Legal Research & Analysis

Innovative

Review Paper

Cybersecurity, Foreign Investment, and the Evolving Meaning of Full Protection and Security

Ali Farahzadi* and Seyedeh Kimia Mousavi Shahri

Centre for Energy Law Studies, Faculty of law and political Sciences, Tehran University, Tehran; Iran;
kimiamousavi@ut.ac.ir
* Correspondence: farahzadi.ali17@ut.ac.ir

Abstract: Foreign investors increasingly rely on digitally mediated assets and operations, like data centres, cloud services, and industrial control systems, that are situated within or controlled by host states. The law governing the obligations of host states to prevent and respond to cyber incidents affecting those investments remains uneven and fragmented. Current study examines whether, and in what manner, the classical investment law standard of full protection and security (FPS) can be interpreted to encompass a positive duty of cyber due diligence. Drawing on treaty practice, arbitral jurisprudence, and general public international law on state responsibility, it traces the conceptual and doctrinal routes through which cyber risks may be characterized as security risks to an investment and brought within the ambit of FPS. The research provides an ordered understanding of cyber due diligence, built around three core dimensions namely regulatory preparedness, operational readiness and remedial responsiveness. Regulatory preparedness is the existence of reasonably up-to-date legal frameworks on cybersecurity and breach notification; operational readiness is the institutional capacity and technical and organizational measures in critical infrastructure; and remedial responsiveness is the incident handling, cooperation with affected investors, and transparency in the aftermath of an attack. These dimensions are tested against hypothetical but realistic scenarios, including ransomware attacks on industrial facilities and systemic data exfiltration from state licensed data centers, to explore how arbitral tribunals approach questions of causation, attribution, and contributory fault in cyber related FPS claims. Recognizing a digital variant of FPS need not transform host states into insurers against all cyber harm. Properly framed as an obligation of conduct, cyber due diligence clarifies the standard of reasonableness in circumstances where regulatory indifference or institutional inaction can significantly magnify transboundary harm. The article concludes with drafting suggestions for next generation investment treaties that seek to integrate cyber due diligence into FPS and related clauses while preserving the regulatory autonomy required for evolving cybersecurity policy.

Keywords: cybersecurity; foreign investment; full protection and security; investment law; due diligence

Citation: Ali Farahzadi and Seyedeh Kimia MousaviShahri. 2025. Cybersecurity, Foreign Investment, and the Evolving Meaning of Full Protection and Security. *Legal Research & Analysis* 3(2), 61-71. https://doi.org/10.69971/lra.3.2.2025.155.

1. Introduction

Foreign investment today is mediated through digital infrastructure to an extent that would have been difficult to imagine even two decades ago. Cross-border projects increasingly rely on data centers, cloud computing services, industrial control systems, and continuous data flows for their everyday functioning (Schmitt 2017). Energy grids are monitored remotely, pipelines are controlled by networked systems, and entire business models hinge on the integrity and availability of digital platforms. This digital turn has brought undeniable efficiencies. It has also generated an additional layer of vulnerability. Ransomware attacks that paralyze industrial plants, intrusions that corrupt or encrypt operational data, and large-scale data exfiltration targeting trade secrets or customer information may disrupt an investment just as seriously as physical destruction, civil unrest, or armed conflict (Schmitt 2017).

Yet legal frameworks for the protection of foreign investors have not fully absorbed this transformation. Classical investment treaty standards, most prominently full protection and security (FPS) and fair and equitable treatment (FET) were drafted with a different paradigm of security in mind. The drafters were concerned with war, riots, police protection, and the stability of the legal environment, not with malware propagation, zero-day vulnerabilities, or supply-chain compromises in software. Treaty language rarely mentions digital infrastructure, cybersecurity, or data governance. Arbitral jurisprudence, for its part, has so far addressed FPS predominantly in relation

to physical harms: the destruction of facilities, looting, or state failure to provide basic policing. Where tribunals have extended FPS beyond strictly physical threats, they have done so in cautious and often fragmented ways. As a result, it remains uncertain whether, and to what extent, cyber-related harms fall within the protective ambit of investment law at all.

By contrast, other fields of public international law have begun to articulate more explicit expectations regarding state conduct in cyberspace. Debates reflected in instruments such as the Tallinn Manual 2.0 and in the reports of the United Nations Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) suggest that states are under a due diligence obligation not to knowingly allow their territory or cyber infrastructure to be used for acts that cause serious adverse consequences to other states (Schmitt 2017). Yet legal frameworks for the protection of foreign investors have not fully absorbed this transformation.[1] More broadly, the law of state responsibility and human rights jurisprudence have long recognized that states may incur responsibility for failing to take reasonable steps to prevent or respond to foreseeable harm caused by non-state actors, whether that harm arises from transboundary pollution, criminal violence, or systemic regulatory failure (United Nation General Assembly 2021). These developments raise an obvious but still largely unexplored question: what follows for the protection of foreign investors when the relevant harm is inflicted through cyberspace rather than through conventional physical means?

This study takes that question as its starting point. It investigates whether, and in what manner, the traditional FPS standard in investment treaties can accommodate a positive duty of cyber due diligence on host states. More concretely, it poses three interrelated questions. First, can, and should, FPS be interpreted as requiring host states to exercise due diligence in preventing and responding to cyber threats that materially affect covered investments? Second, through which conceptual and doctrinal pathways can cyber risks be framed as security risks to an investment, so that they fall naturally within the logic of FPS rather than as an exogenous add-on? Third, assuming that such a digital reading of FPS is defensible, what are the principal dimensions of a state's cyber due diligence, namely regulatory preparedness, operational readiness, and remedial responsiveness, and how might deficiencies along those dimensions translate into a breach of FPS in arbitral practice?

The analysis proceeds on the basis of a doctrinal and jurisprudential inquiry that cuts across several bodies of international law. It examines treaty practice and arbitral reasoning on FPS to distil how tribunals understand the nature and scope of the state's protective obligation, particularly in situations involving third-party actors and structural insecurity. It draws on general international law precedents, including cases on environmental harm and transboundary risk, and on human rights jurisprudence on positive obligations, to reconstruct the core elements of due diligence as a standard of conduct. It also engages with emerging discussions on cyber due diligence, as reflected in expert commentary and soft-law processes, in order to identify what responsible state behavior in cyberspace might entail for investments that depend on digital infrastructure. Finally, it uses hypothetical but realistic scenarios, such as ransomware attacks on industrial facilities or systemic data exfiltration from state-licensed data centers, as testing grounds for the proposed framework and asks how an arbitral tribunal might reason through a cyber-related FPS claim in practice.

FPS is best understood as a flexible and context-sensitive obligation of conduct that can, and in a digitalized economy should, be read to include a digital dimension. Host states are not guarantors of absolute cybersecurity; investment law does not, and should not, make them insurers against every possible cyber incident. However, where an investment is heavily reliant on digital systems located in or regulated by the host state, FPS requires that the state adopt and maintain a baseline of regulatory, institutional, and operational safeguards that is commensurate with foreseeable cyber risks.(United Nation General Assembly 2021) Recognizing such a digital variant of FPS does not radically expand state liability. Instead, it clarifies the standard of reasonableness in an environment in which inaction or regulatory indifference can significantly magnify the scale and cross-border impact of cyber harm.

2. FPS, Due Diligence, and Cyberspace

2.1 FPS in Investment Law

The full protection and security (FPS) standard is a long-standing pillar of investment protection, historically concerned with safeguarding foreign investors and their assets from physical harm (Schreuer 2010). Its origins lie in the customary duty of states to protect alien property from violence and unrest, and early arbitral decisions and treaty practice largely conceptualized FPS in these terms. Tribunals focused on situations involving armed conflict, riots, or other forms of physical disorder and asked whether the host state had taken appropriate steps to shield the investment from these risks. Typical examples included the protection of foreign-owned factories from destruction during civil unrest and the provision of basic security to investors and their personnel in periods of instability.

Over time, however, the understanding of FPS has evolved. It is now commonly characterized as an obligation of conduct, that is, a due diligence standard, rather than as an obligation of result or as a form of strict liability (OECD 2025). The host state is required to exercise reasonable care and to take prudent measures to protect the investment, but it is not automatically responsible for every instance of harm that occurs within its territory. FPS does not transform the state into an insurer of investor losses.[2] Instead, it demands vigilance and preventive action within the bounds of what is reasonable in the circumstances.

FPS also interacts in important ways with other standards of investment protection. It is related to, but distinct from, fair and equitable treatment (FET), which covers issues such as fairness, legal stability, and legitimate expectations, and from specific provisions on expropriation or denial of justice (Schreuer 2010). FPS focuses more narrowly on security, traditionally understood in physical terms, while FET addresses the broader regulatory and administrative environment. Some tribunals have acknowledged

---

1 Corfu Channel (United Kingdom v. Albania), Merits, Judgment of 9 April 1949, ICJ Reports 1949, 22 ("obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States").

2 Asian Agricultural Products Ltd. (AAPL) v. Republic of Sri Lanka, ICSID Case No. ARB/87/3, Final Award (27 June 1990), paras. 49–52, 546–547; paras. 74–76, 556–557.

overlaps and tensions between these standards.[3] A single fact pattern can give rise to both FPS and FET claims, particularly where failures of security are intertwined with regulatory or governance deficiencies.

2.2 Due Diligence in Public International Law

The notion of due diligence is a general principle in public international law. It requires a state to act with a certain standard of care in order to prevent harm, rather than to guarantee a particular outcome (International Law Commission 2001). Classic cases illustrate how this standard operates. In the Corfu Channel case, the International Court of Justice held that Albania had an obligation to warn other states of known dangers in its waters, in that instance naval mines. The Court thereby articulated a duty not to knowingly allow a state's territory to be used for acts that are harmful to others.[4]

A similar logic appears in the jurisprudence on transboundary environmental harm. The Trail Smelter arbitration and later the ICJ's decision in Pulp Mills confirmed that states must prevent and control significant environmental damage that may spread beyond their borders by exercising due diligence.[5] This means putting in place appropriate regulatory schemes, monitoring compliance, and then taking reasonable steps once a danger has been identified.[6] The doctrine of positive obligations is also underpinned by a similar structure in human rights law. Under the European Convention on Human Rights, states are, for instance, obliged to take reasonable measures to protect individuals against real and foreseeable risks created by others, such as through the prevention of criminal violence in circumstances where the risk is known, as in *Osman v United Kingdom*.[7,8]

Across these different fields, certain elements recur. Due diligence presupposes that the risk in question was foreseeable in the sense that the state knew, or ought to have known, about it. It obliges the state to adopt reasonable and proportionate measures in response, considering its resources, institutional capacities, and the seriousness of the threat. It is always a standard of conduct. A state that has taken all reasonable precautions but still suffers an incident will ordinarily not be in breach. Conversely, where harm was foreseeable and could have been prevented or mitigated by reasonable means, inaction or negligence can engage international responsibility (International Law Commission 2001).

2.3 Emerging Cyber Due Diligence Norms

In recent years, international discussion has begun to address what due diligence means in cyberspace. There is no comprehensive, binding global treaty on state behavior in the cyber domain, yet a series of expert processes and soft-law instruments have put forward guiding principles (United Nations General Assembly 2021). The Tallinn Manual 2.0, for instance, is a detailed academic study of how existing international law applies to cyber operations. It suggests that states should not allow their territory, including cyber infrastructure under their control, to be used for operations that cause significant harm to other states (Dias and Antonio 2021). In substance, this transposes the logic of Corfu Channel to the digital realm and implies a duty to monitor and, where feasible, to prevent malicious cyber activities emanating from national networks.[9]

Parallel developments can be observed in the work of United Nations bodies, notably the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG). Their consensus reports affirm that the UN Charter and general international law apply to state conduct in cyberspace and articulate expectations of responsible state behavior. (United Nations General Assembly 2021) These expectations include cooperation to prevent and respond to serious cyber incidents, information sharing about vulnerabilities, and the development of national policies and incident response mechanisms (Dias and Antonio 2021). Although the precise contours of a binding obligation remain contested, an expectation is emerging that states maintain a basic level of cyber governance and capacity (Dias and Antonio 2021).

Cyber due diligence shows some characteristics that set it apart from the classical environmental or security contexts. Most conspicuously, attribution is harder and anonymity of attackers more widespread. Unlike most forms of environmental damage, where the source of pollution can often be spotted, cyber operations are often conducted using techniques of obfuscation, compromised infrastructure, and layered intermediaries. States might not always be aware that a given cyber threat is originated from their territory or that it is affecting targets on their territory. Nevertheless, the direction of travel in international discourse seems to be that states should adopt reasonable cybersecurity policies, institutional arrangements, and technical capabilities in order to minimize the risk of serious cyber harm both internally and externally (Dias and Antonio 2021). Meeting this expectation is demanding, since threats evolve rapidly and often have cross-border ripple effects, but the underlying logic is continuous with established due diligence practice (International Law Commission 2001).

2.4 FPS and Cyber Due Diligence

Conceptually, the link between the security of an investment and the cybersecurity of the digital infrastructure on which it depends is straightforward. Where an investor's assets, operations, or sensitive data are heavily reliant on digital systems, the protection and security of the investment necessarily includes the security of those systems (Malik 2011). Under this perspective, a failure to guard against known cyber risks can be seen as analogous to a failure to guard against physical risks such as vandalism or sabotage. The medium is different, but the underlying interest protected by FPS, namely the safety of the investment against foreseeable harm, remains the same (Malik 2011).

---

3 Azurix Corp. v. Argentine Republic, ICSID Case No. ARB/01/12, Award (14 July 2006), paras. 406–408, 145–146.

4 *Corfu Channel* (United Kingdom v. Albania), Merits, Judgment, I.C.J. Reports 1949, p. 22.

5 *Trail Smelter Arbitration* (United States v. Canada), Award (11 March 1941), 3 R.I.A.A. 1905, 1965.

6 *Pulp Mills on the River Uruguay* (Argentina v. Uruguay), Judgment, I.C.J. Reports 2010, p. 79, para. 197.

7 Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), opened for signature 4 November 1950, ETS No. 5, arts 2, 8.

8 *Osman v. United Kingdom* (App no 23452/94), Judgment (28 October 1998), Reports of Judgments and Decisions 1998-VIII, pp. 33–34, para. 116.

9 See supra note 6.

It is helpful here to distinguish between negative and positive obligations in the cyber context. Negative obligations require the state to refrain from conduct that harms the investor. A host state that directly sponsors or knowingly supports cyberattacks against the investor's assets would clearly breach FPS, since the state itself would be the source of the harm. (International Law Commission 2001) Positive obligations, by contrast, require the state to take reasonable steps to prevent and respond to cyber threats posed by others, for instance criminal groups, hacker collectives, or even other states operating through its networks. It is this positive dimension that lies at the heart of FPS as a due diligence obligation and that is central to the analysis in this article (Malik 2011).

Not every cyber incident will engage state responsibility. Tribunals would likely insist that the threat was foreseeable and that the state failed to take appropriate measures within its power, judged in light of its circumstances and capacities. However, once cyber risks are conceptualized as security risks to an investment, the door is opened to treating inadequate cybersecurity governance as a potential breach of FPS. The crux remains the standard of reasonableness. States are not expected to prevent every attack, but they are expected to maintain a basic framework and to undertake practical efforts to guard against significant cyber risks that could jeopardize foreign investments (Schmitt 2017).

3. Treaty Practice and Arbitral Reasoning on FPS and "Non-Physical" Security

3.1 FPS Clauses in Investment Treaties

Investment treaties, whether stand-alone bilateral investment treaties or trade agreements with investment chapters, almost invariably contain a clause on full protection and security (UNCTAD 2021). The language of these provisions, however, is far from uniform. Many older treaties employ a simple formulation stating that each contracting party shall ensure "full protection and security" to investments of the other party. Other instruments introduce slight variations, referring instead to "constant protection and security" or "full constant protection and security" (UNCTAD 2004). At first sight these differences may appear cosmetic, yet they have given rise to recurring debates over the scope of the obligation.

A central interpretative question is whether FPS is confined to physical security or whether it extends to broader forms of protection. Some more recent treaties attempt to resolve this ambiguity directly. A number of states, concerned that expansive readings of FPS might spill over into matters of legal or regulatory stability that they would rather regulate through fair and equitable treatment, have inserted clarifying language. In such treaties, FPS is expressly limited to the physical security of investors and their assets, and annexes or interpretative notes sometimes state that FPS does not cover regulatory conduct or intangible harms. (UNCTAD 2021).[10]

Other treaties, by contrast, retain more open-ended wording. They refer to the obligation to provide protection and security to investments without specifying that this protection is only "physical." (UNCTAD 2021)[11] Such formulations leave room for arguments that FPS also embraces legal, economic, or infrastructural security, depending on context. A small but growing set of recent treaties even touches on the digital sphere, not by expressly mentioning "cybersecurity" in the FPS clause, but by acknowledging the importance of critical infrastructure, information security, or secure digital trade elsewhere in the treaty text (UNCTAD 2025).[12] Although explicit references to cybersecurity within FPS provisions remain rare, the overall practice reveals a spectrum. At one end lie narrowly drafted clauses that clearly privilege physical safety; at the other are broadly framed provisions that could be interpreted, in light of contemporary conditions, to encompass whatever forms of security are necessary for the effective enjoyment of the investment, potentially including digital security.

3.2 Arbitral Case Law: From Physical Harm to Legal and Economic Security

Arbitral jurisprudence on FPS has historically emerged from fact patterns involving physical violence and instability (OECD 2025). The classical line of cases concerns wartime damage, civil unrest, or direct attacks on investment facilities. A well-known example is *Asian Agricultural Products Ltd. (AAPL) v. Sri* Lanka (1990)[13], where an investor's shrimp farm was destroyed during a period of armed conflict. The tribunal examined whether Sri Lanka had taken adequate measures to protect the investment in light of the prevailing security situation and concluded that FPS required a level of diligence adapted to those circumstances. Similarly, in *American Manufacturing & Trading (AMT) v. Zaire* (1997)[14], looting by state security forces during riots led the tribunal to find a breach of FPS, largely because the authorities had made no serious effort to prevent or halt the attacks on the investor's property.

These early decisions crystallized a fundamental understanding: FPS is violated when a state fails to exercise due diligence in the face of foreseeable physical threats to the investment. Over time, however, claimants began to argue that FPS should be read more broadly. In several cases, they contended that the standard covers "legal security," understood as the maintenance of a stable and secure legal and regulatory environment. The tribunal in *Azurix v. Argentina* (2006)[15], for instance, interpreted FPS as requiring

---

10 Comprehensive Economic and Trade Agreement (CETA) (Canada–European Union), art. 8.10(5) (text as published by the Government of Canada): "For greater certainty, 'full protection and security' refers to the Party's obligations relating to the physical security of investors and covered investments."

11 Energy Charter Treaty, art. 10(1): "Such Investments shall also enjoy the most constant protection and security …"

12 United States–Mexico–Canada Agreement (USMCA), ch. 19 (Digital Trade), art. 19.15(1): "The Parties recognize that threats to cybersecurity undermine confidence in digital trade.

13 *Asian Agricultural Products Ltd. (AAPL) v. Sri Lanka*, ICSID Case No. ARB/87/3, Final Award (27 June 1990) paras 50, 64, 73, 85–87 (PDF pp. 10, 13, 15, 18–19).

14 *American Manufacturing & Trading, Inc. v. Republic of Zaire*, ICSID Case No. ARB/93/1, Award (21 February 1997) paras 1.05, 6.05–6.08 (including "taking no measure whatever"), 6.14 (pp. 2, 14–16).

15 *Azurix Corp. v. Argentine Republic*, ICSID Case No. ARB/01/12, Award (14 July 2006) paras 406–408 (including "not only a matter of physical security") (pp. 5–6).

more than mere physical protection. In that dispute, which concerned a water concession undermined by public unrest and governmental measures, the tribunal suggested that FPS also involves ensuring that the investment can operate within an environment free from undue interference.

Other tribunals have been more hesitant. In Saluka v. Czech Republic (2006)[16], the tribunal emphasized that FPS has traditionally been associated with physical security and expressed reluctance to extend it to issues of legal or commercial stability, reasoning that such matters fall primarily under the FET standard. The resulting case law is thus not consistent. Some awards endorse a more expansive notion of security that integrates elements of legal stability and protection against arbitrary interference. Others insist that FPS must be anchored in protection against physical harm. The case law does not yield any single authoritative definition, but it certainly indicates that FPS is contested, and possibly flexible, a standard whose contours are being determined in practice.

3.3 Digital or Infrastructure-Related FPS

To date, no investment arbitration award is reported to squarely address a cyber incident under the rubric of FPS (Cristani 2020). Nonetheless, some strands of reasoning in disputes involving critical infrastructure and network disruptions suggest how a digital FPS claim might be approached. Tribunals addressing disputes over electricity grids, telecommunications networks, or banking systems have at times touched, at least implicitly, on the host state's role in keeping essential systems operational and secure. Where a failure to maintain public infrastructure or networks has resulted in serious losses, investors have at times framed their claim as a failure of protection, arguing that the state failed to take reasonable steps to protect the underlying systems. Ampal-*American Israel Corp. v. Egypt* is a frequently cited example, still rooted in physical rather than digital sabotage. Repeated attacks on a gas pipeline serving the investor's operations led the claimants to allege a breach of FPS. The tribunal's analysis centered on whether Egypt had adopted reasonable measures to secure a piece of critical infrastructure which was known to be vulnerable. Even though the harm in Ampal was caused by explosives rather than malware, the structure of the tribunal's reasoning can be transposed to the cyber context: If a power grid or telecommunications network or other infrastructure crucial to an investment collapses due to a cyberattack, a tribunal might ask very similar questions about the host state's preparedness, incident response, and capacity to mitigate foreseeable risks.[17] Throughout the diverse jurisprudence on FPS, a standard of conduct required by the host state is one of the recurring themes. Tribunals have repeatedly emphasized that FPS is not an obligation of result, nor does it imply strict liability; it is an obligation of due diligence. The guiding question to be asked is whether the state took measures that could reasonably be expected from it considering the situation in order to safeguard the investment from damage.

In assessing this, tribunals typically consider several factors. These include the nature and intensity of the threat, prior warnings or incidents, the state's resources and institutional capacity, and the extent to which the authorities were aware of the specific risks faced by the investor. In *Pantechniki v. Albania* (2009), which involved damage arising from riots, the sole arbitrator observed that a poor developing state cannot be expected to suppress all unrest immediately and that the content of due diligence must be proportionate to the state's means and the predictability of the situation.[18] Contrarily, in *Wena Hotels v. Egypt* (2000), Egypt was found in breach of FPS because its authorities failed to intervene for several days while agents of a state-owned entity forcibly seized foreign-owned hotels, a situation the tribunal considered reasonably preventable had the state acted with appropriate promptness.[19]

When transposed to cyberspace, these principles suggest an analogous approach. States cannot realistically be required to prevent every hacking attempt or to guarantee that no cyber incident will ever affect a foreign investor. The complexity and evolving nature of cyber threats make such an expectation untenable. However, tribunals may legitimately inquire whether the host state maintained at least a baseline of cybersecurity measures, institutions, and cooperative mechanisms. Where a state lacks any meaningful framework or fails to act despite credible and specific indications of risk, for instance by ignoring intelligence about a planned attack on an investment's digital infrastructure, such inaction may well be regarded as falling below the due diligence standard embedded in FPS.

4. Digital FPS Standard: Three Dimensions of Cyber Due Diligence

4.1 Framing a Digital FPS Obligation

Building on the understanding of full protection and security as a due diligence-based obligation, it is possible to articulate a digital variant that is tailored to contemporary patterns of investment. In many sectors, the value and functioning of an investment now depend directly on the availability, integrity, and confidentiality of digital systems. Data centers, cloud services, supervisory control and data acquisition (SCADA) systems, and platform infrastructures are not merely ancillary tools. They are integral elements of the investment and, in some cases, constitute the investment itself (World Bank 2024; Stouffer et al. 2015). If those systems are seriously compromised by a cyber incident, the investment may be rendered inoperative or lose a substantial part of its value, (OECD 2019). Under these conditions, it would be artificial to confine the FPS obligation to physical security alone. The same functional logic that once justified imposing a duty of vigilance in relation to police protection, riots, and armed conflict can be extended to the digital layer of the investment environment. The host state remains under an obligation of conduct, not of result. It is not bound to guarantee an entirely safe cyberspace, which is unattainable in practice. It is, however, required to take reasonable measures to prevent and respond to cyber threats that pose serious risks to covered investments, particularly where those threats are foreseeable and where the state has meaningful regulatory or institutional leverage over the relevant infrastructure, (OECD 2019).

---

16 *Saluka Investments B.V. v. Czech Republic*, UNCITRAL, Partial Award (17 March 2006) paras 483–484 (including "physical integrity of an investment") (p. 97).

17 Ampal-American Israel Corp., EGI-Fund (08-10) Investors LLC, EGI-Series Investments LLC, and BSS-EMG Investors LLC v Arab Republic of Egypt, ICSID Case No. ARB/12/11, Decision on Liability and Heads of Loss (21 February 2017), pp. 67–68 (paras. 786–788).

18 *Pantechniki S.A. Contractors & Engineers v Republic of Albania*, ICSID Case No. ARB/07/21, Award (30 July 2009), p. 20 (para. 81).

19 Wena Hotels Ltd. v Arab Republic of Egypt, ICSID Case No. ARB/98/4, Award (8 December 2000), 41 International Legal Materials 896 (2002), pp. 912–913 (paras. 82–85).

To make this obligation analytically workable, the article proposes breaking down cyber due diligence for FPS purposes into three interrelated dimensions. The first concerns the regulatory framework that a state maintains in the cybersecurity field. The second relates to operational capacity and institutional practice. The third focuses on the quality of the state's response once a cyber incident occurs. Taken together, these dimensions provide a structured way for arbitral tribunals to assess whether a host state has met, or fallen short of, a digital FPS standard in a given case.

4.2 Regulatory Preparedness

The first dimension of cyber due diligence lies in the design and maintenance of an adequate legal and regulatory framework. At a minimum, a state that hosts substantial foreign investment should have in place laws and regulations dealing with cybersecurity, data protection, and incident reporting.[20,21] These norms set the baseline expectations for both public authorities and private actors, and they signal that the state recognizes and addresses cyber risk as a matter of public policy (World Bank 2024).

Regulatory preparedness is not exhausted by adopting a single cybersecurity statute. Rather, what matters is whether the overall architecture is reasonably adapted to the risk landscape in which investments operate. This includes sector specific rules for operators of critical infrastructure in areas such as energy, telecommunications, finance, transport, and health. It also involves imposing minimum security standards on service providers whose facilities are likely to host or process foreign investors' data and operational systems, for example cloud providers, data centers, and other information service intermediaries. Breach notification obligations and duties to cooperate with competent authorities in the event of serious incidents are another important element, since they enable a timely and coordinated response.

From an arbitral perspective, the inquiry at this stage is not whether the host state has enacted the most sophisticated or cutting-edge framework available. The question is more modest and more realistic. Did the state maintain a reasonably up to date and coherent set of rules addressing key cyber risks that were known, or ought to have been known, at the relevant time? (OECD 2015). Were there obvious gaps in sectors that are particularly exposed, such as industrial control systems or financial infrastructures, which the state could have addressed with relatively modest effort? The answers will vary with the host state's level of development, institutional capacity, and exposure to cyber threats. A low-income state cannot be held to the same regulatory standard as a technologically advanced one.[22] Nonetheless, as cyber incidents become more frequent and receive more international attention, the expectation that states will adopt some form of basic cybersecurity regulation will correspondingly rise (ENISA 2024).

4.3 Operational Readiness

Regulatory preparedness is only meaningful if it is accompanied by effective implementation. Legal rules that exist only on paper cannot, by themselves, protect an investment from cyber harm (OECD 2015). The second dimension of cyber due diligence therefore concerns the host state's operational readiness. This includes the presence of competent authorities and technical bodies capable of preventing, detecting, and managing cyber incidents, as well as the practical patterns of cooperation between these bodies and the private sector (ENISA 2020).

Core elements of operational readiness typically include a national computer emergency response team or similar incident response unit, clear lines of responsibility among ministries and agencies, and established procedures for information sharing and coordination during a crisis (ENISA 2020). Supervisory authorities must have the powers and resources necessary to monitor compliance by critical infrastructure operators and other key actors. Periodic audits, inspections, and stress tests can serve to verify whether private operators, including those whose services are essential to foreign investors, are actually meeting the security standards laid down in law.[23]

In many instances, operational readiness will also depend on sustained engagement with the private sector. States increasingly rely on public private partnerships to manage cyber risk, for example through joint early warning systems, platforms for sharing indicators of compromise, and collaborative exercises simulating attacks on critical systems (OECD 2019). Where foreign investors operate in sectors that are deeply integrated with national infrastructures, such as power generation, transport logistics, or digital communications, regular participation in these cooperative mechanisms can be both a benefit and a source of additional expectations (OECD 2019). A host state that has never conducted a serious cyber risk assessment of its critical sectors, that lacks any functioning incident response capability, and that does not meaningfully enforce its own rules is unlikely to satisfy an FPS based due diligence standard in the event of a serious breach affecting an investment (OECD 2019).

A tribunal assessing this dimension would therefore look at a combination of factors. Did the host state build and maintain institutions with at least basic technical expertise and response capacity, appropriate to its resources and exposure? Were those institutions actually active in monitoring risks and in engaging with private operators, including those hosting or supporting foreign investments? Were there known vulnerabilities or recurrent incidents that the authorities ignored, or failed to follow up on, over a prolonged period? Evidence of consistent effort, even if imperfect, will tend to support a finding that the state has tried in good faith to meet its FPS obligations in the operational sphere.

4.4 Remedial Responsiveness

---

20 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), OJ L 333, 27.12.2022, 80–152, arts. 21(2)(a)–(j), 23(1)–(4), Annex I, Annex II.

21 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), OJ L 119, 4.5.2016, 1–88, arts. 32(1), 33(1), 34(1).

22 *Pantechniki S.A. Contractors & Engineers v. Republic of Albania*, ICSID Case No. ARB/07/21, Award (30 July 2009), para. 81 (supra note 20).

23 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive), arts. 8–11, 21(2), 23 (supra note 22)

Even where robust preventive measures exist, cyber incidents will still occur. The third dimension of cyber due diligence therefore concerns what the host state does once an incident materializes. This is not a purely technical matter. The way in which authorities communicate with affected investors, coordinate between domestic agencies, and cooperate with foreign partners can significantly influence the scale of the damage and the prospects for recovery (Cichonski et al. 2012).

Remedial responsiveness begins with the existence of clear incident handling protocols (Cichonski et al. 2012). When a major attack is detected, competent authorities should have predefined procedures for classifying its severity, notifying relevant stakeholders, and mobilizing resources (Cichonski et al. 2012). For investors, the timeliness and quality of information received may be critical. A timely warning may enable an investor to isolate affected systems, switch to back up infrastructure, or take other mitigation steps. In contrast, delays or vague communications can lead to unnecessary downtime, data loss, or cascading failures.

The host state's willingness to cooperate with the investor in investigating the incident and securing the affected systems is also a relevant consideration. This could include, for example, facilitating forensic analysis, coordinating with law enforcement bodies, or undertaking diplomatic initiatives where there is evidence to suggest that another state may have been involved. It may also mean transparent reporting on the causes of the incident and on the steps being taken to prevent a recurrence, particularly when the attack shows systemic weaknesses in infrastructure affecting multiple users.

From the standpoint of an arbitral tribunal, remedial responsiveness is a means of verifying whether the state took the incident seriously and acted with due diligence once the risk had fully crystallized. Some pertinent questions may be therein presented as follows. How quickly did the authorities become aware of the incident, and what processes were in place for escalating it? Did they notify the investor without undue delay, and was the information provided sufficiently concrete to support meaningful mitigation? Did they coordinate relevant agencies and engage external partners where appropriate? (Cichonski et al. 2012). A pattern of inertia, denial, or opacity, especially in a situation where prompt action could have significantly limited the damage, may be indicative of a lack of due diligence even if the initial cyber-attack had been staged by private actors beyond the control of the state.

4.5 Cyber Due Diligence and Regulatory Space

Interpreting the FPS standard to include these three dimensions of cyber due diligence naturally raises concerns about the potential expansion of state liability. The concern could be that such an approach would open host states to a flood of claims every time a cyber incident affects a foreign investor. That concern should not be dismissed but it can be addressed by recalling the basic features of due diligence. The obligation remains one of conduct not of result. It requires reasonable efforts in light of foreseeable risks, available resources and competing public interests. It does not impose a guarantee of cyber safety.

In addition, a digital FPS standard can and should be articulated in a manner compatible with a state's regulatory autonomy. Robust cybersecurity regulation will often involve the imposition of new obligations on private actors, necessitating investment in security upgrades, or changes in business practices. These measures may raise costs in the short run but constitute part of the state's effort to discharge its protective duties in the long run. A tribunal applying digital FPS should therefore avoid confusing the adoption of stricter cybersecurity measures with a violation of investment protection unless those measures themselves are arbitrary or discriminatory and thus run afoul of other standards, such as fair and equitable treatment (UNCTAD 2015).

Balancing these issues isn't simple. On one side, the government shouldn't be encouraged to ignore cybersecurity or pass on the costs of their weaknesses to investors. But at the same time, they need enough room to regulate a fast-changing tech world aiming to protect things like national security, public safety, and individual rights. Setting clear, thoughtful standards for digital financial service providers, based on careful oversight, can really help in making fair and effective rules. It encourages states to meet a baseline of regulatory preparedness, operational readiness, and remedial responsiveness, while acknowledging that cyber risk management is a shared responsibility between public authorities and private actors in an interconnected environment, (UNCTAD 2015).

5. Digital FPS: Hypothetical Scenarios, Causation, Attribution, and Contributory Fault

The abstract discussion of a digital full protection and security standard gains clarity when tested against concrete situations. Hypothetical but realistic fact patterns help to show how the three dimensions of cyber due diligence might be applied in practice and how questions of causation, attribution, and contributory fault would arise before an arbitral tribunal. The following two scenarios are illustrative rather than exhaustive. They are chosen because they capture recurring features of cyber incidents that are likely to affect foreign investments and because they highlight different facets of the host state's potential responsibility.

5.1 Ransomware Attack on an Investor-Owned Industrial Facility

Imagine a foreign investor that owns and operates an industrial facility, for example a power plant or a manufacturing plant, located in the host state. The facility relies heavily on networked industrial control systems to manage production and to interface with the national grid or with upstream and downstream partners. A criminal group deploys ransomware that infiltrates the facility's systems, encrypts operational data, and forces a shutdown. The attackers will indeed seek payment, however regardless of whether the investor pays, the plant will be offline for an unacceptably long period of time. The investor suffers serious financial losses and alleges that the host state has breached its FPS obligation, even though the perpetrators are private cybercriminals.

In such a case, a tribunal applying a digital FPS framework would examine the host state's conduct through the three dimensions of cyber due diligence. First, it would look at regulatory preparedness. Did the host state impose basic cybersecurity obligations on operators of critical infrastructure, including industrial facilities of the type in question. Were there national or sector specific rules requiring such operators to implement minimum safeguards, such as network segmentation, regular patching, access controls, and incident reporting (Stouffer et al. 2023). If the legal framework was silent on cybersecurity in sectors that were obviously exposed to attack, especially at a time when ransomware campaigns against similar facilities were widely publicized, that silence might indicate a failure to meet the expected duty of care.

Second, the tribunal would consider operational readiness. The key questions here are whether the host state had mechanisms to anticipate and manage the kind of attack that occurred. Was there a functioning national computer emergency response team. Did relevant authorities monitor threats to critical infrastructure and disseminate alerts when comparable ransomware campaigns were

detected. Had the state engaged in any meaningful outreach or joint exercises with operators of industrial control systems. (ENISA 2020; Cichonski et al. 2012; ENISA 2024) A complete absence of institutional capacity, or a situation in which the authorities were repeatedly warned about vulnerabilities in critical sectors yet took no steps to address them, would suggest a lack of reasonable preventive action.

Third, remedial responsiveness would come under scrutiny. Once the attack was underway, how did the host state react. Did competent agencies promptly notify the investor of the nature and scope of the threat, offer technical assistance, or coordinate with law enforcement bodies in an effort to contain the damage. Or did the authorities remain passive, deny the seriousness of the incident, or fail to communicate in a timely and transparent manner (Cichonski et al. 2012). If the investor can show that a quicker or more coordinated response would likely have reduced the duration or severity of the shutdown, prolonged inaction may be regarded as a failure of due diligence in the aftermath of the attack (Cichonski et al. 2012). In this first scenario, the attackers are not linked to the state, and the cyber operation itself would not be attributable to the host state under the law of state responsibility, (International Law Commission 2001). However, lack of attribution does not end the analysis. FPS, understood as an obligation of conduct, still requires the host state to have taken reasonable preventive and responsive measures vis a vis non-state actor. A well governed state that has enacted basic cybersecurity legislation, maintained an operational incident response capacity, and reacted diligently to attacks on critical infrastructure may be found to have complied with its FPS obligations, even if the investor nonetheless suffers harm (Cichonski et al. 2012). By contrast, a state that has systematically neglected cyber risk, in a context where such risk was clearly foreseeable, may be found in breach, notwithstanding the private character of the attackers. FPS does not guarantee absolute security against every cyberattack, but it does insist on a minimum level of vigilance.

5.2 Systemic Data Exfiltration from a State Licensed Data Centre

Consider a second example. A foreign investor relies on a commercial data center in the host state to store sensitive business information, including trade secrets and confidential customer data. The data center operates under a license issued by the host state and is subject to regulatory supervision. Over a period of months, an unknown actor gains persistent access to the data center's systems and exfiltrates large volumes of data. The investor later discovers that its proprietary information has been compromised, with serious competitive consequences. Forensic analysis reveals long standing vulnerabilities in the data center's defenses that should have been evident to a reasonably competent operator. The investor brings a claim arguing that the host state has failed to afford FPS to its investment.

Several legal issues arise. The first relates to attribution. On the facts, the direct perpetrators of the cyber espionage are not organs of the host state and do not act under its direction or control. The host state is thus not responsible as such for their conduct, (International Law Commission 2001). The emphasis then shifts to whether the state has breached its own due diligence obligations. Since the data center is licensed and subject to regulatory control, the host state has some degree of control over the facility, which is central to the investor's operations. Potential state liability thereby arises for a failure to prevent and supervise, rather than any active participation in the attack. Regulatory and supervisory failure is thus central. Did the host state require licensed data centers to adhere to defined security standards that were reasonable in light of prevailing threats. Did it conduct audits or inspections to verify compliance. Were deficiencies detected and, if so, were they followed up with corrective measures. If the investigation reveals that the state had little or no regulatory framework for data security in such facilities, or that it turned a blind eye to obvious vulnerabilities in a critical provider, a tribunal might conclude that the state failed to take measures that were plainly within its reach. In that case, the breach of FPS would lie not in the underlying espionage itself, but in the state's omission to exercise the supervisory powers at its disposal in order to protect the investor's data from a foreseeable risk.

At the same time, the investor's own precautions cannot be ignored. A tribunal might ask whether the investor selected the data center with due care, whether it imposed contractual security requirements, and whether it implemented additional safeguards, such as encryption, that would have reduced the impact of a breach. If the investor unreasonably relied on a provider with a poor security record, or disregarded clear warnings about the provider's practices, this behavior could be considered in reducing any compensation, on the basis of contributory negligence or failure to mitigate loss (International Law Commission 2001).

5.3 Causation in the Cyber Context

Proving causation in a cyber related FPS claim presents distinct challenges. Cyber incidents frequently involve numerous actors, layered infrastructure, and a series of technical events that may be hard to reconstruct. Malware may remain dormant for extended periods, lateral movement across networks can obscure the initial entry point, and logs can be incomplete or manipulated (Cichonski et al. 2012).

Tribunals are nevertheless accustomed to working with imperfect evidence and complex factual patterns. In the cyber context, they are likely to adopt a pragmatic approach that combines a but for analysis with a focus on foreseeability and material contribution (Ripinsky and Williams 2008). The key question is whether the harm suffered by the investor is sufficiently linked to the state's failure to exercise due diligence. For example, if plausible threat intelligence was available and the host state ignored it, leaving critical infrastructure completely unprepared, then it might be reasonable to find that this omission materially increased the likelihood or severity of damage (Ripinsky and Williams 2008). Conversely, where a state has taken reasonable measures and an extremely sophisticated and novel attack nonetheless prevails, the causal link between any residual deficiencies and the harm may be too attenuated to establish liability.

In practice, tribunals may rely heavily on expert evidence to reconstruct the chronology and mechanics of an incident, (International Bar Association 2020). They may also use inferential reasoning, particularly where the state has not maintained adequate logs or has failed to cooperate with forensic investigations. In such circumstances, the evidential consequences of poor record keeping can fall on the state, much as they sometimes do in environmental or human rights cases (International Bar Association 2020; Cichonski et al. 2012). However, causation remains an indispensable element. Even under a generous view of FPS, an investor must show that the state's omissions were a significant factor in the harm, rather than merely coincidental (Ripinsky and Williams 2008).

5.4 Attribution, non-attribution, and the FPS obligation

A further aspect is the relationship between attribution and FPS. In many cyber incidents, the attack will not be attributable to the host state. It may originate from private criminal groups, foreign intelligence services, or loosely organized hacker collectives. In these cases, state responsibility, in the strict sense developed under the Articles on Responsibility of States for Internationally Wrongful Acts, will not attach to the attack itself (International Law Commission 2001). That does not mean, however, that the host state is automatically in the clear. FPS, as a due diligence based standard, focuses on the host state's own conduct. Even when attacks are not attributable, the state may still be bound to take reasonable steps to prevent or mitigate their effects. The distinction is important. Where an attack is attributable, the state can be held responsible for the wrongful act and for the resulting damage, subject to any available defenses. Where the attack is not attributable, the state can only be held responsible for failing to exercise due diligence in relation to third party conduct. Tribunals should therefore keep these two layers of analysis separate. (International Law Commission 2001). An investor alleging a cyber related breach of FPS will often proceed on the latter basis, accepting that the offenders are private actors but arguing that the host state did too little, too late, in terms of regulation, preparedness, or response, (International Law Commission 2001).

5.5 Investor Conduct and Contributory Fault

Finally, any serious account of digital FPS must recognize that investors themselves play a role in managing cyber risk. Investment treaties primarily impose obligations on states, yet tribunals have long accepted that investor behavior is relevant when determining liability and quantum. In cases involving environmental harm, safety standards, or regulatory breaches, awards have reduced compensation where investors neglected their own duties or failed to take obvious precautions (International Law Commission 2001)[24].

The same logic applies in the cyber sphere. An investor that stores valuable data without elementary security measures, ignores industry standards, or declines to follow host state guidance on cyber risk should not be able to shift the entire burden of a cyber incident onto the state. Tribunals may ask whether the investor implemented reasonable technical and organizational measures, such as access controls, encryption, backups, and incident response plans (Cichonski et al. 2012). They may also examine whether the investor properly assessed the reliability of third-party providers, negotiated appropriate contractual safeguards, and maintained adequate cyber insurance (Cichonski et al. 2012).

Where both the host state and the investor have contributed to the conditions that allowed a cyber incident to occur or to escalate, doctrines of contributory fault and failure to mitigate can be used to apportion responsibility (International Law Commission 2001).[1] This does not dilute the core content of the FPS obligation. Rather, it reflects the reality that cybersecurity in complex, networked environments is a shared endeavor. Recognizing the investor's role in this way strengthens, rather than weakens, the credibility of digital FPS claims by ensuring that they rest on a balanced assessment of all relevant conduct (International Law Commission 2001).

6. Cyber Due Diligence in Next-Generation Investment Treaties

The argument that full protection and security should be read in digital terms could, in principle, be developed entirely through interpretation of existing treaties. Yet relying solely on interpretative evolution has its limits. Investors and host states alike have a legitimate interest in knowing, ex ante, what level of cyber governance is expected under international investment agreements. If FPS is to carry a digital dimension, it is therefore worth considering how treaty drafting might reflect that reality in a more transparent and structured way (Gordon 2015).

Treaty drafters face a familiar tension. On the one hand, they may wish to clarify that FPS is not confined to physical harm and can encompass the protection of digital infrastructure and data which are essential to the investment. On the other hand, they will want to avoid language that appears to impose open ended obligations, or that might be read as transforming states into guarantors of cyber safety. Any drafting strategy has to preserve the basic character of FPS as a due diligence standard, while acknowledging that the forms of security relevant to modern investments have diversified (UNCTAD 2015).

One option is to work within the FPS clause itself by adding a limited clarification. A treaty might, for instance, provide that each party shall ensure full protection and security to covered investments, including protection of the physical and digital infrastructure and data that are essential to their operation, in accordance with the customary international law standard of due diligence. This type of formulation does two things. It signals that digital harms are not excluded from the outset, and it anchors the obligation explicitly in an established due diligence paradigm. Tribunals would still need to determine in each case what measures were reasonable in light of the circumstances, but they would no longer have to decide, as a threshold issue, whether digital harms can ever fall within FPS (UNCTAD 2020).

A second, more ambitious technique is to include a dedicated article on cybersecurity and digital infrastructure elsewhere in the treaty, and to link that article to the investment protection standards. Such a provision might set out general commitments to develop and maintain national cybersecurity frameworks, to cooperate on incident response, and to promote the resilience of critical infrastructure. It could then specify that these commitments are relevant to the interpretation and application of FPS and related clauses. The advantage of this approach is that it allows states to articulate a broader policy vision for cyber governance, including objectives that go beyond investment protection, while still creating a bridge to the investor state dispute settlement context. It also creates space for more detailed cooperation or capacity building initiatives that may be particularly important for states with limited resources (UNCTAD 2015)[25].

---

[24] Copper Mesa Mining Corporation v. Republic of Ecuador, PCA Case No. 2012-2, Award (15 March 2016), para. 6.102 (assessing the claimant's "contribution to its own injury" at 30 percent by reference to Article 39 of the ILC Articles).

[25] United States–Mexico–Canada Agreement (USMCA), Chapter 19 (Digital Trade), Article 19.15 (Cybersecurity), official text (USTR), pp. 7–8.

A third possibility is to rely on interpretative instruments and annexes rather than on the main treaty text. States could agree, for example, on a joint interpretative declaration explaining that references to protection and security in the treaty are understood, in light of current technological conditions, to include reasonable measures relating to the cybersecurity of investments. Annexes might list non-binding examples of regulatory, operational, and remedial measures that parties are encouraged to adopt, without turning those examples into rigid obligations. This technique offers flexibility. It can be updated over time, for instance as cyber threats evolve or as new best practices emerge, without reopening the entire treaty for formal amendment (UNCTAD 2020; Gordon 2015)[26].

Whatever drafting route is chosen, certain safeguards against the over expansion of state liability should be built in. It is important to reiterate, in express terms, that the obligations concerning digital protection are obligations of conduct only and that they do not require the prevention of every cyber incident. This can be done by referencing the customary law standard of due diligence or by including language clarifying that states remain responsible only for failures to take reasonable and proportionate measures. Treaties can also acknowledge explicitly that the content of the obligation will depend on the party's level of development, institutional capacity, and exposure to particular risks, thereby reducing the fear that a single uniform standard will be imposed across radically different contexts (OECD 2025; UNCTAD 2015).

In addition, investment treaties could acknowledge, at least in general terms, the role of investors in managing cyber risk. Clauses may note that investors are expected to adopt appropriate cybersecurity measures in line with applicable domestic law and relevant international or industry standards. While such language does not transform investors into duty bearers in the sense of the law of state responsibility, it can guide tribunals when considering contributory fault, mitigation of damages, or shared responsibilities in complex infrastructures. It also signals that cybersecurity is a collaborative endeavor in which both public authorities and private actors have a part to play (UNCTAD 2015; NIST 2024).

A concrete model might therefore combine several elements. The FPS clause would be accompanied by a short clarification including digital infrastructure and data, subject to due diligence; a separate article on cooperation in cybersecurity would set out overarching commitments, including incident response and information sharing. An interpretative annex would indicate, in non-exhaustive terms, that tribunals should consider the host state's regulatory preparedness, operational readiness, and remedial responsiveness when assessing compliance with FPS in cyber related disputes, while also considering the investor's own cybersecurity practices. This package would not eliminate all uncertainty, nor should it. It would, however, provide a clearer frame of reference for tribunals and a more realistic set of expectations for states and investors facing an increasingly dense web of digital risks, (UNCTAD 2020; Gordon 2015).

7. Conclusions

The integration of digital technologies into virtually every aspect of economic life has altered the risk profile of foreign investment in ways that investment law is only beginning to acknowledge. Data centers, industrial control systems, cloud platforms, and interconnected networks are now central to the creation and preservation of value. When these systems are compromised, whether by ransomware, espionage, or disruptive attacks, the resulting harm can be as severe as that caused by physical violence or destruction. It is therefore no longer tenable to treat cybersecurity as an issue at the margins of investment protection. The full protection and security standard, according to this article, provides a reasonable and normatively defensible starting point for integrating cyber due diligence into investment law. Tribunals can rely on established due diligence principles in public international law as well as new expectations in international cyber discourse by interpreting FPS as an obligation of conduct that extends to the digital aspect of investments. The suggested framework, which is organized around operational readiness, regulatory preparedness, and remedial responsiveness, offers a useful instrument for determining whether a host state has fulfilled its protective obligations in situations where harm is caused via cyberspace. Adopting a digital FPS standard does not mean that states will be held strictly liable for each cyber incident that impacts a foreign investor. Instead, it makes clear that states must take reasonable steps, to the best of their abilities, to anticipate and manage foreseeable cyber risks, particularly when those risks jeopardize investments that depend on infrastructure situated in or subject to host state regulation. It also emphasizes that investors have a responsibility to manage cyber risk and that tribunals can still use contributory fault and mitigation doctrines to allocate losses. In the future, treaty practice will be crucial in determining how quickly and how far the law advances in this direction. It is possible to align expectations and prevent purely ad hoc responses to new disputes by explicitly acknowledging digital security concerns in FPS clauses, specific cybersecurity articles, and interpretive tools. Additionally, there is a great deal of potential for cross-fertilization in developing the content of cyber due diligence between investment arbitration, human rights organizations, and specialized cyber governance forums. In the end, the question is not whether or not investment law will address cybersecurity, but rather how logically and openly it will do so. Tribunals will be asked to make decisions in situations where the security of an investment is inextricably linked to the security of its digital environment as cyber incidents increase in frequency and severity. One way to address that issue without skewing the balance that investment law aims to achieve between protection and regulatory autonomy is through a meticulously calibrated digital reading of FPS that is based on due diligence and mindful of both state capacity and investor behavior.

References

Cichonski, Paul, Tom Millar, Tim Grance, and Karen Scarfone. 2012. Computer Security Incident Handling Guide. *National Institute of Standards and Technology (NIST) Special Publication 800-61 Revision* 2: 1-80. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Cristani, Federica. 2020. Cybersecurity of Foreign Investment in the Visegrád Four (V4 Countries). *Visegrad Insight (Think Visegrad)*: 1-53. https://think.visegradfund.org/wp-content/uploads/Federica-Cristani.pdf

26 NAFTA Free Trade Commission, *Notes of Interpretation of Certain Chapter 11 Provisions* (31 July 2001), pp. 1–2.

Dias, Talita, and Antonio Coco. 2021. Cyber Due Diligence in International Law. *Oxford Institute for Ethics, Law and Armed Conflict*: 1-211. https://www.elac.ox.ac.uk/wp-content/uploads/2022/02/Final-Report-BSG-ELAC-CyberDueDiligenceInInternationalLaw.pdf

ENISA (European Union Agency for Cybersecurity). 2020. How to Set Up CSIRT and SOC. *ENISA*. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20How%20to%20setup%20CSIRT%20and%20SOC.pdf

ENISA (European Union Agency for Cybersecurity). 2024. Best Practices for Cyber Crisis Management. *ENISA*: 1-58. https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Study%20Best%20Practices%20Cyber%20Crisis%20Management.pdf

ENISA (European Union Agency for Cybersecurity). 2024. ENISA Threat Landscape 2024. *ENISA.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Gordon, Kathryn and Joachim Pohl. 2015. Investment Treaties over Time—Treaty Practice and Interpretation in a Changing World. *OECD Working Papers on International Investment*: 1-42. https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/01/investment-treaties-over-time-treaty-practice-and-interpretation-in-a-changing-world_g17a25b0/5js7rhd8sq7h-en.pdf

International Law Commission. 2001. Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with Commentaries. *Yearbook of the International Law Commission* 7: 148–170. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_7_2001.pdf

International Law Commission. 2001. Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries. *United Nations*: 31-115. https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf

Malik, Mahnaz. 2011. The Full Protection and Security Standard Comes of Age: Yet another challenge for states in investment treaty arbitration? *International Institute for Sustainable Development*: 1-18. https://www.iisd.org/publications/report/full-protection-and-security-standard-comes-age-yet-another-challenge-states

Stouffer, Keith, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn. 2015. Guide to Industrial Control Systems (ICS) Security. *National Institute of Standards and Technology (NIST), Special Publication 800-82 Revision 2*: 1-248. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

National Institute of Standards and Technology (NIST). 2024. The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). *National Institute of Standards and Technology*. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final

OECD. 2015. Digital Security Risk Management for Economic and Social Prosperity. *Organisation for Economic Co-operation and Development (OECD)*: 1-74. https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_g1g5c3dc/9789264245471-en.pdf

OECD. 2019. Digital Security and Resilience in Critical Infrastructure and Essential Services. *Organization for Economic Co-operation and Development (OECD)*: 1-55. https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/04/digital-security-and-resilience-in-critical-infrastructure-and-essential-services_5593c149/a7097901-en.pdf

OECD. 2025. Clarifying 'Full Protection and Security' Obligations in Investment Treaties: Opportunities for a Joint Interpretation. *Organization for Economic Co-operation and Development (OECD)*: 1-9. https://one.oecd.org/document/DAF/INV/TR2/WD(2025)1/ADD/REV1/en/pdf

Schmitt, Michael N. 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge University Press*. https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4_C3C28FC9CA2FB6C9

Schreuer, Christoph. 2010. Full Protection and Security. *Journal of International Dispute Settlement* 1: 353–369. https://doi.org/10.1093/jnlids/idq002

UNCTAD. 2004. International Investment Agreements: Key Issues. *United Nations, New York and Geneva*: 1-416. https://unctad.org/system/files/official-document/iteiit200410_en.pdf

UNCTAD. 2015. Investment Policy Framework for Sustainable Development. *United Nations Conference on Trade and Development*: 1-157. https://unctad.org/system/files/official-document/diaepcb2015d5_en.pdf

UNCTAD. 2020. International Investment Agreements Reform Accelerator. *United Nations Conference on Trade and Development* : 1-32. https://unctad.org/system/files/official-document/diaepcbinf2020d8_en.pdf

UNCTAD. 2021. International Investment Agreements and Their Implications for Tax Measures: What Tax Policymakers Need to Know. *United Nations Conference on Trade and Development*. https://unctad.org/publication/international-investment-agreements-and-their-implications-tax-measures-what-tax

UNCTAD. 2025. International Investment Agreements Toolbox on Clean Energy, Digital Transformation and Public Health: Insights from Recent Group of 20 Treaties. *United Nations Conference on Trade and Development* : 1-32. https://unctad.org/publication/international-investment-agreements-toolbox-clean-energy-digital-transformation-and

United Nations General Assembly. 2021. Final Substantive Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc. A/75/816.

United Nations General Assembly. 2021. Official Compendium of National Contributions on How International Law Applies to the Use of Information and Communications Technologies by States. UN Doc. A/76/136.

World Bank. 2024. Advancing Cloud and Data Infrastructure Markets: Strategic Directions for Low- and Middle-Income Countries. *World Bank*. https://openknowledge.worldbank.org/entities/publication/2803be81-3545-4584-99ea-cfa29be2bc2d