a standard of attribution in a clearly proscribed set of circumstances. While a fear of expanding State responsibility is understandable, it should be tempered by the limited scope of the doctrine. For these reasons, States will only ever be responsible for cyber operations with serious adverse consequences, which they have the capacity to identify and respond to.

4. *Conclusions and Outstanding Challenges*

The legal regulation of malicious cyber operations should be strengthened through multiple layers of obligations, consisting, *inter alia*, of attribution to States, cyber-crime conventions, and the due diligence principle. These three elements are not mutually exclusive; they can supplement and reinforce each other.

In the cyberspace, the question remains as to whether the State can also be held responsible for the wrongful act committed by a non-State actor. In the international panorama an omission can lead to responsibility for the resultant act if the omission was the

[35] E. SCHMID, A. ÖZGE ERCEIS, *The Attribution of Omissions: Due Diligence in Cyberspace and State Responsibility*, in *Swiss Review of International and European Law*, 2023, pp. 577–596.

[36] A. L. SCIACOVELLI, *Malicious Cyber Operations Committed by States and Non-State Actors: The International Legal Landscape*, in P. GARGIULO, D. GIOVANNELLI, A. L. SCIACOVELLI (eds.), *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, *La Comunità Internazionale, Quaderno 29*, 2024, p. 29 ss.

cause of such act or, in other cases, if the omission occasioned the act.[37] More specifically, although the wrongful act is committed by a third person, it is the expected consequence of the omission. In the Corfu Channel case for example, the Court found that Albania had a general duty of due diligence which included an obligation to prevent any damage from the moment it learned about the existence of mines. Because Albania failed to act, it was responsible not just for dereliction of diligence but for the explosions and the damage and loss of life that resulted from its lack of diligence. Likewise, command responsibility as formulated in the International Criminal Court Statute is responsibility for the crimes of subordinates caused by the superior's failure to prevent their commission.[38]

Unfortunately, considerable uncertainty remains about the concrete operability and boundaries of the principle of due diligence in cyberspace. Where a State is the victim of a serious cyberattack conducted through the networks of a third State and the original perpetrator cannot be identified, it is unlikely to remain patient if that third State fails to act promptly or effectively. In such circumstances, the victim State may resort to its own cyber operations, despite the doubtful legality of such responses, particularly in peacetime.

Among the various application issues in cyberspace, the absence of clear agreement on the obligations of third States to prevent or halt the misuse of their networks therefore creates a tangible risk of escalation. In addressing this issue, useful guidance may be found in the traditional principle of neutrality, which was specifically developed to reduce the risk of conflict escalation between belligerent and non-belligerent States. This body of law regulates conduct in the grey zone at the margins of armed conflict, governing relations between States that remain formally at peace but may nonetheless be connected to an ongoing conflict.

In conclusion, it is therefore important to emphasize that the applicability of due diligence to cyberspace remains an open question in the field of international law. Considering the rapid evolution of this domain, its practical implementation is continuously developing and remains subject to modification and further refinement, within a framework that must address some of the principal current and future challenges faced by States.

[37] ILC, *Draft Articles on the Law of Treaties with commentaries*, cit., Art. 2.
[38] Statute of the International Criminal Court, 1998, Art. 28, *Responsibility of commanders and other superiors*.