INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CYBERSECURITY AS DUE DILIGENCE IN REDEFINING THE FULL PROTECTION AND SECURITY STANDARD

AUTHORS - SHUBHAM SHARMA & DEEKSHA RAMPAL

STUDENTS AT NATIONAL LAW INSTITUTE UNIVERSITY, BHOPAL

BEST CITATION - SHUBHAM SHARMA & DEEKSHA RAMPAL, CYBERSECURITY AS DUE DILIGENCE IN REDEFINING THE FULL PROTECTION AND SECURITY STANDARD, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 968-980, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

International investment law is changing as investments increasingly rely on digital systems, data, and technology rather than physical assets. This shift creates new risks, especially from cyber threats such as data breaches and hacking, which are not fully addressed under the traditional understanding of the Full Protection and Security (FPS) standard. FPS has mainly been seen as a duty to protect investments from physical harm, but this approach is no longer sufficient in the digital age. This paper argues that cybersecurity should be treated as an essential part of the State's duty of due diligence under the FPS standard. While arbitral tribunals have started to recognise that FPS applies to intangible and digital investments, they have not clearly defined what States are actually required to do in cases involving cyber risks. This lack of clarity has led to inconsistent decisions and uncertainty. To solve this problem, the paper proposes a structured, risk-based framework for cybersecurity due diligence. It suggests that States should follow basic cybersecurity measures, take stronger steps for high-risk sectors, and respond effectively to cyber incidents. The paper also emphasises the need to consider technical standards and the capacity of different States.

I. Introduction

International investment law is undergoing a structural transformation driven by the changing nature of foreign direct investment (FDI) in the digital economy. The legal framework governing investment protection, particularly through bilateral investment treaties (BITs), was originally designed in a context where investments were predominantly tangible, territorially anchored, and exposed to risks such as expropriation, civil unrest, and physical destruction. Within this framework, the obligation to provide full protection and security (FPS) ged as a core standard, traditionally understood as requiring host States to exercise due diligence in safeguarding investments against physical harm and maintaining public order.[2293]

This traditional conception reflects what may be described as a "physicalist" orientation of the FPS standard. The duty of protection developed in response to threats that were visible, localised, and attributable, such as violence against property or failure of law enforcement. However, the structure of investment has fundamentally changed. Contemporary investments increasingly consist of intangible assets, including proprietary data, digital platforms, algorithms, and confidential business information. These assets derive their value not from physical presence but from their integration within digital systems and

[2293] Rudolf Dolzer & Christoph Schreuer, *Principles of International Investment Law* 1–3 (2d ed. 2012).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

networks.[2294]

The transformation of investment has also altered the nature of risk. Cyber threats, including data breaches, ransomware attacks, and cyber espionage, present forms of harm that differ significantly from those contemplated under traditional investment law. Such threats are often transnational, technologically complex, and difficult to attribute to specific actors. Moreover, they frequently exploit vulnerabilities in infrastructure that is owned, regulated, or influenced by the host State, including public databases, financial systems, and sector-specific digital platforms. As a result, harm to foreign investment may arise not from direct State interference, but from deficiencies in State capacity, regulatory oversight, or institutional preparedness.

Despite these developments, the FPS standard has not been sufficiently adapted to address the realities of the digital environment. While the concept of due diligence continues to underpin the standard, its content remains underdefined in the context of cybersecurity. The prevailing reliance on general formulations such as "reasonable measures" provides limited guidance in assessing State responsibility for preventing or responding to cyber incidents, particularly given the evolving and technical nature of such risks.

This paper argues that the FPS standard must be reconceptualised in light of the digital transformation of investment. Specifically, it contends that cybersecurity should be understood as a central component of the State's due diligence obligation under FPS. This requires the development of a structured, risk-based framework that defines the content of due diligence by reference to the nature of digital risks, the characteristics of the investment, and the capacity of the host State. By addressing this gap, the paper seeks to contribute to a more coherent and predictable application of investment protection standards in the digital age.

II. Cyber Threats And State Responsibility

The transformation of foreign investment from a predominantly physical to a digital phenomenon has altered both the nature of protected assets and the structure of risks to which such investments are exposed. Traditional investment risks were typically associated with identifiable State conduct, including expropriation, regulatory interference, or failure to maintain public order. These risks were event-based, localised, and attributable to specific acts or omissions. In contrast, digital investments are exposed to diffuse, systemic, and technologically complex threats that do not fit easily within these established categories.

A defining feature of contemporary investment is its reliance on intangible assets, including data, proprietary software, algorithms, and digital platforms. The value of these assets depends on their integrity, confidentiality, and continuous availability, all of which are vulnerable to cyber intrusion. Unlike physical assets, digital investments are not confined to a single location and often operate across interconnected networks that span multiple jurisdictions.[2295] This creates a risk environment in which harm may arise from vulnerabilities embedded within the broader digital ecosystem rather than from direct interference with a specific asset.

A significant dimension of this vulnerability stems from the dependence of investors on infrastructure that is owned, regulated, or influenced by the host State. Public sector databases, financial regulatory systems, licensing platforms, and digital governance frameworks form part of the operational environment within which investments function. Weaknesses in these systems, whether arising from inadequate cybersecurity safeguards, outdated infrastructure, or institutional deficiencies, can expose foreign investments to risks that are beyond the direct control of the

[2294] UNCTAD, *World Investment Report 2021: Investing in Sustainable Recovery* 141–45 (2021).

[2295] UNCTAD, *Digital Economy Report 2021: Cross-Border Data Flows and Development* 65–70 (2021).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

investor.[2296] In this sense, the protection of investment becomes closely linked to the State's capacity to manage and secure its digital environment.

Cyber threats further complicate this landscape by introducing actors and methods that differ fundamentally from traditional sources of harm. Attacks may be carried out by decentralised networks of hackers, organised cybercriminal groups, or politically motivated entities operating across jurisdictions.[2297] Such actors often exploit systemic vulnerabilities rather than targeting specific assets, and their conduct is frequently difficult to attribute under existing rules of international law.[2298] This weakens the traditional reliance on attribution as the primary basis for engaging State responsibility.

As a result, the analytical focus shifts from identifying the author of the harm to assessing the conduct of the host State. In this context, the principle of due diligence assumes central importance. International law recognises that States may incur responsibility not only for their own acts but also for failing to take reasonable measures to prevent harm caused by private actors within their jurisdiction.[2299] This principle has been applied across multiple domains, including environmental protection, human rights, and transboundary harm, and reflects a broader expectation that States must exercise vigilance in managing risks that are foreseeable and preventable.[2300]

However, the application of due diligence to cyber threats presents distinct challenges. Cyber risks are continuous rather than episodic, and their prevention requires ongoing technical and institutional measures rather than isolated acts of protection. Moreover, the assessment of due diligence in this context is inherently complex, as it involves evaluating the adequacy of cybersecurity frameworks, regulatory mechanisms, and institutional capacity.[2301] The absence of commonly accepted legal benchmarks further complicates this analysis, leaving tribunals with limited guidance in determining whether a State has acted with sufficient diligence.

This divergence between traditional conceptions of investment risk and the realities of cyber threats reveals a fundamental limitation in the existing framework of investment protection. While digital assets are increasingly central to foreign investment, the legal standards governing their protection remain anchored in assumptions derived from physical security. The result is a mismatch between the nature of the harm and the doctrinal tools available to address it.

Accordingly, the central issue is not merely whether cyber-related harm falls within the scope of investment protection, but how the content of State obligations should be defined in this context. The absence of a structured and context-sensitive approach to cybersecurity due diligence creates uncertainty in both the interpretation and application of the FPS standard. This gap necessitates a closer examination of the legal foundations of FPS and its capacity to adapt to the demands of the digital age.

III. Legal Architecture Of The Fps Standard

A. Historical foundations of the obligation of protection

The obligation to provide protection to foreign persons and property predates the modern framework of bilateral investment treaties and is rooted in classical international law governing the treatment of aliens. Early jurists such as Emer de Vattel and Christian Wolff conceptualised this obligation as arising from the sovereign authority of the State over its territory, coupled with a duty to ensure the safety of those admitted within it.[2302] Protection

[2296] OECD, *Digital Security Risk Management for Economic and Social Prosperity* 17–22 (2015).
[2297] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 3–5 (Michael N. Schmitt ed., 2017).
[2298] Id. at 79–83.
[2299] Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9).
[2300] James Crawford, *State Responsibility: The General Part* 217–20 (2013).
[2301] Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations* 45–52 (2014).
[2302] Emer de Vattel, *The Law of Nations* bk. II, ch. VIII (1758); Christian Wolff, *Jus Gentium Methodo Scientifica Pertractatum* (1764).

was thus linked to the State's control over internal order and its capacity to prevent harm through the exercise of public authority.

This understanding was reflected in early legal instruments and State practice, where "security" was primarily associated with protection against physical injury, violence, and deprivation of property. Nineteenth-century treaties of friendship, commerce, and navigation reinforced this orientation by emphasising the safeguarding of foreign property within territorial boundaries.[2303] The emergence of the full protection and security (FPS) standard in modern investment treaties inherited this conceptual foundation, embedding a model of protection centred on physical integrity.

However, while the historical basis of the obligation provides conceptual clarity, it also reveals its limitations. The traditional focus on physical protection was shaped by a context in which threats to investment were tangible and localised. As investment has evolved, this foundation has proven insufficient to address more complex and systemic forms of risk.

B. Customary international law and the due diligence standard

The FPS obligation is closely linked to the broader customary international law principle of due diligence, which forms part of the international minimum standard of treatment. This principle requires States to take reasonable measures to prevent harm within their territory, including harm caused by private actors, where such harm is foreseeable.[2304] It does not impose strict liability, but instead evaluates State responsibility based on the adequacy of its conduct.

The International Court of Justice, in *Corfu Channel*, articulated this principle by recognising that States have an obligation not to knowingly allow their territory to be used for acts that cause harm to others.[2305] This formulation has been interpreted as establishing a duty of vigilance, requiring States to act where they knew or ought to have known of a risk.

The International Law Commission (ILC) Articles on State Responsibility further reinforce this understanding by recognising that a breach of an international obligation may arise from an omission where a State fails to take appropriate preventive measures.[2306] The accompanying commentary emphasises that due diligence is a variable standard, dependent on factors such as the level of risk, the importance of the protected interest, and the means available to the State.[2307]

This flexibility allows the due diligence standard to adapt to different contexts. However, it also introduces indeterminacy, as the content of the obligation is not fixed and must be defined in relation to specific circumstances. In the context of cybersecurity, this raises the question of how such a standard should be operationalised in a technologically complex and rapidly evolving environment.

C. Treaty formulation and comparative bit models

The FPS standard is most commonly articulated in bilateral investment treaties, where it is typically expressed in broad and open-ended terms. Many BITs provide that investments shall enjoy "full protection and security" without further elaboration, leaving its interpretation to arbitral tribunals.[2308] This drafting technique has enabled flexibility but has also contributed to divergent interpretations.

Different treaty models reflect varying approaches to the scope of FPS. The 2012 United States Model BIT adopts a restrictive formulation by linking FPS to the customary international law minimum standard of treatment.[2309] This

[2303] Kenneth J. Vandevelde, *Bilateral Investment Treaties: History, Policy, and Interpretation* 25–30 (2010).
[2304] Crawford, supra note 8, at 217.
[2305] Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22.
[2306] Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 2, [International Law Commission], 2001 Y.B. Int'l L. Comm'n, vol. II (Part Two).
[2307] Id. art. 2 cmt. 10.
[2308] Jeswald W. Salacuse, *The Law of Investment Treaties* 236–38 (2d ed. 2015).
[2309] 2012 U.S. Model Bilateral Investment Treaty art. 5.

approach seeks to confine the standard to traditional due diligence obligations and prevent its expansion into broader guarantees of legal or regulatory stability.

In contrast, the United Kingdom Model BIT employs an unqualified formulation of FPS, which has been interpreted as supporting a more expansive understanding of the obligation. This approach allows tribunals greater interpretative flexibility and facilitates the extension of FPS beyond physical protection.

A markedly restrictive approach is evident in the 2016 Indian Model BIT, which explicitly limits FPS to physical security and excludes its application to other forms of protection.[2310] This formulation reflects a deliberate policy choice to prevent expansive interpretations that could impose liability for regulatory or systemic failures, including those arising in digital contexts.

At the same time, developments in Chinese treaty practice and domestic investment law suggest an increasing emphasis on the protection of technological assets and intellectual property.[2311] While not explicitly framed in cybersecurity terms, this trend indicates a gradual recognition of the importance of protecting intangible and digital interests within the investment framework.

These variations demonstrate that the scope of FPS is not uniform but is shaped by treaty design and State policy choices. They also highlight the absence of a consistent approach to the protection of digital investments across different treaty regimes.

D. The ICSID framework and the protection of digital investments

The interpretation and application of the FPS standard operate within the broader framework of the ICSID Convention, which provides the primary institutional mechanism for the resolution of investor-State disputes. Although the Convention does not define substantive standards such as FPS, its jurisdictional provisions, particularly Article 25(1), play a critical role in shaping the scope of protected investments.

Article 25(1) refers to "any legal dispute arising directly out of an investment," without defining the term "investment."[2312] As noted in leading commentaries, this deliberate omission was intended to allow for flexibility and accommodate evolving forms of economic activity.[2313] This has enabled tribunals to adopt a broad interpretation of investment, encompassing both tangible and intangible assets.

In the context of digital investments, this flexibility raises important questions regarding territoriality and control. Digital assets are often not tied to a single physical location, and their operation may involve servers, data flows, and infrastructure distributed across multiple jurisdictions. Scholarship suggests that territorial links may be established through factors such as the location of servers, the deployment of capital within the host State, or regulatory requirements imposed on the investor.[2314]

The ICSID framework also influences the applicable law in investment disputes. Under Article 42, tribunals apply both the law of the host State and relevant rules of international law.[2315] This creates a layered legal structure in which domestic cybersecurity regulations may interact with international obligations under FPS. The result is a complex interplay between national and international legal regimes in determining the scope of State responsibility.

E. Structural indeterminacy in the legal architecture

The foregoing analysis reveals a fundamental characteristic of the FPS standard: its legal architecture is inherently open-ended. The combination of flexible treaty language,

[2310] Model Text for the Indian Bilateral Investment Treaty art. 3.2 (2016).
[2311] Wenhua Shan, *The Legal Framework of EU-China Investment Relations* 112–15 (2016).
[2312] Convention on the Settlement of Investment Disputes Between States and Nationals of Other States art. 25(1), Mar. 18, 1965, 575 U.N.T.S. 159.
[2313] Christoph H. Schreuer et al., *The ICSID Convention: A Commentary* 116–18 (2d ed. 2009).
[2314] UNCTAD, *World Investment Report 2021*, supra note 2, at 142-145.
[2315] ICSID Convention art. 42.

variable due diligence standards, and evolving interpretations has allowed the standard to adapt to new forms of investment. However, this flexibility has come at the cost of doctrinal precision.

While the scope of FPS has expanded to include intangible and potentially digital assets, the content of the obligation has not been correspondingly clarified. The absence of defined benchmarks for assessing State conduct creates uncertainty in the application of the standard, particularly in contexts involving complex and technical risks such as cybersecurity.

This structural indeterminacy forms the basis for the subsequent analysis. It explains how the FPS standard has been able to expand in scope while remaining underdeveloped in content, and it highlights the need for a more structured approach to defining due diligence obligations in the digital age.

IV. Doctrinal Expansion Of The FPS Standard And Its Conceptual Limits

A. The shift from physical protection to systemic stability

The full protection and security (FPS) standard has undergone a significant transformation from its original focus on physical protection to a broader concern with systemic stability. Initially, the obligation was tied to the State's duty to prevent violence and maintain public order, reflecting a context in which investment risks were primarily physical and territorially confined.

Over time, arbitral interpretation has moved beyond this narrow conception. Tribunals have acknowledged that the security of an investment may be undermined by failures in the legal and administrative framework, even in the absence of physical harm. In *Wena Hotels Ltd. v. Egypt*, the tribunal emphasised that the State's obligation includes taking reasonable steps to ensure the protection of the investment within its broader operating environment.[2316] Similarly, in *Lauder v. Czech Republic*, the tribunal recognised that regulatory conduct affecting the functioning of the investment may fall within the scope of protection.[2317]

This evolution reflects a shift from an event-based model of protection to a condition-based one. The focus is no longer limited to preventing discrete acts of harm but extends to maintaining an environment in which the investment can function securely. However, this expansion has occurred incrementally and without a clear articulation of its doctrinal boundaries.

B. The inclusion of intangible and technological assets

The expansion of FPS is closely connected to the growing prominence of intangible assets in international investment. Contemporary investments often consist of intellectual property, digital infrastructure, and data-driven systems, which are fundamentally different from traditional physical assets.[2318]

These assets are particularly vulnerable to disruptions that do not involve physical interference. Cyber intrusions, data breaches, and system failures can compromise the value of an investment without causing any tangible damage. This challenges the traditional understanding of "security" and requires a re-evaluation of the scope of State obligations.

Arbitral practice has implicitly adapted to this shift by recognising that the protection of investment extends to the conditions necessary for its operation. In *Ampal-American Israel Corp. v. Egypt*, the tribunal suggested that failures affecting the operational environment of the investment may engage the FPS standard.[2319] This indicates a movement towards recognising functional and technological dimensions of protection.

[2316] Wena Hotels Ltd. v. Arab Republic of Egypt, ICSID Case No. ARB/98/4, Award ¶ 84 (Dec. 8, 2000).
[2317] Ronald S. Lauder v. Czech Republic, UNCITRAL, Final Award ¶ 308 (Sept. 3, 2001).
[2318] OECD, *Digital Security Risk Management*, supra note 4, at 17–22.
[2319] Ampal-Am. Israel Corp. v. Egypt, ICSID Case No. ARB/12/11, ¶ 261.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

However, while the scope of FPS has expanded to include such interests, the standard has not been recalibrated to address their specific vulnerabilities. The absence of a tailored framework for protecting digital and technological assets creates uncertainty in the application of the standard.

C. The absence of defined obligations and the emerging gap

The expansion of the FPS standard has not been accompanied by a corresponding development in its content. Tribunals continue to rely on general formulations such as "due diligence" and "reasonable measures," without specifying the concrete obligations that arise from these concepts.[2320]

This lack of precision has resulted in a fragmented body of jurisprudence. Different tribunals have adopted varying interpretations of the standard, often influenced by the specific facts of the case rather than by consistent legal principles. The absence of clearly defined benchmarks makes it difficult to assess whether a State has fulfilled its obligations, particularly in complex and technical contexts.

The problem becomes more acute in the context of cybersecurity. Digital risks require continuous monitoring, specialised expertise, and proactive regulatory measures. Generalised standards developed in the context of physical protection are ill-equipped to address these requirements.[2321] As a result, there is a growing mismatch between the expanded scope of FPS and the tools available to implement it.

This mismatch creates a conceptual gap within the FPS framework. While the standard now extends to intangible and technologically complex forms of investment, it lacks the doctrinal clarity necessary to guide its application. The result is uncertainty for both investors and host States, as the boundaries of responsibility remain undefined.

Accordingly, the evolution of the FPS standard has reached a stage where further development requires a more structured articulation of due diligence. Without such clarification, the standard risks becoming either indeterminate or inconsistently applied in cases involving digital risk. The next section addresses this issue by examining the nature of due diligence and its limitations in the cybersecurity context.

V. Due Diligence And Cybersecurity: The Missing Standard

Due diligence under the full protection and security (FPS) standard operates as a core principle through which State responsibility is assessed in cases involving harm to foreign investment. It reflects the broader rule in international law that a State is not automatically liable for injury occurring within its territory, but may incur responsibility where it fails to exercise reasonable care in preventing foreseeable harm.[2322] This positions due diligence as an obligation of conduct, requiring the State to demonstrate that it has taken appropriate measures within its capacity.

Arbitral jurisprudence has consistently affirmed this understanding. In *Pantechniki S.A. Contractors & Engineers v. Albania*, the tribunal emphasised that the obligation of protection must be assessed in light of the specific circumstances, including the State's resources and the conditions prevailing at the time.[2323] Similarly, in *Noble Ventures, Inc. v. Romania*, it was clarified that FPS does not impose strict liability but requires the State to act with vigilance and take reasonable steps to protect the investment.[2324]

At the same time, tribunals have recognised that due diligence is not a static concept. In *EDF (Services) Ltd. v. Romania*, the tribunal noted that the content of the obligation evolves in response to changing economic and

[2320] Andrew Newcombe & Lluís Paradell, *Law and Practice of Investment Treaties* 297–300 (2009).
[2321] Tallinn Manual 2.0, supra note 5, at 3–5.
[2322] Crawford, supra note 8, at 216–18.
[2323] Pantechniki S.A. Contractors & Eng'rs v. Republic of Albania, ICSID Case No. ARB/07/21, Award ¶ 81 (July 30, 2009).
[2324] Noble Ventures, Inc. v. Romania, ICSID Case No. ARB/01/11, Award ¶ 164 (Oct. 12, 2005).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

technological conditions.[2325] This recognition is critical in the context of digital investment, where the nature of risk has fundamentally transformed.

However, despite this acknowledgment of flexibility, arbitral practice has not translated this evolution into concrete standards. Due diligence remains articulated through abstract formulations such as "reasonable measures," without further specification. As a result, while the principle is well-established, its operational content remains underdeveloped.

A. Cybersecurity and the transformation of due diligence obligations

The application of due diligence to cybersecurity fundamentally alters both the nature and scope of the obligation. Cyber risks are not discrete or exceptional events; they are continuous, evolving, and often foreseeable. This requires a shift from reactive protection to proactive risk management.

In this context, due diligence must encompass three interrelated dimensions. First, it requires preventive measures, including the establishment of cybersecurity frameworks, protection of critical infrastructure, and implementation of baseline security standards. Second, it involves monitoring and detection, ensuring that the State possesses institutional mechanisms capable of identifying and responding to emerging threats. Third, it extends to post-incident response, requiring timely action to mitigate harm and investigate breaches.

Arbitral jurisprudence provides partial support for this expanded understanding. In *Jan de Nul N.V. v. Egypt*, the tribunal considered not only the occurrence of harm but also the adequacy of the State's response in assessing compliance with its obligations.[2326] In *Ampal-American Israel Corp. v. Egypt*, the tribunal evaluated the State's failure to take sufficient preventive measures in protecting infrastructure essential to the investment.[2327] These decisions indicate that due diligence encompasses both preventive and reactive elements.

However, the cyber context introduces an additional layer of complexity. Unlike traditional risks, cyber threats often originate from non-state actors operating across jurisdictions, making attribution difficult. In such cases, the focus shifts from identifying the author of the harm to evaluating whether the State has exercised sufficient diligence in managing the risk environment. This aligns with broader principles of international law, which impose responsibility for failure to prevent harm where the State knew or ought to have known of the risk.[2328]

Despite this conceptual alignment, the application of due diligence to cybersecurity remains incomplete. Tribunals have not systematically addressed how preventive, monitoring, and response obligations should be defined in relation to digital infrastructure. As a result, the standard remains conceptually adaptable but practically underdeveloped.

B. The absence of operational benchmarks and doctrinal coherence

The central deficiency in the current framework is the absence of operational benchmarks for assessing due diligence in the cyber domain. While tribunals recognise that States must take "reasonable measures," they rarely specify what those measures entail, particularly in technologically complex contexts.

This absence of specificity stands in contrast to developments in other areas of international law. In environmental law, for example, due diligence has been elaborated through detailed standards relating to risk assessment, prevention, and mitigation.[2329] In the cyber domain, similar guidance exists in the form of soft law instruments and technical frameworks.

[2325] EDF (Servs.) Ltd. v. Romania, ICSID Case No. ARB/05/13, Award ¶ 303 (Oct. 8, 2009).
[2326] Jan de Nul N.V. v. Arab Republic of Egypt, ICSID Case No. ARB/04/13, Award ¶ 157 (Nov. 6, 2008).
[2327] Ampal-Am. Israel Corp. Case, ICSID Case No. ARB/12/11, ¶ 261.
[2328] Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941).
[2329] Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area, Advisory Opinion, 2011 I.T.L.O.S. Rep. 10, ¶ 117.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The Tallinn Manual articulates principles regarding State responsibility for cyber operations, while the UN Group of Governmental Experts (GGE) identifies norms relating to the protection of critical infrastructure and the prevention of harmful cyber activities.

Despite their relevance, these standards have not been integrated into investment arbitration. Tribunals have largely refrained from engaging with technical frameworks such as the NIST Cybersecurity Framework or comparable national standards. This creates a disconnect between the recognition of cyber risk and the tools available to assess State conduct.

The consequences of this gap are evident in the inconsistency of arbitral decisions. Without clear benchmarks, tribunals are left to rely on general notions of reasonableness, leading to divergent interpretations of the FPS standard. This undermines predictability and weakens the normative coherence of the investment regime.[2330]

Moreover, the absence of a structured approach risks distorting the balance between investor protection and State sovereignty. An overly expansive interpretation of due diligence may impose unrealistic obligations on States, while an overly restrictive approach may fail to provide meaningful protection to investors. The lack of doctrinal clarity thus affects both the legitimacy and effectiveness of the FPS standard.

The foregoing analysis demonstrates that due diligence, while conceptually central to the FPS standard, remains insufficiently developed in the context of cybersecurity. The evolution of digital investment has transformed the nature of risk, but the legal framework has not adapted accordingly. The absence of defined benchmarks, combined with the technical complexity of cyber threats, has rendered the current standard inadequate for addressing contemporary challenges.

This gap necessitates a reconceptualisation of due diligence as a structured and context-sensitive obligation. Such a reconceptualisation must integrate technical standards, account for variations in State capacity, and reflect the continuous nature of cyber risk. The following section develops this argument by proposing a risk-based framework for cybersecurity due diligence within the FPS standard.

VI. Structural Gaps In The Existing Framework Of Investment Protection

The preceding analysis demonstrates that while the full protection and security (FPS) standard has expanded to accommodate increasingly complex forms of investment, its doctrinal structure has not evolved at the same pace. The result is a framework that is broad in scope but deficient in operational clarity. This tension becomes particularly acute in the context of cybersecurity, where the assessment of State responsibility requires engagement with continuous, technical, and systemic risks. The existing framework, however, continues to rely on abstract legal formulations and doctrines developed for fundamentally different contexts. These limitations are not incidental but structural in nature, reflecting deeper inconsistencies within the investment protection regime.

A. Indeterminacy of due diligence and inconsistent arbitral practice

The primary structural weakness of the FPS framework lies in the indeterminacy of the due diligence standard. Although tribunals consistently affirm that States are required to take "reasonable measures" to protect investments, there is no agreed methodology for determining what constitutes reasonableness in practice. This lack of precision leaves tribunals with broad interpretative discretion, resulting in divergent and often unpredictable outcomes.

Arbitral jurisprudence illustrates this inconsistency. In *Asian Agricultural Products Ltd. v. Sri Lanka*, the tribunal adopted a relatively deferential approach, assessing the State's conduct in light of its limited capacity during

[2330] Zachary Douglas, *The International Law of Investment Claims* 106–09 (2009).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

internal conflict.[2331] By contrast, in *BG Group plc v. Argentina*, the tribunal engaged in a more exacting evaluation of State measures, suggesting a higher threshold of diligence.[2332] These differences are not merely reflective of factual variation; they point to the absence of a coherent standard guiding the assessment of State conduct.

This indeterminacy is particularly problematic in the context of cybersecurity. Unlike traditional risks, cyber threats require continuous monitoring and proactive management. The absence of clear criteria for evaluating such conduct means that tribunals are left to apply generalised notions of reasonableness to highly technical situations. This not only undermines consistency but also reduces the predictability of the FPS standard, making it difficult for States to calibrate their behaviour and for investors to assess the level of protection available.

B. Absence of Technical Benchmarks and Contextual Differentiation

A second structural gap lies in the failure of the existing framework to incorporate technical benchmarks and contextual factors into the assessment of due diligence. The evaluation of State conduct is typically conducted in abstract terms, without reference to the practical realities of risk management in technologically complex environments.

In the cyber domain, this omission is particularly significant. The adequacy of State measures cannot be assessed without considering the existence of cybersecurity infrastructure, regulatory standards, and institutional capacity. Technical frameworks such as the NIST Cybersecurity Framework and international norms developed through the UN Group of Governmental Experts (GGE) provide detailed guidance on risk management and system resilience.[2333] However, these frameworks remain largely external to investment arbitration and are rarely used as reference points by tribunals.

At the same time, the framework does not adequately account for differences in State capacity. Due diligence is inherently a relative standard, shaped by the resources and capabilities of the State. This principle has been recognised in general international law, where the content of due diligence varies according to the circumstances.[2334] However, arbitral practice has not consistently applied this logic, often evaluating State conduct without sufficient regard to technological or institutional constraints.

The absence of both technical benchmarks and contextual differentiation creates a double deficiency. On one hand, it deprives tribunals of objective criteria for assessing State conduct. On the other hand, it generates uncertainty for States and investors, who lack clarity regarding the expectations imposed by the FPS standard.

C. Doctrinal misfit of state responsibility in cyber context

The limitations of the FPS framework are further exposed when considered in light of general principles of State responsibility. Doctrines such as force majeure and necessity, as codified in the International Law Commission (ILC) Articles, were developed in relation to discrete and exceptional events.[2335] Their application to cybersecurity, which is characterised by continuous and foreseeable risk, is therefore inherently problematic.

The defence of force majeure requires that the event be unforeseeable and beyond the control of the State. In the cyber context, however, many threats arise from known vulnerabilities and persistent risk environments. A failure to address such vulnerabilities is difficult to reconcile with the requirement of unforeseeability, limiting the applicability of the defence.

[2331] Asian Agric. Prods. Ltd. v. Sri Lanka, ICSID Case No. ARB/87/3, Award ¶ 77 (June 27, 1990).
[2332] BG Grp. plc v. Republic of Argentina, UNCITRAL, Final Award ¶¶ 324–326 (Dec. 24, 2007).
[2333] U.N. GGE Report, U.N. Doc. A/70/174 (2015); NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (2018).
[2334] Responsibilities & Obligations of States Sponsoring Persons & Entities, Advisory Opinion, 2011 I.T.L.O.S. Rep. 10, ¶ 117.
[2335] Draft Articles on Responsibility of States for Internationally Wrongful Acts arts. 23–25 (2001).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Similarly, the doctrine of necessity imposes a stringent threshold, requiring that the State's action be the only means of safeguarding an essential interest.[2336] In cyber situations, this condition is rarely satisfied, as States typically have multiple options for responding to threats. Moreover, where the State's own regulatory or institutional deficiencies contribute to the risk, the defence is further weakened.

These limitations reveal a deeper doctrinal misalignment. The existing framework of State responsibility is not designed to address the characteristics of cyber risk, including its persistence, technical complexity, and dependence on infrastructure. As a result, its application does not provide a coherent basis for resolving disputes involving cybersecurity under the FPS standard.

The cumulative effect of these structural gaps is a framework that is ill-suited to address the realities of digital investment. The indeterminacy of due diligence, the absence of technical benchmarks, and the misalignment of State responsibility doctrines collectively undermine the effectiveness of the FPS standard in the cyber context.

These deficiencies cannot be resolved through incremental interpretation alone. What is required is a structured and context-sensitive approach to due diligence, capable of integrating technical standards and adapting to the evolving nature of cyber risk. The following section develops such an approach by proposing a risk-based framework for cybersecurity within the FPS standard.

VII. Towards A Cybersecurity-Based Due Diligence Standard

To address the indeterminacy of the FPS standard in the cyber context, due diligence must be reconceptualised as a structured and risk-based obligation. Rather than relying on abstract notions of "reasonable measures," tribunals should assess State conduct through a tiered framework that reflects the nature of cyber risk and the characteristics of the investment.

At the first level, States must comply with baseline obligations that apply across all sectors. These include the establishment of minimum cybersecurity infrastructure, such as secure data storage protocols, basic encryption standards, and access control mechanisms. The presence of national cybersecurity strategies, incident response teams, and regulatory frameworks governing data protection should form part of this baseline.[2337] The absence of such foundational measures should, in principle, indicate a failure to meet the minimum threshold of due diligence.

At the second level, due diligence must be risk-sensitive, taking into account the nature of the investment and the sector in which it operates. Investments involving critical infrastructure, financial systems, or sensitive personal data require a higher standard of protection than those operating in less sensitive domains. This aligns with the logic of proportionality embedded in international law, where the degree of care expected of the State increases with the gravity and foreseeability of the risk.[2338]

At the third level, the framework must incorporate reactive obligations, focusing on the State's response to cyber incidents. This includes the timeliness and effectiveness of measures taken to contain the breach, investigate its causes, and mitigate its consequences. The failure to act promptly or to coordinate an adequate response may constitute a breach of due diligence, even where the initial attack was not preventable.

This tiered approach transforms due diligence from an abstract standard into a structured method of assessment, enabling tribunals to evaluate State conduct in a more consistent and transparent manner.

[2336] Id. art. 25.

[2337] NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (2018).

[2338] Tarcisio Gazzini, *Interpretation of International Investment Treaties* 192–94 (2016).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

A. Integration of Technical Standards and Contextual Factors

A structured due diligence framework must also incorporate technical benchmarks and contextual considerations. The assessment of State conduct in the cyber domain cannot be meaningfully undertaken without reference to existing standards that define best practices in cybersecurity.

International norms, such as those articulated in the UN Group of Governmental Experts (GGE) reports, provide guidance on the protection of critical infrastructure and the prevention of harmful cyber activities.[2339] Similarly, technical frameworks such as the NIST Cybersecurity Framework outline concrete measures relating to risk identification, protection, detection, response, and recovery. These instruments should be treated as interpretative tools that inform the content of due diligence under the FPS standard.

At the same time, the framework must account for **contextual factors**, particularly the capacity of the host State. Due diligence is not a uniform standard; it varies according to the resources and institutional capabilities available to the State.[2340] A developing State with limited technological infrastructure cannot be expected to meet the same level of sophistication as a technologically advanced State. However, this does not absolve such States of responsibility; rather, it requires that they make reasonable use of the means available to them.

Foreseeability also plays a critical role. Where a State is aware, or ought reasonably to be aware, of specific vulnerabilities or threats, the expectation of diligence increases. The failure to address known risks such as widely publicised software vulnerabilities or repeated cyber incidents targeting a particular sector may constitute a breach of due diligence.

B. A Coherent Standard of Review for Arbitral Tribunals

The effectiveness of a cybersecurity-based due diligence framework ultimately depends on how it is applied by arbitral tribunals. To ensure consistency and predictability, tribunals must adopt a structured standard of review that balances investor protection with State autonomy.

First, tribunals should apply a reasonableness test grounded in the tiered framework outlined above. This involves assessing whether the State's conduct meets baseline obligations, whether it has responded appropriately to the specific risk profile of the investment, and whether it has taken adequate measures in response to any incident. This approach allows for a nuanced evaluation of State conduct without imposing strict liability.

Second, tribunals should recognise a margin of appreciation for States in determining how to implement cybersecurity measures. Given the technical complexity and evolving nature of cyber risk, States must retain a degree of discretion in designing and implementing their regulatory frameworks.[2341] However, this discretion is not unlimited; it is constrained by the requirement that the measures adopted be reasonable and proportionate in light of the risks involved.

Third, tribunals should avoid conflating due diligence with outcome-based liability. The occurrence of a cyber incident does not, in itself, establish a breach of the FPS standard. The focus must remain on the adequacy of State conduct, assessed in light of the structured framework and relevant contextual factors.

The proposed framework addresses the central deficiencies identified in the preceding sections. By introducing a tiered structure, integrating technical benchmarks, and clarifying the standard of review, it provides a coherent method for applying due diligence in the cyber context. This approach preserves the flexibility

[2339] U.N. GGE Report, U.N. Doc. A/70/174 (2015).

[2340] Responsibilities & Obligations of States Sponsoring Persons & Entities, Advisory Opinion, 2011 I.T.L.O.S. Rep. 10, ¶ 117.

[2341] Stephan Schill, *International Investment Law and Comparative Public Law* 389–92 (2010).

of the FPS standard while enhancing its precision and predictability.

In doing so, it bridges the gap between the expanded scope of investment protection and the absence of defined obligations. Cybersecurity is no longer treated as an implicit or peripheral concern but as a central component of the State's duty to provide full protection and security. The reconceptualisation of due diligence along these lines enables international investment law to respond more effectively to the challenges posed by the digital age.

VIII. CONCLUSION

The evolution of the full protection and security (FPS) standard reflects a broader transformation within international investment law, driven by the shift from tangible to digital forms of investment. While the standard has expanded in scope to encompass legal, institutional, and intangible dimensions of investment, this expansion has not been accompanied by a corresponding development in its doctrinal content. The result is a framework that is conceptually flexible but operationally indeterminate, particularly in the context of cybersecurity.

This paper has demonstrated that the existing articulation of due diligence under FPS is insufficient to address the characteristics of cyber risk. Traditional formulations, grounded in notions of physical protection and reactive State conduct, fail to capture the continuous, technical, and systemic nature of digital threats. The absence of defined benchmarks, coupled with inconsistent arbitral practice and the limited applicability of general principles of State responsibility, has created a structural gap within the investment protection regime.

To address this gap, the paper has proposed a reconceptualisation of due diligence as a structured and risk-based obligation. By introducing a tiered framework, integrating technical standards, and incorporating contextual factors such as State capacity and foreseeability, this approach provides a coherent method for assessing State conduct in the cyber domain. It preserves the flexibility of the FPS standard while enhancing its precision and predictability, thereby aligning legal doctrine with the realities of digital investment.

The significance of this reconceptualisation extends beyond cybersecurity. It reflects a broader need for international investment law to adapt to evolving forms of economic activity and emerging sources of risk. As digital infrastructure becomes central to global investment flows, the legitimacy of the investment regime will increasingly depend on its ability to provide meaningful and predictable protection in technologically complex environments.

Ultimately, the transition from a framework centred on physical protection to one grounded in digital resilience is not an expansion of State obligation, but a necessary evolution of its content. The effective protection of modern investment requires not only the maintenance of order, but the capacity to manage risk within dynamic and interconnected systems. By redefining due diligence in these terms, the FPS standard can continue to fulfil its core function of ensuring a secure and stable environment for investment in the digital age.