Grotius Centre Working Paper Series

No 2021/095-IEL — 27 April 2021

International Investment Law and Arbitration in Cyberspace

Eric de Brabandere

Universiteit Leiden
Grotius Centre for International Legal Studies

Unedited Version – Forthcoming
'International Investment Law and Arbitration in Cyberspace' in Nicholas Tsagourias and Russel Buchan (ed.), Research Handbook on International Law and Cyberspace (2nd Ed.) (Edward Elgar, 2021).

INTERNATIONAL INVESTMENT LAW AND ARBITRATION IN CYBERSPACE

Eric De Brabandere*

Introduction

Cybersecurity in international investment law and arbitration is a recent point of attention. Foreign investors, as any other businesses, are increasingly subjected to cyberattacks as part of the general rise of cyberattacks. Cyberattacks also have increased in terms of sophistication.[1]

In 2015, it was estimated that up to 50% of small businesses had been victims of cyberattacks, and 60% of those who suffered a significant cyberbreach went out of business within six months.[2] On average, one out of three businesses confronted with cyberattacks ended up paying a 'ransom' to the perpetrators.[3] The past years have witnessed several major cyberattacks on multinational enterprises, such as the well-

[1] For a general discussion, see Scott J Shackelford and others, 'Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties' (2015) 52(1) American Business Law Journal 1, 7 ff.
[2] International Bar Association, 'Cybersecurity Guidelines' (2018) 4.
[3] Karsten Lemmens, 'Eén bedrijf op drie betaalt losgeld aan cybercriminelen' (*De Standaard*, 12 May 2020) <www.standaard.be/cnt/dmf20200512_04955876> accessed 13 May 2020.

reported 2010 attack on Google[4], the attacks on Exxon Mobile that same year[5], and also less reported attacks on companies such as the January 2020 large-scale ransomware attack on the Belgian company Picanol Group which resulted in a temporary halt of production capacity and hence important financial losses.[6]

Cyberattacks result in various forms of damage, such as information loss, business disruption, revenue losses and damage to equipment.[7] In general, it has been reported that businesses lose on average '0.8 percent of their market value in the seven days following news of an adverse cyber event'.[8] This in turn has resulted in average financial losses ranging from $2.7 million[9] to $498 million per adverse cyber event.[10]

The question of cybersecurity, and the role and responsibility of the host State in which the foreign investor has invested has thus gained prominence, although so far based on the current publicly available information, no claim on that ground seems to have been brought. First of all, States seem to increasingly rely on concerns relating to the digital economy, such as security and consumer protection, in order to take measures or adopt a certain conduct which in itself may be considered detrimental to foreign investors and constitute a breach of the State's investment treaty obligations. Secondly, investment claims by targeted foreign investors against the host State for failure to provide the necessary security cannot be excluded.

When analysing these issues from the perspective of international investment law and arbitration, and before turning to possible violations of investment protection standards by host States, one first will need to identify whether the 'digital assets', which are the subject of cybersecurity and targeted by cyberattacks qualify as 'investments'. Moreover,

---

[4] Melanie Lee and Lucy Hornby, 'Google attack puts spotlight on China's "red" hackers' (*Reuters*, 20 January 2010) <www.reuters.com/article/us-google-china-hackers/google-attack-puts-spotlight-on-chinas-red-hackers-idUSTRE60J20820100120> accessed 30 April 2020.

[5] David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12(2) Journal of World Investment and Trade 225, 234.

[6] See 'Press release: cyber attack' (*PICANOL*, 31 January 2020) <www.picanol.be/news/press-release-cyber-attack-update-january-31-2020> accessed 30 April 2020.

[7] The Council of Economic Advisers, 'The Cost of Malicious Cyber Activity to the U.S. Economy' (February 2018) 7 <www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf> accessed 6 May 2020.

[8] The Council of Economic Advisers, 'The Cost of Malicious Cyber Activity to the U.S. Economy' (February 2018) 8 <www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf> accessed 6 May 2020.

[9] PWC, '*Managing cyber risks in an interconnected world* – Key findings from The Global State of Information Security® Survey 2015' (30 September 2014) 10 <www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf> accessed 6 May 2020.

[10] The Council of Economic Advisers, 'The Cost of Malicious Cyber Activity to the U.S. Economy' (February 2018) 8 <www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf> accessed 6 May 2020.

the question of the precise location of the assets will be determinative since investment treaties often provide for investments to have been made 'in the territory' of the host economy. A related question is whether entry requirements for foreign investors, that is the 'admission' and 'establishment' of foreign investors, which are sometimes, but not always, included in investment treaties may also present specific issues in relation to cybersecurity threats and concomitant security screening that may be organised by host States for foreign investment in digital assets.[11] Once it can be established that digital assets constitute an investments under the applicable legal instruments, the question then is whether international investment treaties can provide a basis for claims by foreign investors against host states for internationally wrongful acts caused to their digital assets.

In line with the general approach adopted in this book, this chapter does not attempt to provide definitive answers to all issues potentially relevant to foreign investment in cyberspace. Rather, the objective is to map out possible connections between contemporary international investment law and arbitration, and foreign investment in cyberspace.

In this chapter, I will first address the question of whether digital assets can qualify as 'investments', as defined both in international investment treaties and under the Convention on Settlement of Investment Disputes (ICSID Convention).[12] I will next address the related question of entry requirements for foreign investors and security screening operated by host States for investments in digital assets.[13] I will then turn to analysing possible claims by foreign investors against host States for breaches of their obligations, under applicable international investment treaties, in relation to cybersecurity. This will be done through an analysis of what I consider to be the two most relevant provisions regularly found in international investment treaties: fair and equitable treatment (FET) and (full) protection and security (FPS).

1. Digital Assets as an 'Investment'

[11] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 88.
[12] Convention on the Settlement of Investment Disputes between States and Nationals of Other States (opened for signature 18 March 1965, entered into force 14 October 1966) 575 UNTS 159.
[13] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 88.

Digital assets, which can comprise websites, consumer and customer data and contracts[14], and computer systems[15], are broad categories which are difficult to define in abstract terms. The UNCTAD 2017 World Investment Report[16] however has classified most relevant multinational enterprises (MNEs) active in the 'digital economy' into two groups: The first are the so-called 'Digital MNEs', which are 'characterized by the central role of the internet in their operating and delivery model. They include *purely digital players* (internet platforms and providers of digital solutions) that operate entirely in a digital environment and *mixed players* (e-commerce and digital content) that combine a prominent digital dimension with a physical one.'[17] These include businesses active in the following fields: internet platforms, digital solutions, e-commerce, and digital content.[18] The second group are so-called 'ICT MNEs', which 'provide the enabling infrastructure that makes the internet accessible to individuals and businesses. It includes IT companies selling hardware and software, as well as telecom firms' [19]. For ease of reference, I will hereafter refer to these forms of investments as composed of 'digital assets'.

Legally, digital assets are difficult to categorize, not only because they are mostly intangible by their very nature and constituted by a variety of distinct sub-components, but also because digital assets in and of themselves often do not often exist as stand-alone 'investments'. In other words, digital assets often form part of a broader (set of) investment(s). The question then is whether digital assets can be considered as 'investments' either in and om themselves or as part of a broader investment made by a foreign investor.

[14] On this, see Andrew D Mitchell, Tania Voon and Jarrod Hepburn, 'Taxing Tech: Risks of an Australian Digital Services Tax under International Economic Law' (2019) 20(1) Melbourne Journal of International Law 88, 115-118.
[15] See Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549, 556ff.
[16] UNCTAD, 'World Investment Report 2017 – Investment and the Digital Economy' (2017) UN Doc UNCTAD/WIR/2017 <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1782> accessed 28 April 2020.
[17] UNCTAD, 'World Investment Report 2017 – Investment and the Digital Economy' (2017) UN Doc UNCTAD/WIR/2017, 165 <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1782> accessed 28 April 2020.
[18] UNCTAD, 'World Investment Report 2017 – Investment and the Digital Economy' (2017) UN Doc UNCTAD/WIR/2017, 165 <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1782> accessed 28 April 2020.
[19] UNCTAD, World Investment Report 2017 – Investment and the Digital Economy (2017) UN Doc UNCTAD/WIR/2017, 165 <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1782> accessed 28 April 2020.

1.1. 'Investment' under International Investment Treaties and ICSID Convention

In order to benefit from the protection of an international investment treaty, the digital assets invariably need to fall under the definition of 'investment' in that treaty either as such or as part of a larger investment. Moreover, in case disputes relating to the digital assets are brought to arbitration under the ICSID Convention, such assets need to be captured also by the notion of 'investment' as understood by Article 25 of the ICSID Convention which defines and delimits the jurisdiction of the ICSID.

The vast majority of investment treaties contain wide and broad definitions of what constitutes an 'investment'. The wide definitions usually present in investment treaties often are similarly structured and consequently follow a similar approach. Yet, and this is a point generally valid for the entire chapter, international investment treaties are not identical which means that most treaties, while containing similar definitions of 'investment', do leave room for nuance and hence any attempt at generalization is hazardous for that reason only.

Nonetheless, it is safe to say that most treaties employ a so-called 'asset-based definition'[20]. The asset-based definition can stand by itself, that is, the term 'asset' is not defined. Any 'asset', then, can technically constitute an investment. An example of a broad 'stand-alone' asset-based definition is the 2006 Mexico-United Kingdom (UK) Bilateral Investment Treaty (BIT): '"investment" means an asset acquired in accordance with the laws and regulations of the Contracting Party in whose territory the investment is made (…)'.[21]

Other treaties contain a broad asset-based definition which adds substantive characteristics to investments, such as the 'commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk.'[22]

Such clauses have usually been interpreted as attempts to 'distinguish investments from transactions of an ordinary, short-term character (for example the sale of a good or a

[20] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 176. There are however exceptions. The Canada-Serbia 2014 Bilateral Investment Treaty for instance contains only a (rather broad) list of what constitutes an investment and has no broad asset-based definition. See Agreement between Canada and the Republic of Serbia for the Promotion and Protection of Investments (signed 1 September 2014, entered into force 27 April 2015) (Canada-Serbia BIT) art 1.

[21] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United Mexican States for the Promotion and Reciprocal Protection of Investments (signed 12 May 2006, entered into force 25 July 2007) (Mexico-UK BIT) art 1.

[22] Treaty between the Government of the United States of America and The Government of the Republic of Rwanda concerning the Encouragement and Reciprocal Protection of Investment (signed 19 February 2008, entered into force 1 January 2012) (US-Rwanda BIT) art 1.

service or a short-term financial transaction) in order to exclude the latter from the treaty' protection'.[23]

Sometimes[24], the broad definition is followed by a non-exhaustive list of examples of forms investments can take with or without exclusions, or, less commonly, by an exhaustive list[25] of examples of forms investments can take. The 2006 Mexico-UK BIT provides an example of a non-exhaustive list.[26] While the level of detail of the list varies[27], most lists can often be brought down to five categories: 1) movable and immovable property, 2) various interests in companies and enterprises such as shares, 3) claims or titles to money, 4) intellectual property rights, and 5) concessions or licences.[28] In any event, since more often than not these lists are merely examples of forms investments may take, Tribunals have regularly confirmed that the broad asset-based definitions 'are designed to protect as wide a range of investment forms as possible'.[29]

Even when treaties include a broad asset-based definition, purely commercial transactions may be excluded from the scope of application of investment treaties. The Mexico-UK BIT mentioned above, for instance, clearly excludes purely commercial transactions, such as 'claims to money' if these are not part of or related to a form of investment which falls under the scope of application of the treaty.[30] Other treaties, however, contains generic references to 'claims to money, to other assets or to any performance having an economic value'[31] which has been interpreted as to broaden the definition of 'investment' beyond the traditional understanding of the term 'asset'.[32]

---

[23] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 181.
[24] See eg Agreement between the Government of Sweden and the Government of the Socialist Federal Republic of Yugoslavia on the mutual protection of investments (signed 10 November 1978, entered into force 21 November 1979) (Serbia-Sweden BIT) art 1.
[25] For an example of an exhaustive list, see Agreement between Canada and the Republic of Serbia for the promotion and protection of investments (signed 1 September 2014, entered into force 27 April 2015) (Canada-Serbia BIT) art 1.
[26] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United Mexican States for the promotion and reciprocal protection of investments (signed 12 May 2006, entered into force 25 July 2007) (Mexico-UK BIT) art 1.
[27] Cf Agreement on encouragement and reciprocal protection of investments between the Kingdom of the Netherlands and the Federal Republic of Yugoslavia (signed 29 January 2002, entered into force 1 March 2004) (Netherlands-Serbia BIT) art 1, with the Mexico-UK BIT cited in the previous note.
[28] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 177.
[29] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn OUP 2015) 180.
[30] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United Mexican States for the promotion and reciprocal protection of investments (signed 12 May 2006, entered into force 25 July 2007) (Mexico-UK BIT) art 1 (i)-(J).
[31] Agreement on encouragement and reciprocal protection of investments between the Kingdom of the Netherlands and the Federal Republic of Yugoslavia (signed 29 January 2002, entered into force 1 March 2004) (Netherlands-Serbia BIT) art 1(a)(iii).
[32] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 180.

In defining what constitutes an 'investment' under a treaty, international investment treaties may add the requirement for the investment to be made in the territory of one of the contracting parties, in order for the investment to be 'international'. The 2006 Mexico-UK BIT mentioned above, for example, provides that the investment needs to be made in the territory of one of the States.[33] While the 'territoriality' question is relatively easy to answer in the case of tangible assets, which by their very nature are located somewhere, the location of intangible assets is more difficult to determine. In relation to financial instruments, the Tribunal in *Fedax v Venezuela* decided that these can be considered to have been made in the territory of the host State if the available funds are used by or put at the disposal of the beneficiary State.[34] Also, while single operations may not have taken place in the territory of the host State, Tribunals have looked at the question whether investments 'considered as a whole' are made in the territory of the host State.[35]

In relation to financial instruments, the Tribunal in *Abaclat v Argentina* also accepted that 'the relevant criteria should be where and/or for the benefit of whom the funds are ultimately used.'[36] The decision however was taken only by a majority, and heavily criticized, including on this particular point, by Arbitrator Georges Abi-Saab in his dissenting opinion who argued that 'a territorial link or nexus is inherent in the concept of "investment"'.[37]

Before looking at the implications of the preceding principles and practices for the question whether digital assets could be categorized as 'investments', it is important to

[33] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United Mexican States for the promotion and reciprocal protection of investments (signed 12 May 2006, entered into force 25 July 2007) (Mexico-UK BIT) art 1. Other treaties include the requirement in provisions relating to the substantive protection standards contained in the treaty, such as the Albania-Serbia Bilateral Investment Treaty which extends protection to 'investments made by investors of one Party in the territory of the other Party': Agreement between the Federal Government of the Federal Republic of Yugoslavia and the Council of Ministers of the Republic of Albania on the reciprocal promotion and protection of investments (signed 26 November 2002, entered into force 14 May 2004) (Albania-Serbia BIT) art III (1).

[34] *Fedax NV v The Republic of Venezuela*, ICSID Case No ARB/96/3, Decision of the Tribunal on Objections to Jurisdiction (11 July 1997) para 41. For a discussion, see Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn OUP 2015) 188 and Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 189.

[35] *SGS Société Générale de Surveillance SA v Republic of the Philippines*, ICSID Case No ARB/02/6 , Decision of the Tribunal on Objections to Jurisdiction (29 January 2004) para 112.

[36] *Abaclat and Others v Argentine Republic*, ICSID Case No ARB/07/5 (formerly *Giovanna a Beccara and Others v The Argentine Republic*), Decision on Jurisdiction and Admissibility (4 August 2011) para 374.

[37] *Abaclat and Others v Argentine Republic*, ICSID Case No ARB/07/5 (formerly *Giovanna a Beccara and Others v The Argentine Republic*), Dissenting Opinion to Decision on Jurisdiction and Admissibility by Georges Abi-Saab (4 August 2011) para 74.

add that, in case of arbitration under the ICSID Convention, the 'investment' must not only be captured by the definition contained in the investment treaty, but also fall under the scope of Article 25 ICSID Convention. Article 25 ICSID extends the jurisdiction of the Centre to 'any legal dispute arising directly out of an investment' but fails to further define 'investment'. The lack of a clear definition of what constitutes 'investment' for the purposes of Article 25 ICSID has triggered a 'wide-ranging debate'[38] in scholarship and practice. I do not intend to engage in that debate here, but it is necessary to explain the two main theories or approaches on the question.

A first approach consists of considering that the notion of 'investment' under Article 25 ICSID has an objective meaning that is independent of the parties' understanding of the concept. Thus construed, 'investment' under Article 25 ICSID requires four features: a substantial commitment, a certain duration of performance, participation in the risks of the transaction, and a contribution to the development of the host state.[39] These criteria were set out by the Tribunal in *Salini v. Morocco*[40] and have since then been referred to as the 'Salini criteria'.

A second approach consists of operating a 'renvoi' to the definition of investment agreed by the States in their investment treaty which contains the consent to arbitration, thus emphasizing party autonomy in defining what constitutes an 'investment'.[41] This, it has been argued is in conformity with the drafting and negotiating history of ICSID.[42]

Tribunals essentially follow one or the other approach, or adopt a reasoning which combines both.[43] However, in general, and whichever the approach to the notion of 'investment' under the ICSID Convention, one-time ordinary commercial transactions usually are considered to fall outside of the concept of 'investment', based on the fact the ordinary meaning or general understanding of 'investment', even in the case of a renvoi

[38] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 65.
[39] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 66.
[40] *Salini Costruttori SpA and Italstrade SpA v Kingdom of Morocco*, ICSID Case No ARB/00/4, Decision on Jurisdiction (23 July 2001) para 56.
[41] See for a discussion: Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 68-76. See also eg *Pantechniki SA Contractors & Engineers (Greece) v The Republic of Albania*, ICSID Case No ARB/07/21, Award (30 July 2009) para 42ff.
[42] See for a discussion: Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 68-76. See also eg *Pantechniki SA Contractors & Engineers (Greece) v The Republic of Albania*, ICSID Case No ARB/07/21, Award (30 July 2009) para 42ff.
[43] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 69.

to the treaty definitions agreed by the parties, refers to transactions other than purely commercial transactions.[44]

1.2. Can Digital Assets Qualify as 'Investments' ?

Based on the principles set out above, several issues arise when dealing with digital assets as 'investment' for the purpose of international investment law:

First of all, the broad asset-based definitions usually present in international investment treaties, extending the coverage of these treaties to all assets without any limitation might, because of its broad and non-exhaustive nature, be interpreted as to cover digital assets or businesses.[45] As put by UNCTAD, such definitions suggest 'that the term embraces everything of economic value, virtually without limitation.'[46] As a consequence, authors have argued that digital assets can, because of their intrinsic or extrinsic value, fall under the broad asset-based definitions.[47]

In addition to the broad-asset based definition, the list of forms investments may take, which some treaties also provide, can further confirm that digital assets cannot, merely because of their intangible nature, be excluded from the definition of 'protected investment'[48], especially if the list refers generically to 'intangible assets'. Art 1(g) of the Mexico-UK BIT, for example, mentions 'real estate or other property, tangible or intangible, including intellectual property rights, acquired in the expectation or used for the purpose of economic benefit or other business purposes'.[49]

Aside for the possibility of considering digital assets as 'investments' in and of themselves, a holistic approach to 'investment' may also lead to the conclusion that digital assets are 'covered investments'. Under a holistic approach, the individual elements of

---

[44] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 75.

[45] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549, 557-8.

[46] UNCTAD, 'Series on Issues in International Investment Agreements: Scope and Definition' (2011) UN Doc UNCTAD/ITE/IIT/11(Vol.II) 18 <https://unctad.org/en/pages/PublicationArchive.aspx?publicationid=341> accessed 30 April 2020.

[47] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 529, 559.

[48] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549, 559.

[49] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United Mexican States for the promotion and reciprocal protection of investments (signed 12 May 2006, entered into force 25 July 2007) (Mexico-UK BIT) art 1.

digital businesses are not viewed in isolation but assessed from the perspective of the 'unity of an investment operation'.[50] Individual components of investment operations, such as digital assets, may thus be considered as an 'investment' if they form part of a broader investment operation. Investment in the digital sector indeed usually implies other forms of investment, such as investment in infrastructure.[51] As noted by Nicolas Tsagourias in his chapter in this book, 'cyberspace has three layers: a physical layer which consists of computers, integrated circuits, cables, communications infrastructure and the like; a second layer which consists of the software logic; and, finally, a third layer which consists of data packets and electronics.'[52]

However, one should keep in mind that certain treaties do contain more narrow definitions, and that investments need to be distinguished from 'transactions of an ordinary, short-term character (for example the sale of a good or a service or a short-term financial transaction) which may be excluded from the treaty's protection'[53]. This is the case notably for those treaties which add additional characteristics of investments to the broad asset-based definition.[54] Hence, there remains a certain uncertainty and categorically positing that digital assets would always qualify as 'investment' under an investment treaty is difficult.

For the same reason, whether or not digital assets would fall under the Article 25 ICSID notion of 'investment' is difficult to establish with certainty, especially if a tribunal decides to adhere (even partly) to the 'Salini-criteria' which require a substantial commitment, a certain duration of performance, participation in the risks of the transaction, and a contribution to the development of the host state.[55] Here again, the main principle would be that single one-off commercial transactions of digital businesses would not be captured by the notion of 'investment' under the ICSID Convention, while

[50] Andrew D Mitchell, Tania Voon, and Jarrod Hepburn, 'Taxing Tech: Risks of an Australian Digital Services Tax under International Economic Law' (2019) 20(1) Melbourne Journal of International Law 88, 116. See also Christoph Schreuer and Ursula Kriebaum, 'At What Time Must Legitimate Expectations Exist?' in Jacques Werner and Arif H Ali (eds), *A Liber Amicorum: Thomas Wälde. Law Beyond Conventional Thought* (2009) 267. See also *Ceskoslovenska Obchodni Banka, AS v The Slovak Republic*, ICSID Case No ARB/97/4, Decision of the Tribunal on Objections to Jurisdiction (24 May 1999) para 72.
[51] UNCTAD, World Investment Report 2017 – Investment and the Digital Economy (2017) UN Doc UNCTAD/WIR/2017, 190ff <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1782> accessed 28 April 2020.
[52] See the chapter by Nicholas Tsagourias in this volume 'The Legal Status of Cyberspace' 15.
[53] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 181.
[54] Treaty between the Government of the United States of America and the Government of the Republic of Rwanda concerning the encouragement and reciprocal protection of investment (signed 19 February 2008, entered into force 1 January 2012) (US-Rwanda BIT) art 1.
[55] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 66.

transactions which have a long-term commitment and meet the other criteria would not necessarily be excluded.[56]

In respect of the territorial link, as noted by UNCTAD, '[b]ecause "investment" includes many intangible rights, the location of a particular asset may be difficult to identify'.[57] In general, factors such as location, possession and control over the digital assets will be important and determinant for the establishment of the territorial link between the digital assets and the host State.[58] In respect of the 'physical layer'[59] of digital businesses, the territorial nexus will be less difficult to ascertain, as will be the case for digital assets such as software which are contained on a physical device.[60] The most tricky part will be establishing the territorial link for purely intangible digital assets such as data. Based on the case-law discussed above, one can only conclude that the answer to this question is difficult also. If one accepts the approach to look at whether investments 'considered as a whole' are made in the territory of the host State[61], hence at the investment operation as a whole of which digital assets form a part, the territorial nexus can be established to the extent of course that the entire investment operation is made in the territory of the host State. Looking at the digital assets as stand-alone or individual investment operations, one may need to look at 'where and/or for the benefit of whom' the assets are ultimately used.[62] The link 'to a specific economic enterprise or operation taking place in the territory of the Host State'[63] would then play a minor role. However, looking at the same question from the perspective of the dissent of Georges Abi-Saab in that case, in

[56] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21 Vanderbilt Journal of Entertainment & Technology Law 549, 562-3.
[57] UNCTAD, 'Series on Issues in International Investment Agreements: Scope and Definition' (2011) UN Doc UNCTAD/ITE/IIT/11(Vol.II) 45 <https://unctad.org/en/pages/PublicationArchive.aspx?publicationid=341> accessed 30 April 2020.
[58] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549, 564.
[59] Nicholas Tsagourias in this volume 'The Legal Status of Cyberspace' 15.
[60] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549, 565.
[61] *SGS Société Générale de Surveillance SA v Republic of the Philippines*, ICSID Case No ARB/02/6, Decision of the Tribunal on Objections to Jurisdiction (29 January 2004) para 112.
[62] *Abaclat and Others v Argentine Republic*, ICSID Case No ARB/07/5 (formerly *Giovanna a Beccara and Others v The Argentine Republic*), Decision on Jurisdiction and Admissibility (4 August 2011) para 374.
[63] *Abaclat and Others v Argentine Republic*, ICSID Case No ARB/07/5 (formerly *Giovanna a Beccara and Others v The Argentine Republic*), Decision on Jurisdiction and Admissibility (4 August 2011) para 375.

which he had argued that there should be a 'specific economic anchorage' in the host economy[64], one could arrive at the opposite conclusion.[65]

2. Digital Assets, Entry Requirements, and Security Screening

Before turning to the substantive protection standards in their application to digital investments, it is important to consider entry requirements for foreign investors, that is 'admission' and 'establishment' of foreign investment. 'Admission' refers to the entry of the investment as such, while 'establishment' of foreign investors, refers to the 'conditions under which the investor is allowed to carry out its business during the period of the investment'.[66]

In relation to investment in the digital economy, admitting foreign investment, and authorizing foreign investors to invest or establish themselves in the territory of a State may indeed pose distinct problems. Notably, security concerns may affect the entry of investors to foreign markets. This is the case for investment in the defence industry, critical infrastructure and strategic economic sectors, which have typically been subjected to more profound scrutiny and screening by the host economy.[67] For several years, some States have toughened their security screening for foreign investment[68], notably to assess possible security risks in relation to investment in the digital economy by foreign State-Owned Enterprises (SOEs).[69]

There are roughly two models of investment treaty provisions when it comes down to admission and establishment. In a first set of treaties typically concluded by European states or treaties concluded by other States but modelled on 'European' treaties, foreign investment is not granted a right of admission or establishment.[70] Admission or

[64] *Abaclat and Others v Argentine Republic*, ICSID Case No ARB/07/5 (formerly *Giovanna a Beccara and Others v The Argentine Republic*), Dissenting Opinion to Decision on Jurisdiction and Admissibility by Georges Abi-Saab (4 August 2011) para 108.
[65] A link here can also be made with the question of whether the State can exercise jurisdiction over the digital assets. See *in extenso* the chapter by Nicholas Tsagourias in this volume 'The Legal Status of Cyberspace' 19-20 and the chapter by Uta Kohl 'Jurisdiction in cyberspace'.
[66] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 88.
[67] UNCTAD, World Investment Report 2016 – Investor Nationality: Policy Challenges (2016) UN Doc UNCTAD/WIR/2016, 95 <https://unctad.org/en/PublicationsLibrary/wir2016_en.pdf> accessed 13 May 2020.
[68] UNCTAD, World Investment Report 2016 – Investor Nationality: Policy Challenges (2016) UN Doc UNCTAD/WIR/2016, 94ff <https://unctad.org/en/PublicationsLibrary/wir2016_en.pdf> accessed 13 May 2020.
[69] See generally Lu Wang, 'Chinese SOE Investments and the National Security Protection under IIAs' in Julien Chaisse, China's International Investment Strategy: Bilateral, Regional, and Global Law and Policy (OUP 2019), 67-86.
[70] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 89.

establishment is only possible in accordance with the host State's legislation.[71] Such investment treaties thus mostly provide for 'post-entry' treatment, and contain no commitments to admit foreign investors, or authorize establishment of foreign investors. Domestic law only regulates admission and may authorize differentiated treatment of foreign investors.

Under a second model, mostly followed by Canada, Japan and the United States, a limited right of admission is granted under the investment treaty.[72] The right of admission is limited, since it in fact extends national treatment (NT) and often also most-favored nation treatment (MFN) to the establishment, acquisition or expansion of the investment.[73] In other words, a form of guarantee of non-discrimination in relation to the establishment, acquisition or expansion of the investment is provided. Most treaties which contain such admission rights also usually contain a list of sectors or activities to which the clauses on national treatment and most-favoured-nation treatment do not apply.[74] These sectors are then listed in a 'positive list' – including all sectors that are 'open' to foreign investment, or a 'negative list' which contains only the exceptions to the general 'openness' of all sectors or activities. 'Closed' sectors in investment treaties may include, for example, banking, insurance, securities, and 'one-way satellite transmissions of direct-to-home (DTH) and direct broadcast satellite (DBS) television services and of digital audio services.'[75] Security screenings are thus possible, provided that they respect the provisions of the applicable treaties. Several other States have also over the past years added further restrictions to access their market, notably through the addition of security screening and review procedures for investments in the digital economy and more specifically for investment in communication networks and services.[76]

---

[71] See eg Treaty between the Federal Republic of Germany and the Kingdom of Bahrain concerning the Encouragement and Reciprocal Protection of Investments (signed 5 February 2007, entered into force 27 May 2010) (Bahrain-Germany BIT) art 2(1).

[72] Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 89.

[73] See eg 2012 Treaty between the Government of the United States of America and the Government of [Country] concerning the encouragement and reciprocal protection of investments (US Model BIT) arts 3 and 4.

[74] See eg 2012 Treaty between the Government of the United States of America and the Government of [Country] concerning the encouragement and reciprocal protection of investments (US Model BIT) art 14(2).

[75] Treaty between the Government of the United States of America and the Government of the State of Bahrain concerning the encouragement and reciprocal protection of investment (signed 29 September 1999, entered into force 30 May 2001) (Bahrain-US BIT) (2000) art 2, Annex.

[76] See UNCTAD, World Investment Report 2016 – Investor Nationality: Policy Challenges (2016) UN Doc UNCTAD/WIR/2016, 96, <https://unctad.org/en/PublicationsLibrary/wir2016_en.pdf> accessed 13 May 2020.

Finally, while the 2012 US Model BIT authorizes the submission of claims to arbitration in relation to allegations of breaches of investment authorizations[77], other treaties containing market access provisions precisely remove such question from the States' consent to arbitration. For example, Article II(4)(a) of the Canada-Egypt BIT carves out decisions relating to whether or not to permit an acquisition from the provisions of Articles XIII [Settlement of Disputes between an Investor and the Host Contracting Party] or XV [Disputes between the Contracting Parties].[78]

This precise provision was the subject of a very recent decision[79] relating to a national security screening and review decision by Canada. The national security screening was based on the 'Investment Canada Act' which provides for specific regulations and conditions for admission to the Canadian market.[80] This screening had prevented Global Telecom Holding from acquiring Canadian telecom operator because of concerns about one of Global Telecom Holding's shareholders, which was reported to be owned by Russian investors and which made us of equipment by the Chinese manufacturer Huawei.[81] The Tribunal, however, by majority, considered that under the specific facts of the case, the acquisition of control by Global Telecom Holding over Wind Mobile was not an 'acquisition' in the sense of Article II(4)(a) of the Canada-Egypt BIT.[82] The Tribunal thus confirmed jurisdiction.

3. Applying Investment Protection Standards in Cyberspace

Moving to the 'substantive part of international investment law, two distinct types of situations deserve special consideration. The first question is to what extent measures taken by the host State in the area of cybersecurity can, if harmful to the investment, result in a successful investment treaty claim by the harmed foreign investor. Secondly, in the event of cyberattacks on or cybersecurity issues related to the assets of foreign

[77] Treaty between the Government of the United States of America and the Government of [Country] concerning the encouragement and reciprocal protection of investments (US Model BIT) art 24(1)(a)(i)(C).
[78] Agreement Between the Government of Canada and the Government of the Arab Republic of Egypt for the promotion and protection of investments (signed 13 November 1996, entered into force 3 November 1997) (Canada-Egypt BIT) art II.
[79] *Global Telecom Holding SAE v Canada*, ICSID Case No ARB/16/16, Award of the Tribunal (27 March 2020).
[80] For an overview, see UNCTAD, World Investment Report 2016 – Investor Nationality: Policy Challenges (2016) Do No UNCTAD/WIR/2016, 96, <https://unctad.org/en/PublicationsLibrary/wir2016_en.pdf> accessed 13 May 2020.
[81] Damien Charlotin, 'Analysis: in Global Telecom v Canada, arbitrators unanimously reject FET, FPS and free transfer claims, but disagree on national treatment argument and national security exception' (*IAReporter*, 29 April 2020) <https://www.iareporter.com/articles/analysis-in-global-telecom-v-canada-arbitrators-unanimously-reject-fet-fps-and-free-transfer-claims-but-disagree-on-national-treatment-argument-and-national-security-exception/> accessed 15 May 2020.
[82] *Global Telecom Holding SAE v Canada*, ICSID Case No ARB/16/16, Award of the Tribunal (27 March 2020) para 328.

investors, the role and responsibility of the host State in which the foreign investor has invested may result in an investment claim brought by the targeted foreign investors. The question then is to what extent an international investment treaty may successfully be used to remedy the damage caused by cyberattacks. The question will be to what extent the state can be held responsible firstly for the cyberattack itself, and secondly, for not having exercised the necessary due diligence to prevent such a cyberattack and/or to bring the perpetrators to justice.

I will look at both questions from the perspective of two investment treaty provisions regularly found in international investment treaties: FET and FPS.[83] Both provisions will be predominantly, but not exclusively, relevant for one of the two particular situation: FET mostly will be relevant for the question of harm caused by the adoption of cybersecurity regulations, while FPS mostly will apply in case of cyberattacks on the assets of foreign investors.[84]

3.1. Fair and Equitable Treatment and Cyber Regulations

3.1.1. The FET Standard

FET generally is referred to as a non-contingent, absolute standard of treatment as opposed to contingent, relative standards, such as national treatment (NT) or most which ask the State to act in a certain way as required under international law, irrespective of how other investors or investments are treated. The obligation to treat foreign investors fairly and equitably is stipulated in the vast majority of BITs.[85]

The FET standard clearly is a flexible and rather vague concept, but based on the existing caselaw and scholarship, it is generally accepted that the following obligations form part of FET: observance of the investor's legitimate expectations, non-discrimination, proportionality, due process, transparency, freedom from coercion and harassment, stability, predictability and a general duty of due diligence.[86]

---

[83] The exact relation between FPS and FET, and the so-called 'international minimum standard' (IMS) is still subject to much debate, but I do not intend to engage in that question. See for a discussion Christoph Schreuer, 'Full Protection and Security' (2010) 1(2) Journal of International Dispute Settlement 353.

[84] While some authors have also explored the question of direct or indirect expropriation of digital assets in the context of cyber-theft and economic espionage, the challenges and difficulties in invoking such a provision are important and hence I will not discuss it here. See Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549, 585-587.

[85] Roland Kläger, 'Fair and Equitable Treatment: A Look at the Theoretical Underpinnings of Legitimacy and Fairness' (2010) 11 The Journal of World Investment & Trade 436.

[86] Andrew P Newcombe and Lluis Paradell, *Law and Practice of Investment Treaties: Standards of Treatment* (Kluwer Law International 2009) 277-279; Ioana Tudor, *The Fair and Equitable Treatment Standard in the International law of Foreign Investment* (OUP 2008) 157, 186; Roland Kläger, 'Fair and

While there are different models and formulations of FET clauses[87], I will here focus only on the question whether certain sub-components of the FET standards – without taking a position on whether or not these components are by necessary implication always part of the FET standard in all treaties – may provide a basis for a claim in relation to regulations in the cybersphere. The requirement of a stable legal framework, the legitimate expectations of the foreign investor, and the prohibition of arbitrary and unreasonable measures seem to be most relevant here.

3.1.2. The FET Standard and Cyber Regulation

While general regulations can be adopted by the host State affecting foreign investors, and hence can result in the initiation of an investment treaty claim, host State regulatory activity in relation to digital activities may present specific challenges. Besides general regular activities of States which may be found in breach of investment treaty obligations, government policies and regulations in a digital investment environment may require specific regulation to address issues such as privacy and data protection, consumer protection for e-commerce, content restrictions, the protection of intellectual property rights, or data location requirements obliging digital business to store local data within a specific country because of privacy and national security considerations.[88]

Regulations in those areas, of course, may not be legally problematic in and of themselves, and hence be compatible with the State's obligations under international investment treaties. While the digital business environment may require specific regulatory activity, and while such regulations may be more prone to rapid changes[89], the idea that States, in general terms, have the right to regulate, including in relation to digital businesses, remains unaffected as a matter of principle. In this respect, there is, in the practice of arbitral tribunals, a tendency to a more cautious approach to FET through the recognition of the States' right to regulate and thus for States to maintain sufficient regulatory

Equitable Treatment: A Look at the Theoretical Underpinnings of Legitimacy and Fairness' (2010) 11 The Journal of World Investment & Trade 436. See also for an overview of the contents of the standard in function of arbitral practice: Katia Yannaca-Small, 'Fair and Equitable Treatment Standard: Recent Developments' in August Reinisch (ed), *Standards of Investment Protection* (OUP 2008) 118ff.

[87] See Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn, OUP 2012) 132ff and Eric De Brabandere, 'States' Reassertion of Control over International Investment Law – (Re)Defining 'Fair and Equitable Treatment' and 'Indirect Expropriation' in Andreas Kulick (ed), *Reassertion of Control over the Investment Treaty Regime* (CUP 2016) 285-308.

[88] See, also for a more complete list of areas of regulation: UNCTAD, World Investment Report 2017 – Investment and the Digital Economy (2017) UN Doc UNCTAD/WIR/2017, 207-209 <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1782> accessed 28 April 2020.

[89] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21 Vanderbilt Journal of Entertainment & Technology Law 549, 572.

space.[90] A certain regulation or measure adopted by the State relating to social or consumer protection, may thus be fall under the exercise by the State of its right to regulate in the public interest.

However, one cannot exclude that the imposition of certain requirements and regulations which impact foreign investments negatively may be considered a breach of certain investment protection standards, such as FET. It has for instance been argued that regulations adopted by a state in the pursuit of the regulation of cyberspace and providing cybersecurity, such as source code disclosure, or limitations to cross-border dataflows[91] may be captured by several components of FET. Also, there have been reports on possible claims by Chinese investor Huawei in relation to assertions by the Czech Republic that the telecom company's 'technologies and equipment pose a security threat'.[92]

Despite the specificity of regulating the digital economy, acts of the State in breach of the State's investment treaty obligations will be assessed by reference to the usual understandings and interpretations of investment treaty provisions. Since there have not yet been any investment dispute submitted to arbitration or any other type of settlement in relation to the harm caused by cybersecurity regulations, it is difficult to provide any firm answer as to whether such regulations might constitute a breach of FET. Indeed, applying FET to regulations is very fact-specific and will inevitably depend on the precise formulation of the regulations, the general objective and context of their adoption, their scope of application, and their impact on the investment. An important aspect also might be whether regulations or acts target one specific investor or apply more broadly to all investors investing in a certain territory.

Measures taken by the host State which are unreasonable and arbitrary, for instance because the decision is not based on 'legal standards, but on discretion, prejudice or personal preference', or that is taken 'for reasons that are different from those put

[90] See for a discussion also Ursula Kriebaum, 'FET and Expropriation in the (Invisible) EU Model BIT' (2014) 15(3-4) The Journal of World Investment & Trade 471. See also Consolidated CETA Text (26 September 2014) art 8.9(1) <http://trade.ec.europa.eu/doclib/docs/2014/september/tradoc_152806.pdf> accessed 7 June 2020.

[91] Julien Chaisse and Cristen Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' (2019) 21(3) Vanderbilt Journal of Entertainment & Technology Law 549, 570.

[92] Jarrod Hepburn and Luke Eric Peterson, 'Analysis: as Huawei invokes investment treaty protections in relation to 5G network security controversy, what scope is there for claims under Chinese treaties with Czech Republic, Canada, Australia and New Zealand?' (*IAReporter*, 11 February 2019) 1 <www.iareporter.com/articles/analysis-as-huawei-invokes-investment-treaty-protections-in-relation-to-5g-network-security-controversy-what-scope-is-there-for-claims-under-chinese-treaties-with-czech-republic-canada-australia-a/> accessed 7 June 2020.

forward by the decisions maker'[93], have been considered in breach of the FET standard. In relation to consistency and legitimate expectations, it is clear, also in the context of investment in digital assets that 'the state is certainly not responsible for all the imaginable factors that could frustrate an investor's legitimate expectations'.[94] For instance, foreign investors cannot expect that the host State would not alter existing or adopt new cyber-related legislation, especially if it responds to certain genuine concerns. There is also no general stabilization requirement, in the sense that the host State would not be able to make changes to the regulatory environment, or to be more precise be held liable under the investment treaty if it were to do so.[95] Yet, it remains that a State should generally respect the expectations resulting from the host State's conduct in respect of commitments or representations made by the State.[96]

3.2. (Full) Protection and Security, and Cyberattacks

3.2.1. The FPS Standard

Provisions granting protection and security to investments and investors vary in nature. Some treaties refer to 'full protection and security', while others provide for 'protection and security' or 'constant protection and security'. It is not the purpose here to engage in a discussion of these variances. Thus, the standard will be referred to here as FPS despite the existing different wordings. Some tribunals moreover have argued that the differences in wording do not make a substantive difference.[97]

In principle, the obligation to provide protection and security covers both an obligation for the state itself to abstain from infringing the physical protection and security of aliens, which applies to all State organs and entities the acts of which are attributable to the State, and an obligation of due diligence in relation to acts of third-parties other than State organs. The State's duty to abstain itself is not tested by reference to the due diligence standard[98]. In that case, contrary to the responsibility of States for acts of third-parties other than State organs, the wrongful act is *the act that has caused harm*.

---

[93] Rudolf Dolzer and Christoph Schreuer, Principles of International Investment Law (2nd edn, OUP 2012) 193.
[94] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 255.
[95] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 255.
[96] Andrew Newcombe and Lluis Paradell, *Law and Practice of Investment Treaties: Standards of Treatment* (Kluwer Law International 2009) 279.
[97] *Parkerings-Compagniet AS v Republic of Lithuania*, ICSID Case No ARB/05/8, Award (11 September 2007) para 354.
[98] Riccardo Pisillo-Mazzeschi, 'The Due Diligence Rule and the Nature of the International Responsibility of States (1992) 35 German Yearbook of International Law 23.

Conversely, in case of acts of third-parties other than State organs, the internationally wrongful act is *the failure to prevent* the occurrence of the act or the failure to apprehend or punish those responsible for the act. The breach of that obligation, then, is assessed through the due diligence standard and implies no strict liability for the host State.[99] This applies equally to the obligation for States to act with due diligence to apprehend and punish those responsible for the act, which also is part of the FPS standard.[100] In the words of the Tribunal in *El Paso v. Argentina*, States have a duty of prevention and a duty of repression.[101]

Besides the requirement of providing physical protection and security, certain tribunals have, in particular when the word 'full' precedes 'protection and security', extended the application of the standard to 'legal protection and security', making this understanding of the standard in fact relatively similar to the FET standard.[102] Legal protection and security, in certain interpretations, in essence would require States to refrain from taking legal or governmental acts or measures that would hinder the proper functioning of the investment or would contravene investor's rights.[103] Certain case law suggests that FPS requires host States to provide to foreign investors a legal framework that guarantees legal protection to investors.[104] Others however, have limited the scope of the provision to the more traditional understanding of physical protection and security.[105]

3.2.2. FPS and Cyberattacks

Before turning to the obligations of States in relation to cyberattacks, it is important to first analyse whether at all FPS obligations can apply to intangible assets, such as digital assets. I do not consider this question to be necessarily linked to the issue of whether FPS covers not only 'physical or police protection' but also *legal* protection which more

[99] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 132, 209-10. See also *Asian Agricultural Products Ltd v Republic of Sri Lanka*, ICSID Case No ARB/87/3, Final Award (27 June 1990) para 77.
[100] Campbell McLachlan, Laurence Shore and Matthew Weiniger, *International Investment Arbitration: Substantive* Principles (OUP 2008), p. 262, para 7.190 and Andrew Newcombe and Lluis Paradell, *Law and Practice of Investment Treaties: Standards of Treatment* (Kluwer Law International 2009) 246, para 6.8.
[101] *El Paso Energy International Company v. The Argentine Republic,* ICSID Case No. ARB/03/15, Award (31 October 201) para 523.
[102] For a discussion, see Eric De Brabandere, 'Host States' Due Diligence Obligations in International Investment Law' (2015) 42(2) Syracuse Journal of International Law and Commerce 319-361.
[103] See, for a discussion, Christoph Schreuer, 'Full Protection and Security' (2010) 1(2) Journal of International Dispute Settlement 358-360.
[104] *Ibid.* 363.
[105] *Noble Ventures, Inc v Romania*, ICSID Case No ARB/01/11, Award (12 October 2005) para 164. Since the 'legal' aspect of FPS is very close to the FET standard, I will not discuss that aspect of FPS here. Indeed, the requirement that States should refrain from taking legal or governmental acts or measures that would hinder the proper functioning of the investment or would contravene investor's rights adds little do what has been discussed above in relation to FET.

broadly could apply to tangible and intangible assets. Rather, the question is whether the 'physical' aspect of FPS can be interpreted so as to cover 'police protection' in relation to intangible assets, and thus whether this aspect of FPS can be effectively used to cover host State measures, or lack thereof, in case of cyberattacks on the foreign investor's digital assets.

While it has been considered that it is 'difficult to understand how the physical security of an intangible asset would be achieved'[106], the argument has been made that to make the FPS effective in case of intangible assets of foreign investors, the 'traditional assurances offered by the common FPS standard must be enlarged'.[107] In this context, applying FPS to digital assets does not necessarily need to imply that FPS is intended to cover 'legal' protection and security in general. Indeed, if one goes back to the original purpose and origins of the FPS standard[108], it becomes clear that it was mainly intended to protect the physical integrity of investments against interference by the 'use of force'.[109] The 'use of force' was originally targeting acts of a criminal nature, such as isolated acts of individuals relating to the theft of parts of locomotives[110], acts of the State in relation to the killing of a family member by a third party[111], or acts in relation to mob violence, riots or civil unrest[112], and insurrectional movements.[113]

Based on this, one could argue that the essence of FPS is not only to protect the tangible assets of foreign investors, but rather a more general duty for the State to prevent harmful acts of third parties from violence by third parties and its own organs. In such case, the transposition of the more traditional conception of FPS as covering 'physical protection' of foreign investors' tangible assets to include also protection in case of cyberattacks on digital assets is easier to argue and does not need to engage in the question on the expansion of PFS to 'legal' protection and security.[114]

---

[106] *Siemens AG v The Argentine Republic*, ICSID Case No ARB/02/8, Award (17 January 2007) para 303.
[107] David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12(2) The Journal of World Investment and Trade, 225, 236.
[108] See Eric De Brabandere, 'Host States' Due Diligence Obligations in International Investment Law' (2015) 42(2) Syracuse Journal of International Law and Commerce 319-361.
[109] Saluka Investments BV v The Czech Republic, UNCITRAL, Partial Award (17 March 2006) para 484.
[110] General Claims Commission (Mexico and United States), *H G Venable (USA) v United Mexican States*, Decision of 8 July 1927, IV UNRIAA 219-261.
[111] General Claims Commission (Mexico and United States), *Laura M B Janes et al (USA) v United Mexican States*, Decision of 16 November 1925, IV UNRIAA 82-98.
[112] *Affaire des biens britanniques au Maroc espagnol (Espagne contre Royaume-Uni) (British Property in Spanish Morocco)*, Decision of 1 May 1925, II UNRIAA 615, 642, 645. See also Great-Britain United States Mixed Commission, *Home Frontier and Foreign Missionary Society of the United Brethren in Christ,* Decision of 18 December 1920, IX UNRIAA 144.
[113] Mixed Claims Commission (Italy-Venezuela), *Sambiaggio Case* (1903) X UNRIAA 499, 524.
[114] Moreover, if one looks at contemporary treaties which refer to the FPS standard in its relation to customary law, one can see that the FPS standard is directly linked to 'police protection', without references to mob violence, riots or civil unrest, and insurrectional movements, or to tangible assets only. See eg 2012

If we extrapolate and try to apply these general principles to the specific context of cyberattacks and cybercrime, it is necessary to keep in mind that digital assets often exist in conjunction with some form of physical infrastructure. The application of FPS to the latter is more straightforward, in the sense that the obligation for the host State to physically protect the tangible assets of the foreign investor is very much in line with the contemporary conception of FPS and existing case-law on the subject.[115] I will thus focus here generally on the obligations towards digital assets generally.

To turn to the application of the FPS standard: the State itself of course is first responsible for not engaging in cyberattacks against foreign investors who have invested on the State's territory, and will be responsible under the investment treaty if such would occur. But more importantly, in the context of cyberattacks, the responsibility of the State under the FPS standard involves exercising due diligence to prevent cyberattacks by third parties, and to apprehend and punish those responsible for the acts.[116]

In general, establishing precise obligations of states to act in due diligence to prevent cyberattacks on foreign investors' digital assets is challenging. First of all, and contrary to tangible assets located in the territory of the host States, the precise location of the digital assets is difficult to determine. One criterion can be the location of the server that hosts the digital assets for the foreign investor, which probably is the most straightforward one, since it also links the obligation to the notion of investment 'in the territory' of the host State.[117] Applying that criterion, it has been argued that States would have an obligation to 'ensure that the websites which it hosts are not attacked'.[118] But the difficulty is that foreign investors' digital assets are, as most digital assets, managed through internet service providers which are private entities[119], and it seems difficult to argue that States would have a general obligation – even of due diligence – to prevent

Treaty between the Government of the United States of America and the Government of [Country] concerning the encouragement and reciprocal protection of investments (US Model BIT) art 5(2)(b).

[115] See eg *Ampal-American Israel Corporation and others v Arab Republic of Egypt*, ICSID Case No ARB/12/11, Decision on Liability and Heads of Loss (21 February 2017) paras 235ff.

[116] Even beyond the FPS standards, it has been argued that States may have an obligation of prevention and cessation in relation to cyberattacks committed by enterprises on their territory. See Philippe Achilleas, 'Entreprises, cyberattaques et responsabilité. Aspects de droit international et européen' in Frédérick Douzet, *Cyberattaques et droit international – Problèmes choisis* (Pedone 2018) 148 and Claire Crépet-Daigrement, 'Responsabilité de l'Etat-auteur d'une cyberattaque' in Frédérick Douzet, *Cyberattaques et droit international – Problèmes choisis* (Pedone 2018) 161.

[117] David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12(2) The Journal of World Investment and Trade 225, 237.

[118] David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12(2) The Journal of World Investment and Trade 225, 237.

[119] David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12(2) The Journal of World Investment and Trade 225, 237.

cyberattacks targeting specific investors' digital assets or websites which are stored on or located on servers held or managed by non-state internet service providers. For instance, contrary to the State's possibility to send police forces to an investor's facilities which are on the verge of an attack by a mob, it is more difficult to imagine how a State could exercise due diligence to prevent a cyberattack on that same investor's digital systems located on servers hosted by private parties.[120]

However, the argument has been made that the State would be under a general obligation to provide a certain form of internet security, and notably for those parts of the cyberspace where the State can in fact intervene. One can think of the internet infrastructure generally, or the stability of communications networks.[121] Here again, however, much depends on whether or not the general infrastructure is in the hands of the State or agencies of the State and whether any action by the State is possible at all.

The State's obligation to exercise due diligence to apprehend and punish those responsible for cybercrime or cyberattacks may play an important role also. This requires from the State to make available to the foreign investors, its legal, judicial and administrative apparatus to detect and effectively prosecute those responsible. The obligations imply also an obligation of due diligence to investigate cyberattacks and where possible, use all prosecutorial means available to bring the perpetrator to justice.[122] Here also, the fact that we are dealing with cybercrime implies that the effectiveness of such an obligation may prove difficult to implement in practice: the origins of cyberattacks, and the capacity to bring to justice foreign perpetrators is not straightforward and may fail on jurisdictional grounds. And one should keep in mind that the obligation is one of due diligence, not of strict liability. Can one expect from a State to create special mechanisms only for the protection of foreign investors' digital assets ? The due diligence standard, in turn, implies that liability might be easier to find in case of evident and predictable attacks.[123]

4. Cybersecurity and Security Exceptions in International Investment Law

After having discussed the possible claims foreign investors may have in relation to investments in cyberspace, one needs to consider whether, in the event of a breach of the applicable investment treaty, such a breach may fall under a so-called 'security exception'

[120] Cf. David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12(2) The Journal of World Investment and Trade 225, 238.
[121] David Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12(2) The Journal of World Investment and Trade 225, 238.
[122] See Eric De Brabandere, 'Host States' Due Diligence Obligations in International Investment Law' (2015) 42(2) Syracuse Journal of International Law and Commerce 319, 340.
[123] Levon Golendukhin, 'Chapter 6 - Full Protection and "Cyber" Security? (Panel Discussion)' in Ian A Laird and others (eds), *Investment treaty arbitration and international law* (Juris 2018) 137.

often contained in investment treaties. Much has already been written on security clauses in international investment treaties, notably because of their use as a defense against responsibility in relation to the Argentinian economic and financial crisis in the late 1990s and early 2000s, and the subsequent divergent decisions of arbitral tribunals in that respect.[124]

In general, measures taken by the host State in the post-entry stage which are in breach of the investment protection provisions in that treaty – mostly under the FET standard of treatment in case of adoption of cybersecurity legislation – might be covered by the security exception of the treaty and hence result in a finding of conformity with the treaty nonetheless.[125]

There are a variety of exceptions which potentially can come into play. I will first look at security exception clauses in BITs, also called 'non-precluded measures provisions', before turning to circumstances precluding wrongfulness under the general customary norms relating to state responsibility.

4.1. General Security Exception Clauses

Many investment treaties, but clearly not all[126], include a provision aimed at excluding certain measures from potentially constituting a breach of the investment treaty. An example of such a clause is Article 12(2) of the India-Serbia BIT:

> […] nothing in this Agreement precludes the host Contracting Party from taking action for the protection of its essential security interests or in circumstances of extreme emergency in accordance with its laws normally and reasonably applied on a non discriminatory basis.[127]

[124] See amongst others: Giorgio Sacerdoti, 'The application of BITs in time of economic crisis: limits to their coverage, necessity and the relevance of WTO law' in Giorgio Sacerdoti (ed), *General Interests of Host States in International Investment Law* (CUP 2014) 3-25. More generally, see Caroline Henckels, 'Investment treaty security exceptions, necessity and self-defence in the context of armed conflict' in Katia Fach Gómez, Anastasios Gourgourinis and Catharine Titi (eds), *European Yearbook of International Economic Law: International Investment Law and the Law of Armed Conflict* (Springer 2019) 319-340.

[125] Lu Wang, 'Chinese SOE Investments and the National Security Protection under IIAs' in Julien Chaisse, *China's International Investment Strategy: Bilateral, Regional, and Global Law and Policy* (OUP 2019) 70.

[126] See eg Treaty between the Federal Republic of Germany and the Republic of Venezuela for the promotion and reciprocal protection of investments (signed 14 May 1996, entered into force 16 October 1998) (Germany–Venezuela BIT).

[127] Agreement between the Government of the Republic of India and the Federal Government of the Federal Republic of Yugoslavia for the reciprocal promotion and protection of investments (signed 31 January 2003, entered into force 24 February 2009) (India-Serbia BIT) art 12(2).

Other treaties are slightly more detailed, such as the 2012 US Model BIT[128], or specify the areas for which legislation and regulation is carved-out.[129]

It has been noted that, while such clauses conform to an understandable need to carve out legislative and regulatory measures necessary to safeguard important national interests, the usual vagueness and generality of the terms leave open the door for an unjustified reliance on these.[130] This may be even more the case if the clause is intended to be of a self-judging nature[131], such as Article 18(2) of the US Model BIT which provides that the treaty shall not be construed as to preclude a Party from applying measures 'that it considers necessary'.[132]

Without wanting to engage in a full analysis of the question of the application and precise scope of essential security interest clauses, it is of course important to point out that in case the State is successful in arguing that the measures where necessary to protect the State's essential security interests, the measures would indeed not be in violation of the treaty since the treaty's substantive protection obligations of the State do not apply.[133] . The application of the clause to FPS would be more difficult, since the State would have to argue quite paradoxically that the lack of due diligence in preventing an attack or in finding and prosecuting those responsible for the attack would be necessary to maintain its essential security interests.

While such clauses have not yet been tested in the specific context of cybersecurity legislation, there have been several reports of possible claims by Chinese investor Huawei in relation to assertions by the Czech Republic that the telecom company's 'technologies and equipment pose a security threat'.[134] While no claims have been filed at this stage, it

[128] 2012 Treaty between the Government of the United States of America and the Government of [Country] concerning the encouragement and reciprocal protection of investments (US Model BIT) art 18(2).
[129] Agreement for the promotion and protection of investments between the Republic of Colombia and the Republic of India (signed 10 November 2009) (Colombia-India BIT) art 13.
[130] Jeswald W Salacuse, *The Law of Investment Treaties* (2nd edn, OUP 2015) 379.
[131] The precise effects of a self-judging clause on the competence of an arbitral tribunal to review the reliance by the State on the clause is still open to much debate. For a discussion see Stephan Schill and Robyn Briese '"If the State Considers": Self-Judging Clauses in International Dispute Settlement' (2009) 13 Max Planck Yearbook of United Nations Law 61-140.
[132] 2012 Treaty between the Government of the United States of America and the Government of [Country] concerning the encouragement and reciprocal protection of investments (US Model BIT) art 18(2).
[133] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Decision of the Ad Hoc Committee on the Application for Annulment of the Argentine Republic (25 September 2007) para 129.
[134] Jarrod Hepburn and Luke Eric Peterson, 'Analysis: as Huawei invokes investment treaty protections in relation to 5G network security controversy, what scope is there for claims under Chinese treaties with Czech Republic, Canada, Australia and New Zealand?' (*IAReporter*, 11 February 2019) 1 <www.iareporter.com/articles/analysis-as-huawei-invokes-investment-treaty-protections-in-relation-to-5g-network-security-controversy-what-scope-is-there-for-claims-under-chinese-treaties-with-czech-republic-canada-australia-a/> accessed 7 June 2020.

is interesting to note that the China-Czech Republic BIT contains no security clause. Other States such as Canada, Australia and New Zealand have similarly 'closed the doors on Huawei involvement in building national 5G networks'[135] and most of the investment treaties signed between China and these States also do not contain an essential security clause. However, as was discussed earlier in relation to another BIT involving Canada, in case of the Canada-China BIT the treaty does carve out security screening from investor-State arbitration in relation to a decision by Canada following a review under the Investment Canada Act, whether or not to 'initially approve an investment that is subject to review', or to 'permit an investment that is subject to national security review'.[136]

But the general question whether security exceptions could apply to regulations which would cause harm to certain investors because they are considered 'security risks' is worth exploring. Two recent and related cases deserve attention, since they map out quite clearly the possibilities of the use of essential security interests clauses in relation to cybersecurity. The cases involved investments in the telecom sector in India, and were not related to cybersecurity, but the question whether the essential security interests clause could be relied on by India was discussed in detail in both cases. In both cases[137], an Mauritian (CC Devas) and an German investor (Deutsche Telekom) had participated in an 'Agreement for the Lease of Space Segment Capacity' with an Indian state-owned enterprise in order to offer 'broadband wireless access and audio-video services throughout India'.[138] The dispute related to the cancellation of that agreement following 'The annulment of the Devas Agreement followed a 'policy decision taken by the Government of India to reserve a part of the electromagnetic spectrum known as the S-band "for national needs, including for the needs of defence, para-military forces, railways and other public utility services as well as for societal needs, and having regard to the needs of the country's strategic requirements."'[139]

---

[135] Jarrod Hepburn And Luke Eric Peterson, 'Analysis: as Huawei invokes investment treaty protections in relation to 5G network security controversy, what scope is there for claims under Chinese treaties with Czech Republic, Canada, Australia and New Zealand?' (*IAReporter*, 11 February 2019) 2 <www.iareporter.com/articles/analysis-as-huawei-invokes-investment-treaty-protections-in-relation-to-5g-network-security-controversy-what-scope-is-there-for-claims-under-chinese-treaties-with-czech-republic-canada-australia-a/> accessed 7 June 2020.

[136] Agreement Between the Government of Canada and the Government of the People's Republic of China for the promotion and reciprocal protection of investments (signed 9 September 2012, entered into force 1 October 2014) (Canada-China BIT) Annex D.34.

[137] *CC/Devas (Mauritius) Ltd, Devas Employees Mauritius Private Limited and Telecom Devas Mauritius Limited v India*, PCA Case No 2013-09, Award on Jurisdiction and Merits (25 July 2016) and *Deutsche Telekom v India*, PCA Case No 2014-10, Interim Award (13 December 2017).

[138] For the facts of the cases, see, *CC/Devas (Mauritius) Ltd, Devas Employees Mauritius Private Limited and Telecom Devas Mauritius Limited v India*, PCA Case No 2013-09, Award on Jurisdiction and Merits (25 July 2016) paras 5ff.

[139] *CC/Devas (Mauritius) Ltd, Devas Employees Mauritius Private Limited and Telecom Devas Mauritius Limited v India*, PCA Case No 2013-09, Award on Jurisdiction and Merits (25 July 2016) para 6.

In both cases India relied on the differently worded 'essential security interests'-clauses in the respective applicable treaties.[140] In *CC Devas*, the Tribunal, by majority, considered after a lengthy analysis that the decision to reserve a part of the electromagnetic spectrum only was partly 'directed to the protection of its essential security interests', the other part being subjected to the investment protection standards in the treaty.[141] The Tribunal, in its decision, however accepted that it should give the State a 'wide measure of deference':

> An arbitral tribunal may not sit in judgment on national security matters as on any other factual dispute arising between an investor and a State. National security issues relate to the existential core of a State. An investor who wishes to challenge a State decision in that respect faces a heavy burden of proof, such as bad faith, absence of authority or application to measures that do not relate to essential security interests.[142]

In *Deutsche Telekom v. India*, the applicable BIT's clause was formulated slightly differently and included the term 'to the extent necessary' before 'for the protection of its essential security interests'.[143] The Tribunal noted that the question whether a measure is 'necessary for the protection' of a State's essential security interests, is 'subject to review by the Tribunal'.[144] In reviewing the decisions, the Tribunal considered that it will

> undoubtedly recognize a margin of deference to the host state's determination of necessity, given the state's proximity to the situation, expertise and competence. Thus, the Tribunal would not review de novo the state's determination nor adopt a standard of necessity requiring the state to prove that the measure was the 'only way' to achieve the stated purpose. On the other hand, the deference owed to the state cannot be unlimited, as otherwise unreasonable invocations of Article 12 would render the substantive protections contained in the Treaty wholly nugatory. [145]

---

[140] In *CC Devas v India,* art 11(3) of the Agreement between the Government of the Republic of Mauritius and the Government of the Republic of India (signed 4 September 1998, entered into force 20 June 2000, terminated on 22 March 2017) (Mauritius-India BIT) applied.
[141] *CC/Devas (Mauritius) Ltd, Devas Employees Mauritius Private Limited and Telecom Devas Mauritius Limited v India*, PCA Case No *2013-09*, Award on Jurisdiction and Merits (25 July 2016) para 371.
[142] *CC/Devas (Mauritius) Ltd, Devas Employees Mauritius Private Limited and Telecom Devas Mauritius Limited v India*, PCA Case No 2013-09, Award on Jurisdiction and Merits (25 July 2016) para 245.
[143] Agreement between the Federal Republic of Germany and the Republic of India for the promotion and protection of investments (signed 13 July 1998, entered into force 13 July 1998, terminated on 3 June 2017) (Germany-India BIT) art 12.
[144] *Deutsche Telekom v India*, PCA Case No 2014-10, Interim Award (13 December 2017) para 238.
[145] *Deutsche Telekom v India*, PCA Case No 2014-10, Interim Award (13 December 2017) para 238.

The Tribunal also explained that it will examine whether 'the measure was principally targeted to protect the essential security interests at stake and was objectively required in order to achieve that protection, taking into account whether the state had reasonable alternatives, less in conflict or more compliant with its international obligations.' [146] In the end, the Tribunal; contrary to the decision in *CC Devas*, argued that India failed to establish that the decision was 'necessary to protect those essential security interests'.[147]

These two recent cases show that the invocation by a State of essential security interests as a shield against treaty claims, is not straightforward. Notably, much discussion still exists as to the appropriate standard applicable to the review by the Tribunal, which of course depends heavily also on the specific formulation of the clause.

4.2. Circumstances Precluding Wrongfulness

Since not all treaties include a provision aimed at excluding certain measures from potentially constituting a breach of the investment treaty because of 'essential security interests', the customary law circumstances precluding wrongfulness as embodied in the ILC Articles on States Responsibility may play an important role.

The dozens of cases initiated against Argentina in the 2000s following the State's economic and financial crisis, in which Argentina has systematically invoked both the treaty-specific essential security interests-clauses and the customary norm of 'necessity' as a circumstance precluding wrongfulness, have resulted in a series of decisions relating to the precise relation between both. The decision of the Annulment Committee in *CMS v Argentina*[148] was one of the first to attempt to clarify the precise relation between both norms, thereby departing from decisions which had argued that the treaty-specific essential security interests-clauses should be interpreted in light of the customary norm on necessity[149]. The Committee, established that both provisions are formulated differently and contain different requirements.[150] It then confirmed that the 'state of necessity in customary international law goes to the issue of responsibility', which makes it a secondary rule of international law[151] In other words, Tribunals confronted to the invocation of both provisions – the treaty norm and the customary norm of necessity –

[146] *Deutsche Telekom v India*, PCA Case No 2014-10, Interim Award (13 December 2017) para 239.
[147] *Deutsche Telekom v India*, PCA Case No 2014-10, Interim Award (13 December 2017) para 285.
[148] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Decision of the Ad Hoc Committee on the Application for Annulment of the Argentine Republic (25 September 2007).
[149] See for a discussion: Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd ed, OUP 2012) 189.
[150] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Decision of the Ad Hoc Committee on the Application for Annulment of the Argentine Republic (25 September 2007) para 130.
[151] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Decision of the Ad Hoc Committee on the Application for Annulment of the Argentine Republic (25 September 2007) para 134.

are under an obligation to consider first whether the breach of the BIT was excluded by the essential security interests clause, and if that was not the case, whether responsibility could be precluded in whole or in part under customary international law.'[152]

Irrespective of the position taken on the precise relation between the two, it is clear that both provisions are formulated differently. It has been made clear on various occasions that the requirements under Article 25 of the ILC Articles are stricter than those under the usual essential security interests-clauses one founds in BITs.[153] The invocation of necessity, as codified in Article 25 of the ILC Articles on State Responsibility, requires amongst others, that a certain act 'is the only way for the State to safeguard an essential interest against a grave and imminent peril' and it may not be invoked if 'the State has contributed to the situation of necessity.' Essential security interests-clauses, however, usually are formulated in such a way as to exclude the application of the protection standards to protect an 'essential security interest'.

As the Argentinian cases have shown, Tribunals have confirmed that as a matter of principle, economic crisis may give rise to a plea of necessity under customary international law, and there is no reason to doubt that such may not be the case in the event of acts or measures taken in the event of a cybersecurity crisis. However, pleas of necessity are in general very hard to make and therefore succeed only very occasionally.[154] This will be no different in case of claims by States that the wrongfulness of certain acts adopted in the cybersecurity context, found in breach of investment protection standards, is precluded because it was 'the only way for the State to safeguard an essential interest against a grave and imminent peril'. Moreover, the requirement that the plea of necessity may not be invoked if 'the State has contributed to the situation of necessity' could also be pivotal. Certain tribunals in the context of the Argentinian crisis indeed have argued that necessity may not be invoked because 'government policies and their shortcomings significantly contributed to the crisis and the emergency'.[155]

Conclusion

[152] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Decision of the Ad Hoc Committee on the Application for Annulment of the Argentine Republic (25 September 2007) para 134. For a criticism of the decision on these issues, and for other cases which have departed from the *CMS Committee's decision,* see Rudolf Dolzer and Christoph Schreuer, *Principles of International Investment Law* (2nd edn OUP 2012) 189.
[153] *Deutsche Telekom v India*, PCA Case No 2014-10, Interim Award (13 December 2017) para 229.
[154] David Collins, *An Introduction to International Investment Law* (CUP 2020) 303.
[155] *CMS Gas Transmission Company v Argentine Republic*, ICSID Case No ARB/01/8, Award (12 May 2005) para 329.

This chapter has attempted to give an overview of the main issues related to foreign investment in cyberspace. The 'cyber'-nature of the assets involved, as has been shown, presents several distinct challenges to the use of investment protection standards in international investment treaties.

First, digital assets need to qualify as 'investment' under the applicable investment treaty, and in case of ICSID Arbitration, also under the notion of 'investment' contained in Article 25 ICSID Convention. The digital and hence intangible nature of investments in cyberspace presents peculiarities, but as I have shown, the broadness of definitions in investment treaties does not seem to include digital assets *per se*. However the usual limitations to acknowledging certain investments as such remain applicable, both for definitions in investment treaties and under the ICSID Convention. Secondly, admission and establishment of foreign investors in the digital economy might be subjected to restrictions. Even if treaties accept a limited right of admission by extending national treatment and most-favored-nation treatment to the admission of the investment, sectors such as a telecommunication are often excluded.

Based on the hypothesis that digital assets are 'protected investments' under the applicable international investment treaties, either individually or taken as a whole with other components of an investment operation, the question I have addressed is whether what protection international investment treaties may offer in case of harm caused to the investment in the event of cyberattacks on the assets of foreign investors, or in case of cybersecurity regulations and/or legislation adopted by the host State and which are harmful to the investment.

In light of increased cybersecurity concerns, States have also increasingly adopted specific laws and regulations in relation to cybersecurity. Such legislation and regulations, may, in certain situations cause harm to investors, and hence result in an invocation by the foreign investor of the State's obligations under investment treaties. I have noted that in such case, the general principles applicable to most forms of investment apply, notably those under the FET standard of treatment. The requirements of stability, consistency, and transparency of the legal framework, the prohibition of arbitrary and unreasonable measures and the legitimate expectations of foreign investors may play an important role.

In relation to cyberattacks, which I have discussed from the perspective of the FPS clause, a clear distinction needs to be made between attacks originating from the host state of the investment, and attacks originating from a third country. The question will, in the first scenario be to what extent the state can be held responsible for the cyberattack itself, and in the latter scenario for not having exercised the necessary due diligence to prevent such an cyberattack and/or bring the perpetrators to justice.

This chapter has also considered the possible invocation of 'essential security interests' clauses. Measures taken by the host State in the post-entry stage which are in breach of the investment protection provisions in that treaty – mostly under the FET standard of treatment in case of adoption of cybersecurity legislation – might be covered by the security exception of the treaty and hence result in a finding of conformity with the treaty nonetheless. This, I have noted, is still subject to much discussion, notably on the applicable standard of review of the Tribunal. Moreover, circumstances precluding wrongfulness under the general customary norms relating to state responsibility may also play a role if the 'essential security interests' clause has been discarded by the Tribunal.