Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration

Julien Chaisse[*] *& Cristen Bauer*[**]

ABSTRACT

The digital era provides many opportunities, yet it also presents several unique challenges with regard to cybersecurity and the protection of digital assets. Cybercrime has changed the international legal landscape as nations, businesses, and legislators grapple with how to deal with this rapidly evolving, multifaceted problem. As there is no international mechanism for protection of foreign investors in this regard, some scholars are advocating for the use of Bilateral Investment Treaties (BITs) as part of a "polycentric" approach to cyber peace. With an uptick in digital development and more development on the horizon, it will be important to establish what protections—if any—BITs can provide for these digital assets. This Article explores this issue by (1) addressing digital assets as covered investments and (2) examining three potential investment claims.

TABLE OF CONTENTS

---

* Ph.D., Aix-Marseille University, 2008; Professor of the Faculty of Law, The Chinese University of Hong Kong; Co-Founder, Internet Intellectual Property Institute (IIPI).

** J.D., Chinese University of Hong Kong, 2017; Consultant, Trade, Investment and Innovation Division, United Nations Economic and Social Commission for Asia and the Pacific (UN-ESCAP). The Authors would like to thank Danny Friedmann, Jyh-An Lee, and Keith Ji their comments on earlier drafts of this Article. The views expressed herein by Authors are their own personal ones.

I. INTRODUCTION

We live in a new era—a time when allegations of state-sponsored economic espionage are redefining how society thinks about expropriation,[1] and when weaponized finance, data breaches, and cyber hacks are being compared to aggressions of war.[2] Cybercrime has changed the international legal landscape, and nations, businesses, and legislators must grapple with how to deal with this rapidly evolving, multifaceted problem. From Equifax to eBay, Deloitte to Google, as well as projects linked to China's Belt and Road Initiative (BRI),[3] the news and recent scholarship is riddled with tales of cyberattacks.[4] In 2015,

1. *See* Scott J. Shackelford et al., *Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties*, 52 AM. BUS. L.J. 1, 2–3 (2015); Eric J. Hyla, Note, *Corporate Cybersecurity: The International Threat to Private Networks and How Regulations Can Mitigate It*, 21 VAND. J. ENT. & TECH. L. 309, 310–11 (2018).

2. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 199–201 (2009); Joanna Diane Caytas, Note, *Weaponizing Finance: U.S. and European Options, Tools, and Policies*, 23 COLUM. J. EUR. L. 441, 441–44 (2017); Hyla, *supra* note 1, at 314.

3. *See* Rozanna Latiff, *China-Linked Cyberattacks Likely as Malaysia Reviews Projects: Security*, REUTERS (Aug. 15, 2018, 4:43 AM), https://www.reuters.com/article/us-malaysia-cyber/china-linked-cyberattacks-likely-as-malaysia-reviews-projects-security-firm-idUSKBN1L00X8 [https://perma.cc/NL2B-UB6P]; Stefania Palma, *China Accused of Using Belt and Road Initiative for Spying*, FIN. TIMES (Aug. 14, 2018), https://www.ft.com/content/d5ccb654-a02c-11e8-85da-eeb7a9ce36e4 [https://perma.cc/FZZ9-HXUG].

4. *See, e.g.*, James R Silkenat, *Privacy and Data Security for Lawyers*, 38 AM. J. TRIAL ADVOC. 449, 450–52 (2015); Kelly Phillips Erb, *Big Four Accounting Firm Deloitte Confirms Cyber Attack*, FORBES (Sept. 26, 2017, 3:04 PM), https://www.forbes.com/sites/kellyphillipserb/2017/09/26/big-four-accounting-firm-deloitte-

the CEO of IBM warned that "[c]ybercrime is the greatest threat to every company in the world."[5] Cyber hackers are targeting and disrupting companies across all industries, especially as companies increase digitalization and business models sprawl across traditional sectors to intersect the digital world in new ways.[6] By 2021, experts estimate that cybercrimes will cost the world $6 trillion annually.[7]

The many consequences of cybercrime are clear. What is less clear, however, is how to combat this problem on an international level. The borderless and anonymous nature of cyber threats paints a complex legal picture.[8] Cyberlaw experts recognize the need for a multifaceted, "polycentric" approach that encompasses cooperation across local, national, and international bodies.[9] The need for this cross-border collaboration is further highlighted by a desire for global digital development and the inherently transnational nature of the digital

---

confirms-cyber-attack/#6d131142ae10 [https://perma.cc/7T5K-ZAEQ]; Hyla, *supra* note 1, at 309–10.

5. *See* Steve Morgan, *IBM's CEO on Hackers: 'Cyber Crime Is the Greatest Threat to Every Company in the World'*, FORBES (Nov. 24, 2015, 6:46 AM), https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#45a465c73f07 [https://perma.cc/LU5M-U6UD].

6. *See* U.N. CONFERENCE ON TRADE AND DEV., WORLD INVESTMENT REPORT 2017: INVESTMENT AND THE DIGITAL ECONOMY, at 158, 185–87, 209, 212, U.N. Sales No. E.17.II.D.3 (2017).

7. Cybercrime costs reflect losses to companies, investors, individuals, and governments. *See* STEVE MORGAN, CYBERSECURITY VENTURES, 2017 CYBERCRIME REPORT 3 (2017) ("Cybercrime costs includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm."). Moreover, Forbes reports that in the case of companies, cybercrime costs account for direct, quantifiable costs of a breach. *See* Nick Eubanks, *The True Cost of Cybercrime for Businesses*, FORBES (July 13, 2017, 10:00 AM), https://www.forbes.com/sites/theyec/2017/07/13/the-true-cost-of-cybercrime-for-businesses/#7d15cf214947 [https://perma.cc/XKJ7-Y58Y]. Actual losses from damage to shareholder and investor trust, perception, and reputation can be significantly worse than the $6 trillion figure. *See id.*

8. *See* Sandeep Mittal & Priyanka Sharma, *A Review of International Legal Frameworks to Combat Cybercrime*, 8 INT'L J. ADVANCED RES. COMPUTER SCI. 1372, 1372 (2017).

9. Shackelford, *supra* note 2, at 216. A "polycentric" approach to cyber peace is described as a "multi-level, multi-purpose, multi-functional, and multi-sectoral model" comprising of private-sector cybersecurity "best practices, along with national, bilateral, and regional bodies acting as norm entrepreneur" that promotes "a global culture of cybersecurity." Scott J. Shackelford, *The Law of Cyber Peace*, 18 CHI. J. INT'L L. 1, 7 (2017). For more information on the concept of polycentric governance more generally, see Bryan Druzin, *Why Does Soft Law Have Any Power Anyway?*, 7 ASIAN J. INT'L L. 361 (2017) (manuscript at 13, 17) (on file with author) (arguing that network effects, if unchecked, naturally diminish legal polycentricity). Indeed, network effects may render polycentric governance difficult to maintain. *See* Bryan Druzin, *Towards a Theory of Spontaneous Legal Standardization*, 8 J. INT'L DISP. SETTLEMENT 403 (2017) (manuscript at 3, 14, 19) (on file with author). As such, there is a clear advantage to firmly embedding such regulatory controls in BITs.

value chain.[10] In a 2015 McKinsey poll of US companies, most executives "consider[ed] digital manufacturing and design to be a critical driver of competitiveness."[11] However, these executives also reported feeling far from being able to capitalize on the economic potential of digital development due to a lack of industry standards and related cybersecurity concerns.[12]

A relationship exists between the goals for global digital development, the investment necessary to achieve such development, and the need to mitigate cybersecurity concerns in order to boost consumer confidence and trust in these developing industries. To this end, the Organisation for Economic Co-operation and Development (OECD) recommends that governments and stakeholders treat their cybersecurity risk management framework as part of a wider economic and social policy.[13] International economic agreements could, therefore, be at the center of the digital development nexus by helping to quell cybersecurity concerns as part of a more comprehensive strategy.

Much of the cybersecurity strategy to date has involved using international humanitarian law, harmonizing criminal law legislation, and enacting intellectual property right (IPR) protections.[14] For example, both the World Trade Organization (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) and the Council of Europe Convention on Cybercrime (Budapest Convention) assist cybersecurity efforts by prescribing solutions, such as domestic IPR protection, and coordinating law enforcement and extradition efforts.[15] None of these current international approaches, however, provide enforceable remedies for economic actors operating in less secure digital environments.[16] As such, some scholars advocate for the use of Bilateral Investment Treaties (BITs) as part of a polycentric approach to cyber peace.[17]

---

10. *See* ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, OECD 2016 MINISTERIAL MEETING ON THE DIGITAL ECONOMY: INNOVATION GROWTH AND SOCIAL PROSPERITY: BACKGROUND PAPER 5 (2016) [hereinafter OECD 2016 BACKGROUND PAPER].

11. John Nanry, Subu Narayanan & Louis Rassey, *Digitizing the Value Chain*, MCKINSEY & CO. (Mar. 2015), https://www.mckinsey.com/business-functions/operations/our-insights/digitizing-the-value-chain [https://perma.cc/PZQ8-W4L7].

12. *See id.*

13. *See* OECD 2016 BACKGROUND PAPER, *supra* note 10, at 7.

14. *See* Mittal & Sharma, *supra* note 8, at 1372; Shackelford, *supra* note 9, at 3–4, 23.

15. *See* Julien Chaisse & Puneeth Nagaraj, *Changing Lanes: Intellectual Property Rights, Trade and Investment*, 37 HASTINGS INT'L & COMP. L. REV. 223, 225 (2014); Mittal & Sharma, *supra* note 8, at 1372; Shackelford, *supra* note 2, at 245.

16. *See* Shackelford, *supra* note 2, at 225, 228.

17. *See, e.g.*, David Collins, *Applying the Full Protection and Security Standard of International Investment Law to Digital Assets*, 12 J. WORLD INV. & TRADE 225, 225–27 (2011); Shackelford, *supra* note 2, at 229.

BITs are international agreements between two states seeking to balance the risks of foreign investment in potentially less stable environments by ensuring baseline protections for investments, as well as allowing for dispute settlement in a neutral, international forum.[18] Despite the benefits of BITs, their application to digital assets and potential claims raises many questions. For example, do foreign investors have any protection for their digital assets in BITs under current investment definitions? With such a pervasive cybercrime problem, can foreign investors really expect to hold states accountable for cybercrimes against those assets? Does a lax regulatory or prosecutorial regime for cybercrime create an unsafe investment environment? Could rapid changes to legislation requiring source code disclosure or data breach notification substantially undermine a foreign investment or the investor's legitimate expectations? This Article provides answers to some of these questions as it assesses potential investment claims.

Against this backdrop, this Article explores whether cyberattacks and data breaches could give rise to viable investment claims against host states. An analysis of BITs and investment arbitration decisions reveals that there are potential claims to pursue; but these claims are not without limitations and significant challenges. Foreign investors may find their digital assets woefully unprotected under the current state of BITs. States may also be overly exposed with regard to several BIT provisions, including fair and equitable treatment, expropriation, and full protection and security. This Article discusses these issues by looking at (1) digital assets as "covered investments" and (2) potential investment claims in the digital era.

II. COULD DIGITAL ASSETS QUALIFY AS "COVERED INVESTMENTS"?

The Investor-State Dispute Settlement (ISDS) system encompasses various options for dispute settlement, including domestic court remedies, state-to-state mediation, and arbitration.[19] These procedural options for dispute settlement within BITs functioned to depoliticize disputes and move beyond the gunboat diplomacy and war that previously engulfed international economic disputes involving

18. *See* Ignacio Suarez Anzorena & William K. Perry, *The Rise of Bilateral Investment Treaties: Protecting Foreign Investments and Arbitration*, IN-HOUSE DEF. Q., Summer 2010, at 58; Julien Chaisse & Rahul Donde, *The State of Investor-State Arbitration: A Reality Check of the Issues, Trends, and Directions in Asia-Pacific*, 51 INT'L LAW. 47, 50, 53, 59 (2018).

19. *See* Susan D. Franck, *Development and Outcomes of Investment Treaty Arbitration*, 50 HARV. INT'L L.J. 435, 442 (2009); Matthew C. Poterfield, *Exhaustion of Local Remedies in Investor-State Dispute Settlement: An Idea Whose Time Has Come?*, 41 YALE J. INT'L L. 1, 6 (2015); Anzorena & Perry, *supra* note 18, at 60.

governments.[20] The dispute settlement provisions within BITs specify the details of which remedies are available to investors—with most treaties allowing for investor-state arbitration.[21] Where investors decide to initiate an arbitration, they decide on the applicable institutional rules, and—while the mechanics of arbitrator appointment vary under each institution—the investors and government appoint three arbitrators to hear and render a binding decision for the dispute.[22]

Before assessing any potential claims, a claiming investor must establish whether the digital assets in question could even constitute covered investments within the jurisdiction of BITs. BITs are designed to be a transparent framework of investment protections and state obligations.[23] They are seen as instruments capable of changing and adapting to the future.[24] However, in order to maintain legitimacy, they must not extend too far beyond what the states envisioned at the time of signing.[25] Investors need consistency, transparency, and reliability from BITs, and the investment regime needs buy-in from the states.

As Tribunals begin to hear and interpret cybercrime claims in the coming years, they will have to grapple with these classic international investment law policy arguments. When viewed through a digital lens, these interpretations and expansions of BIT provisions will have potentially enormous consequences for investors, states, and the ISDS system at large.[26] Given the potential for investment claims in the digital era, the jurisdiction and admissibility of such claims is likely to be a divisive issue.

Although generally assessed holistically, two issues must be unpacked in order to understand whether digital assets are treaty

---

20. *See* Franck, *supra* note 19, at 442.

21. *See* Anzorena & Perry, *supra* note 18, at 60. Dispute settlement provisions in BITs cover several options—including access to domestic remedies, international arbitration, and state to state dispute settlement. *See id.*

22. *See* Franck, *supra* note 19, at 443. BITs vary and will specify dispute settlement procedures and institutional options including: "(1) an ad hoc tribunal under the United Nations Commission on International Trade Law ('UNCITRAL') Arbitration Rules, (2) the Stockholm Chamber of Commerce, or (3) a tribunal organized through the World Bank's [International Centre for Settlement of Investment Disputes (ICSID)]." Both the investors and state choose one arbitrator each and the procedure for the appointment of the third, presiding arbitrator may vary according to the institutional framework and specific rules. *Id.*

23. *See* M. SORNARAJAH, THE INTERNATIONAL LAW ON FOREIGN INVESTMENT 205–06 n.4 (4th ed. 2017). *But see* Prabhash Ranjan, *ISDS Transparency Provisions in the Indian Model BIT: A Half-Hearted Attempt?*, 15 TRANSNAT'L DISP. MGMT. J. 1, 1 (2018).

24. *See* SORNARAJAH, *supra* note 23, at 212.

25. *See id.* at 225–26.

26. *See* Julien Chaisse, *The Shifting Tectonics of International Investment Law: Structure and Dynamics of Rules and Arbitration on Foreign Investment in the Asia-Pacific Region*, 47 GEO. WASH. INT'L L. REV. 563, 563–65 (2015).

ready: whether there is (a) an investment and (b) a territorial link to the host state.

A. Is There an Investment?

To bring a claim under a BIT, the dispute must involve an applicable "investment" (*ratione materiae*) as one of three cumulative admissibility requirements.[27] BIT-covered investments historically included physical assets, such as machinery, property, or land.[28] As the nature of foreign investments shifted and evolved over time, the definition of an investment expanded to include things such as intangible assets, IPRs, and administrative rights.[29] Through this evolution, digital assets could be envisioned as covered investments under BITs.

First, it is important to address what kind of investments are on the horizon for the fourth industrial revolution.[30] To bridge the digital divide and provide broad digital development, countries will need wide-ranging investment strategies, including investment in digital infrastructure, digital firms, and the digitalization of companies across industries.[31] Information and communication technology (ICT) infrastructure, such as fiber-optic cables and internet exchange points (IXPs), is needed to establish and improve internet and mobile connectivity.[32] These physical assets are likely included under more

27. KRISTA NADAKAVUKAREN SCHEFER, INTERNATIONAL INVESTMENT LAW: TEXT, CASES AND MATERIALS 69 (2d ed. 2016). The other two admissibility requirements are *ratione personae*—that claimants must be protected investors under the BIT—and *ratione temporis*—that the BIT must already be in force at the time the dispute arose. *See* Kingdom of Lesotho v. Swissbourgh Diamond Mines (Pty) Ltd., [2017] SGHC 45 (Sing.).

28. *See* SORNARAJAH, *supra* note 23, at 14–15.

29. *See id.* at 15.

30. *See* LAXMI RAMASUBRAMANIAN, GEOGRAPHIC INFORMATION SCIENCE AND PUBLIC PARTICIPATION 19 (2008); KLAUS SCHWAB, THE FOURTH INDUSTRIAL REVOLUTION 12 (2016). According to the World Economic Forum founder Klaus Schwab, the fourth industrial revolution is a transformative period beginning at the turn of this century that is "characterized by a fusion of technologies . . . blurring the lines between the physical, digital, and biological spheres." Klaus Schwab, *The Fourth Industrial Revolution: What It Means, How to Respond*, WORLD ECON. F. (Jan. 14, 2016) https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ [https://perma.cc/RP5L-3T5R]. Beyond a simple expansion of the digital revolution that began in the 1960s, the fourth industrial era is distinguished from its predecessor by an unprecedented and exponential growth pattern that will reorganize global value chains and significantly transform the way that people work. The fourth industrial revolution encompasses breakthroughs in artificial intelligence, nanotechnology, biotechnology, robotics, and quantum computing, to name a few. *See* SCHWAB, *supra*, at 7–8.

31. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 158. Investing in digital development also contributes to achieving several interrelated sustainable development goals (SDGs), such as enrollment in higher education and women's empowerment. *See id.* at 195.

32. *See id.* at 194–96.

traditional definitions of investment and thus fall outside the scope of this Article.[33]

Another vital aspect of digital development involves investment in local digital firms that provide purely digital and mixed (i.e., physical and digital) goods and services, such as electronic payment support, cloud storage, e-commerce platforms, content and media, search engines, and social networks.[34] Finally, as companies turn to data to gain competitive advantage, the digitalization of all industries across existing global supply chains generates perhaps the farthest-reaching implications for ISDS claims.[35] These new digital goods and services and the digitalization of companies create innumerable cyber vulnerabilities[36] and generate even more questions about how BITs—designed for physical investments—will apply to these new digital assets.

Whether digital assets—from websites to customer data to computer systems and more—could qualify as "covered investments" under BITs will be contingent upon the specific facts of the dispute and the exact wording in the treaty. However, a theoretical assessment of the *ratione materiae* sheds some light on the admissibility of digital assets. To determine whether there is an investment, tribunals (1) use the investment definition in the applicable BIT and (2) assess certain economic criteria in order to distinguish an investment from a one-off commercial transaction.

1. Investment Definitions

A "covered investment" is defined by the parties to the BIT.[37] Where there is uncertainty about the *ratione materiae*, tribunals have several tools at their disposal for interpretation.[38] Approaches vary, but a typical starting point is article 31 of the Vienna Convention on the Law of Treaties, which incorporates an assessment of the ordinary

---

33. Note that fiber cables and IXPs are usually established by telecommunications operators, an industry often restricted from foreign direct investment (FDI). Several industries with some of the highest digital impact potential—such as media, telecommunications, textiles, and financial services—also rank at the top of FDI restricted industries, which could be problematic for growth and investment. *See id.* at 187.

34. *See id.* at 194. UNCTAD says this digitalization of supply chains has the potential to make the greatest global economic impact and will require an enormous amount of investment to create an end-to-end digital supply chain. *See id.* at 175, 179.

35. *See id.* at 175. For example, by creating digital systems to track inventory, using data analytics to improve customer service, or by automating certain manufacturing processes. *Id.*

36. *See* Shackelford, *supra* note 2, at 200.

37. SCHEFER, *supra* note 27, at 112.

38. *See* Kingdom of Lesotho v. Swissbourgh Diamond Mines (Pty) Ltd., [2017] SGHC 91 (Sing.).

meaning of the words in the investment definition, both in context of the other provisions and in light of the object and purpose of the BIT.[39] Many treaties also provide a nonexhaustive list of examples of qualifying assets, which could assist the Tribunal in deciding whether or not the disputed digital assets should fall under the definition.[40] For example, the German Model BIT states that:

> 1. [T]he term "investments" comprises every kind of asset . . . The investments include in particular:
>
> (a) movable and immovable property as well as any other rights in rem, such as mortgages, liens and pledges;
>
> (b) shares of companies and other kinds of interest in companies;
>
> (c) claims to money which has been used to create an economic value or claims to any performance having an economic value;
>
> (d) intellectual property rights, in particular copyrights and related rights, patents, utility-model patents, industrial designs, trademarks, plant variety rights;
>
> (e) trade-names, trade and business secrets, technical processes, know-how, and goodwill;
>
> (f) business concessions under public law, including concessions to search for, extract or exploit natural resources[.][41]

Support for including digital assets as investments can be seen in this type of "broad" asset-based investment definition.[42] These broad definitions are found in the majority of BITs and usually refer to an inclusion of "every kind of asset," as seen in the first sentence.[43] Giving credence to the ordinary meaning of the words, the United Nations Conference on Trade and Development (UNCTAD) Series on Issues in International Investment Agreements stated that the broad, "every kind of asset" terminology supports the idea that the investment definition "embraces everything of economic value, virtually without

---

39. *See id.* at 41 ("[T]he meaning must emerge in the context of the treaty as a whole (including the text, its preamble and annexes, and any agreement or instrument related to the treaty and drawn up in connection with its conclusion) and in the light of its object and purpose . . . The approach under Art 31 of the VCLT is a holistic one . . . ."). For a deeper discussion on the various methods of interpreting a treaty's "object and purpose" within the VCLT, see David S. Jonas & Thomas N. Saunders, *The Object and Purpose of a Treaty: Three Interpretive Methods*, 43 VAND. J. TRANSNAT'L L. 565, 577–82 (2010).

40. *See* RUDOLF DOLZER & CHRISTOPH SCHREUER, PRINCIPLES OF INTERNATIONAL INVESTMENT LAW 61 (2d ed. 2012).

41. FED. MINISTRY FOR ECON. & TECH., GERMAN MODEL TREATY art. 1(1) (2008) [hereinafter GERMAN MODEL BIT].

42. Shackelford et al., *supra* note 1, at 61.

43. *Id.* at 60; *see also* U.N. CONFERENCE ON TRADE AND DEV., UNCTAD SERIES ON ISSUES IN INTERNATIONAL INVESTMENT AGREEMENTS II: SCOPE AND DEFINITIONS, at 24, U.N. Sales No. 11.II.D.9 (2011).

limitation."[44] This suggests that digital assets could also fall within this broad type of investment definition.

Digital assets come in many forms, but—while the term has become more commonplace—there is no universally agreed upon technical or legal definition of a "digital asset."[45] However, digital asset managers, estate and tax planning experts, and various domestic legislators have begun to examine the definition more closely.[46] From their analysis, some basic characteristics have emerged, best summarized by this simple definition: "[A] digital asset is a collection of binary data which is self-contained, uniquely identifiable and has a value."[47]

The OECD describes data as a "core asset" in the digital economy, and assets are commonly understood to have economic value.[48] The value of digital assets is directly linked to their data, and the value of an asset can be better examined by breaking it into two categories: intrinsic and extrinsic.[49] The intrinsic value constitutes the primary data in a digital asset or the fundamental reason why someone might want the data.[50] Data with intrinsic value can be found in Bitcoin, in a company logo (i.e., a visual representation of binary data), or in a coveted domain name.[51] The extrinsic value of digital assets is represented by metadata, which contextualizes the data. Essentially, it is "data about data."[52] Typical metadata includes information, such as who created the data and when, a description of the data, and who has access to it.[53] According to a 2018 World Bank Report on Data

---

44. U.N. CONFERENCE ON TRADE AND DEV., *supra* note 43, at 24.

45. *See* Jonathan Bick, *All Digital Assets Are Not Legally Equal*, L.J. NEWSLETTERS (Nov. 2017), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/11/01/all-digital-assets-are-not-legally-equal/ [https://perma.cc/3FAM-GTUW]; Ralph Windsor, *Defining Digital Assets*, DIGITAL ASSET NEWS (Aug. 11, 2017), https://digitalassetnews.org/assets/defining-digital-assets/ [https://perma.cc/VCD6-5PCU].

46. *See, e.g.*, S.B. 301, 154th Gen. Assemb., Reg. Sess. (Ga. 2018); *see also* Bick, *supra* note 45; Windsor, *supra* note 45. For example, legislators across the United States have been updating and attempting to unify probate and estate planning laws to deal with the legal questions surrounding digital assets. *See, e.g.*, Ga. S.B. 301; REVISED UNIFORM FIDUCIARY ACCESS TO DIGITAL ASSETS ACT § 2 (UNIF. LAW COMM'N 2015).

47. Windsor, *supra* note 45.

48. OECD 2016 BACKGROUND PAPER, *supra* note 10, at 7.

49. *See* Ralph Windsor, *Re-Defining the Meaning and Scope of Digital Assets – Part 1*, DIGITAL ASSET MGMT. NEWS, https://digitalassetmanagementnews.org/features/re-defining-the-meaning-and-scope-of-digital-assets-part-1/ [https://perma.cc/8G3M-G5R5] (last visited Jan. 29, 2019).

50. *Id.*

51. *See* Windsor, *supra* note 45.

52. *Id.* For more information on metadata with relevant examples, see Piotr Kononow, *What is Metadata (With Examples)*, DATAEDO (Sept. 16, 2018), https://dataedo.com/blog/what-is-metadata-examples [https://perma.cc/X9ZW-XR74].

53. *See* Kononow, *supra* note 52.

Driven Development, "unprocessed data has relatively little value and needs to be mined, refined, stored, and sold on to create value."[54] As such, extrinsic value has become enormously important, as some of the world's leading companies generate the majority of their revenue from metadata by selling customer metadata to advertisers, sales companies, and data analytics firms.[55] For example, Alibaba—a retail platform with no physical inventory—has been valued at $450 billion.[56] Alibaba's user metadata holds enormous potential, as Alibaba uses its customer metadata from related purchases, search history, and buying patterns, and sells that information to third parties.[57] Experts predict that metadata will increase the company's value to $5 trillion over the next ten years.[58]

If tribunals accept the meaning that "every kind of asset" includes everything of economic value, then digital assets will clearly fall under these broad definitions. When facing a broad definition, some tribunals have adopted a straightforward approach of applying the rule that "any asset should be included."[59] However, this expansive view of interpretation is not universal. Some scholars advocate for a more cautious interpretation to avoid overburdening host states with obligations beyond their original contemplation.[60]

Nonexhaustive lists of assets further support the argument that digital assets are included in the definition of investment.[61] The

54. WORLD BANK, INFORMATION AND COMMUNICATIONS FOR DEVELOPMENT 2018: DATA-DRIVEN DEVELOPMENT 1 (2019).

55. *See* WORLD BANK, *supra* note 54, at 63; Peter Cohan, *Mastercard, AmEx and Envestnet Profit from $400M Business of Selling Transaction Data*, FORBES (July 22, 2018, 10:41 AM), https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/#3caff88d7722 [https://perma.cc/99LC-M8XF]. For more details on the new value for the commercialization of data, see WORLD BANK, *supra* note 54, at 55.

56. *See Early Backer of Alibaba Sees Trillion Dollar Value on User Data*, BLOOMBERG (Apr. 24, 2018, 5:00 PM), https://www.bloomberg.com/news/articles/2018-04-24/early-backer-of-alibaba-sees-trillion-dollar-value-on-user-data [https://perma.cc/W4VG-J4W7].

57. *See* WORLD BANK, *supra* note 54, at 18–22, 80.

58. *See Early Backer of Alibaba Sees Trillion Dollar Value on User Data*, *supra* note 56.

59. *See* Anderson et al. v. Republic of Costa Rica, ICSID Case No. ARB(AF)/07/3, Award, ¶ 46 (May 19, 2010), https://www.italaw.com/sites/default/files/case-documents/ita0031.pdf [https://perma.cc/282D-PEAE]; RosInvestCo UK Ltd. v. Russian Fed'n, SCC Case No. V079/2005, Final Award, ¶ 388 (Sept. 12, 2010), https://www.italaw.com/sites/default/files/case-documents/ita0720.pdf [https://perma.cc/8GBP-9QCF]; CAMPBELL MCLACHLAN, LAURENCE SHORE & MATTHEW WEINIGER, INTERNATIONAL INVESTMENT ARBITRATION: SUBSTANTIVE PRINCIPLES 227 (2d ed. 2017).

60. *See* SORNARAJAH, *supra* note 23, at 22.

61. The nonexhaustive list of assets is an area where tribunals often focus a lot of attention and place emphasis when they are assessing whether the asset falls under the investment definition in the BIT. *See* MCLACHLAN, SHORE & WEINIGER, *supra* note 59, at 229; Jan de Nul N.V. v. Arab Republic of Egypt, ICSID Case No. ARB/04/13, Decision on Jurisdiction, ¶¶ 28, 32 (June 16, 2006), https://www.italaw.com/sites/default/files/case-documents/ita0439.pdf [https://perma.cc/N85U-AN2P]; Petrobart Ltd. v. Kyrgyz Republic, SCC Case No. 126/2003,

categories inside the investment definition—such as intangible assets, IPRs, and business secrets—all support the inclusion of digital assets as well.[62] Digital assets are intangible and common examples include software, source codes, data packages, Internet of Things' data collections, email accounts, domain names, databases, designs, trade secrets, and digital currency.[63] Many of these examples could also be categorized as "business secrets" or IPRs. Additionally, a large part of the technology industry and digital economy is wrapped up in licensing agreements, similar to other types of foreign direct investment already covered under BITs.[64] Evidencing a link between these digital assets and examples inscribed in the included investments would be fairly straightforward in this context.

While digital assets could fall more easily into broad investment definitions and enumerated categories, not all definitions are drafted broadly. Some BITs use narrowing language in the investment definition to limit the applicable claims covered under the agreement, such as closed lists, restrictions on IPRs, or explicit exclusions.[65] A review of the new generation BITs from 2017 indicates more exclusions to the investment definition.[66] This may indicate states are taking steps to reduce their exposure regarding digital investments.

Arbitral Award, at 70 (Mar. 29, 2005), https://www.italaw.com/sites/default/files/case-documents/ita0628.pdf [https://perma.cc/8FY9-MWH3].

62. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 43, at 24; GERMAN MODEL BIT, *supra* note 41, art. 1(1)(d)–(e).

63. *See Digital Asset*, TECHOPEDIA, https://www.techopedia.com/definition/23367/digital-asset [https://perma.cc/JJB5-QD62] (last visited Jan. 29, 2019); John Spacey, *11 Examples of Digital Assets*, SIMPLICABLE (Mar. 9, 2017), https://simplicable.com/new/digital-asset [https://perma.cc/VD9S-2LS7]; Windsor, *supra* note 45.

64. *See* Raymond T. Nimmer, *Licensing in the Contemporary Information Economy*, 8 WASH. U. J.L. & POL'Y 99, 101 (2002). Foreign direct investment already includes license agreements, management contracts, and service agreements. *See* Catherine Yannaca-Small, *Definition of Investor and Investment in International Investment Agreements*, *in* INTERNATIONAL INVESTMENT LAW: UNDERSTANDING CONCEPTS AND TRACKING INNOVATIONS 7, 47 n.159 (2008). For example, Qualcomm, like many tech companies, derives a large portion of its profit from licensing agreements. *See Qualcomm, National Security, and Patents*, STRATECHERY (Mar. 13, 2018), https://stratechery.com/2018/qualcomm-national-security-and-patents/ [https://perma.cc/L73Y-57JF]. These agreements are dependent on stable regulatory environments, which raises concerns for investors about certainty in jurisdictions like China and—to an extent—the United States under the current Trump administration. *See* Alexis Blane, Note, *Sovereign Immunity as a Bar to the Execution of International Arbitral Awards*, 41 N.Y.U. J. INT'L L. & POL. 453, 475, 478 (2009); *Fact Sheet: Key Barriers to Digital Trade*, OFFICE U.S. TRADE REPRESENTATIVE (Mar. 2016), https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade [https://perma.cc/V65B-U545]; *Qualcomm, National Security, and Patents*, *supra*. For more on the tech industry's business models and investment strategies, see *Qualcomm, National Security, and Patents*, *supra*.

65. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 43, at 28–29.

66. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 120.

2. Economic Factors

Other factors beyond the investment definition will impact the interpretation of whether digital assets are "covered investments." Tribunals often consider a number of economic factors when assessing an investment, such as contribution of resources, duration of the investor's commitment, expectation of profits, economic development of the host state, and assumption of risk.[67] These factors arose from *Salini v. Morocco*, in which the Tribunal attempted to reconcile the investment definition in the BIT with a reference to "investment" in article 25(1) of the International Centre for Settlement of Investment Disputes (ICSID) Convention.[68] This undefined reference to the term "investment" in the jurisdictional clause of the ICSID Convention has created uncertainty for tribunals, which has led to a somewhat fragmented application of economic criteria when determining the admissibility of an investment.[69] At their core, these economic factors are used to distinguish and exclude one-off commercial transactions that do not display the envisioned qualities of a covered investment within the scope of BITs, such as pure commercial transactions for the sale of goods or services.[70] However, these criteria have not been universally accepted, receiving notable criticism from the Tribunal in *Biwater v. Tanzania* and the Annulment Committee in *Malaysian Salvors v. Malaysia*.[71]

Where does this leave the assessment of digital assets with regard to these economic factors? The answer is a bit ambiguous, as it is uncertain how tribunals will apply these factors.[72] Although not bound to follow previous arbitral decisions, a "soft" body of precedent has emerged in international investment law whereby tribunals extract

67. *See* DOLZER & SCHREUER, *supra* note 40, at 66; SCHEFER, *supra* note 27, at 79–81; Collins, *supra* note 17, at 4.

68. *See* DOLZER & SCHREUER, *supra* note 40, at 66. For a discussion on the various approaches and starting points for interpreting jurisdiction when Article 25 ICSID is involved, see *id.* at 61–76. The precursor to the *Salini* Criteria came from *Fedax v. Venezuela* where the Tribunal used some economic criteria to examine whether the dispute concerned an investment or merely a commercial transaction that would not be protected under the agreement. *See id.* at 66.

69. *See id.* at 66–67.

70. *See* Yannaca-Small, *supra* note 64, at 61, 75.

71. *See* Biwater Gauff (Tanz.) Ltd. v. United Republic of Tanz., ICSID Case No. ARB/05/22, Award, ¶¶ 314, 318 (July 24, 2008) [hereinafter *Biwater Gauff*, Award], https://www.italaw.com/sites/default/files/case-documents/ita0095.pdf [https://perma.cc/6N79-GBJ2]; Malaysian Historical Salvors v. Gov't of Malay., ICSID Case ARB/05/10, Decision on the Application for Annulment, ¶ 57 (Apr. 16, 2009), https://www.italaw.com/sites/default/files/case-documents/ita0497.pdf [https://perma.cc/B5ZJ-R5F4]; MCLACHLAN, SHORE & WEINIGER, *supra* note 59, at 222–23.

72. *See* MCLACHLAN, SHORE & WEINIGER, *supra* note 59, at 224.

and utilize persuasive principles from previous awards.[73] That said, two things are clear: First, in light of the confusion between the investment definition in article 25(1) ICSID and the investment definition in a BIT, digital assets would likely face even greater admissibility hurdles under an ICSID arbitration.[74] Although digital assets potentially satisfy these economic criteria, the types of digital assets vary greatly, which could affect the analysis. Contrastingly, digital assets more easily fall into the BIT "investment" definition. Therefore, investors should consider bringing claims related to digital investments in an ad hoc arbitration in order to avoid an added layer of jurisdiction analysis involving the *Salini* criteria. However, this is not foolproof, as many non-ICSID tribunals still use the *Salini* test, or some combination of additional criteria, to determine the admissibility of the investment.[75] Second, states could consider limiting the scope of the definition of investments by clarifying which economic factors are to be considered. In fact, some BITs already limit their definition by requiring an investment to have a connection to specific economic factors such as expectation of profits, a sustained duration of time, or assumption of risk.[76] For example, the US Model BIT defines an investment as "every asset that an investor owns or controls, directly or indirectly, that has the characteristics of an investment, including such characteristics as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk."[77]

This part of the investment definition is followed by an illustrative asset list similar to the one seen above in the German Model BIT.[78] Some tribunals, such as the one in *Romak SA v. Uzbekistan*, have given more credence to these purposeful economic connections and accordingly are more restrictive when interpreting investment

73. *See* Neil Q. Miller, Holly Stebbing & Ayaz Ibrahimov, *Precedent in Investment Treaty Arbitrations*, *in* INTERNATIONAL ARBITRATION REPORT 10, 10–12 (2017).

74. *See Biwater Gauff*, Award, *supra* note 71, ¶¶ 314, 318; *Malaysian Historical Salvors*, Decision on the Application for Annulment, *supra* note 71, ¶ 57; DOLZER & SCHREUER, *supra* note 40, at 61–76; MCLACHLAN, SHORE & WEINIGER, *supra* note 59, at 222–23.

75. *See* Romak S.A. (Switz.) v. Republic of Uzb., PCA Case No. AA280, Award, ¶ 188 (Nov. 26, 2009), https://www.italaw.com/sites/default/files/case-documents/ita0716.pdf [https://perma.cc/SUD2-EANB]; MCLACHLAN, SHORE & WEINIGER, *supra* note 59, at 217–218. In any forum for arbitration (SCC, UNCITRAL, PCA, ICC), the tribunal will have to establish jurisdiction through an analysis of the investment definition. *See* MCLACHLAN, SHORE & WEINIGER, *supra* note 59, at 217. However, where parties have agreed to an ICSID arbitration, there is potentially another layer of analysis beyond the relevant BIT arising out of another treaty, the ICSID convention. *See* DOLZER & SCHREUER, *supra* note 40, at 61–76; Yannaca-Small, *supra* note 64, at 53, 59–73.

76. *See* DOLZER & SCHREUER, *supra* note 40, at 66.

77. OFFICE OF THE U.S. TRADE REPRESENTATIVE, EXEC. OFFICE OF THE PRESIDENT, 2012 U.S. MODEL BILATERAL INVESTMENT TREATY art. 1 (2012).

78. *See* GERMAN MODEL BIT, *supra* note 41, art. 1.

definitions.[79] On the one hand, given the wide ranging and occasionally tenuous nature of digital assets, establishing these economic connections could be challenging.[80] On the other hand, the digital economy often operates on a long-term business model.[81] Tech companies usually require a significant amount of initial investment funding for research and development and market access over an extended period of time to see any significant economic benefit and return on their investment.[82] This model continues to be highly relevant in today's current tech growth market, as companies rely greatly on long-term accrual data and metadata as one of their main commodities.[83] This data mining process requires a large amount of initial investment and risk. Moreover, it is contingent upon operating over a significant period of time to produce scalable revenue.[84] As such, many digital investments would likely meet the core economic criteria to differentiate them from single commercial transactions.

Taken together, both a broad definition of investment and a consideration of economic factors support an arguable path for including digital assets as investments under BITs. However, another factor of the jurisdiction analysis—territoriality—might further complicate admissibility.

B. Is There a Territorial Link?

Some BITs require a physical nexus or territorial link between the investment and the host state, which in turn may pose challenges to establishing *ratione materiae* for digital assets. When present, the territorial requirement prescribes that the investment was "made in the territory of the host [state]."[85] The location and control of traditional physical assets such as a hotel or factory is uncomplicated, and tribunals have taken a narrow view of the territorial link where

79. *See* SCHEFER, *supra* note 27, at 75–77.

80. *See id.* at 113; Collins, *supra* note 17, at 3–6.

81. *See* Andrew D. Mitchell & Neha Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, 20 VAND. J. ENT. & TECH. L. 1073, 1129 (2018); *Lessons from Spotify*, STRATECHERY (Mar. 5, 2018), https://stratechery.com/2018/lessons-from-spotify/ [https://perma.cc/YEB7-CKK4]; *Qualcomm, National Security, and Patents*, *supra* note 64.

82. *See Lessons from Spotify*, *supra* note 81.

83. *See id.* The telecommunication network business models for investment "typically have high up-front costs, but very long-term returns." WORLD BANK, *supra* note 54, at xvii. Now, there is a shift from data transport towards data storage with giant aggregators and platforms paving the way for new operations. *See id.* Although the market has shifted, the model is similar, as these data storage companies rely on high up-front costs and long-term market access to customers before they see any returns. *See id.*

84. *See id.*

85. SCHEFER, *supra* note 27, at 112.

physical assets were involved.[86] Investors, however, have experienced difficulty establishing this link in cases involving financial instruments, such as loans.[87]

The extraterritorial nature of digital assets is already being debated among internet actors and will likely be a highly contentious jurisdictional issue in any digital asset investment case.[88] Establishing a territorial link to the host state might depend on the nature of the disputed digital asset itself.[89] Jonathan Bick, e-commerce and IP lawyer, scholar, and former IBM counsel, differentiates digital assets into three legal categories based on their location:

> 1. Class One. The first class of digital assets is contained on a device that is in the owner's control. Usually, this device is a computer or storage device. Class-one digital assets include emails, software, and content and data stored in tangible property, typically a decedent's home computer.
>
> 2. Class Two. A second class of digital assets are access rights and use rights to Internet assets located in a computer or other storage device owned by a person other than the digital asset owner. Class-two digital assets are emails, software, content and data stored in tangible property on a third-party's computer or other tangible property.
>
> 3. Class Three. Class-three digital assets are access and use rights related to internet assets, but unlike class-two digital assets, class-three digital assets do not have any physical point of presences (i.e., their existence is not dependent upon storage), hence they need not be stored anywhere. A domain name is an example of a class-three digital asset.[90]

With these distinctions in mind, location, possession, and control of digital assets might all become relevant factors in determining a

---

86. *See* Grand River Enters. Six Nations, Ltd. v. United States, UNCITRAL, Award, ¶¶ 5, 105 (Jan. 12, 2011), https://www.italaw.com/sites/default/files/case-documents/ita0384.pdf [https://perma.cc/Q5BK-GVQZ]; Bayview Irrigation Dist. et al. v. United Mexican States, ICSID Case No. ARB(AF)/05/1, Award, ¶ 44 (June 19, 2007), https://www.italaw.com/sites/default/files/case-documents/ita0076_0.pdf [https://perma.cc/3D7X-PS5P]; Canadian Cattlemen for Fair Trade v. United States, UNCITRAL, Award on Jurisdiction, ¶ 55 (Jan. 28, 2008), https://www.italaw.com/sites/default/files/case-documents/ita0114.pdf [https://perma.cc/8WSK-LBET]; DOLZER & SCHREUER, *supra* note 40, at 76–78.

87. *See* Abaclat & Others v. Argentine Republic, ICSID Case No. ARB/07/5, Decision on Jurisdiction and Admissibility, ¶ 374 (Aug. 4, 2011), https://www.italaw.com/sites/default/files/case-documents/ita0236.pdf [https://perma.cc/XGH2-J489]; Fedax N.V. v. Republic of Venez., ICSID Case No. ARB/96/3, Decision of the Tribunal on Objections to Jurisdiction, ¶¶ 23, 37 (July 11, 1997), https://www.italaw.com/sites/default/files/case-documents/ita0315_0.pdf [https://perma.cc/GS4C-PP68]; DOLZER & SCHREUER, *supra* note 40, at 66–67; SCHEFER, *supra* note 27, at 114.

88. *See Abaclat*, Decision on Jurisdiction and Admissibility, *supra* note 87, ¶ 8; *Fedax N.V.*, Decision of the Tribunal on Objections to Jurisdiction, *supra* note 87, ¶¶ 18, 24–26; DOLZER & SCHREUER, *supra* note 40, at 66, 76–77; SCHEFER, *supra* note 27, at 114. For an analysis of some of the challenges of internet jurisdiction, see WILLIAM J. DRAKE, VINTON G. CERF & WOLFGANG KLEINWÄCHTER, WORLD ECON. FORUM, INTERNET FRAGMENTATION: AN OVERVIEW 41–45 (2016).

89. *See* Bick, *supra* note 45.

90. *See id.*

territorial link with the host state.[91] It will be important to parse out the specific nature of the assets involved in the dispute.

Class One appears to be the easiest path to establish a territorial connection. For class-one digital assets, a territorial connection to the host state can be established if the claimant foreign investor has a physical presence in the host state where the relevant data is stored on local servers.[92] This could include internet service providers, online publishers, and telecommunications operators.[93] This class might also include digital service providers, such as online market places, online search engines, and cloud computing services, who "house" data on local servers within the territory.[94] Establishing physical connections, however, might turn on factual distinctions rather than industry ones. For example, cloud-based providers might house their servers locally, regionally, or on a server farm outside of the host state.[95] Where class-one assets are located on a physical entity—a computer or server—under the company's control inside the host state, a territorial link could likely be established.

Both class-one and class-two digital assets, as characterized in the definition above, exist in some physical form on a server or computer. An element of control distinguishes the classes: the physical storage or device is either in the owner's control or in the control of a third party. For example, class-two assets could include software, which grant use and access rights through licensing agreements to third parties.[96] Notably, software publishing comprises 31 percent of all information technology-related US outward foreign direct investment (FDI).[97] Since such software made by US investors is often made outside the host state in which the software is deployed, this

91. *See id.* These inquiries of "location" and "control" of the digital assets will also likely play a decisive role in determining state's liability for cyberattacks on such assets. *See* Collins, *supra* note 17, at 20–21.

92. *See* Bick, *supra* note 45.

93. *See* U.S. INT'L TRADE COMM'N, *International Trade and Investment in Digital Trade-Related Industries*, *in* DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, PART 1, at 4-10 (2013) [hereinafter U.S. INT'L TRADE COMM'N]. These three sectors made up 73 percent of all information services supplied abroad by US multinational corporations, through their US majority-owned foreign affiliates (MOFAs). *See id.*

94. *See* Simon Shooter & Esme Strathcole, *What Exactly Is a Digital Service Provider in the Context of NIS Directive? Could You Be a DSP and Not Know It?*, BIRD & BIRD (Apr. 2018), https://www.twobirds.com/en/news/articles/2018/uk/what-is-a-digital-service-provider-in-context-of-nis-directive [https://perma.cc/58SH-YJYQ].

95. *See* Quentin Hardy, *Where Does Cloud Storage Really Reside? And Is It Secure?*, N.Y. TIMES (Jan. 23, 2017), https://www.nytimes.com/2017/01/23/insider/where-does-cloud-storage-really-reside-and-is-it-secure.html [https://perma.cc/8QG2-8DAP].

96. *See Lessons from Spotify*, *supra* note 81; *Qualcomm, National Security, and Patents*, *supra* note 64.

97. U.S. INT'L TRADE COMM'N, *supra* note 93, at 4-15.

example would seem to, on its face, fail the territorial nexus requirement.

Class-three assets pose a new type of challenge, as by definition they have no physical presence anywhere. Data processing and Internet industries include a host of class-three activities, including data visualization and social media providers.[98] These data and Internet industries pose an interesting dilemma because their activities, transactions, and data exchanges often occur without any physical presence of the company inside the host state.[99] To this point, the United States International Trade Commission has indicated that FDI has potentially diminished in importance because "digital networks now allow companies to perform international business without a physical presence in a given country."[100]

Class One most clearly establishes a requisite territorial link to the host state, as the assets are "physically" located inside the host state within the control of the investor. Class Two—where the digital assets are outside the control of the investor—and Class Three—where the digital assets have less firm, physical connections—both pose challenges for establishing a territorial connection.[101] Since their locations fall outside the traditional understanding of "territory" and they are not "made in the host state," they appear to fail the prima facie territorial nexus requirement. However, there is hope for Class Two and Three assets, as the territorial link test might be applied differently to intangible assets.

In *Abaclat v. Argentina*, a case involving sovereign bond investments, the Tribunal used different criteria for intangible assets with regard to the territorial link, as compared to traditional tangible assets.[102] The Tribunal said that the "determination of the place of the

98. *See* Bick, *supra* note 45. Data processing and internet industries make up a significant portion of FDI coming out of the US. *See* U.S. INT'L TRADE COMM'N, *supra* note 93, at 4-14–4-16.

99. *See* U.S. INT'L TRADE COMM'N, *supra* note 93, at 4-3, 4-7–4-8, 4-18–4-19. Some big-name internet and data companies involved in providing these services (e.g., Google, Facebook, and Twitter) have established a physical presence inside the host state. *See* Jon Russell, *Vietnam's New Cyber Security Law Draws Concern for Restricting Free Speech*, TECHCRUNCH (June 12, 2018), https://techcrunch.com/2018/06/12/vietnams-new-cyber-security-law-draws-concern-for-restricting-free-speech/ [https://perma.cc/PYM5-GPYV] (noting that Google and Facebook, while maintaining overseas locations in places like Singapore and Hong Kong, are being pressured into establishing physical presences in other countries as well).

100. *See* U.S. INT'L TRADE COMM'N, *supra* note 93, at 4-9 n.24.

101. *See* SCHEFER, *supra* note 27, at 112; Collins, *supra* note 17, at 21.

102. *See Abaclat*, Decision on Jurisdiction and Admissibility, *supra* note 87, ¶ 713; Matthew Gearing, *Abaclat and Others v The Argentine Republic (Formerly Giovanna A Beccara and Others v The Argentine Republic)*, ALLEN & OVERY (Dec. 8, 2011), http://www.allenovery.com/publications/en-gb/Pages/Abaclat-and-Others-v-The-Argentine-Republic-(Formerly-Giovanna-A-Beccara-and-Others-v-The-Argentine-Republic).aspx [https://perma.cc/U6LC-VVK7].

investment firstly depends on the nature of such investment" and "the relevant criteria should be where and/or for the benefit of whom the funds [were] ultimately used, and not the place where the funds were paid out or transferred."[103] If financial instruments can be equated to digital assets through the fact that they are both intangible assets, then it is likely that the same test could apply. Therefore, it could be argued that Class Two and Class Three assets are sufficiently tied to the host state via the benefit these digital assets provide to the host state. The use of software, access to information via search engines, or the use of online retail platforms for the spreading of e-commerce arguably provide benefits to the host state.[104] These services could be proven factually to benefit the host state, which could in turn provide a sufficient link to satisfy the territoriality requirement.

The *Abaclat* test for intangible assets eliminates some of the ambiguities regarding the location of the digital assets by emphasizing whether or not they are used to create benefits inside the host state.[105] However, the dissenting opinion against this interpretation of the territorial nexus might reduce the strength of this argument.[106] In his dissent, Professor Georges Abi-Saab's objectied to the territorial nexus focusing mostly on the fact that the financial instruments in dispute were international securities being traded on secondary markets outside of Argentina and thus, could not be territorially linked to the host state in any way.[107] Professor Abi-Saab distinguished *Abaclat* from the previous cases where a "benefit to the host state" argument was used to establish a territorial requirement.[108] He stated that the "security entitlements in question are free-standing, and totally unhinged . . . [and] do not form part of an economic project, operation or activity in Argentina."[109] However, the *Abaclat* test could still find that Class Two and Three assets meet the territorial requirement, as evidence of their benefits to the host state could be easily demonstrated.

---

103. *Abaclat*, Decision on Jurisdiction and Admissibility, *supra* note 87, ¶ 374.

104. *See* DRAKE, CERF & KLEINWÄCHTER, *supra* note 88, at 3. With regard to how to apply the test of where the investments are being used, the Tribunal in *Abaclat* said, "Thus, the relevant question is where the invested funds ultimately made available to the Host State and did they support the latter's economic development?" *Abaclat*, Decision on Jurisdiction and Admissibility, *supra* note 87, ¶ 374.

105. *See Abaclat*, Decision on Jurisdiction and Admissibility, *supra* note 87, ¶¶ 374–78.

106. *See* Abaclat & Others v. Argentine Republic, ICSID Case No. ARB/07/5, Dissenting Opinion of Georges Abi Saab, ¶¶ 73–102 (Aug. 4, 2011), https://www.italaw.com/sites/default/files/case-documents/italaw4085.pdf [https://perma.cc/66S7-BUXT].

107. *See id.* ¶¶ 78, 99.

108. *Id.* ¶¶ 96–97. The *Abaclat* Tribunal relied on analysis of *SGS v. Paraguay*, *SGS v. Philippines*, and *Fedax v. Venezuela*. *See id.* ¶¶ 100–01, 108 (discussing the distinctions).

109. *Id.* ¶ 108.

C. Summary of Digital Assets as Covered Investments

To the extent that investment definitions are drafted broadly—set on a framework capable of expanding to include new types of investments, together with a list of assets including things like intangible property and IPRs—it is possible to see how digital assets could fall within most definitions of a "covered investment." However, recent trends towards limiting the definition could indicate that states are being more cautious and trying to limit their exposure to claims involving digital assets.[110] Additional difficulties arise when determining the location of digital assets, and this will likely be a source of contention when trying to establish a territorial nexus with the host state.[111] Counsel should consider the enormous variety of assets and cybercrime-related scenarios involved in digital development when contemplating whether or not to bring a claim.

From websites and software used by digital firms to big data processes used by traditional supply chains, the potential for ISDS claims surrounding digital assets is extremely difficult to consider in the abstract. Current investor-state disputes turn crucially on the facts of the case, and disputes in the digital era will be no different.[112] Whether a digital asset will qualify as an investment or not will largely depend on the context of the specific facts and the exact wording in the BIT at issue.[113] The gravity of the interpretation of the investment definition with regard to digital assets cannot be emphasized enough, as the definition is a threshold criterion and is inextricably linked to the power and force of the substantive BIT protections.

III. ARE THERE VIABLE INVESTMENT CLAIMS FOR THE DIGITAL ERA?

Can BITs provide any meaningful protection for investors in cases of cybercrime? If cybercrime claims are to be addressed in the ISDS system, a large number of cases may arise given the pervasive, global nature of the problem. From law firms to retail companies to insurance providers, companies across most industries now mine vast amounts of information to transform their operations and, in turn, improve their business models.[114] As a result of this digitalization, a

110. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 120.

111. *See supra* discussion and sources cited Section II.B.

112. *See* Jean Kalicki & Suzana Medeiros, *Fair, Equitable and Ambiguous: What Is Fair and Equitable Treatment in International Investment Law?*, 22 ICSID REV.: FOREIGN INV. L.J. 24, 25–26 (2007).

113. *See* DOLZER & SCHREUER, *supra* note 40, at 63, 65, 70.

114. *See, e.g.*, Shahar Markovitch & Paul Willmott, *Accelerating the Digitization of Business Processes*, MCKINSEY & CO. (May 2014), https://www.mckinsey.com/business-functions/

company's value is now inextricably intertwined with its information portfolio.[115] These information portfolios are threatened by cyber theft, economic espionage, data breaches, and system interferences, all of which could result in huge losses for investors.[116]

A 2017 study found that the global average cost of one data breach for a single company was $3.62 million.[117] The costs are calculated using direct and indirect expenses including in-house investigations, outside forensic experts, and a decrease in customers.[118] However, the cost calculations do not fully capture the potential losses for companies and investors, as the loss from damage to the company's reputation, trade secrets, privileged information, or other proprietary data could threaten to destroy a business altogether.[119] Cybersecurity law professor Jeff Kosseff states, "As an increasing amount of data is stored on computers and in remote data centers, espionage and . . . the theft of confidential business information such as trade secrets could undercut a company's entire economic model."[120] In this context, and with the above policy considerations in mind, this section will examine the viability of three potential cyber claims rooted in BIT provisions: (a) violation of fair and equitable treatment, (b) full protection and security, and (c) expropriation.

A. Fair and Equitable Treatment

The fair and equitable treatment (FET) provision requires that the host state must provide fair and equitable treatment to investors at all times.[121] FET provisions provide a lens through which to view changes to government regulations, laws, administration, and systems

---

digital-mckinsey/our-insights/accelerating-the-digitization-of-business-processes [https://perma.cc/67PT-K6WY]; *see also supra* sources cited and text accompanying notes 55–58.

115. *See* PONEMON INSTITUTE, 2016 COST OF CYBER CRIME STUDY & THE RISK OF BUSINESS INNOVATION 12 (2016); Shackelford et al., *supra* note 1, at 3; *see also supra* sources cited and text accompanying notes 55–58.

116. *See* PONEMON INSTITUTE, *supra* note 115, at 12; Shackelford et al., *supra* note 1, at 3; Hyla, *supra* note 1, at 318.

117. *See* PONEMON INSTITUTE, 2017 COST OF DATA BREACH STUDY: GLOBAL OVERVIEW 1 (2017).

118. *See id.* at 7.

119. *See id.*; Shackelford et al., *supra* note 1, at 66; Eubanks, *supra* note 7; Gary Miller, *60% of Small Companies That Suffer a Cyber Attack Are out of Business Within Six Months*, DENVER POST (Mar. 24, 2017, 12:29 PM), https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/ [https://perma.cc/8TY2-VSZN].

120. JEFF KOSSEFF, CYBERSECURITY LAW 233 (2017).

121. For an illustration, see DEP'T OF FOREIGN AFFAIRS & INT'L TRADE, AGREEMENT BETWEEN CANADA AND [COUNTRY] FOR THE PROMOTION AND PROTECTION OF INVESTMENTS art. 5(1) (2004) [hereinafter CANADA MODEL BIT] ("Each Party shall accord to covered investments treatment in accordance with the customary international law minimum standard of treatment of aliens, including fair and equitable treatment and full protection and security.").

as they relate to and impact foreign investment.[122] This obligation is general and undefined in both meaning and scope.[123] As a result of the vagueness of the provision, interpretations of the standard can vary greatly, with tribunals using some combination of the Vienna Convention, title of the provision, and neighboring provisions to provide insight on how to interpret the standard.[124] This mix of interpretive tools can lead to inconsistencies in tribunal decisions.[125] However, the undefined nature of FET provisions makes them a very attractive option for investors, as FET is capable of adapting to different circumstances and to modern times, in an effort to uphold the rule of law.[126]

Therefore, FET provisions may allow investors to pursue cyber claims where, for example, the host state implements new regulations, such as source code disclosure requirements or changes that impact cross-border dataflows or data localization requirements.[127] These types of measures might substantially undermine the value of an investment if they are being applied arbitrarily or where the administrative process lacks transparency. These measures could also amount to an indirect expropriation of digital assets, which will be discussed in the expropriation section below.[128] FET provisions, however, could provide more flexible protection that is easier to apply than the test for indirect expropriation.[129]

In an FET assessment, a tribunal must determine if the new measure or state action is manifestly arbitrary or contrary to the reasonable, legitimate expectations of the investor.[130] This determination is made with help from some core principles of FET, such as consistency, reasonableness, nondiscrimination, transparency, or due process.[131] Breaches of FET are often the result of measures or acts

---

122. *See* CHRISTOPHER F. DUGAN ET AL., INVESTOR-STATE ARBITRATION 502–05 (2011).

123. *See id.* at 504–05.

124. *See* Kalicki & Medeiros, *supra* note 112, at 25, 43.

125. *See id.* at 43.

126. *See* DUGAN ET AL., *supra* note 122, at 505.

127. *See* RACHEL F. FEFER ET AL., CONG. RESEARCH SERV., R44565, DIGITAL TRADE AND U.S. TRADE POLICY 12–14 (2018). Changes to cyber regulations, such as data localization requirements or source code disclosure requirements, can be used for legitimate public policy objectives. However, these policies are often used as a way to favor domestic industries or IPRs at the expense of foreign investors and can also operate as nontariff barriers blocking market access for digital trade. *See id.*

128. *See infra* Section III.C.

129. *See* Kalicki & Medeiros, *supra* note 112, at 25.

130. *See* DUGAN ET AL., *supra* note 122, at 507–10. Tribunals have taken diverging approaches when assessing the FET standard, with some looking at the investors "legitimate expectation" as the main factor in deciding claims, while others have found state liability on the basis of "manifestly arbitrary" conduct. Kalicki & Medeiros, *supra* note 112, at 45–52.

131. *See* Kenneth J. Vandevelde, *A Unified Theory of Fair and Equitable Treatment*, 43 N.Y.U. J. INT'L L. & POL. 43, 49–54 (2010).

that are contrary to a combination of these core principles.[132] These core principles overlap and intersect, and tribunals rarely separate them out completely in practice.[133] However, for the purposes of this analysis, this Article focuses on a few principles that could be applicable to digital assets.[134] As states seek to navigate and regulate cybercrime, they face a challenging regulatory dichotomy giving rise to two types of potential FET claims. This in turn raises the questions: (1) Do changes to national cybersecurity measures lack consistency or reasonableness? (2) Could there be a claim of denial of justice or due process?

1. Do Changes to National Cybersecurity Measures Lack Consistency or Reasonableness?

Stability and transparency of the legal and regulatory framework for conducting business in the host state is a reasonable right for investors to expect and key to the investor's ability to function as a business.[135] Accordingly, states must act in ways that provide consistency for foreign investors.[136] US foreign investors operating in China, for example, claim that ambiguous and vaguely worded administrative and licensing requirements have driven certain digital service providers, such as cloud computing firms, out of the Chinese market.[137] States may change and adapt their policies over time,[138] and cybersecurity and privacy concerns can lead to necessary policy changes.[139] US investors, however, complain that opaque changes to cyber legislation has led to forced technology transfer—via changes in

---

132. *See id.* at 54.

133. *See* DUGAN ET AL., *supra* note 122, at 513.

134. In addition to its principles of consistency, nondiscrimination, due process, and reasonableness, FET normative content also includes factors such as transparency and good faith. *See* Vandevelde, *supra* note 131, at 52.

135. *See* Occidental Expl. & Prod. Co. v. Republic of Ecuador, LCIA Case No. UN3467, Final Award, ¶ 183 (July 1, 2004), https://www.italaw.com/sites/default/files/case-documents/ita0571.pdf [https://perma.cc/N3US-Q6VN].

136. *See* Vandevelde, *supra* note 131, at 66.

137. *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, EXEC. OFFICE OF THE PRESIDENT, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECHNOLOGY TRANSFER, INTELLECTUAL PROPERTY, AND INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974, at 39 (2018).

138. *See* PSEG Global, Inc. v. Republic of Turkey, ICSID Case No. ARB/02/5, Award, ¶¶ 250–56 (Jan. 19, 2007) [hereinafter *PSEG Global*, Award], https://www.italaw.com/sites/default/files/case-documents/ita0695.pdf [https://perma.cc/49WR-7NHJ].

139. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 209–10. In fact, cybersecurity and privacy concerns have already resulted in policy changes. For an overview of global cybersecurity policy changes as of 2017, see Daniella Terruso & Adam Palmer, *2017 Global Cybersecurity Policy: Challenges & Highlights*, CYBERSEC F. (Feb. 6, 2017), http://2016.cybersecforum.eu/en/2017-global-cybersecurity-policy-challenges-highlights/ [https://perma.cc/3J5L-Q7AJ].

source code disclosure requirements, for example—and discrimination against foreign investors who have difficulty navigating the sometimes unwritten rules of the regulatory process in China.[140]

Administrative changes are permissible as the host state has the right to regulate to achieve legitimate public policy goals.[141] At times, fast action is necessary to combat the dynamic cybercrime situation; however, quick back-and-forth "roller coaster" changes to the law, like those seen in *PSEG Global v. Republic of Turkey*, could violate the consistency principle under FET.[142] In *PSEG Global*, the Tribunal found that Turkey's continuous legislative and administrative changes violated the Turkey-USA BIT's FET provision.[143] These roller coaster changes undermined PSEG's investment, especially with regard to the shifting legal corporate status of PSEG's mining project and tax concessions.[144] Hasty modifications to digital regulations may make compliance impracticable or impossible where the changes threaten to shut down operations in the host state.[145] Rapidly evolving cyber threats call for rapid action and legislation from governments. Too many changes in cyberlaws, however, could lead to too much uncertainty for investors and to FET violations.[146]

Where the state adopts two simultaneously inconsistent policies, such action could also violate the FET standard.[147] As digital trade and investment are multisectoral industries involving many ministries, states are responsible for adequately consulting relevant arms of government when considering changes to digital and cyber policy that could be contrary to their obligations under their BITs.[148] In *MTD Equity v. Republic of Chile*, the Chilean investment authority approved a project with a Malaysian company to develop serviced apartments.[149] However, once the project was ostensibly complete, local zoning officials refused to grant certain licenses needed to open and operate the apartments.[150] The tribunal found that Chile had violated the FET provision, as it had taken two inconsistent positions with the investor.

---

140. *See* OFFICE OF THE U.S. TRADE REPRESENTATIVE, *supra* note 137, at 37.

141. *See* AES Summit Generation Ltd. v. Republic of Hungary, ICSID Case No. ARB/07/22, Award, ¶¶ 10.3.7–10.3.9, 13.3.2 (Sept. 23, 2010), https://www.italaw.com/sites/default/files/case-documents/ita0014_0.pdf [https://perma.cc/2ZG2-QWVB].

142. *See PSEG Global*, Award, *supra* note 138, ¶ 250.

143. *See id.* ¶¶ 250–56.

144. *See id.* ¶¶ 286, 304.

145. *See id.* ¶¶ 250–56.

146. *See id.* ¶¶ 253–56.

147. *See* MTD Equity Sdn. Bhd. v. Republic of Chile, ICSID Case No. ARB/01/7, Award, ¶¶ 165–66 (May 25, 2004), https://www.italaw.com/sites/default/files/case-documents/ita0544.pdf [https://perma.cc/R28R-A5JR].

148. *See id.* ¶¶ 166–67.

149. *See id.* ¶¶ 40, 53.

150. *See id.* ¶¶ 74, 80.

[151] Similar circumstances have arisen where states have implemented subsequent data localization policies requiring "digital firms to store and process local data within a country."[152] Data localization has been touted by some states as a way to protect national security or privacy, while others attribute those policies up to digital protectionism.[153] Meanwhile, tech experts challenge the veracity of protecting privacy or cybersecurity via data localization.[154] These data localization policies significantly increase costs and reduce investment. They can also force smaller digital firms to leave the host state, resulting in less proficient service providers for domestic businesses and customers.[155]

Data localization can also limit cross-border dataflows and content restrictions, which can amount to substantial internet censorship and fragmentation.[156] Changes to regulations on content restrictions in the name of cybersecurity could pose interesting challenges for investors. Per the 2017 World Investment Report, "[c]ontent restrictions, ranging from filtering to internet shutdowns, can undermine opportunities in a country and fuel uncertainty for investors."[157] In 2015, temporary internet shutdowns resulting from changes to content restrictions and censorship laws cost an estimated $2.4 billion globally.[158] In a recent example, the Vietnamese government passed a cybersecurity law requiring data localization—tightening up restrictions on internet dataflows and content.[159] Google,

151. *See id.* ¶ 166.

152. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 208.

153. Data localization can be defined generally as "laws that limit the storage, movement, and/or processing of data to specific geographies." There are several types of territorially-based data localization policies, including physical "housing" of data, network architecture requirements, routing changes, and cross border dataflow restrictions. Data localization requirements have been debated on the international forum since the 1970s. The latest iteration of the debate was brought to the forefront by the Snowden revelations and a rise in nationalist trade policies seeking "information sovereignty." For a more detailed view on data localization as it impacts the wider internet ecosystem, see DRAKE, CERF & KLEINWÄCHTER, *supra* note 88, at 41–45; FEFER ET AL., *supra* note 127, at 13–14.

154. *See* DRAKE, CERF & KLEINWÄCHTER, *supra* note 88, at 43–45.

155. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 208.

156. *See* DRAKE, CERF & KLEINWÄCHTER, *supra* note 88, at 41; FEFER ET AL., *supra* note 127, at 13; Susan Ariel Aaronson, *At the Intersection of Cross-Border Information Flows and Human Rights: TPP as a Case Study* 2–4 (George Washington Univ. Inst. for Int'l Econ. Policy, Working Paper No. IIEP-WP-2016-12, 2016); Terruso & Palmer, *supra* note 139.

157. U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 210 (citing to Table IV.6).

158. *See id.* at 208.

159. *See* Mai Nguyen, *Vietnam Lawmakers Approve Cyber Law Clamping down on Tech Firms, Dissent*, REUTERS (June 11, 2018, 11:04 PM), https://www.reuters.com/article/us-vietnam-socialmedia/vietnam-lawmakers-approve-cyber-law-clamping-down-on-tech-firms-dissent-idUSKBN1J80AE [https://perma.cc/YC8V-9GB7]; Russell, *supra* note 99.

Twitter, and Facebook have all objected to the changes not only on economic grounds, but also in a broader human rights context.[160]

In order to bring a hypothetical claim resulting from these data limits and content restrictions, investors would have had to rely in some capacity on assurances from the Vietnamese government for open, cross-border dataflows.[161] Were that reliance in place, the changes to Vietnam's cybersecurity laws might have fallen below the FET standard, as the new laws are inconsistent with the original assurances.[162] However, a foreign investor's reliance on such assurances must be "reasonable" following *International Thunderbird v. Mexico*.[163] In that case, International Thunderbird invested in gaming operations and equipment in Mexico, relying on an opinion from the Mexican authorities that the claimant's operations were legal.[164] The Mexican government later declared the operations illegal, Thunderbird brought a claim, and the Tribunal found that Thunderbird's reliance on Mexico's letter was not reasonable.[165] While Vietnam has made commitments to open cross-border dataflows in the Comprehensive and Progressive Agreement Trans-Pacific Partnership (CPTPP), investors may doubt whether they can *reasonably* expect completely open dataflows, given Vietnam's prior history of internet censorship, policies on content restriction, and high level of data

160. *See* Nguyen, *supra* note 159; Russell, *supra* note 99. Vietnam is a signatory to the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP—formerly known as TPP), for example, where it agreed to open cross-border dataflows—as delineated in article 14.11—with the hopes of some at the negotiating table that this might lead to knock-on human rights benefits for citizens via more access to information. For a view on open dataflows in the TPP and human rights, see Aaronson, *supra* note 156, at 16, 22–25.

161. *See* Katia Yannaca-Small, *Fair and Equitable Treatment: Have Its Contours Fully Evolved?*, *in* ARBITRATION UNDER INTERNATIONAL INVESTMENT AGREEMENTS: A GUIDE TO THE KEY ISSUES 501, 517–18, 520–21 (Katia Yannaca-Small ed., 2d ed. 2018).

162. To bring a challenge of the CPTPP e-commerce chapter under ISDS, a company would have to argue that the restrictions on open cross-border dataflows found in article 14.11 violate the FET standard. However, article 14.11 includes a wide exception—dataflows are subject to regulatory requirements to achieve legitimate public policy objectives. For more on the CPTPP's open cross-border dataflows, data localization, and exceptions, see Neha Mishra, *The Role of the Trans-Pacific Partnership Agreement in the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance?*, 20 J. INT'L ECON. L. 31, 37–39 (2017); *The TPP's Electronic Commerce Chapter: Strategic, Political, and Legal Implications*, COUNCIL ON FOREIGN REL. (Nov. 9, 2015), https://www.cfr.org/blog/tpps-electronic-commerce-chapter-strategic-political-and-legal-implications [https://perma.cc/U42P-P55B]. On exception, see Julien Chaisse, *Exploring the Confines of International Investment and Domestic Health Protections—Is a General Exceptions Clause a Forced Perspective?*, 39 AM. J.L. & MED. 332, 336–42 (2013).

163. *See* Int'l Thunderbird Gaming Corp. v. United Mexican States, Arbitral Award, ¶¶ 147–48 (Jan. 26, 2006), https://www.italaw.com/sites/default/files/case-documents/ita0431.pdf [https://perma.cc/8XHJ-BQUE].

164. *See id.* ¶¶ 50, 151–55, 163, 166.

165. *See id.* ¶¶ 151–55, 163, 166.

restriction.[166] Also, Vietnam has the right to regulate to achieve legitimate public policy goals, and regulatory action is necessary to combat cybercrime, which could make FET claims difficult.[167] On the one hand, these regulatory changes might be more about digital protectionism and information sovereignty than about cybersecurity, which could give hope to investors seeking similar FET claims on the basis of arbitrary or unjustified changes to the law.[168] On the other hand, national security will likely be a powerful exception for states to rely on to fend off these FET claims.[169]

In trying to bridge the global digital divide, countries seek to attract and engage foreign investors to help develop their digital prowess in areas such as ICT infrastructure, internet services, and digital solutions providers.[170] Increased regulation for privacy, data protection, and consumer protection can stimulate the digital economy, as online security measures build trust for users, businesses, and investors. However, navigating new cybersecurity or national security policies that are inadvertently (or intentionally) arbitrary, ambiguous, or lacking in transparency might undermine an investor's legitimate expectations of operating in that host state, resulting in FET claims.

2. Is There a Claim of Denial of Justice or Due Process?

Where investors are denied procedural justice with regard to digital assets, there is potential for an FET claim. There is some overlap between FET and full protection and security (FPS) obligations with regard to legal protections; the relationship between FET and FPS in these claims is explored in greater detail in Section III.B.3 below.

---

166. *See* MARTINA FRANCESCA FERRACANE ET AL., EUROPEAN CTR. FOR INT'L POLITICAL ECON., DIGITAL TRADE RESTRICTIVENESS INDEX 8, 51, 52, 57, 59–61 (2018); Aaronson, *supra* note 156, at 19; Richard Paddock, *Vietnamese Blogger Jailed for Environmental Reports*, BBC NEWS (Nov. 28, 2017), https://www.bbc.com/news/world-asia-42153142 [https://perma.cc/XG88-J79Q].

167. *See* AES Summit Generation Ltd. v. Republic of Hungary, ICSID Case No. ARB/07/22, Award, ¶ 13.3.2 (Sept. 23, 2010), https://www.italaw.com/sites/default/files/case-documents/ita0014_0.pdf [https://perma.cc/2ZG2-QWVB]; Nguyen Phuong Dung, *The Fair and Equitable Treatment Standard in Investor-State Arbitration in Vietnam*, INT'L ARB. ASIA (July 12, 2016), http://www.internationalarbitrationasia.com/vietnam-fair-and-equitable-treatment-in-investor-state-arbitration [https://perma.cc/9PVZ-G9XZ]; Nguyen, *supra* note 159.

168. *See* Anh Minh, *New Cybersecurity Law Won't Hassle Businesses: Deputy PM*, VNEXPRESS (June 27, 2018, 1:15 PM), https://e.vnexpress.net/news/business/new-cybersecurity-law-won-t-hassle-businesses-deputy-pm-3769528.html [https://perma.cc/B8PN-J9JK]; Nguyen, *supra* note 159. Vietnam's Deputy Prime Minister says that the law aims to protect Vietnam's sovereignty on the network space. *See* Minh, *supra*. At the same meeting, the Deputy Prime Minister tried to assuage businesses that the government will work to clear regulatory barriers and hurdles for foreign investors and companies operating in the country. *See id.*

169. *See* Shackelford et al., *supra* note 1, at 13, 32–33.

170. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 157, 190, 200.

The procedural protection provided by FET provisions affords foreign investors due process and the right to be heard.[171] While this obligation has been widely recognized by tribunals, these legal protections are fairly limited and the threshold for claimants to succeed on a claim of denial of justice is high.[172] In the context of cyber claims, where a host state lacks cyber legislation or prosecutorial remedies, host states might fall below the FET standard by failing to provide adequate access to local remedies in order to hear these types of claims.[173] The tribunal in *Waste Management Inc. v. The United Mexican States* noted that "in respect of a claim of judicial action—that is, a denial of justice—what matters is the *system* of justice and not any individual decision in the course of proceedings."[174] Thus, it is unclear whether the inability to hear or adequately try one cyber claim would amount to a legal system that falls short of the FET provision. Although the application of "legal" protections under FET is quite limited and may seem to be innocuous, the obligation under FET, because of its vagueness, could instead present an issue for host states with regard to digital assets and cyber-related crime.

B. Full Protection and Security

The FPS standard is a dual obligation for states to both refrain from any harmful acts and prevent harm to the investment from state and nonstate actors.[175] The FPS provision is usually coupled with the FET provision and generally states that "each Contracting Party shall accord to such investments full physical security and protection."[176] This protection was typically seen in cases of an uprising, insurrection, or other conflict situations.[177] However, now that investors' security concerns have expanded beyond armed rebels or angry rioters to include cybercriminals, perhaps the FPS provisions should include protections against these modern threats as well.

---

171. *See* Yannaca-Small, *supra* note 161, at 511–12.

172. *See id.* at 511–12.

173. *See* Collins, *supra* note 17, at 6, 19–20; Joyce Hakmeh, *Building a Stronger International Legal Framework on Cybercrime*, CHATHAM HOUSE (June 6, 2017), https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cybercrime [https://perma.cc/DG2S-7RCW].

174. Waste Mgmt, Inc. v. United Mexican States, ICSID Case No. ARB(AF)/00/3, Award, ¶ 97 (Apr. 30, 2004), https://www.italaw.com/sites/default/files/case-documents/ita0900.pdf [https://perma.cc/2KUP-PRQZ] (emphasis in original).

175. *See* Christoph Schreuer, *Full Protection and Security*, 1 J. INT'L DISP. SETTLEMENT 1, 1 (2010).

176. NETH. MINISTRY OF FOREIGN AFFAIRS, NETHERLANDS DRAFT MODEL BIT art. 9 (2018).

177. *See* MAHNAZ MALIK, INT'L INST. FOR SUSTAINABLE DEV., THE FULL PROTECTION AND SECURITY STANDARD COMES OF AGE: YET ANOTHER CHALLENGE FOR STATES IN INVESTMENT TREATY ARBITRATION? 5 (2011).

The FPS provision is rooted in customary international law principles and the belief that states are responsible for the protection of aliens inside their territory.[178] In the context of digital assets, cyberattacks from state actors may constitute state-sponsored economic espionage, which in turn could amount to a taking of foreign assets.[179] The remainder of this Section will address the host state's duty to protect foreign investors from nonstate actors.

Threat actors in a cyberattack include anyone seeking to disrupt one of the three fundamental pillars of security—confidentiality, integrity, or availability (CIA)—and prevent a system from performing as needed.[180] A cyberattack can involve unauthorized access to and theft of pertinent information, unsanctioned changes to data, or blocking the use or access to information or systems.[181] The consequences of such attacks have ranged from money losses and information theft[182] to full scale infrastructure destabilization.[183] Examples of cyberattacks are numerous and the motivations for these attacks have included political retaliation,[184] discrimination,[185] revenge,[186] and ideological criticisms.[187] It is important to note, "[I]t

178. *See* Collins, *supra* note 17, at 8–10.

179. *See* KOSSEFF, *supra* note 120, at 99–100; *infra* Section III.C.

180. *See id.* at 2, 63, 244l.

181. *See id.* at 1–2, 36.

182. *See* Jose Pagliery, *Premera Health Insurance Hack Hits 11 Million People*, CNN BUS. (Mar. 17, 2015, 7:07 PM), https://money.cnn.com/2015/03/17/technology/security/premera-hack [https://perma.cc/FE9V-7F5S]; *SWIFT Banking System Was Hacked At Least Three Times This Summer*, FORTUNE (Sept. 26, 2016), http://fortune.com/2016/09/26/swift-hack/ [https://perma.cc/9LRZ-A6W4].

183. *See* Shackelford, *supra* note 2, at 237; Andy Greenberg, *'Crash Override': The Malware That Took Down a Power Grid*, WIRED (June 12, 2017, 8:00 AM), https://www.wired.com/story/crash-override-malware/ [https://perma.cc/4HT8-6NVU].

184. *See* Ben Gilbert, *Hillary Clinton's Campaign Got Hacked by Falling for the Oldest Trick in the Book*, BUS. INSIDER (Oct. 31, 2016, 11:13 AM), https://www.businessinsider.com/hillary-clinton-campaign-john-podesta-got-hacked-by-phishing-2016-10 [https://perma.cc/4CLX-EQHR]; Jason Scott, *Vietnam-Aligned Hackers Attack Foreign Firms, FireEye Says*, BLOOMBERG (May 15, 2017, 3:18 AM), https://www.bloomberg.com/news/articles/2017-05-15/vietnam-aligned-hackers-attack-foreign-companies-fireeye-says [https://perma.cc/6TG4-SR9U].

185. *See* Scott, *supra* note 184.

186. *See* Catalin Cimpanu, *Revenge Hacks Cost Former Employee 34 Months in Prison, $1.1 Million in Damages*, BLEEPING COMPUTER (Feb. 17, 2017, 11:46 AM), https://www.bleepingcomputer.com/news/security/revenge-hacks-cost-former-employee-34-months-in-prison-1-1-million-in-damages/ [https://perma.cc/CS8T-E3ZQ].

187. *See* Robert Hackett, *What to Know About the Ashley Madison Hack*, FORTUNE (Aug. 26, 2015), http://fortune.com/2015/08/26/ashley-madison-hack/ [https://perma.cc/2PHX-8ZSW]. Cyber mischief may be especially difficult to counteract when conducted by national governments. *See* Bryan Druzin & Jessica Li, *Censorship's Fragile Grip on the Internet: Can Online Speech Be Controlled*, 49 CORNELL INT'L L.J. 369, 386 (2016). States frequently engage in cyberattacks where it relates to issues of domestic censorship. *See id.*; Andy Greenberg, *When Cyber Terrorism Becomes State Censorship*, FORBES (May 14, 2008, 6:00 PM), https://www.forbes.com/2008/05/14/cyberattacks-terrorism-estonia-tech-security08-

does not matter that the host state itself did not cause the damage, as long as the damage occurred within the territory."[188] Therefore, under the FPS obligation, a state may have an onerous duty to take steps to prevent cyberattacks from private actors that inflict damage to foreign investments inside the state.

However, not all cyberattacks are created equal. Targeted cyberattacks against specific companies might not fit the model of a civil disturbance as part of a larger, widespread conflict typical in FPS cases.[189] Similarly, FPS would not likely encompass protection against a major internet meltdown, an emergency situation, or some other wholly unprecedented event.[190] Tribunals have viewed these types of situations as outside the purview of FPS provisions, as a way to balance the state's obligations with the potentially wide breadth of the FPS provision.[191]

To better understand whether an FPS claim arising out of a cyberattack could succeed, it is necessary to first explore a few questions: (1) Does security extend beyond just "physical" protection?; (2) What is the host state's standard of liability?; and (3) How does FPS overlap with FET with regard to legal protection?

1. Does Security Extend Beyond Just "Physical" Protection?

The interpretation of the FPS security obligation began with more straightforward physical protections from actors, such as army, militants, and rioters.[192] Physical protection, however, is no longer an investor's only security concern. Crucially, as the investment definition has expanded, so too has the application of FPS.[193] To establish a

---

cx_ag_0514attacks.html [https://perma.cc/PV9N-HLY4]. Because of their political sensitivity, this may be particularly challenging to regulate. *See* Druzin & Li, *supra*, at 386. For more information on state-sponsored systems of cyber censorship, see *id.*; Bryan Druzin & Gregory S. Gordon, *Authoritarianism and the Internet*, 43 L. & SOC. INQUIRY 1, 1, 4 (2017) (citing fifteen states that notoriously manipulate online communication); Bryan Druzin & Jessica Li, *The Art of Nailing Jell-O to the Wall: Reassessing the Political Power of the Internet*, 24 J.L. & POL'Y 1, 1 (2016). Given its political sensitivity, committing states to address the issue of cyber manipulation through BITs may prove to be a sophisticated approach to this growing and serious problem. *See* Henry Gao, *The Doha Problem*, INT'L ECON. L. & POL'Y BLOG (Aug. 5, 2017, 12:51 AM), https://worldtradelaw.typepad.com/ielpblog/trade_and_the_internet/ [https://perma.cc/7W4A-ENJB].

188. Collins, *supra* note 17, at 10.

189. *See id.* at 18.

190. *See* Pantechniki S.A. Contractors (Greece) v. Republic of Alb., ICSID Case No. ARB/07/21, Award, ¶ 77 (July 30, 2009), https://www.italaw.com/documents/PantechnikiAward.pdf [https://perma.cc/S3BZ-786U].

191. *See* Collins, *supra* note 17, at 21–22, 29.

192. *See* Schreuer, *supra* note 175, at 2, 4.

193. *See* MALIK, *supra* note 177, at 7. FPS has been expanded to intangible assets and other protections including legal instability, regulation from states, and from an unsafe investment

breach, the claimant must show damage to either the physical asset or harm to the "stability of the overall investment," which has emerged as a way to protect new covered investments that are no longer simply physical in nature.[194]

Digital assets can include physical components such as hardware and data servers, which may be required to be located inside the host state to meet data localization requirements.[195] However, digital assets also include nonphysical components, such as logical software, customer and employee data, databases, information, digital goods, and company trade secrets.[196] Given the sometimes ethereal and intangible nature of digital assets, the expansion of the FPS protection is an important consideration when analyzing whether assets are adequately protected from cyberattacks. The convoluted mixture of tangible and intangible aspects of digital assets, along with a current lack of definitional clarity, means that FPS claims in this area will be highly fact specific as to which assets are involved in the dispute.[197]

The security obligation, qualified by the word "full" and in conjunction with a broad investment definition, has evolved over the years into a requirement to provide an overall safe investment environment following the standard set out in *Azurix v. Argentina*[198] and confirmed in *Compañia de Aguas and Vivendi v. Argentina,*[199] among other cases. If a host state fails to provide a safe investment environment in relation to cybersecurity (e.g., cybercrime laws, related extradition agreements), it may amount to a breach of the state's FPS obligation, even without physical damage.[200]

Evidence shows that poor cybersecurity protections and a lack of preparations by the state leave companies in that jurisdiction more vulnerable to cyberattacks.[201] This was seen in the 2007 and 2008

---

environment. *See id.* at 7, 9. For a detailed evolution of the case law expanding the definition, see *id.*

194. *Id.* at 1, 3.

195. *See* FEFER ET AL., *supra* note 127, at 13–14 17, 36.

196. *See id.* at 10, 16–17. Digital goods are defined as "[a]ny goods that are electronic in form and stored on some computer medium, for example a film or an electronic book." *Digital goods*, DICTIONARY OF THE INTERNET (Darrel Ince ed., 3d ed. 2013).

197. *See* Joseph Ronderos, *Is Access Enough?: Addressing Inheritability of Digital Assets Using the Three-Tier System Under the Revised Uniform Fiduciary Access to Digital Assets Act*, 18 TENN. J. BUS. L. 1031, 1047–49, 1064 (2017).

198. Azurix Corp. v Argentine Republic, ICSID Case No. ARB/01/12, Award, ¶¶ 406, 408 (July 14, 2006), https://www.italaw.com/sites/default/files/case-documents/ita0061.pdf [https://perma.cc/W8M7-STGK].

199. *See* Compañía de Aguas del Aconquija, S.A. v. Argentine Republic, ICSID Case No. ARB/97/3, Award, at 1, (Nov. 21, 2000), https://www.italaw.com/sites/default/files/case-documents/ita0206.pdf [https://perma.cc/ZT5E-KDHC].

200. *See* Collins, *supra* note 17, at 1–2, 19–20.

201. *See id.* at 16–17, 26–27.

cyberattacks in Estonia and Georgia, where each states' lack of vigilance was seen as contributing to the attacks' success.[202] Additionally, states without cybercrime laws provide sanctuary for criminals and hackers on two fronts.[203] First, they are not legally equipped to prosecute such crimes. Second, the lack of corresponding cybercrime laws also means that those individuals cannot be extradited internationally for prosecution in other jurisdictions where the cybercrimes are being investigated.[204] There is overlap here between how the FPS and FET provisions might be applied to digital assets in relation to a state's duty to have a well-functioning legal system.[205] In the context of FPS, for states with inadequate cyber protections, this lax approach to cybersecurity could constitute an unsafe investment environment, as it would leave digital assets more vulnerable to attacks.

Confirming the beginning of a trend in applying the FPS protection beyond physical protections and coming a year after *Azurix*, the Tribunal in *Siemens v. Argentina* began postulating about how FPS could apply to intangible assets.[206] In this case, Siemens contracted to provide a number of public services for Argentina. A dispute began over the renegotiation of the contract, which was found to have violated Siemens' legal security.[207] A key aspect of the Tribunal's reasoning, as noted above, was based on the investment definition in the Argentina-Germany BIT, which explicitly included "intangible assets."[208] However, the Tribunal qualified this expansion by adding that "[i]t is difficult to understand how the physical security of an intangible asset would be achieved."[209] The following year, the Tribunal in *Biwater v. Tanzania* further reiterated the trend of expanding protection beyond

202. *See id.* at 16–17.

203. *See* Hakmeh, *supra* note 173. In order to extradite cybercriminals for prosecution to another jurisdiction, most extradition treaties require "double criminality" meaning for the cybercriminal to be prosecuted, both countries in the process need a similar cybercrime law criminalizing the offense. *See id.*

204. *See id.*

205. *See* Schreuer, *supra* note 175, at 2, 9, 16. For further discussion, see *supra* Section III.B.3.

206. *See* Siemens A.G. v. Argentine Republic, ICSID Case No. ARB/02/8, Award, ¶ 303 (Jan. 17, 2007) [hereinafter *Siemens A.G.*, Award], https://www.italaw.com/sites/default/files/case-documents/ita0790.pdf [https://perma.cc/US7Y-Y5NA]; *see generally* Azurix Corp. v. Argentine Republic, ICSID Case No. ARB/01/12, Award (July 14, 2006), https://www.italaw.com/sites/default/files/case-documents/ita0061.pdf [https://perma.cc/W8M7-STGK].

207. *See Siemens A.G.*, Award, *supra* note 206, ¶¶ 81–84, 308. Note, the tribunal found a breach of legal security under both FPS and FET because the parties did not make a distinction. *See id.* at ¶¶ 302, 309.

208. *Id.* ¶¶ 69, 303.

209. *Id.* ¶ 303.

"physical" by emphasizing the word "full."[210] The *Biwater* Tribunal also included the possibility of expanding the definition to include commercial and legal protections.[211] The concept of legal protections was later developed in *Mohammad Ammar Al-Bahloul v. The Republic of Tajikistan*, where the Tribunal focused on the procedural aspect of the FPS standard and stated that it could "arguably cover a situation in which there has been a demonstrated miscarriage of justice."[212]

Digital assets are largely categorized as intangible, and thus could be contemplated as covered investments eligible for protection under the FPS standard. Certainly, harm to digital assets can occur due to a cyberattack, as data breaches of information systems and loss of company data can be extremely detrimental.[213] Like the tribunal in *Siemens v. Argentina*, it is difficult to envision what that protection should look like for these nontraditional expansions of the definition; however, a few ideas on how protection could be expanded are considered below.[214]

2. What Is the State's Standard of Liability?

When a foreign investor brings an FPS claim against a host state, the tribunal must first assess that state's standard of liability.[215] Full protection and security is an absolute standard, but it is not a standard of strict liability.[216] States are under an obligation to take some steps to ensure security for the investment,[217] which in turn requires states to exercise some due diligence to prevent harm.[218] One such step could be ratifying the Budapest Convention, an agreement widely regarded as the most comprehensive international agreement on cybercrime cooperation, which seeks to harmonize local laws and facilitate cross-border investigatory efforts.[219] However, international

---

210. Biwater Gauff (Tanz.) Ltd. v. United Republic of Tanz., ICSID Case No. ARB/05/22, Award, ¶¶ 729–31 (July 24, 2008), https://www.italaw.com/sites/default/files/case-documents/ita0095.pdf [https://perma.cc/6N79-GBJ2].

211. *See id.* ¶ 729.

212. Mohammad Ammar Al-Bahloul v. Republic of Taj., SCC Case No. V (064/2008), Partial Award on Jurisdiction and Liability, ¶ 246 (Sept. 2, 2009), https://www.italaw.com/sites/default/files/case-documents/ita0023_0.pdf [https://perma.cc/6644-2H7Q].

213. *See* PONEMON INSTITUTE, *supra* note 115, at 1, 12, 30.

214. *See Siemens A.G.*, Award, *supra* note 206, ¶ 303.

215. *See* MALIK, *supra* note 177, at 10–11.

216. *See id.* at 10.

217. *See id.*

218. *See* Collins, *supra* note 17, at 27.

219. *See* Hakmeh, *supra* note 173. The Convention on Cybercrime of the Council of Europe, also known as the Budapest Convention, has been ratified by most EU countries—as well as other countries, including the United States, Japan, Australia, and Canada. *See id.* The Convention was adopted in 2001 and is open for accession by non-convention parties. *See* Francesco Calderoni, *The*

commitments are perhaps beyond the standard of due diligence as they are time consuming and political, and they require states to relinquish some sovereignty.[220] Alternatively, states could take steps to amend their legislation and simply use the Budapest Convention—or aspects of it—as a model text for cybercrime legislation as some states and organizations have opted to do already.[221]

Additionally, since a lack of law enforcement capabilities and international cooperation can lead to a safe harbor for cybercriminals, updates to cyber-related legal institutions can also provide much-needed safeguards and enhance cybersecurity.[222] Specifically, states could enhance their ability to handle, collect, and preserve fragile evidence; they might also address international cooperation with regard to extraditing cybercriminals.[223] Such action could assist in creating a safe investment environment by preventing cybercriminals from seeking shelter in their jurisdiction and making states less vulnerable to cyberattacks.[224]

The expectation of states to exercise due diligence in cybersecurity measures is an objective standard, but it should be tempered with a modicum of subjectivity.[225] In practice, proportionality introduces an element of relativity for the states.[226] The tribunal in *Pantechniki v. Albania* explained that the duty for a state to comply with FPS is relative to the resources available to it.[227] This will be particularly relevant when working with digital assets, as "there is still a significant digital divide between developed and developing countries."[228] As foreign investors begin to implement digital development strategies in less developed countries, they cannot expect equivalent cybersecurity protections to those in developed countries.[229] Thus, in situations where there might be an unsafe investment environment as a result of a lax cybersecurity environment, states will

---

European Legal Framework on Cybercrime: Striving for an Effective Implementation, 54 CRIME L. & SOC. CHANGE 339 (2010) (manuscript at 1, 3 n.3) (on file with authors). Notably, Russia, China and India have not ratified. *See* Hakmeh, *supra* note 173. For more information, see Calderoni, *supra*, at 11 n.12.

220. *See* Hakmeh, *supra* note 173.

221. *See id.*

222. *See* Calderoni, *supra* at 219, at 3; Hakmeh, *supra* note 173.

223. *See* Calderoni, *supra* at 219, at 2; Hakmeh, *supra* note 173.

224. *See* Hakmeh, *supra* note 173.

225. *See* MCLACHLAN, SHORE & WEINIGER, *supra* note 59, at 332–33.

226. *See* MALIK, *supra* note 177, at 10.

227. *See* Pantechniki S.A. Contractors (Greece) v. Republic of Alb., ICSID Case No. ARB/07/21, Award, ¶ 76 (July 30, 2009), https://www.italaw.com/documents/PantechnikiAward.pdf [https://perma.cc/S3BZ-786U]; Schreuer, *supra* note 175, at 4.

228. U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 189.

229. *See* Collins, *supra* note 17, at 27.

likely only be held responsible to the extent that they would have been capable of providing a better environment.

The FPS standard is a reasonable pathway for cyber claims, as it contains the groundwork for including protection of intangible assets, and investors might seek recourse where states have allowed an unsafe investment environment prone to cyberattacks. However, these claims will be limited by the relativity of the proportionality standard, whereby those states vulnerable to cybercrime might also lack the means to provide adequate cybersecurity protections.

3. Does FPS Overlap with FET?

The FPS standard has a point of conjunction with FET in relation to legal security. While the FPS provision implies a positive obligation of due diligence on behalf of the state, requiring the state to take measures to prevent the investment from suffering harm caused by state agencies or third parties,[230] the FET standard entails both a negative obligation—to avoid issuing measures that negatively impact the investment—and positive duties, such as the duty to guarantee due process.[231]

The case law on this point has reached contradictory conclusions. While in some cases the two standards seem compatible, in others they exclude one another. To exemplify, in *Wena Hotels LTD v. Egypt*[232] and *Occidental Exploration and Protection Company v. Ecuador*, the Tribunal, having found a breach of the FET standard, automatically excluded the breach of the FPS.[233] On the contrary, the opposite solution was reached in *Jan de Nul v. Egypt*[234] and *Houben v. Burundi,*[235] where the tribunals stressed, in both cases, that the two standards were placed in different provisions within the applicable treaty. Scholars express varied opinions on the matter as well. According to Palombino, FPS is "no more than a specific instance of

230. *See* DOLZER & SCHREUER, *supra* note 40, at 149.

231. *See* DUGAN ET AL., *supra* note 122, at 491–93; Yannaca-Small, *supra* note 161, at 501, 511–12.

232. *See* Wena Hotels Ltd. v. Arab Republic of Egypt, ICSID Case No. ARB/98/4, Award, ¶ 95 (Dec. 8, 2000), https://www.italaw.com/sites/default/files/case-documents/ita0902.pdf [https://perma.cc/8M36-K6NG].

233. *See* Occidental Expl. & Prod. Co. v. Republic of Ecuador, LCIA Case No. UN3467, Final Award, ¶ 187 (July 1, 2004), https://www.italaw.com/sites/default/files/case-documents/ita0571.pdf [https://perma.cc/N3US-Q6VN].

234. *See* Jan de Nul N.V. v. Arab Republic of Egypt, ICSID Case No. ARB/04/13, Award, ¶ 269 (Nov. 6, 2008), https://www.italaw.com/sites/default/files/case-documents/ita0440.pdf [https://perma.cc/ATU7-ED7B].

235. *See* Joseph Houben v. Republic of Burundi, ICSID Case No. ARB/13/7, Award, ¶ 260 (Jan. 12, 2016), https://www.italaw.com/sites/default/files/case-documents/italaw7220.pdf [https://perma.cc/7NDH-ZNUA].

FET."[236] The connection between the two provisions can be found in their origin, as the two standards derive from the same norm of customary international law.[237]

While the International Telecommunication Union of the United Nations placed Singapore as the most committed country in the Global Cybersecurity Index (GCI) level,[238] the European Union is also dedicating attention to the issue.[239] In particular, the Directive on Security of Network and Information Systems (NIS Directive),[240] adopted on July 6, 2016, and entered into force in August 2016, sets various targets for member states, all to be transposed into national legislation by May 9, 2018.[241] The NIS Directive determined that member states shall designate computer security incident response teams (CSIRTs) and a Competent National NIS Authority.[242] It also created a cooperation group and set up a CSIRT network, aimed at promoting swift operational cooperation and exchanging information regarding cybersecurity incidents and risks.[243]

Through the implementation of the NIS Directive, a claim under FPS against a member state would be a difficult one. However, FET is much broader in scope; therefore, claims for a breach of FET cannot be excluded a priori.

Taking one step back, in the case of a state's absolute lack of cyberlaws, where the courts can apply analogical reasoning, courts could extend related, existing laws of theft, privacy, data management, intellectual property, damage to property, or trespassing to cybersecurity claims. However, if this extension is not possible, the absence of law on the matter could amount to an FPS violation, as the FPS standard imposes upon the state the obligation to provide a solid legal framework granting security to the investments even if the enforcement is delegated to agents or experts in the field.[244] Within this

236. F.M. PALOMBINO, *FET and the Ongoing Debate on Its Normative Basis*, *in* FAIR AND EQUITABLE TREATMENT AND THE FABRIC OF GENERAL PRINCIPLES 19, 26 (2018). For a legal and economic perspective on analyzing regulatory frameworks, see generally Julien Chaisse & Christian Bellak, *Navigating the Expanding Universe of International Treaties on Foreign Investment: Creation and Use of Critical Index*, 18 J. INT'L ECON. L. 79 (2015).

237. *See* George K. Foster, *Recovering "Protection and Security": The Treaty Standard's Obscure Origins, Forgotten Meaning, and Key Current Significance*, 45 VAND. J. TRANSNAT'L L. 1095, 1103 (2012).

238. *See* INT'L TELECOMM. UNIT, GLOBAL CYBERSECURITY INDEX (GCI) 29 (2017).

239. *See* Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 6.

240. *See id.* at 25.

241. *See id.* at 14.

242. *See id.* at 26.

243. *See id.* at 1–2.

244. *See* DOLZER & SCHREUER, *supra* note 40, at 14.

duty to provide cyber protection, the state faces two different challenges: First, if the legislation is too strict, it might limit the investors' range of action and impose burdensome responsibilities on them. Second, a complete regulatory gap should be avoided.

The claim for FPS does not exclude that a parallel claim for FET could be successful, if they address two different aspects of the state's conduct, for instance, if the host state does not guarantee due process.[245] On the other side of the spectrum, host states should exercise caution when making legislative changes, as a sudden change of cybersecurity laws imposing excessively burdensome duties on investors may also amount to an FET violation.

C. Expropriation

A final consideration in the digital assets debate is that of expropriation. Expropriation includes the outright taking of assets by the host state and more commonly takes the form of measures, regulations, or acts that, when viewed together, constitute the de facto taking of assets, known as indirect expropriation.[246] However, there might be a shift back towards claims for direct expropriation if digital assets could be covered under the investment regime.[247] Expropriation can extend to intangible assets, which could include digital assets as long as they can fall within the relevant investment definition.[248] This again highlights the significance of the investment definition and its relationship to the power of every other provision in the BIT as a threshold criterion.[249]

The digitalization of company data and information has made intellectual property such as trade secrets and other digital assets much harder to protect.[250] Evidence and accusations of state-sponsored cyber theft and economic espionage have become a developing issue in recent years.[251] The key question is whether these allegations can be framed and substantiated as viable claims in the form of expropriation

245. *See* Schreuer, *supra* note 175, at 13–14.

246. August Reinisch, *Expropriation*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL INVESTMENT LAW 408, 408 (Peter Muchlinski et al. eds., 2008); Julien Chaisse, *Promises and Pitfalls of the European Union Policy on Foreign Investment—How Will the New EU Competence on FDI Affect the Emerging Global Regime*, 15 J. INT'L ECON. L. 51, 84 (2012).

247. *See* Reinisch, *supra* note 246, at 448; Shackelford et al., *supra* note 1, at 7–12.

248. *See* Tokios Tokelés v. Ukraine, ICSID Case No. ARB/02/18, Award, ¶¶ 73–78 (July 29, 2007), https://www.italaw.com/sites/default/files/case-documents/ita0866.pdf [https://perma.cc/4M7K-X9RZ]; Reinisch, *supra* note 246, at 410.

249. *See* JESWALD SALACUSE, THE LAW OF INVESTMENT TREATIES 174–75 (2d ed. 2015).

250. *See* Shackelford et al., *supra* note 1, at 70.

251. *See id.*

violations. There are significant challenges to bringing a claim in this area.

Expropriation is, by definition, the taking of assets by the state.[252] Thus, it will be necessary to show the state's involvement in order to prevail on a claim. However, there are notorious attribution problems in cyber cases, meaning there are difficulties in pinpointing with certainty where an attack originated.[253] Attribution in cybercrimes is problematic, in part, because it is competing with the fundamental idea that the internet is one massive interconnected space, and therefore, a cyberattack cannot be treated in isolation.[254] For example, a US law firm was hacked with an infectious, system-threatening malware after filing a $2.2 billion claim against China.[255] Cyber experts suspected that the malware originated from China, but these claims were difficult to confirm with certainty, which prevented any legal action.[256] There are different levels of confidence in the tech sphere about the degree of certainty of attribution; and while some more vigorous methods of detection are available, they stand on questionable ethical ground, due to shifting legal rules around the use of these hacking detection tools.[257]

The attribution problem leaves room to question how tribunals will weigh evidence in cyber disputes.[258] Investors and states will need a clear understanding of how this kind of evidence will be evaluated, including burdens and standards of proof.[259] Another difficulty with connecting these attribution claims directly to the state is that there is often only a tenuous connection to the acquisition of the data or digital asset through a third-party actor.[260] Finally, states may hide behind "national security" reasons in response to alleged cyber espionage or acquisition of digital assets.[261] This is true especially for countries

252. *See* Reinisch, *supra* note 246, at 408.
253. *See* Shackelford et al., *supra* note 1, at 51.
254. *See id.*
255. *See* Silkenat, *supra* note 4, at 453.
256. *See id.*
257. *See* Shackelford et al., *supra* note 1, at 51; Praveen Dalal, *International Legal Issues of Cyber Attacks, Cyber Terrorism Cyber Espionage, Cyber Warfare and Cyber Crimes*, PERRY4LAW (June 28, 2016), http://perry4law.co.in/cyber_security/?p=89 [https://perma.cc/AN43-GFDA]; Hannah Kuchler, *Cyber Insecurity: Hacking Back*, FIN. TIMES (July 27, 2015), https://www.ft.com/content/c75a0196-2ed6-11e5-8873-775ba7c2ea3d [https://perma.cc/LV2S-6XW3]; David Strom, *What Are the Legalities and Implications of 'Hacking Back'?*, SECURITY INTELLIGENCE (May 29, 2018), https://securityintelligence.com/what-are-the-legalities-and-implications-of-hacking-back/ [https://perma.cc/857K-KERX].
258. *See* Strom, *supra* note 257.
259. *See* Shackelford et al., *supra* note 1, at 51.
260. *See id.* at 62.
261. *See id.* at 64.

which view economic interests as matters of national security.[262] Although the usurping of digital assets through state-sponsored cyberattacks creates a plausible claim for expropriation, tenuous state connections, political sensitivities, and attribution problems will significantly limit the potential success of these claims.

An indirect expropriation claim may also be possible with regard to digital assets. An indirect expropriation does not always resemble a "taking of assets," but rather it must be "deduced from a pattern of conduct, conception, implementation, and effects . . . even if intent is to avoid expropriation at every step."[263] There are many measures and regulations that are cause for concern in this area, particularly source code disclosure and content regulation.[264] These concerns could lead to significant value deprivation of the assets over time, particularly if the proprietary value of the asset is linked to its continued privacy.[265] The complexities of such a claim, however, fall outside the scope of this Article and will be addressed in a future work.

IV. CONCLUSION

There are many challenges to bringing a digital claim in the international investment law system. Given the rapidly changing cyber sphere, digitalization of companies, and the forecast for investment in digital infrastructure globally, however, future claims are likely to emerge.[266] To avoid uncertainty and eliminate risk, states can proactively address these issues by updating their BIT language to include language relating to cyber risk and digital assets. As the FDI discussion shifts towards a state's rights to regulate and emphasizes the importance of sustainable development, finding the right policy balance between protecting the public interest while still reducing digital protectionism will be key for creating digital-ready BITs.

---

262. *See* Shackelford et al., *supra* note 1, at 64; James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES (Feb. 15, 2014), https://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html [https://perma.cc/D738-GBQT]. The national security exception in BITs has evolved from thwarting military threats to "tackling economic crisis and protecting strategic industries." *See* U.N. CONFERENCE ON TRADE AND DEV., UNCTAD SERIES ON INTERNATIONAL INVESTMENT POLICIES FOR DEVELOPMENT: THE PROTECTION OF NATIONAL SECURITY IN IIAS, at 7–16, U.N. Sales No. 09.II.D.12 (2009).

263. Quasar de Valores SICAV S.A. v. Russian Fed'n, SCC Case No. 24/2007, Award, ¶ 45 (July 20, 2012), https://www.italaw.com/sites/default/files/case-documents/ita1075.pdf [https://perma.cc/85VE-LVTR].

264. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 209–11.

265. *See* Shackelford et al., *supra* note 1, at 7, 22–23.

266. *See* U.N. CONFERENCE ON TRADE AND DEV., *supra* note 6, at 158, 165–67, 195; Chaisse, *supra* note 26, at 612.

It will be particularly important for states to clarify the definition of "investment," as this acts as a gatekeeper for claims. Under current broad asset-based definitions, there is a path emerging to qualify digital assets as covered investments, as they are intangible property of enormous economic value.[267] This is particularly acute where data are kept on local servers inside the host state.[268] However, establishing a territorial connection might be a challenge for certain assets with tenuous links to the host state.[269] Depending on the nature of the assets involved in the dispute, the admissibility of the claim could be caught up in the complex debate surrounding internet jurisdiction.

While vague investment definitions initially existed to allow BITs to evolve over time, the exponential development and growth accompanying the fourth industrial revolution has been unprecedented.[270] The pace of the evolution of technology and surrounding investment is perhaps outside the scope of what was originally envisioned by the parties, and as a result, might have left states quite vulnerable to claims.[271] States are in a difficult position because, while it might be tempting to shut out protection for digital assets, a more nuanced approach to redefining investment definitions is advantageous to the overall growth of their economies.[272] A comprehensive digital development strategy for attracting FDI will likely include BITs, and as such, states must strike a delicate balance as they seek to redefine investment definitions for the digital era.

Additional BIT clarifications might include adding language specifically addressing cyberattacks with regard to the scope of the security protections envisioned under the FPS provision. The final consideration is related to the national security exception. National security arguments have the potential to thwart any claims or protections afforded by BITs—an issue that has also plagued IPRs and trade secret protection with regard to the WTO TRIPS Agreement.[273] Since trade secrets and IPR protection largely overlap with the cyber sphere and protection of digital assets, this exception will need to be addressed and solutions advised. Genuine solutions are important,

267. *See* OECD 2016 BACKGROUND PAPER, *supra* note 10, at 7; WORLD BANK, *supra* note 54, at 1; Shackelford et al., *supra* note 1, at 60–61; *supra* Section II.A.1.

268. *See* Shackleford et al., *supra* note 1, at 4–6; Bick, *supra* note 45; Shooter & Strathcole, *supra* note 94.

269. *See* SCHEFER, *supra* note 27, at 112; Collins, *supra* note 17, at 21; U.S. INT'L TRADE COMM'N, *supra* note 93, at 4-3, 4-7, 4-8, 4-18, 4-19.

270. *See* SCHWAB, *supra* note 30, at 11–13.

271. *See id.*; SORNARAJAH, *supra* note 23, at 206–08.

272. *See* FERRACANE ET AL., *supra* note 166, at 6.

273. *See* Shackelford et al., *supra* note 1, at 67.

particularly, in light of the need to balance genuine political sensitivities with the importance of bridging the digital divide.

Within the larger context of the internet, the aspirations for bridging the digital divide, and the imperative need for global cybersecurity, there are a few final points to consider. To achieve effective internet governance, states must exercise restraint in policy making. To prevent letting the pendulum swing too far in one direction due to knee-jerk, ideology-based reactions to cyberattacks, policy makers must maintain an evidence- and expert-based approach in order to create sustainable, effective cyber resilience.[274] Fear and anger towards attacks on the integrity of personal information and privacy is understandable. However, it is important to think broadly about policy decisions that will have a long-term impact on the future of the internet. In order to maximize the economic benefits of global online activity across populations, states and investors must build trust, and robust, cross-border security measures will be required. As such, governments and stakeholders should consider using BITs as a part of their wider cybersecurity risk management framework.

274. Antihacking legislation lacking nuance and an understanding of cybersecurity issues and operations in the United States has received wide criticism and pushback from cybersecurity experts, academics, and researchers. *See* Ms. Smith, *Hackers Protest Georgia's SB 315 Anti-hacking Bill by Allegedly Hacking Georgia Sites*, CSO ONLINE (May 2, 2018, 7:49 AM), https://www.csoonline.com/article/3269535/security/hackers-protest-georgias-sb-315-anti-hacking-bill-by-allegedly-hacking-georgia-sites.html [https://perma.cc/XY2K-SDEV]. New privacy and data protections are inadvertently solidifying the competitive advantage of giants like Facebook and Google—which already hold the lion's share of resources. Due to their position as data aggregators, widely framed legislation has walled out competitors. *See The Facebook Brand*, STRATECHERY (Mar. 19, 2018), https://stratechery.com/2018/the-facebook-brand/ [https://perma.cc/2CR6-82NG].