Applying the Full Protection and Security Standard of Protection to Digital Investments

by David Collins*

ABSTRACT: This article considers the possibility that digital assets of foreign investors such as websites and computer systems could be protected by the full protection and security ('FPS') standard common to many bilateral investment treaties. Such assets can properly be described as investments and the flexible nature of the FPS standard observed in recent arbitration practice could be extended to cover civil disturbances such as cyber attacks against companies. The article considers host state liability with respect to the prevention of harm to digital assets as well as failure to enforce laws that prohibit it. The lack of governmental control over websites suggests that it would be difficult to ascribe state liability under an FPS clause, except possibly in situations of large scale internet infrastructure collapse. A duty to prosecute attacks against digital assets, while common to many jurisdictions and seen in international instruments, is inappropriate as an investment treaty claim because of difficulties in compensation. The FPS standard further appears to incorporate a degree of contextual proportionality linked to the host state's resources and this may prevent successful claims against Developing States where many cyber attacks occur.

I Introduction

In international investment law, the phrase Full Protection and Security ('FPS') refers to a standard of protection for foreign investments that provides security against physical damage that may occur to a foreign investors' property arising from war or civil unrest in the host state. The FPS standard are now common to many of the more than two thousand Bilateral Investment Treaties ('BIT')s concluded between states to

* Senior Lecturer, The City Law School, City University London; Visiting Fellow, Asian Institute of International Financial Law, Hong Kong University. <david.collins@utoronto.ca>

attract foreign direct investment ('FDI') and protect multinational investors.[1] While the FPS standard was traditionally held to govern the physical security of investors' tangible assets, this understanding may need to be modified to fit the nature of security threats faced by investors in the 21st Century, namely the integrity of digital investments like computer systems and websites from attacks levied through or against the internet. However, as we shall see, by extending FPS protection in this manner, a host state's fulfilment of its FPS commitment in a treaty instrument may involve security undertakings that are beyond its economic capacity, especially in the case of Developing States, where many so-called 'cyber attacks' are believed to originate.

This article will examine the nature and scope of the FPS standard as it has developed in international investment law, including recent arbitral decisions that appear to extend its scope as well as apply it in a contextual manner. Outlining the phenomenon of organized attacks against websites and computer systems through the internet, the article will link this to the FPS's concept of civil disturbance as well as to the observed extensions to the FPS standard. The host state's associated duty to prevent damage to digital assets and to prosecute them once they have transpired will be discussed in light of trends in international law as it relates to internet security. The article will conclude with an assessment of the way in which such obligations may be modified in the case of Developing States because of the FPS standard's proportionality to particular societal circumstances. Before embarking on the analysis of the application of the FPS standard to an age of digital investments, we will first establish that foreign investors' digital assets, such as websites and computer systems,

[1] J Salacuse, *The Law of Investment Treaties*, (OUP, 2010) at 210; C Schreuer and R Dolzer, Principles of International Investment Law (OUP, 2008) at 149, M Sornarajah, *The International Law on Foreign Investment* (CUP, 2010) at 359

should be viewed as investments for the purposes of international investment law and accordingly attract the protections afforded by BIT provisions like the FPS standard.

II Digital Assets as Investments

In order for a foreign investor's digital assets such as websites and computer systems to be protected by its home state's investment treaty commitments, it must first be established that these constitute 'investments' as defined under the relevant treaty. While this will depend obviously on the specific wording of the BIT in question, some common principles emerge from treaty practice. Most BITs contain a general phrase defining investments as constituting 'all assets' with several groups of illustrative categories. Relevant for the purposes of websites and other computer data systems are treaty references to intangible property as well as movable and intellectual property.[2] Digital investments such as websites could be viewed as a species of intellectual property in as much as they are the products of technical knowledge and often artistic creativity. The BIT between Argentina and the United States includes the expansive phrase: 'inventions in all fields of human endeavour' and 'confidential business information' in its definition of intellectual property.[3] Under the BIT between the Ukraine and Denmark, an investment is stated to mean every kind of asset connected with economic activities for the purpose of establishing lasting economic relations,[4] which would seem to cover websites and computer systems as long as they were connected to a commercial activity with a long term time frame, which may mean more than simply a few transactions. Salacuse writes that these rather broad, open-ended definitions are intended to provide as wide a range

[2] Schreuer and Dolzer, ibid at 63; Salacuse, ibid at 160. Examples of such a definition can be found in article 1(6) of the European Energy Charter Treaty and Art 1(1) of the 2001 BIT between Germany and Bosnia Herzegovina.
[3] Art 1 iv (entered into force 20 October 2004)
[4] Art 1 (entered into force 23 Oct 1992)

of investment forms as possible.[5] Even if an alleged investment does not fall within any of the categories specified in the treaty, it may still qualify for BIT protection unless it falls into a category of things that are explicitly not investments, such as the extension of credit or claims to money, as outlined in the North American Free Trade Agreement ('NAFTA'),[6] exceptions which are not relevant here.

Additional common characteristics of investments that appear in treaties include the commitment of capital or other resources, the expectation of gain or profit or the assumption of risk.[7] These criteria are also reflected in Article 25 of the International Centre for the Settlement of Investment Disputes ('ICSID') Convention, giving that tribunal competence over disputes. Clearly a website or computer system is implemented by a company for the purpose of earning a profit, possibly unless it was for charitable purposes relating to a discrete project. Of course the investment must be controlled by a foreign investor; however there is no additional requirement that the investment itself must be foreign in terms of its origin.[8] Neither of these criteria should be contentious with respect to digital assets.

BIT commitments are typically restricted to investments made within the territory of the respective contracting parties.[9] This practice exists because an investment is meant to benefit the economy of a host state, either by bringing in capital or creating new jobs[10] in a manner that simply trading goods or services would not. Territoriality is a more problematic attribute to ascribe to a website on the internet, which may simply be accessible by consumers in the host state as a means of advertising foreign goods or services. Such on-line advertisement alone may still be

[5] Salacuse, above note 1 at 162
[6] Art 1139 (entered into force 1 January 1994)
[7] Seen for example in Article 1 of the US – Uruguay BIT, (entered into force 20 October 1994)
[8] Schreuer and Dolzer, above note1 at 67-68 referring to the *Tradex v Albania* award, 5 ICSID Reports 70, (29 April 1995)
[9] Seen for example in Art 1 of Canada-Peru BIT (2006)
[10] Salacuse, above note 1 at 169

sufficient, provided that the company itself has a physical presence in the territory, such as an office or factory. As such the focus of the investigation into the territoriality would not be the 'location' of the website on the internet,[11] but rather the location of the company with which it was associated. For the purposes of international investment law and investment treaty interpretation, however, likely the strongest claim that a website is within the territory of a state for the purposes of attracting BIT protection would be where the website is hosted by a server physically located within the host state, which would appear to follow the conventional understanding of internet jurisdiction.[12] Therefore, following the reasoning of the arbitration tribunal in *SGS v Pakistan*, it would assist the investor's claim of territoriality if evidence of expenditures to establish the investment within the host state could be adduced.[13] Thus an investor might demonstrate that it had paid a local web hosting company to host its website, or that it had purchased or leased local property to house the relevant server. In contrast, if the website was simply accessible within the jurisdiction through the internet, the link to the jurisdiction would likely be too tenuous, especially if the company had no physical presence within the territory. It is perhaps more obvious to assert that a computer network for a company that is physically located in the territory of the host state, such as the computer systems maintaining the functionality of an oil company, would satisfy the territoriality requirement because they are obviously within the borders of a party state.

---

[11] It is beyond the scope of this article to consider jurisdictional issues relating to the internet, which is a highly complex subject that has received much attention by scholars. See further e.g. M Sussman, 'The Critical Challenge from International High-Tech and Computer Related Crime at the Millenium' 9 Duke Journal of International and Comparative Law 451 (1999) and R August, 'International Cyber-Jurisdiction: A Comparative Analysis' 39 America Business Law Journal 531 (2002); and D Powers, 'Cyberlaw: The Major Areas, Development and Information Security Aspects' in H Bidgoli ed *Global Perspectives in Information Security* (John Wiley and Sons Inc., NJ, USA, 2009)

[12] As generally observed by commentators, ibid.

[13] *SGS Society Generale de Surveillance SA v Islamic Republic of Pakistan*, ICSID Case No ARB/01/13 (6 Aug 2003) at [137] under the Swiss-Pakistan BIT (entered into force 6 May 1996)

Given the very broad language used to define investments in BIT practice, digital assets such as websites and computer systems should be viewed as investments and consequently covered by BIT provisions, provided that they serve a commercial purpose and that there is a meaningful territorial link to the host state. Digital investments therefore can in theory attract the protection of FPS clauses that appear in standard investment treaties. Before applying the FPS standard to digital investments, we must explore the precise meaning of the FPS clause as it has developed in international investment law.

III The FPS Standard Elaborated

Unlike other standards of investment protection found in international treaties, such as that of Fair and Equitable Treatment ('FET') (essentially due process) and guarantees against expropriation (government takings), there has been remarkably little academic treatment of the FPS standard.[14] While FPS is expressed in a variety of different ways in various treaties,[15] it is often evaluated in conjunction with the FET standard, as if the former standard merely expands and elaborates upon more general concepts of fair treatment contained in the latter.[16] FPS also often appears in BITs in the same provision regarding compensation for expropriation.[17] Further investigation reveals that FPS is a stand alone obligation relating to fairly specific types of situations and harm suffered. While some commentators have observed that it is becoming increasingly difficult to discern how minimum standard provisions in BITs, such as

[14] Possibly the only example of academic commentary exclusively on FPS is a chapter by G Cordero Moss in A Reinisch ed, *Standards of Investment Protection* (OUP, 2008).
[15] Cordero Moss, ibid at 133-134
[16] E.g. S Subedi, *International Investment Law: Reconciling Policy and Principle* (Hart, Oregon, 2008) at 134, A Qureshi and A Ziegler, *International Economic Law* (2d ed, Thomson Sweet & Maxwell, 2007) at 400
[17] E.g. German Model BIT Art 4 <http://ita.law.uvic.ca/investmenttreaties.htm> (last accessed September 2010)

FPS are actually being interpreted and applied,[18] some general features of the FPS standard have emerged that should operate as guidance in future investment treaty practice.

i) Background and Relationship to Customary International Law

The FPS standard was seen as early as the 1833 Friendship, Commerce and Navigation Treaty between the United States and Chile[19] and the first BIT, concluded between Germany and Pakistan in 1959 contains an FPS clause.[20] The FPS standard appeared in these early treaties in response to various waves of outright and creeping expropriations of the assets of Western companies in the Developing world, eventually becoming a norm in most BITs.[21] The invocation of state responsibility for the omission of the state to provide protection to aliens existed in international law before the explosion of BITs seen in the early 21st Century. Indeed it was explicitly recognized by the International Court of Justice in the *Tehran Hostages Case*.[22]

The precise wording of the clause has varied from treaty to treaty, sometimes the word 'full' is omitted in favour of 'constant' and others put 'security' before 'protection'.[23]

Many investment treaties link the FPS standard to general international law, whereas some treaties speak of protection and security as well as treatment in

[18] T Grierson-Weiler and I Laird, 'Standards of Treatment' in P Muchlinski, F Ortino and C Schreuer eds. *Oxford Handbook of International Investment Law* (OUP, 2008) at 261 and T Weiler, International Investment Arbitration (Cameron & May, 2005) at 667 where FPS and FET are described as 'malleable concepts'.

[19] Art X. See also US / Paraguay Treaty of Friendship Commerce and Navigation of 1859 Art IX

[20] Treaty for Promotion and Protection of Investment (West German – Pakistan) Art 3(2) (signed 25 November 1959)

[21] Subedi, above note 16 at 133. See e.g. The Friendship, Commerce and Navigation Treaty between Italy and Venezuela (1861) and the Traité d'Amité de Commerce et de Navigation (France / Mexico) 1886

[22] *Case Concerning US Diplomatic and Consular Staff in Tehran* (US v Iran) (Merits) [1980] ICJ Rep 3

[23] Schreuer and Dolzer, above note 1 at 149

accordance with international law as though they were separate and distinct standards.[24] The provision of protection to investors against physical harm has been viewed as an embodiment of customary international law standards relating to the protection of aliens.[25] This is particularly seen in customary international law as developed by the United States.[26] Montt has gone so far as to suggest that the FPS standard was simply another way of referring to the traditional international minimum standard of protection provided in customary international law. He claims that FPS corresponded to indirect responsibility of states, meaning failures to maintain public order and to operate the system of criminal law that were seen as core responsibilities of states in the 19th Century. Direct responsibility, meaning the duty to proactively act to protect foreign investors, was therefore a feature of the more general FET standard.[27] In contrast, Subedi writes that FPS, like FET is meant to imply that foreign investors are entitled to protection over and above their entitlement to non-discriminatory treatment under international law.[28]

The controversy regarding whether the FPS standard is autonomous or merely incorporates customary international law has led to some investment treaties addressing the issue directly. NAFTA states that FPS does not require treatment in addition to or beyond that which is required by the customary international law minimum standard of treatment of aliens.[29] The NAFTA Free Trade Commission reiterates that the FPS clause in NAFTA represents the current manifestation of the customary international law minimum standard.[30] Canada's Model Treaty Art 5.2 and

[24] C Schreuer and Dolzer, above note 1 at 152
[25] Sornarajah, above note 1 at 237
[26] Sornarajah, ibid at 342
[27] S Montt, *State Liability in Investment Treaty Arbitration: Global Constitutional Administrative Law in the BIT Generation* (Hart: Oregon, 2009) at 70
[28] Subedi, above note 16 at 134. This is reflected for example in the text of NAFTA, see below note 30
[29] Above note 6 at Art 1105(1)
[30] NAFTA Free Trade Commission Notes of Interpretation of Certain Chapter 11 Provisions (NAFTA Free Trade Commission, 31 July 2001)

US Model Treaty Art 2 b) states that the FPS standard is only that provided by customary international law. Similarly the Central American Free Trade Agreement outlines that FPS requires each Party to provide the level of police protection required under customary international law.[31] This would appear to suggest that there is some bare minimum level of protection against civil unrest that a state must offer foreigners who cross its borders. Some commentators have claimed that FPS protection in BITs expanded upon the existing international minimum standard, requiring host states to proactively defend investors against others.[32] This is in keeping with the theory that BITs are themselves a *lex specialis* which are separate from general international law.

ii) The Content of the Standard

As noted above, the FPS standard traditionally referred to the need to protect the investor against various form of physical violence resulting from war or civil disturbances, including the invasion of the premises of the investment.[33] This can be seen as a dual standard in as much as harm can befall an investment either through direct action of the state, or by its failure to protect when harm has come from somewhere else. Schreuer and Dolzer suggests that FPS clauses establish the host state's obligation to take active measures to protect the investment from adverse effects, which may have been caused either by the actions of the host state or by third parties.[34] Thus the Iran-US Claims tribunal established that the failure to provide protection to an alien who is threatened by violence creates responsibility in the host

[31] Art 10.1(2). The term 'police protection' is used to describe the FPS standard in Art 2 b) of the US Model Investment Treaty, <http://ita.law.uvic.ca/investmenttreaties.htm> (last accessed September 2010)
[32] A Lowenfeld, *International Economic Law* (2d ec Oxford, 2008) at 558 and S Subedi, above note 16 at 57
[33] Schreuer and Dolzer, above note 1 at 149
[34] Schreuer and Dolzer, ibid at 149

state, whether the duty is not fulfilled either negligently or wilfully.[35] The irrelevance of direct causality in the breach of the standard must be emphasized – it does not matter that the host state itself did not cause the damage, as long as the damage occurred within its territory.[36] This dual nature of the standard can be found in its historic origins in the political volatility of Latin America of the 20th Century. First, the investor's property must not be harmed by action of the host state's military (duty not to harm), and second, the investor's property must be protected against the actions of a riotous mob (affirmative duty to protect).[37] The responsibility to ensure that foreign investors' property is not damaged exists irrespective of the lack of connection between the state and the party which caused the injury. This view should be contrasted with the principle drawn from International Law Commission's Draft Articles on State Responsibility stating that actions of private parties do not normally engage the international responsibility of the state.[38] Still, under international law if an attack by a third party was foreseeable, then a duty of protection is owed to an alien.[39] Thus the FPS standard contemplates a state's responsibility for the consequences of actions of private parties because of a failure of its police or other such agencies charged with maintaining peace. The state will have a duty to prevent the harm-causing action by the private entity.[40]

The FPS standard of protection against physical damage is rooted in the state's failure to exercise a proper level of care, or 'due diligence.'[41] Although FPS has been

[35] Sornarajah, above note 1 at 342
[36] Cordero Moss, above note 14 at 138.
[37] Sornarajah, above note 1 at 134
[38] International Law Commission Draft Articles on Responsibility of States for Internationally Wrongful Acts, 2001 Art 4. <http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf> (last accessed September 2010)
[39] *Home Missionary Society Case* (1920) 6 UNRIAA 20
[40] Weiler, *International Investment Arbitration*, above note 18 at 679
[41] C McLachlan, L Shore, M Weiniger, *International Investment Arbitration: Substantive Principles* (OUP, 2007) at 247

referred to as an absolute standard of treatment,[42] the 'due diligence' approach suggests that the host state must only make its best efforts to protect foreign investors from physical harm that may result from civil unrest or other such disturbances.[43] Accordingly, a violation of FPS is dependant on whether the state exercised a reasonable level of effort in affording protection to foreign investors. Liability will therefore exist in the state if a capacity to exercise control exists and there was a failure to exercise that control.[44] Commentators have noted a reluctance on the part of investment tribunals to extend the FPS standard beyond the requirement of due diligence.[45]

In this sense, under an FPS obligation, the host state must demonstrate that it has taken all measures of precaution to protect the investment of the investor and its territory; there is no strict liability imposed upon the state.[46] As indicated by a tribunal of the Permanent Court of Arbitration: 'the [FPS] standard obliges the host state to adopt all reasonable measures to protect assets and property from threats or attacks which may target particularly foreigners or certain groups of foreigners.'[47] The ICJ later stated that a reference to 'full protection and security' could not be viewed as a warranty that property should never be disturbed under any circumstances, with emergencies or wars being the most obvious defences.[48] Cordero Moss suggests that this limitation should characterize a state's FPS duty as an 'obligation of means' – the extent to which a host state must provide security will be

[42] T Grierson-Weiler and I Laird, above note 18 at 263
[43] E.g. Montt above note 27 at 70
[44] Wena Hotels Ltd v Arab Republic of Egypt, ICSID Case No. ARB/98/4 [84]
[45] McLachlan, Shore and Weiniger, above note 41 at 250
[46] *Noble Ventures v Romania,* ICSID Case No. ARB/01/11(12 Oct 2005) at [164]
[47] *Saluka Investments (The Netherlands) v the Czech Republic* (Partial Award, 17 March 2006) [483] and [484]. Here the measures taken by the host state were viewed as a reasonable response under the circumstances.
[48] *Electronica Sicula SpA (ELSI) (USA v Italy)* ICJ Reports 1989 at [108]

linked to its resources. [49] As such, in his words: 'the state enjoys a rather wide discretion to discharge this obligation in accordance with its own sovereign appreciation.'[50] This contextual approach to the FPS standard is highly relevant when assessing internet security in impoverished states. Before examining that issue, it is illustrative to consider some of the leading arbitration decisions that have considered the FPS standard and the types of situations in which it will operate.

iii) Some Leading Arbitration Decisions on FPS

It should be noted that the language of a BIT is not the decisive factor in understanding the scope of application of the standard,[51] thus arbitration decisions will be highly relevant in applying the FPS to digital assets affected by cyber attacks.

AMT v Zaire[52] concerned a dispute initiated under the US-Zaire BIT brought due to the alleged failure of Zaire to protect the US investor from property damage sustained as a result of activities of the Zairian armed forces in Kinshasa. Zaire claimed that it had not violated the FPS standard because it had not treated AMT any less favourably than it treated other investors, including nationals and those from other countries. The ICSID tribunal held that Zaire had breached the FPS provision because it had taken no measures whatsoever to ensure the protection of AMT's property and the fact that the host state had also failed to protect other investors was irrelevant. It was important to the tribunal's conclusion that the losses sustained by AMT were caused by actions of Zaire's armed forces acting individually and not in their official capacity as the Zairian military, and as such their actions did not fall within the combat operations exception to the standard contained in the BIT. As in

[49] Cordero Moss, above note 14 at 139
[50] Cordero Moss, ibid at 150
[51] Cordero Moss, ibid at 134-135
[52] ICSID Case No. Arb/93/1 (1997) (10 February 1997) [hereinafter *AMT*]

this situation, FPS clauses in investment treaties may contain built-in exceptions for the host state, such as warfare. Similarly, a declaration of an emergency situation, because of a national security threat, such as might arise during a serious attack against a country's internet, could potentially obviate the host state from its FPS obligations.

In *Asian Agricultural Products (AAPL) v Sri Lanka*[53] the tribunal examined the FPS clause in a BIT between the UK and Sri Lanka which was engaged because of property damage suffered by the British Hong Kong shrimp farm during an armed Tamil uprising. The tribunal held that the phrase 'full protection' in a BIT did not refer to any standards higher than the minimum standard of treatment in required by general international law. In times of civil conflicts, there was a duty on the part of the host state to confer adequate protection to foreign investment and that the failure to give such protection will engage the liability of the state, namely to compensate the investor for damage suffered. This obligation, existing independently of the express FPS, was violated by Sri Lanka. The FPS provision in this dispute was unhelpful to the investor, largely because it was included with a wide exception: no compensation would be payable if the damage resulted from necessary combat action taken by the host state's military, which included the action taken against the Tamil rebels.

A similar approach was taken by an ICSID tribunal in *Noble Ventures v Romania*[54], where it was held that a FPS clause should not be understood as being wider in scope than the general duty to provide protection and security to foreign nationals found in the customary international law of aliens. The tribunal stated that in order to claim FPS it was necessary to demonstrate that the measure implemented by the host state that caused the damage was directed specifically against a certain

[53] (1992) 17 YCA 106 [hereinafter *AAP*]
[54] ICSID Case No. ARB/01/11(Award) 12 Oct 2005) [hereinafter *Noble Ventures*]

investor by reason of its nationality.[55] Thus if all investors are injured during a widespread attack against the country itself, then FPS may not be engaged.

The FPS standard received some consideration in the *Wena Hotels v Egypt*[56] dispute brought by a British company against Egypt for the country's failure to prevent the state-owned Egyptian Hotels Corporation attacks against the hotel's properties. Guests of the hotels had been forcibly evicted and property damaged due to political unrest. Although the investor could not establish that the host state had actually participated in the attacks against the hotels, Egypt was held liable for breach of the FPS standard because it was aware of the hotel seizures and yet did nothing to prevent them.[57]

Azurix v Argentina[58] concerned breaches of a water and sewer concession granted by an Argentinean province in favour of a US corporation. Panic ensued among the public when an algae outbreak occurred, causing citizens to break contracts with the water supplier. Finding a breach of the FPS standard in the host state's conduct in failing to complete work on systems critical to algae removal as well as exacerbating the public's response to the events, the tribunal noted that although other arbitration tribunals had clearly limited the FPS standard to a baseline level of police protection, it could be extended under the applicable US-Argentina BIT. Importantly, FPS did not simply concern physical protection but also contained a further requirement that host governments ensure the 'stability afforded by a secure investment environment,'[59] although the precise feature of the BIT that led to this conclusion is not explored. It is significant that the *Azurix* dispute predated the

[55] Ibid at [111]
[56] ICSID Case No. ARB/98/4 (8 December 2000)
[57] Ibid at [84] – [95]
[58] ICSID Case no. ARB/01/12 (14 July 2006) [hereinafter *Azurix*]
[59] Ibid at [408]

Argentinean economic crisis and therefore had no relation to any emergency measures taken by the state in that regard.

Finally, the recent ICSID decision *Pantechniki v Albania*[60] concerning riots by citizens (following the collapse of a government run Ponzi scheme) which damaged an investor's remote road works project suggests that an element of proportionality is required when assessing violations of the FPS standard, an issue to which we will return below. Proportionality is needed because, unlike denials of justice which result from a conscious lack of diligence with respect to governance, a failure in providing protection and security is likely to arise in:

> 'an unpredictable instance of civil disorder which could have been readily controlled by a powerful state but which overwhelms the limited capacity of one which is poor and vulnerable…[I]t seems difficult to maintain that a government incurs international responsibility for failure to plan for unprecedented trouble of unprecedented magnitude in unprecedented places.'[61]

Consequently a host state should not bear international responsibility for the failure to respond to a violent incident that is wholly unprecedented in nature and size. Thus under FPS the host state must exercise the level of due diligence of a country in similar circumstances, a feature that becomes relevant when applying the standard to Developing States.

Having now established a sense of what the FPS standard has come to mean in international investment law, we will now consider how it might be applied to provide protection against modern threats to digital investments.

IV 'Cyber Attacks' as Civil Disturbances

[60] ICSID Case no. ARB/07/21 (30 July 2009) [hereinafter *Pantechniki]*
[61] Ibid at [77]

There is a voluminous amount of academic literature on legal issues raised by attacks against perpetrated through the internet, so-called 'cyber attacks'.[62] Suffice it to say that instances of cyber attacks against corporations and governments are becoming commonplace as the level of sophistication of malevolent software increases. Some high profile examples of cyber attacks can be mentioned briefly. A series of cyber attacks against three US oil companies, including Exxon Mobile, were initiated in early 2010 from network servers located in China for the purpose of obtaining data on the location and precise value of oil discoveries.[63] In February 2010, the computers of nearly 2,800 companies were breached by 'hackers' located in Europe, allowing them access to sensitive personal data, including that of customers. An unidentified Australian multinational financial company was attacked through the internet in 2010, allegedly from within China, disabling that company's server for several hours.[64] Similar attacks occurring in recent years have been launched from 'infected' computers located in states such as China, Egypt, Mexico, Saudi Arabia and Turkey, where the risk of detection by authorities is thought to be low.[65]

Cyber attacks are not always linked to theft of information but may be simply intended to damage property, possibly for political or ideological reasons, so-called 'cyber terrorism'. Highly publicized cyber attacks were launched against the state of Estonia in 2007 and Georgia in 2008, both believed to have originated from Russia, rendering the internet inoperative and bringing parts of these countries to a standstill. These attacks were thought to be successful because of increasing sophistication of cyber terrorists as well as the lack of preparedness of the Estonian and Georgian

[62] Perhaps the best recent example of a treatment on this topic in one volume is I Carr ed. *Computer Crime*, Second Series (Ashgate, UK, 2009). See also H Bidgoli ed. *Global Perspectives in Information Security* above note 11.
[63] L Barrett, 'Cyber Attack Threat Keeps CEOs Up at Night' Internetnews.com (28 January 2010)
[64] R Sullivan, 'Company: Chinese Cyber Attack Targets Australia' <http://www.physorg.com/news190524906.html> (last accessed August 2010)
[65] S Gorman, 'Broad New Hacking Attack Detected' Wall Street Journal (18 Feb 2010)

governments.[66] Politically motivated attacks can also be directed against commercial organizations. Perhaps the most notorious destructive cyber attack against a company was levied in early 2010 against Google China by hackers within that country, allegedly intending to disable the e-mail accounts of human rights protesters.[67] If not deserving of the description 'war', these instances call to mind the notion of a 'civil disturbance' in the tradition of the FPS standard, especially where the effect is a widespread one, interfering with the proper functioning of an important element of civil society.

In addition to the obvious danger posed by cyber attacks in situations where vital infrastructure systems are concerned, cyber attacks can be very costly to private parties, such as foreign investors located within the affected region. Disrupted websites can cost suppliers lost contracts as well as damage to reputation. Interference with computer systems could disable production as well as damage associated physical assets. Foreign investors might be particularly vulnerable given the level of resource commitments relative to profit in the early years of an overseas project. A report by the US Congressional Research Service determined that attacks against computer systems resulted in an average shareholder loss for publicly traded corporations between US$50 million and $200 million.[68] This figure does include the injury that may be inflicted on companies' reputations due to a cyber attack, which could be incredibly damaging to the banking sector where the security of customer's details is an essential component of the service. Clearly foreign investors stand to

[66] E MacAskill, 'Countries Are Risking Cyber Terrorism: Security Expert Tells World Summit' The Guardian (London) 5 May 2010. See further S Shackelton, 'Estonia Three Years Later: A Progress Report on Combatting Cyber Attacks' 13:8 Journal of Internet Law 22 (2010)

[67] A Jones and M Helft, 'Google, Citing Attack, Threatens to Exit China' New York Times, 12 January 2010. Industrial espionage was also thought to be a purpose behind the attack on Google's operations in China: A Eunjung Cha and E Nakashima, 'Google China Attack Part of Vast Espionage Campaign' Washington Post, 14 January 2010

[68] B Cashell, WD Jackson, M Jickling, and B Webel, 'The Economic Impact of Cyber-Attacks' Congressional Research Service, The Library of Congress (US) (1 April 2004)

suffer significant financial losses through internet-based criminal damage against digital assets like websites and computer systems,

Instances of civil disturbances that have led to findings of FPS violations appear to involve situations in which there was a violent situation and resulting damage to the investor's property was an indirect consequence of a larger conflict. Thus a purposeful, targeted criminal attack against a particular firm's website might not fit within this model. The application of widespread cyber attacks to the FPS standard must also be balanced by observed limitations on the standard associated with emergency situations, as in *AMT*. Collapse of internet infrastructure could be viewed as an emergency situation, which could relinquish the state from its treaty obligations to protect foreign investors. Furthermore, a large scale cyber attack that affects all investors, not just foreign ones, may fail the test established in *Noble Ventures*, which suggests that foreigners must be disproportionately injured during an instance of public disorder such as a catastrophic assault on internet communications. The applicability of emergency type defences will depend on the nature of the disaster and the proportionality of the measures taken in response to it.

If it is to be asserted that foreign investors should expect protection from such civil disturbances by the host states in which they operate, then in the absence of express promises to that effect in the language of the BIT, traditional assurances offered by the common FPS standard must be enlarged. This trend has been observed with arbitration tribunals demonstrating an 'expansionary interpretation' of the FPS standard.[69] For example, as noted above, the *Azurix* tribunal established that FPS may be breached even if no physical violence or damage occurs. It stated

[69] Sornarajah, above note 1 at 360, citing *Azurix,* above note 58

> It is not only a matter of physical security; the stability afforded by a secure investment environment is as important from an investor's point of view …where the terms 'protection and security' are qualified by 'full' and no other adjective or explanation, they extend, in their ordinary meaning, the content of this standard beyond physical security.[70]

A stable investment environment could conceivably contemplate the integrity of internet infrastructure generally, and a digital asset such as a computer network could be precisely the type of investment susceptible to non-physical security breaches. In another dispute *Siemens v Argentina*, the tribunal held that FPS could cover investments of an intangible nature, concluding however that: 'it is difficult to understand how the physical security of an intangible asset would be achieved.'[71] It seems that computer networks and websites precisely fit into this notion, although they are not physical in the sense of solid and dimensional, they can be damaged in a measurable way. We will now consider the extent to which FPS obligations might actually serve this purpose in light of host governments' role in these areas.

V Host State Liability under an FPS Obligation

Under the FPS standard, the host state must use due diligence in its provision of protection and security for foreign investments. In terms of digital investments, this obligation can be broadly divided into the host state government's obligation to prevent damage to the assets of foreign investors and its obligation to detect and prosecute those who have inflicted it.

i) Obligation to Prevent Harm to Digital Investments

[70] *Azurix*, above note 58 at [408]
[71] *Siemens v Argentina*, ICSID Case No. ARB/02/8 (6 February 2007) at [303]

It may be suggested that under an FPS clause the host state has a duty to prevent harm inflicted upon digital assets by providing a secure on-line environment, meaning one that impairs the ability of cyber criminals to launch attacks successfully. If the server that hosts a foreign investor's website is located within the territory, as per establishing BIT coverage, it could be argued that the host government has a responsibility to ensure that the websites which it hosts are not attacked. Following this line of thought, commentators such have urged that computer network security should be understood as a public good,[72] which suggests it is a beneficial and normal aspect of a functioning society. This characterization is especially relevant in that host states seek to provide a stable environment for foreign investments as a means of augmenting their own economic position. In that sense internet security is a means to by which the integrity of the economic system of the state is achieved, including that system's capacity to attract foreign capital. A stable investment environment is offered to investors in exchange for the economic advantages it brings.

Moreover, it could be argued that the need to maintain an adequate level of protection against cyber crimes features in international legal instruments, which may be indicative of what a reasonably secure digital environment should be for the purpose of establishing an FPS standard, or an international minimum standard, if that is what FPS is taken to mean. The 2002 Organization for Economic Cooperation and Development ('OECD') Guidelines for the Security of Information Systems and Networks recommended that states should implement rapid and effective co-operation to prevent criminal attacks that arise in an on-line environment.[73] The UN also enacted resolutions aimed at curtailing terrorist activity instigated through the

[72] J Trachtman, 'Global Cyberterrorism, Jurisdiction and International Organization' in M Grady and F Parisi eds. *The Law and Economics of Cybersecurity* (Cambridge, 2006) at 271

[73] OECD, 2002. Art III.3 <http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html> (last accessed September 2010)

internet, such as may damage the functionality of computer systems.[74] In light of these instruments, it could be suggested that in accepting an FPS obligation in a BIT, the host state has incurred the responsibility to provide internet security to a degree recognized as necessary by the international community in order to prevent damage against the websites and computer systems of foreigners that may occur as a direct or indirect result of a coordinated cyber attack.

However, it is unlikely that an obligation could ever be placed upon a host state government to protect individual websites from targeted cyber attacks. This is because internet service provision remains in the hands of private companies – governments are not in the practice of operating or maintaining servers that host websites, this is the domain of private telecommunications companies, or Internet Service Providers ('ISP's). Host states may provide licenses to ISPs that sell internet connection and as such governments provide a degree of oversight, but this does not extend to practical control of the functionality or security of the network or individual websites that appear on it. It is more difficult to propose meaningful government oversight of a website than it would in the case of, for example, a factory, where the police can normally gain access and intervene if an attack occurs. Thus there is almost certainly an insufficient level of governmental control to attribute any security failures related to specific websites to the state so as to ground FPS responsibility. Rather private parties, such as ISP providers may be the most plausible actors in terms of preventing future harm.[75]

It may be fair to assert that large scale internet security issues, such as the integrity of a country's internet infrastructure generally, or the stability of

[74] UN General Assembly Resolution 51/210 (16 Jan 1997); UN Security Council Resolution 1373 (2001) (28 Sep 2001). It should be noted that these instruments contemplate on-line violence aimed at de-stabilizing society itself rather than industry or a particular private investor.
[75] D Lithtman and E Posner, 'Holding Internet Service Providers Accountable' in M Grady and F Parisi eds. *The Law and Economics of Cybersecurity* (CUP, 2006)

communication networks that affect millions of users such as those affecting the supply of utilities, should be within the domain of governments.[76] Internet architecture is increasingly an integral component of a functioning society and should be seen as within the sphere of a government's responsibility to its citizens, even where some essential utilities such as internet connectivity, electricity and water are directly provided by private companies. Disruptions therein seem to be the essence of the concept of 'civil disturbance' upon which the FPS standard is based. As such, liability for property damage, even as an indirect consequence of the disarray caused to the larger system, may conceivably be the fault of the state. Under this view, a foreign company operating within Estonia might have sought damages from the government of that state for the collapse of the internet in that state, particularly if this was caused due to some oversight or carelessness on the part of the government. This rationale must be tempered with potential emergency situation defences that a government could assert, such as those seen in *AMT*. The more serious the attack on the state's computer systems, the more likely the state will be able to claim that its actions were dictated by the urgency of the situation. It should be mentioned that clearly where the host state plays a direct role in sponsoring or coordinating a cyber attack against a foreign investor's website that has a commercial presence within its borders, FPS obligation to prevent harm would clearly be violated.[77]

Any assessment of the duty of 'due diligence' owed by states under an FPS clause must further be balanced against the reasonable measures that the investor should be expected to implement to protect their own assets, much as a business owner would be expected to lock their premises at night. Failure of the investor to

[76] Trachtman, above note 72 at 270

[77] State responsibility under general international law will also be engaged, potentially raising entitlements to self-defence and the entitlement to use of force: S Shackelton, 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law' 27 Berkeley Journal of International Law 192 at 235

maintain some rudimentary level of security for its own on-line presence would most probably mitigate any host state liability in this matter, or at least reduce the level of compensation awarded by a tribunal. As Trachtman has argued, companies should be responsible for the basic security for their own systems, such as firewalls against e-mail spam and maintaining anti-virus software, because they can prevent such harms at lower cost.[78]

Were a breach of an FPS clause to be found in relation to a cyber attack on an investor's digital investments, an arbitration tribunal would then be charged with the difficult task of assessing an appropriate level of compensation. Calculating damages for breach of investment treaty standards of protection is a notoriously complicated issue in international law and cannot be fully examined here.[79] It would be expected that damages for failing to prevent a cyber attack would likely consist of some combination of lost business or profits during the period where the website or computer system was down, the cost of repairs and or replacement value of associated damaged physical assets, such as machinery and computer hardware.

ii) Obligation to Detect and Prosecute Cyber Criminals

The second application of an FPS obligation to cyber attacks is the provision of a functioning legal system that maintains and enforces laws against the commission of violence against computer systems and other digital assets of foreign investors. First, the integrity of the host state's legal system with respect to the detection and prosecution of cyber crimes might be viewed as a more process-based feature of the host state environment and therefore more appropriately classified under the FET standard. Pursuing the analysis under FPS, while the timely prosecution of criminals

[78] Trachtman, above note 72 at 270
[79] See further: I Marboe, *The Calculation of Compensation and Damages in International Investment Law* (OUP, 2009)

ex post may offer little by way of compensation to an injured investor claiming FPS violation, an efficient legal response to cyber crimes could deter future cyber attackers, reducing the probability that such attacks will occur again.[80] It is therefore unclear what form of compensation an injured investor would be seeking from an arbitration tribunal when pleading a host state's failure to enforce the criminal law, except the highly contingent claim that criminals who perpetrated the cyber attack would not have committed the offence if they had feared detection and punishment. This would be exceedingly difficult to quantify when assessing damages.

Still, laws relating to the sanctity of digital property are common in international law and as such could fall within a reasonable level of security as provided by the FPS. For example, the World Trade Organization's ('WTO') Trade Related Measures of Intellectual Property Agreement mandates a minimum level of protection for intellectual property within the WTO Member states' domestic legal systems, which could assist where commercially valuable digital assets, such as customer information, is copied or otherwise stolen during a cyber attack. The Council of Europe Convention on Cyber Crimes requires that parties must adopt legislative measures to establish as a criminal offence the hindering of functioning of a computer system by intentionally inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing of computer data. [81] Many domestic legal systems also maintain laws that have been enacted to prosecute criminals for crimes against computer systems, such as attacks on commercial websites. For example, Canada's Criminal Code establishes a criminal offence for destroying, altering or

[80] W McGarvan, 'Intended Consequences: Regulating Cyber Attacks' 12 Tulane Journal of Technical and Intellectual Property 259 (2009)

[81] 23.XI.2001, Budapest, Art 5. As of 2006 the Convention had 28 signatory states, of which 15 had ratified. The Convention has received praise from commentators such as M Miquelon Weismann: 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process' in I Carr ed., *Computer Crime*, above note 62.

interfering with the use of data.[82] State practice of this nature is evidence of customary international law in favour of protection against violence to on-line property[83] and consequently should inform an understanding of a due diligence level of legal protection against cyber attacks that may be associated with an FPS undertaking. Thus it could be concluded that a foreign investor benefiting from a BIT commitment should expect some reasonable level of police investigation, criminal prosecution and punishment for attacks on its websites and computer systems.

This view must be tempered, however, with the realities of cyber attacks and associated jurisdictional problems on the internet, a full discussion of which is beyond the scope of this article. It would be difficult to argue that a host state was liable to prosecute cyber criminals who launched an attack from outside the state's borders because the state would have no jurisdiction over the matter, unless the criminals happened to also be nationals of the host state.[84] The Council of Europe Convention on Cyber Crimes states simply that jurisdiction will be established if the offence occurs, *inter alia*, in the territory of a state,[85] offering nothing about how this will be defined. FPS is engaged where damage is suffered within the territory of the host state, a condition which, as noted above, would probably be satisfied if the website server or computer system was located within its borders. But it is not clear that international practice in relation to cyber crime enforcement is definitive to the point that it could constitute a standard. Many commentators have criticized the lack of

[82] Criminal Code of Canada s. 430(1.1). See also Title 18 ch 47 United States Code s.1030 establishing the criminal offence of knowingly accessing a computer without authorization to obtain information or cause damage. In *Cyber Law and Security in Developing and Emerging Economies* (Edward Elgar, 2010), authors ZK Shalhoub and SL Al Qasimi report that only 26 countries in the world have developed some kind of legislation dealing with cyber issues, at 224

[83] R Garnett and P Clarke, 'Cyberterrorism: A New Challenge in International Law' in A Bianchi ed. *Enforcing International Law Norms Against Terrorism (*Hart, Oxford, 2004) at 477

[84] However, a UK Court of Appeal held that criminal territorial jurisdiction could be established in the jurisdiction where the website contents *could* be accessed and downloaded: *R v Graham Waddon*, 2000 WL 41456 (2 April 2000), in that sense as long as the website was accessible in the host state, then it could take jurisdiction over the matter.

[85] Art 22.1 a)

international regulation for crimes perpetrated on the internet,[86] such as those which would damage the value of a company's commercial investments. This is especially the case in Developing States, which may require a contextual modification of the FPS standard.

VI Developing States and the FPS Standard

As much as half of all worldwide FDI now flows into the Developing world,[87] where the legal and political conditions are often not as stable as in the states from which most of the capital originates. Commentators caution that not all governments will have the resources operate functional computer networks, let alone prevent destructive acts against them.[88] In addition to poor levels of internet connectivity[89] and associated lack of technical knowledge to prevent cyber attacks, few Developing States have enacted laws to deal with these issues and have consequently been incapable of prosecuting criminals.[90] Harmful cyber attacks may be more prevalent in states where there is a general mistrust of the government and where small groups with limited resources may be empowered by the anonymity and destructive potential of the internet.[91] Such countries often have weak infrastructures or low capacity to respond to internet-based security issues. These conditions describe many of the capital importing states of the Developing world which have concluded BITs for the

[86] U Draetta, 'The Internet and Terrorist Activities' and R Garnett and P Clarke, 'Cyberterrorism: A New Challenge in International Law' in A Bianchi ed. *Enforcing International Law Norms Against Terrorism (*Hart, Oxford, 2004); Shalhoub and Al Qasimi, above note 82; and W McGarvan, above note 80

[87] World Investment Report, UNCTAD, 2010. <http://www.unctad.org/templates/webflyer.asp?docid=13423&intItemID=2068&lang=1> (last accessed September 2010)

[88] Trachtman, above note 72 at 273

[89] This phenomenon is known as the 'Digital Divide' see further R Kariyawasam, *International Economic Law and the Digital Divide: A New Silk Road* (Edward Elgar, 2007)

[90] Shalhoub and Al Qasimi cite the example of the Philippines, which had evidence of those responsible for the 'Love Bug' virus of 2000 which cost the country more than US $10 billion in damage, but was unable to prosecute because of a deficient legal regime, above note 82 at 224

[91] R Crelinsten, 'Terrorism and Counter-Terrorism in a Multi-Centric World: Challenges and Opportunities' in M Taylor and J Horgan eds. *The Future of Terrorism* (Routledge, London, 2006)

very purpose of placating foreign investors. Uptake of security measures necessary to prevent cyber attacks against computer systems in these countries is reported as sporadic, with many developing nations failing to maintain adequate prevention measures.[92]

A foreign investor should not expect the same level of internet security from every state in which it operates, as security against cyber crimes can be expensive and require a high level of technical proficiency and human resources.[93] This is the embodiment of the *Pancheckniki* dicta: 'an unpredictable instance of civil disorder…which overwhelms the limited capacity of [a state] which is poor and vulnerable.'[94] The elaboration of 'due diligence' under the FPS standard as offered by *AAP* hints that investors should have a lower expectation in Developing States: '[due diligence means] reasonable measures of prevention which a well-administered government could be expected to exercise under similar circumstances.'[95] While a reasonable level of administration can be expected, this must be balanced against the context in which the events have occurred. Sornarajah writes that this will include the intensity of the strife and the resources that could be diverted for the purposes of protection.[96] In addition to intensity, possibly meaning the number of individuals harmed, this balancing should include the nature of the civil disturbance. States with lower internet connectivity will inevitably have a diminished capacity to address highly technical disturbances such as cyber attacks.

---

[92] S Baker, S Waterman and G Ivanov, 'In the Crossfire: Critical Infrastructure in the Age of Cyber War' Centre For Strategic and International Studies (CSIS) and McAfee Inc. 2010.China, the US, Australia and the UK have the best record of maintaining secure computer networks at 20
[93] Ibid
[94] At [77]
[95] Salacuse, above note 1 at 132. This phrase is itself a quote from AV Freeman, 'Responsibility of States for Unlawful Acts of their Armed Forces' (1856) 88 Receuil des Courts 261
[96] at 135

This flexibility and the risk it engenders to investors reflect the strategic advantage offered by Developing States. Poor infrastructure and weak governance may be the very reason a foreign state can offer low production costs that are attractive to foreign investors. Lower costs to investors may be offset in higher premiums for Political Risk Insurance ('PRI'), however the World Bank's Multilateral Investment Guarantee Agency's ('MIGA') Guidelines do not mention host state internet connectivity or the existence of cyber laws when establishing insurance premium levels for PRI applicants,[97] suggesting that risk of cyber attacks against investors has not yet penetrated into the policy logic of development agencies. It should be mentioned that some Developing States have shown a greater willingness to combat cyber crimes than others[98] and that improvements in this regard are not only an issue of technological expertise but also involve social and cultural dimensions, including the need for greater internet connectivity as well as the inclusion of local content.[99]

VII Conclusion

It appears that construing an obligation on the part of host states to protect foreign investors' digital assets through an application of the FPS standard in a BIT will be difficult. While governments may have some responsibility to maintain the integrity of underlying internet architecture within their territory, it is doubtful that this could

[97] MIGA provides PRI to eligible foreign investors operating in Developing States. It is noteworthy that while MIGA does provide insurance against war and civil disturbances, it only covers losses sustained to 'tangible' assets or if there is a 'total business interruption', which may be the case if an essential computer network malfunctions. <http://www.miga.org/documents/IGGenglish.pdf> (last accessed August 2010)

[98] For example, fearing espionage as well as conventional terrorism, the Indian Department of Telecommunications required that telecommunication carriers must have their equipment certified by an approved international audit agency in case there is embedded technology that can intercept sensitive communications: D Tripathy, 'India Restricts Telecom Suppliers, Carriers' The National Post (Canada) 29 July 2010. Peru is cited as another example of a Developing Country that is taking a very proactive role in internet security: Shalhoub and Al Qasimi, above note 82 at 227.

[99] Shalhoub and Al Qasimi, ibid at 216-217

be extended to security for particular servers or to websites which are maintained by private service providers and or the investors themselves, and emergency exceptions could negate state liability for large scale attacks. A state's obligation to prosecute cyber criminals is more likely, however laws of this nature are far from universal and consequently it might be difficult to fit this obligation within the contextual nature of the FPS standard that has emerged in international investment law and any compensation for such failures would be difficult to establish. Even were the FPS standard be held to offer protection for digital investments against cyber attacks, recent tribunal decisions have implied that FPS obligations will be linked to the level of development of the host state and the nature of the threat which occurs. As few Developing States have advanced level of internet connectivity, foreign investors should not expect a high level of cyber security within these states.

Clearly the nature and scope of an FPS clause will depend on its precise wording in the treaty instrument in which it appears. A specific reference to websites and computer systems in the definition of covered investments in the BIT would assist a tribunal in finding that a host state had breached its FPS obligations when such assets are stolen or damaged due to an organized cyber attack. Even more advisable for home states of foreign investors would be to include an explicit reference to protections against 'cyber crimes' or 'attacks on data systems' as types of civil disturbances. Given the increasing regularity of computer based attacks against governments and companies, phrasing of this nature should feature more prominently in future BITs concluded with states in the Developing world, or else investors will find themselves without legal recourse and host states without investors willing to bear these significant risks. Ultimately establishing state liability in this manner should be viewed as a positive force in the technological advancement of Developing

States that currently have low levels of internet connectivity and commensurately low levels of internet security.