



RESEARCH ARTICLE

Due Diligence in General International Law

Veronica Bujac¹

¹ Research Scholar, Department of Law, Anglia Ruskin Cambridge University, United Kingdom. Email: dj4632415@gmail.com

ARTICLE HISTORY

Received **01-09-2025**
Accepted **11-12-2025**
Published **30-12-2025**

KEYWORDS

International law, due diligence, transborder, ijc, international court of justice

CORRESPONDING AUTHOR

Veronica Bujac
dj4632415@gmail.com



<https://doi.org/10.68740/wcj2tj88>

ABSTRACT

This article reviews the scope of the general international law obligation to "take all necessary measures" to prevent serious transboundary harms of cyber operations, and, somewhat tentatively, State-related algorithmic activity. It does this because it considers due diligence to be a starting point for the conduct rules – different from the rules of attribution and consequences of internationally wrongful acts. This analysis is based mainly on the decisions of the International Court of Justice, the work of the International Law Commission on the law of State responsibility and the law of due diligence, and a few official statements regarding the law applicable to cyberspace. The article posits that the concept of the due diligence is a well-known practice in general international law, including in the context of a State's legally relevant relationship to a source of risk and its knowledge or reasonable knowledge of a serious risk for the enjoyment of rights guaranteed by international law. The same is not the case regarding its use in cyberspace, however. Views vary on the legal nature and content of cyber due diligence among the States: some States explicitly state that cyber due diligence is customary, and others acknowledge the principles but not the idea that there is a rule in cyber due diligence. The article suggests using a four-part analytical structure for the evaluation of alleged omissions: a legal nexus, knowledge or foreseeability, reasonable and feasible measures, and a threshold of legal cognizability of a risk or harm. It then examines whether a similar approach can be used for algorithmic systems that are associated with the State. The author concludes that technological novelty does not eliminate the current international-law obligations but also does not automatically involve new ones. That is why it is best to argue a cyber and algorithmic case in a disciplined way; that is, predispositions from due diligence can be applied to a cyber and algorithmic case where the legal requirements are met; and that the requirements for cyber-specific legal rules as to their status and content are still subject of ongoing State practice and legal development. This is a list of topics covered in the document. This is a list of the topics addressed in the document.

1. INTRODUCTION

International law does not depend on technological continuity. Its rules are applied all the time to new factual situations in which the same legal interests are still present. Cyberspace is an example. Networked infrastructure enables states to communicate, run public services, engage in diplomacy, and collect intelligence and deploy military forces. Much of the infrastructure used for these activities is run by private entities. One cyber operation can cross multiple jurisdictions, may include compromised devices in multiple States, and can have impacts well removed from the geographic area where the operator is based. AI is further complicated by the fact that systems can be trained, deployed, processed and tuned in various jurisdictions and the relationship between a system and a harmful outcome can be spread out across various groups of people: developers, deployers, users and infrastructure providers. The presence of these technological features is not in itself evidence to answer the legal question. The question which arises is whether the facts can be understood in the light of existing international obligations and what conditions must be met for an omission on the part of a State to be regarded as an internationally wrongful act. Due diligence is relevant because it provides a basis for a category of situations where a State has no itself guilty of the harmful act, but may have obligations with regard to something or someone in its territory, jurisdiction or other legally relevant sphere of control. An early formulation of the ICJ in Corfu Channel was that no State may use its territory for acts inconsistent with the rights of other States "with knowledge of such use. Later, the environmental jurisprudence termed prevention a rule of custom, whose roots were in the duty on the part of the State in its territory. In the Genocide case, the Court considered the obligation to prevent genocide to be an obligation of conduct that would have different intensities based on the State's capacity to influence the actors. These are statements of important propositions of prevention and diligence, but they come from different legal circumstances. They don't without further analysis, create a universal rule for every transboundary technological harm. This difference is revealed in the cyber context. In numerous occasions, the United Nations process has reiterated the applicability of international law to the behavior of States in cyberspace. Meanwhile, States have been divided with respect to the legality of specific rules, and as to the extent of customisation of concepts like sovereignty and due diligence. The 2021 national statement, for instance, for the United Kingdom confirmed that international law governs State actions in cyberspace, but that there is no specific customary international-law rule of due diligence relating to cyberspace as yet established as a practice of the States. The Netherlands and Norway, on the other hand, have specific instructions that due diligence is a customary rule in the cyber context. This disagreement leads to the main research question. The issue is not if States have responsibilities under international law if they are themselves involved in wrongful cyber operations, but rather on how attribution and breach are dealt with within the framework of the ordinary rules of State responsibility. What international law demands in the case of harmful cyber activity by another State or by private actors with infrastructure located in, or otherwise legally linked to, a third State is another question. A related issue is where there is transboundary harm created or enabled by an algorithmic system without a simple series of decisions by human decision-makers. The risk is double: on the one hand, the theory of due diligence could make every cyber incident an international wrong of the territorial State, and on the other, it could be so narrow that it would fail to address legitimate duties of prevention recognised by International law. The real issue is thus whether there is a "due diligence" obligation under general international law to cover serious transboundary cyber harm and what constitutional framework and limitations can be applied to extend this obligation to State-related algorithmic activities. There are four sub questions that follow. First, let's just figure out what the ICJ decisions and the work of the International Law Commission tell us about due diligence. Secondly, what is the relationship between due diligence and attribution, sovereignty and non-intervention? Third, what does the legal landscape of cyber due diligence show by the selected State positions?

Second, how does due diligence interact with attribution, sovereignty and non-intervention? Third, what do selected State positions reveal about the legal status of cyber due diligence? Fourth, under what conditions, if any, can due-diligence reasoning be applied to State-linked algorithmic systems?

The article adopts a doctrinal method supplemented by structured comparative analysis of official State positions. It does not claim to provide a statistical measurement of global State practice. Instead, it compares positions that expressly address the application of international law to cyberspace and uses them to identify areas of convergence and disagreement. This distinction is essential because the existence of a customary rule cannot be established simply by counting published statements. State practice and *opinio juris* must be assessed qualitatively, across the international community and in relation to the precise rule claimed.

The article proceeds as follows. Section 2 identifies the literature and the research gap. Section 3 explains the methodology and the analytical framework. Section 4 reconstructs due diligence in general international law. Section 5 distinguishes due diligence from attribution and other rules of State responsibility. Section 6 examines State positions on cyber due diligence. Section 7 applies the framework to transboundary cyber harm. Section 8 considers State-linked algorithmic activity. Section 9 addresses objections and limits. Section 10 considers the implications for general international law, followed by the conclusion.

2. LITERATURE REVIEW AND RESEARCH GAP

2.1 Due diligence in general international law

The literature on due diligence treats it as a standard of conduct rather than a guarantee of outcome. The distinction is important because prevention obligations often require a State to take measures that are reasonable in light of the circumstances, risk and means available to it. The International Law Commission's 2024 syllabus on due diligence traces the concept through nineteenth-century practice, neutrality, protection of aliens and twentieth-century judicial decisions. In 2025 the Commission placed due diligence in its programme of work and appointed Penelope Ridings as Special Rapporteur. In 2026 the Commission considered the Special Rapporteur's first report. The topic is therefore not merely historical: the content and legal status of due diligence are currently the subject of formal codification and progressive-development work.

Environmental scholarship has been particularly influential. The no-harm and prevention principles are associated with *Trail Smelter*, the *Nuclear Weapons Advisory Opinion* and *Pulp Mills*. *Pulp Mills* stated that the principle of prevention, as a customary rule, has its origins in the due diligence required of a State in its territory. The Court also connected due diligence with environmental impact assessment where there is a risk of significant adverse transboundary impact. These authorities are important, but their legal propositions must remain tied to the environmental setting in which the Court addressed them.

The *Genocide* judgment supplies a different example. The Court held that the duty to prevent genocide is an obligation of conduct and that the duty arises when a State learns, or should normally have learned, of a serious risk. The required diligence depends on the State's capacity to influence the actors concerned. This reasoning is highly relevant to the structure of due diligence, but the source of the obligation is Article I of the *Genocide Convention*. It should therefore be used as an illustration of the conduct-and-capacity logic of prevention, not as evidence that every due-diligence principle has identical customary content.

2.2 Cyber operations and international law

Cyber scholarship has moved from the question whether international law applies to more specific questions concerning attribution, sovereignty, intervention, force, countermeasures and due diligence. The Tallinn Manual 2.0 is influential as an expert restatement, but it is not a treaty and does not itself establish customary law. Its treatment of due diligence has nevertheless influenced academic debate and State positions.

Efrony and Shany's study of State practice after the first Tallinn Manual demonstrated uneven acceptance of the Tallinn Rules and cautioned against assuming that the Manual itself represents settled State practice. Akande, Coco and de Souza Dias later emphasized the technology-neutral character of international law and argued that non-binding recommendations cannot displace existing international law. Delerue's comprehensive treatment of cyber operations similarly demonstrates that State responsibility provides important tools but does not resolve every problem created by technical uncertainty and non-State actors.

Official practice is especially important. Australia, the Netherlands, Norway and the United Kingdom have all published positions explaining how international law applies to cyber conduct, but they do not speak with one voice on due diligence. The United Nations framework also distinguishes binding international law from voluntary norms of responsible State behaviour. The 2025 final report of the Open-ended Working Group for 2021–2025 confirmed the continuing international-law framework and established a permanent Global Mechanism for further discussion and implementation.

2.3 Artificial intelligence and international responsibility

The AI literature is broader than the international-law question addressed here. Scholarship has examined algorithmic accountability, human rights, autonomous weapons, legal personality and the possibility that automated systems create responsibility gaps. McGregor, Murray and Ng demonstrate the relevance of international human rights law to algorithmic accountability. Chesterman examines the limits of treating AI as a new legal person. Maas considers how AI may affect the development and operation of the global legal order. These works establish that AI creates legal problems, but they do not establish a general rule of State responsibility for every harm associated with AI.

The research gap therefore lies at the intersection of these literatures. Whereas existing scholarship identifies AI accountability issues, it also is catching up around due diligence in general international law, and its role in cyber operations. Useful is a process oriented approach to choosing when those strands can be woven together and that it doesn't require that novelty equates to a new customary rule. This article fills that gap, by distinguishing between settled propositions from contested extensions, and by utilizing contested extensions as the probe for official State positions.

3. METHODOLOGY AND ANALYTICAL FRAMEWORK

3.1 Doctrinal method

Doctrinal legal analysis is the main approach. The study defines treaties, materials on customary law, ICJ jurisprudence and International Law Commission work as means of establishing rules of international law. Judicial opinions and official State documents are the primary source of information for the analysis. The primary sources are used to be interpreted and critiqued, but they are not used in place of expert manuals and academic commentary. The analysis separates the three propositions. The first is that there is a range of duties aspecting due care, which are clearly acknowledged in specific areas of international law. Second, due diligence in cyber is

backed by a developing practice at the State level, though as yet there are various interpretations regarding its status and scope. Thirdly, any application of due-diligence reasoning to AI harm is another step in analysis that needs to fulfil the legal preconditions of an appropriate primary obligation.

3.2 Comparative analysis of State positions

Comparative part is a purposeful one, not statistical. It takes into account official documents from States that have released comprehensive representations, such as Australia, France, Germany, Netherlands, Norway, the United Kingdom, the United States and China. The selection is designed to highlight discord as the intent never was to represent the point of view of all States. The comparison is mainly aimed at distinguishing between the State descriptions of due diligence as a customary norm, an unsettled term, or a voluntary norm, and extracting comparisons between due diligence and other major rules. This way there will be no false impression that the numbers are precise. Published position constitutes evidence of a State's public legal position, but not necessarily general State practice or *opinio juris*. No talk should be interpreted as a positive rejection or positive acceptance. Of course, the number of published position papers does not provide an answer to the question of the existence or not of custom.

3.3 Analytical framework

The article presents four questions that can be used as an evaluation of alleged due diligence. The first is the legal connection – what is the legal connection between the State and source of the risk (territory, infrastructure, legal jurisdiction, governmental control or other legal connection recognised in the applicable jurisdiction)?

Second is knowledge or foreseeability: did the State know, or in the circumstances should it reasonably have known, of the relevant activity or serious risk? Third is reasonable and feasible measures: what steps were available to the State, given the risk, its legal powers and its capacity? Fourth is the legal threshold: did the risk or harm concern a right or interest protected by an applicable international obligation and reach the seriousness required by that obligation?

These four questions are not presented as a newly codified universal cyber rule. They are an analytical synthesis of recurring features in the authorities. Their purpose is to prevent two errors. The first is treating every harmful event originating from a State's territory as a wrongful omission. The second is treating uncertainty about attribution as eliminating all possible obligations of prevention.

4. DUE DILIGENCE IN GENERAL INTERNATIONAL LAW

4.1 Corfu Channel and the knowledge-based obligation

Corfu Channel remains a foundational authority. The ICJ held that Albania was responsible for failing to warn of a minefield in its territorial waters. The Court stated that every State has an obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States. The importance of its proposition lies in the fact that it is related to the behaviour of those whose mining activity was not assigned to the Albanian as an act of an Albanian organ. The evidences point, however, needs to be expressed properly. Corfu Channel did not say that presuming territorial control means presuming the knowledge, that a State must have all the knowledge on all the things that are unlawful in its territory. The Court specifically warned against such an assumption of territorial control. The case thus establishes a knowing requirement, in addition to an evidentiary inquiry into the circumstances, rather than a constructive or other blanket rule. Prevention and transboundary harm is covered in section

4.2. The environmental cases focused on the preventative aspect.

4.2 Prevention and transboundary harm:

Pulp Mills states that in its interpretation, prevention is a "preserving" rule that has its roots in the requirement of due process and judgment, and that environmental assessment is required when a proposed activity has potential for significant adverse transboundary effects. The Court again acknowledged in *Certain Activities* the existence of a customary duty to perform due care to prevent "significant transboundary harm" from occurring. The choices demonstrate that international law can place a duty on a State to prevent where the conduct or jurisdiction of the State poses a serious threat to another State's rights and interests. The analogy to cyber operations is helpful, but not inevitable. Environmental prevention has evolved into a specific field of practice on physical and ecological damage as well as resources and environmental assessments. As a result, an independent mechanism of evidence associating the elements of the obligation is necessary for a cyber application. A sound methodical strategy would be to examine the cases to determine the related understandings and expected reasoning regarding prevention, knowledge, risk, and feasible measures that could be taken to prevent harm in the physical environment, and to build these understandings and expectations into a growing knowledge base when considering actions to take for prevention in the cyberspace environment. They are the ability to prevent genocide and to have an impact.

4.3 Prevention of genocide and capacity to influence

. Another important model is provided by the *Bosnia Genocide* judgment. The Court found that the obligation to take reasonable measures to prevent genocide is triggered when a State comes to know, or is 'informationally certain' to know, of a serious risk of genocide. The nature of the task is contingent on the State's ability to impact those actors most likely to commit genocide. The Court handled the requirement in a manner that deemed it nonappearance to be one of conduct and not result. This is a line of reasoning that applies to a general theory of diligence, as it gives away by denying a guaranteed success. In the same time, the genocide as context reveals a caution to be used. The duty stems from the Genocide Convention and the weight of the interest protected is particular. The case does not establish a hard and fast rule to cross all types of transboundary harms, but just a method to analyse these preventive duties.

4.4 The International Law Commission and the current due-diligence project:

The contemporary importance of due diligence is reinforced by the work of the International Law Commission. The Commission put due diligence on its agenda for 2025, and designated Penelope Ridings as Special Rapporteur. In 2026, a Special Rapporteur gave a first presentation to the Commission, and a chapter on the issue was adopted by the Commission in its 2026 report. There are no updates or modules for this topic. There are two implications with this development. Firstly, it establishes the fact that the concept of due diligence is sufficiently important and general to be considered on a systematic level at the codification stage. Second, it cautions against regarding what is due as a general due-diligence obligation as having been resolved.

. The Commission's current work itself demonstrates that questions of scope, terminology, sources and legal effect remain open to further analysis.

5. DUE DILIGENCE, ATTRIBUTION AND STATE RESPONSIBILITY

5.1 Primary obligations and secondary rules

The distinction between primary and secondary rules is central. A primary rule sets out what law of the land obligates a State to do or not do. Apart from the primary rules introduced in the

Convention on Responsibility of States for Internationally Wrongful Acts (ARSIWA) are also included rules in Appendix IV, with reference to attribution, breach, circumstances precluding wrongfulness, invocation and consequences. Hence, it can't be simply regarded as an alternative to attribution as part of due diligence.

Article 2 of ARSIWA defines an internationally wrongful act through two elements: conduct consisting of an action or omission attributable to the State under international law and a breach of an international obligation of the State. The reference to omission is important in due-diligence cases. A State may breach a primary obligation by failing to take required measures even though the underlying harmful act was committed by a private actor or another State.

5.2 Attribution of cyber operations

Where a cyber operation is attributable to the State that conducted it, the ordinary law of State responsibility applies. ARSIWA Article 4 covers State organs; Article 8 addresses persons or groups acting on the instructions of, or under the direction or control of, the State; and Article 11 addresses conduct acknowledged and adopted by the State as its own.

The ICJ's Nicaragua judgment remains important for the effective-control approach to attribution of the conduct of non-State actors. An alternative to the ICTY's overall-control is not the ICJ's rule for State responsibility. The difference is important as cyber operations often use proxies, contractors and criminal groups, and technical attribution does not necessarily translate into legal attribution.

5.3 Due diligence is not a substitute for attribution

The greatest opportunity for due diligence occurs when harmful conduct itself is not attributable to the State, but the State does have an obligation in regard to conduct or risk that is related to its territory, jurisdiction and/or control. The host State is not liable just because the malicious traffic was and passed through its infrastructure. There must be a primary obligation, a legally relevant connection, knowledge or foreseeability (where required) and failure to take measures demanded by the primary obligation.

This distinction protects both sides of the problem. It prevents victim States from converting technical routing into automatic legal attribution, while also preventing a State from treating the absence of attribution as an automatic exemption from obligations of prevention

6. DUE DILIGENCE IN CYBERSPACE: STATE PRACTICE AND COMPETING POSITIONS

6.1 The United Nations framework

In 2013 and again in 2015, the UN GGE reaffirmed that international law – including the UN Charter – is applicable to State action in cyberspace, and that the OEWG from 2021 continued this trend in its reporting. The framework of 2015 also involved voluntary norms of responsible behaviour by States, such as a call on States to not knowingly allow its territory to be used in relation to internationally wrongful acts via ICTs. It is important to note some of the differences between the binding international law and what are considered voluntary norms. Since these 2021 reports, the UN process has gone further. The Open-ended Working Group, which was set up for 2021-2025, finished its work in 2025, with a consensus final report, and States agreed to a permanent Global Mechanism on ICT security and responsible State behaviour. The Global Mechanism started substantive work in 2026. It is, therefore, a more appropriate context to look at the contemporary State practice with the current institutional framework, rather than having a retrospective analysis up to the reports of 2021.

6.2 States supporting a customary due-diligence obligation

The Netherlands' 2019 position is explicit: it regards due diligence as an obligation in its own right and states that a State may incur responsibility where it knows that cyber activities from its territory or infrastructure cause serious adverse consequences for another State's rights and fails to act. Norway's 2021 position similarly describes due diligence as a customary international-law obligation applicable to cyber operations. Norway also emphasizes that the obligation is one of conduct, not result, and that the State is not generally required to monitor all cyber activity on its territory.

Australia's public materials are supportive of the application of existing international law in cyberspace, and the implementation of responsible-behaviour norms. Whether a State is held responsible and liable for another under existing international law, including the State responsibility law, depends on the conduct of that State in Cyberspace, as stated in its 2021 Strategy. They help to advance the main thesis, which is that cyberspace is not beyond international law, but that it should be reviewed closely before making judgements regarding the exact nature of the customary law component of due diligence.

6.3 States expressing caution

The United Kingdom is a significant counter-position. In its 2021 statement, it reiterates that international law applies to the conduct of States in cyberspace, but it expressly clarifies that the mention of a non-binding norm related to territorial misuse does not mean that there is already enough State practice to define a specific customary international-law rule on due diligence with regard to activities in cyberspace. It is a direct and important qualification to any claim of settled custom.

If the parties differ, it does not mean that there is no legal duty. It does, however, make it more challenging to assert, unequivocally, that a rule for cyberspecific due diligence is the settled law. The right answer is that the general law does include some of the concepts of prevention, but the exact customary elements of their application with respect to cyber operations are still in development.

6.4 What State practice can and cannot establish

State positions are important pieces of evidence, but should be interpreted carefully. A national statement can show the laws that a certain State has in place. It does not create a general rule of custom. Similarly, a voluntary norm can be concurrent with an existing legal requirement, but not create the legal requirement. The analytical question is thus what is the legal proposition that the State is making, and whether that proposition is supported by the more general practice and *opinio juris*.

The comparative evidence singles out a tentative proposition: international law is accepted as having applicability to the conduct of states in cyberspace and that the misuse of territorial or infrastructural space might warrant preventive measures. They differ, however, on whether this would already be a specific customary rule of cyber-due-diligence and on exactly what the due-diligence obligation entails. It is a more defensible conclusion than one that this percentage or that percentage of States hold a legal position.

7. TRANSBOUNDARY CYBER HARM: APPLYING THE ANALYTICAL FRAMEWORK

7.1 Legal nexus

The first question is related to the linkage of the State and the source of risk. In *Corfu Channel*, the appropriate link was one of the areas that were under the control of the State. In the context of cyber cases the nexus might be between servers, network infrastructure, data centres or other systems within the State, but not physical location alone. There may also be a jurisdictional and governmental issue where it is recognized under the primary rule.

The nexus requirement becomes especially significant because it is common for cyber operations to be conducted using compromised devices, without the owners' knowledge. A State is not responsible for stopping any malicious use of infrastructure in its territory just because the packets traveled through it. The nexus will therefore have to be linked to the legal principle mentioned and to the capacity of the State to take the measures the legal principle calls for.

7.2 Knowledge and foreseeability

As part of the doctrine of due diligence, knowledge is a recurring theme. The facts of the case can be a factor in determining if the State was aware of a risk, as shown in *Corfu Channel*. The Norwegian position in cyberspace is similar: the actual knowledge is contrasted with situations where a State should have reasonably known about harmful activity. Constructive knowledge, however, should not be an on-going monitoring duty.

A defensible cyber application would thus be able to tell the difference between general information about cyber threats and specific information about a serious cyber threat. A diplomatic notification about credible technical indicators, repeated attacks from identified infrastructure, or evidence of malicious activity that a reasonably capable authority would be expected to detect may be relevant. However, the fact that malicious traffic is found on the internet alone should not be sufficient.

7.3 Reasonable and feasible measures

Obedience to the duty of 'due diligence' is a duty of conduct. The State is typically not obligated to ensure that bad behavior will never happen.

The necessary steps are dependent on legal context, the severity and predictability of the risk, the powers of the State and the reasonably available means.

Examples of measures in a cyber context could include investigations of credible reports, cooperation with an affected State, action against infrastructure where the State has lawful authority to act, enhancing incident response capacity, and exercising available domestic regulatory or law enforcement powers. Having a viable option does not necessarily mean that it is legally mandated.

. The measure must relate to the relevant main obligation and be commensurate with the risk it aims to tackle.

7.4 Seriousness and legally protected interests:

A due diligence claim requires an identification of an international right or interest that is said to have been affected. International law does not make all nuisance or technical matters international responsibility matters; seriousness matters. A significant-harm threshold is a common approach for environmental cases; a serious adverse consequences formulation is used for cyber scholarship and State positions. The level of threshold may be different depending on the prime responsibility.

Potentially serious cyber harm includes disruption of critical public infrastructure, interference with critical medical services, destruction or corruption of data needed for government operations, cyber operations with physical consequences. The examples do not provide a standard of universal application outside of the specific rule and are representative of the kind of harm that can be a matter of international law

8. ALGORITHMIC RISK AND STATE-LINKED AI ACTIVITY

8.1 Why AI changes the evidentiary problem

AI systems make due diligence more difficult due to the possibility of a distributed causal chain. A model can be developed in one State, trained in a different State, published in a third State's cloud service, and deployed in a different State by the users. The system can also generate outputs, which are not intentionally designed by the developer or the State authority. These facts make it hard to attribute and predict, but do not leave a legal void.

The simplest case is the use of AI as a tool by the State. The use of an AI system by a State organ in an internationally wrongful operation does not exclude the operation from the law of State responsibility. Attribution and breach remain the legal issues. The harder case is a private system which causes significant transboundary harm and where there is no evidence that the State was involved in a way that caused the harm.

8.2 State regulation and the legal nexus:

In this section, in the curriculum covering State regulation and the legal nexus. The case for due diligence is magnified if the State has a legally legitimated jurisdiction or regulatory interest in the activity and information regarding the serious foreseeable risk. The weaker it is, because the only relationship is that the developer is incorporated or physically situated in the State. International law does not automatically make domestic regulatory authority an international obligation to regulate all activities of non-governmental entities and persons. Questions therefore have to be posed as to whether such an international obligation needs to be addressed in a manner of prevention or protection in the circumstances. International human rights law might apply when State action or jurisdiction impinges upon protected rights. When the activity is aided by AI and results in known transboundary environmental damage, international environmental law might be applicable. The cyber due-diligence analogy could be appropriate for the situations in which AI is utilized for critical cyber operations. There must be a primary rule to be applied to each case.

8.3 Knowledge, capability and risk assessment

Knowledge, capability and risk assessment AI systems generate novel kinds of evidence for knowledge. Other evaluation results, incident reports, credible warnings, incidents that were demonstrated to be misuse or information provided by other States could create a higher foreseeability of a risk. It should be noted that it is not sufficient for a feasibility study to be reported to devise a plan for how to avoid a specific future harm. In a similar fashion the idea of feasible measures should be situation-specific. Reporting obligations, assisting investigations, controls, incident-response processes, or restrictions on the use of materials aimed at known serious misuse are examples of measures. Technology policy alone cannot determine what, if anything, is required under international law. This is dependent on the obligation concerned, State jurisdiction and powers, possibility and severity of the risk, and proportionality of the responses. "Artificial Intelligence has never replaced people

8.4 What AI does not establish

AI does not replace people. AI does not create a presumption that all breakdowns, biased answers or improper usage by a data developer, cloud service provider or user are "internationally wrongful acts" of the location where the developer, cloud provider or user resides. Also, the '[algorithmically opaque] does' not diminish nor means proof of the elements of an international obligation are absent. The application of an obligation to prevent should not be defeated by that an algorithm mediates the risk if an existing international duty does.

9. LIMITS, OBJECTIONS AND THE STATUS OF THE PROPOSED FRAMEWORK

9.1 Objection: due diligence is too vague

Objection; "Too Vague" The frequency of the proposed medicine is reasonable since a simple formula does not exist for the standards of reasonableness found in international law. Vagueness, however, is not dealings only exclusive to due diligence. The answer is not to impose a rule that the sources reject; it is to look at those factors that determine the ease of administration of the standard by the courts. The 4-part structure recommended here (the legal basis, the gathering of information, the feasibility and the seriousness that is legally recognized) is not more precise than the sources justify.

9.2 Objection: the duty would impose impossible burdens

Capacity is relevant to the conduct required, particularly where the duty is one of means rather than result. The Bosnia Genocide judgment demonstrates that capacity to influence may affect the intensity of the duty. The same reasoning may be relevant in cyber contexts, but it should not be converted into a universal rule that excuses States simply because they have limited resources. Capacity must be assessed together with the legal powers and risk faced by the State.

9.3 Objection: public attribution is political

Public attribution can be political and technically uncertain. It should not be treated as equivalent to judicial attribution. At the same time, a State may receive information through diplomatic or technical channels that is relevant to its knowledge of a risk even if the evidence would not establish attribution of the underlying operation to a particular State. The distinction between attribution and notice is therefore important.

9.4 Objection: only a new treaty can solve cyber and AI risks

cyber and AI risks are possible solutions only by a new treaty A treaty can help clarify some terms, develop cooperation tool sets and set sector-specific standards. However, the loss of a new treaty does not give license for the remainder of the time to ignore existing international law. On the other hand, scholars would not have grounds to assume that the lack of a treaty gives them permission to say anything they like becomes law. A middle ground is found between them

9.5 The status of the proposed framework

It is noted that the four part framework is not equivalent to a pronouncement by the ICJ of a general cyber rule of this nature. The value of its holds methodology, in that it allows future cases, and State practice, to be measured in a consistent way, yet maintains the separation between established law and progress development. This is especially the case because the current examination of the general content of due diligence, as carried out by the International Law Commission, identifies that there is an ongoing examination of that content.

10. IMPLICATIONS FOR GENERAL INTERNATIONAL LAW

The Rights of Children in the Public Interest (ROKPI) This cyber debate is representative of a general characteristic of general international law. The facts to which a rule applies can change as the result of any technological development without changing the legal characteristics of the rule. Corfu Channel was interested in mines and Pulp Mills in an industrial plant, the Genocide case in mass atrocity. It is not because cyber operations are akin to mines, factories or genocide that they are of interest in cyberspace. It occurs because it deals with recurring legal issues with regard to knowledge, prevention, capacity and the use of territory or jurisdiction which could create new factual scenarios. Simultaneously, analogical reasoning is bounded up. There is a problem with transferring a rule from one regime to another without accounting for its origin, protected interests and conditions of breaches. It is therefore far from settled whether due diligence is deemed to be legally international or the general existence of due-diligence techniques. The proper scholarly exercise should be to determine the paragraphs where the analogy is effectively accepted as legitimate and those where it will require more State practice or development of treaties. The 2025 UN OEWG and 2026 Global Mechanism closure will provide an institutional forum for continued discussion and development of these questions. The mechanism has a future role in helping States state with precision their views on the application of international law in cyber operations.

The ILC's due diligence project could also help to spread knowledge of due diligence in other areas of international law. As of September 2026, both processes are yet to create any definitive cyber-specific rule of due diligence. That itself should not be looked upon as a vacuum of law but as a good opportunity for careful doctrinal development. Scholarship, as it is used here, is a methodological implication. Statements regarding cyber law should specify if it is in regard to *lex lata*, circumstantial development or suggestions for progressive development. This applied learning is to be carried out in the same discipline as AI scholarship. The benefit of this vocabulary is that it distinguishes between the elements that are fixed by the sources and those the author attempts to add to the text.

11. CONCLUSION

The article has explored the possibility of drawing a framework of due-diligence on both the part of general international law and due-diligence in the context of serious transboundary cyber harm and in respect of State-led algorithmic risk. The analysis leads to three conclusions. First, the term "first due" is a accepted technique of International law. Finally, the work of the ICJ, in the e.g. Corfu Channel cases, the environmental prevention jurisprudence and the Genocide judgment of the ICJ, and the ongoing activities of the International Law Commission, show how international law can impose obligations of conduct toward risks a State does not directly create itself. Second, the principles of due diligence on cyberspace are legally potentially feasible but not entirely established as a customary rule. UN Confirms international law as applicable in cyber. In the United Kingdom, it has expressly taken the position that State practice "up to now" does not meet the requirement of a very specific rule, whereas State positions as in the Netherlands have tended to back up a Cyber Due Diligence Obligation. Based on this reasoning, a qualified argument can be made for relying on the principles already available in international law, but conflicting proposals are offered concerning the actual customary obligations and the evolution of the rules of cyber due diligence. Third, Artificial Intelligence does not provide an excuse to disregard the concept of international law, and not an excuse to breach it, either. If a State utilizes an AI system, ordinary attribution and breach rules are in play. The claim for due-diligence must be based on the existence of a "primary obligation", a "legally relevant connection" (the plaintiff had to receive information that counts as a connection to the internationally guaranteed right or interest), a

legally-duly known or foreseeable relationship between the information provided and the acts of the applicant or the conduct that is at issue, and a serious violation of the right or interest guaranteed by the international agreements. The proposed four-part framework proposed in the article is therefore best interpreted in terms of a disciplined approach to the analysis and not a new customary rule. Questions raised include: Is there a legal relationship, did the State have, or should it have, been aware of the relevant risk, were reasonable and feasible measures available and should the risk or harm be considered to be within the scope and threshold of any applicable international obligation? This system maintains the separation of attribution from omission whilst not granting its opponent the perfect defence of non-attribution. State usage, case law, institutional development and national legal positions, more clearly defined and expressed, will be the basis for the further development of the law. The upcoming work of the International Law Commission in 2026 is important, as are also the new forums set up under the UN Global Mechanism. So far, the best legal case is that cyberspace is not regulated and that there is no currently established universal rule of 'due diligence' with regard to every type of harm from a cyberspace or algorithm. The more correct view would be that general international law includes 'constants' of prevention whose use to recently emerging technologies is to be made and substantiated in the case-to-case manner by means of the legal grounds.

REFERENCES

- Akande, D., Coco, A., & de Souza Dias, T. (2022). Drawing the cyber baseline: The applicability of existing international law to the governance of information and communication technologies. *International Law Studies*, 99(1).
- Australia. Department of Foreign Affairs and Trade. (2021). Australia's international cyber and critical technology engagement strategy: Annex B—Australia's position on how international law applies to State conduct in cyberspace.
- Chesterman, S. (2020). Artificial intelligence and the limits of legal personality. *International & Comparative Law Quarterly*, 69(4), 819–844. <https://doi.org/10.1017/S0020589320000366>
- Crawford, J. (2013). *State responsibility: The general part*. Cambridge University Press.
- Delerue, F. (2020). *Cyber operations and international law*. Cambridge University Press. <https://doi.org/10.1017/9781108780605>
- Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent State practice. *American Journal of International Law*, 112(4), 583–657. <https://doi.org/10.1017/ajil.2018.86>
- Gattini, A. (2007). Breach of the obligation to prevent and reparation thereof in the ICJ's Genocide judgment. *European Journal of International Law*, 18(4), 695–713. <https://doi.org/10.1093/ejil/chm038>
- International Court of Justice. (1949). *Corfu Channel (United Kingdom v. Albania)*, Merits, Judgment, I.C.J. Reports 1949, p. 4.
- International Court of Justice. (1980). *United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran)*, Judgment, I.C.J. Reports 1980, p. 3.
- International Court of Justice. (1986). *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment, I.C.J. Reports 1986, p. 14.
- International Court of Justice. (1996). *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, I.C.J. Reports 1996, p. 226.
- International Court of Justice. (2007). *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro)*, Judgment, I.C.J. Reports 2007, p. 43.
- International Court of Justice. (2010). *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment, I.C.J. Reports 2010, p. 14.
- International Court of Justice. (2015). *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua)*, Judgment, I.C.J. Reports 2015, p. 665.
- International Law Commission. (2001). Draft articles on responsibility of States for internationally wrongful acts, with commentaries. *Yearbook of the International Law Commission*, 2001, Vol. II, Part Two.

- International Law Commission. (2001). Draft articles on prevention of transboundary harm from hazardous activities, with commentaries. Yearbook of the International Law Commission, 2001, Vol. II, Part Two.
- International Law Commission. (2024). Due diligence in international law: Syllabus by Penelope Ridings. Annex II to the Report of the International Law Commission on the work of its seventy-fifth session.
- International Law Commission. (2026). First report on due diligence in international law by Penelope Ridings, Special Rapporteur (A/CN.4/792).
- International Law Commission. (2026). Report on the work of the seventy-seventh session, Chapter XI: Due diligence in international law (A/81/10).
- McGregor, L., Murray, D., & Ng, V. (2019). International human rights law as a framework for algorithmic accountability. *International & Comparative Law Quarterly*, 68(2), 309–343. <https://doi.org/10.1017/S0020589319000046>
- Maas, M. M. (2019). International law does not compute: Artificial intelligence and the development, displacement or destruction of the global legal order. *Melbourne Journal of International Law*, 20(1), 29–57.
- Milanović, M. (2006). State responsibility for genocide. *European Journal of International Law*, 17(3), 553–604. <https://doi.org/10.1093/ejil/chl019>
- Netherlands. Ministry of Foreign Affairs. (2019). International law in the cyber domain.
- Norway. Ministry of Foreign Affairs. (2021). Norwegian positions on selected questions of international law relating to cyberspace.
- Risse, M. (2019). Human rights and artificial intelligence: An urgently needed agenda. *Human Rights Quarterly*, 41(1), 1–16. <https://doi.org/10.1353/hrq.2019.0000>
- Roguski, P. (2020). Application of international law to cyber operations: A comparative analysis of States' views. The Hague Program for Cyber Norms.
- Sands, P., Peel, J., Fabra, A., & MacKenzie, R. (2018). *Principles of international environmental law* (4th ed.). Cambridge University Press.
- Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations* (2nd ed.). Cambridge University Press.
- Schmitt, M. N., & Vihul, L. (2017). Respect for sovereignty in cyberspace. *Texas Law Review*, 95(7), 1639–1670.
- United Kingdom. Foreign, Commonwealth & Development Office. (2021). Application of international law to States' conduct in cyberspace: UK statement.
- United Nations. (2013). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (A/68/98).
- United Nations. (2015). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (A/70/174).
- United Nations. (2021). Report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (A/75/816).
- United Nations. (2021). Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security (A/76/135).
- United Nations. (2025). Final report of the Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (A/80/257).

◆ Funding

This research received no external funding

◆ Conflict of Interest

The authors declare that they have no known financial or personal conflicts of interest that could have influenced the work reported in this paper.

◆ Data Availability Statement

All data used in this study are derived from publicly available legal sources, including statutes, judicial decisions, treaties and published academic literature cited in the references. No new datasets were generated or analysed.

◆ Ethical Statement

Ethical approval was not required because this study is based exclusively on publicly available legal documents, judicial decisions, treaties and published literature, and did not involve human participants, animals or confidential data.

◆ AI Use Disclosure

Generative artificial intelligence tools were used in a limited and assistive capacity during the preparation of this manuscript, primarily for idea development, language refinement, and grammatical correction. The authors retain full responsibility for the originality, accuracy, analysis, interpretation, and final content of the manuscript.

JOURNAL POLICIES JuriSocial Journal of International Law

OPEN ACCESS & LICENCE

All articles are freely available on publication under CC BY-NC 4.0. Readers may share and adapt the work for non-commercial purposes with proper attribution.

COPYRIGHT

Authors retain copyright and grant JJIL the right of first publication.

PEER REVIEW

Every research article undergoes double-blind peer review by at least two independent reviewers.

PUBLICATION ETHICS

JJIL follows the Committee on Publication Ethics (COPE) Core Practices and guidelines.

PLAGIARISM POLICY

All submissions are screened with similarity-detection software; plagiarism in any form leads to rejection.

GENERATIVE AI POLICY

AI tools cannot be listed as authors. Any substantive use must be disclosed; authors remain fully responsible for the content.

CORRECTIONS & RETRACTIONS

Errors are corrected through published corrigenda; retractions follow COPE guidelines.

ARCHIVING & INDEXING

Content is preserved through [PKP Preservation Network / LOCKSS]. DOIs are registered with Crossref.

PUBLICATION CHARGES

No article publishing fee charged

DISCLAIMER

The views expressed are those of the authors and do not necessarily reflect the views of the editors or the publisher.

HOW TO CITE THIS ARTICLE

Submissions & enquiries editor@jjil.jurisocial.org