

The Boğaziçi Law Review

ISSN: 3023-4611

Journal homepage: <https://dergipark.org.tr/tr/pub/blr>

The Need to Apply FPS Standard to Cyber Security: Digital Assets *Siber Güvenlikte Tam Koruma Ve Güvenlik (FPS) Standardını Uygulama Gerekliliği: Dijital Varlıklar*

Onyema Awa Onyeani

To cite this article: Onyema Awa Onyeani, ‘The Need to Apply FPS Standard to Cyber Security: Digital Assets’ (2023) 1(1) The Boğaziçi Law Review 15.

Submission Date: 27 May 2023

Acceptance Date: 6 August 2023

Article Type: Research Article



© 2023 Onyema Awa Onyeani. Published with license by Boğaziçi University Publishing



Published online: October 2023




Submit your article to this journal [↗](https://dergipark.org.tr/tr/pub/blr)

Full Terms & Conditions of access and use can be found at
<https://dergipark.org.tr/tr/pub/blr>

THE NEED TO APPLY FPS STANDARD TO CYBER SECURITY: DIGITAL ASSETS

SİBER GÜVENLİKTE TAM KORUMA VE GÜVENLİK (FPS) STANDARDINI UYGULAMA GEREKLİLİĞİ: DİJİTAL VARLIKLAR

Onyema Awa Onyeani 

Dr., Brunel University London, Faculty of Law

ABSTRACT

This article will discuss a general overview of cyber security and cyber threats but will focus more on the digital aspect of cyber-attacks in the form of websites and computers than other areas of cyber security protection. But before going into detail about the possibility of including cyber security to BITs, it would be appropriate at this juncture to firstly elucidate on the issues relating to cyber threats that may be initiated from foreign countries to other States, by addressing the issues relating to State sovereignty, jurisdiction, and control over cyber infrastructure, and in addition to those issues that deals with the application of typical public international laws of State Responsibility to cyber operations. This may be relevant as some cyber-attacks are known to have their links from abroad. This article will be rounded up by analysing the employability of BITs and trade agreements to promote global cyber security via the lens of polycentrism of governance.

Keywords: cyber security, cyber-attack, BIT, foreign investment.

ÖZET

Bu makale siber güvenlik ve siber tehditlere genel bir bakışı tartışacaktır ancak diğer siber güvenlik koruma alanlarından daha çok internet sitesi ve bilgisayar formunda siber saldırıların dijital boyutlarına odaklanacaktır. Fakat siber güvenliğin BIT'lere dahil edilmesi ihtimalinin detaylarına inmeden önce, bu bağlamda devlet egemenliği, yargı yetkisi ve siber altyapı üzerinde kontrol ve siber faaliyetlerden devletin tipik uluslararası hukuk sorumluluğu ile ilgili bu meselelere ek olarak ilk olarak yabancı ülkelerden gelen siber tehditleri ele almak uygun olacaktır. Bazı siber saldırılar yurt dışı kaynaklı olmaları ile bilindiğinden bu husus önemlidir. Bu makale, çok merkezli yönetim merceğinden küresel siber güvenliği arttırmak için BIT'lerin ve ticaret anlaşmalarının kullanılabilirliğinin analizleri ile oluşturulacaktır.

Anahtar kelimeler: siber güvenlik, siber saldırı, BIT, yabancı yatırım.

1. INTRODUCTION

Cyber-attacks have been a problem that investors could suffer adverse effects to their investments. The principle of Full Protection and Security (FPS) that should be accorded investment protection is in the area of digital assets. The standard of full protection and security concerns a practice of physical and legal protection for foreign investments security, which a foreign investor may suffer against its investment and which can arise via war, civil strife or contraventions of the right of the investor by legislations and directives in the host country. FPS is common among many BITs concluded to draw foreign direct invest-

ment (FDI) and to provide protection to multinational investors.¹ To some people, the FPS principle in the past was originally used to provide protection for physical protection to shield investor's tangible assets, times have now changed, therefore the interpretation of the standards need to be adjusted so as to go along with the nature of threats that investors have to deal with in the 21st Century, specifically, the digital investments solidarity like computer systems and websites from harms imposed by, or directed at the internet, otherwise generally known as cyber security. Cyber-attacks or cyber-crime, even theft of trade secrets and corporate espionage by internet hackers are not immune from this threat. In order to combat and prevent the adverse effects caused to investors' digital assets by these attackers this article argues for an extension of FPS State's obligation that is stretched to cover cyber security generally, and the argument will be supported by the tribunal's statements while interpreting Article 1105 of the NAFTA, in *ADF v United States* which states as follows:

"that the traditional international law that was made reference to under Article 1105 (1) is not fixed for a particular period of time and that the minimum level of treatment can change... what traditional international law forecast cannot be an unchangeable picture of the minimum level of treatment of foreigners just as it was in 1927 during the ruling of the Neer Award.² For both traditional international law and foreigners' minimum level of treatment that it inserted, are steadily under a mechanism of evolution."³

Cyber-attacks represent a gigantic, progressing and disputable class of occurrences. Truly, today there are vast numbers of "cyber weapons" in progress globally without any candid dialogue concerning the conditions in which it may be applied.⁴ The menace of cyber conflict is not only the singular element of cyber harms; cyber threats, cyber-attacks, cyber offences and espionage are increasing and constitute great difficulties to corporations (investments) and States uniformly.⁵ This necessitates international law/s formulation of cyber peace so as to help in monitoring the broad diversity of cyber threats, encompassing trade secrets theft, cyber offences, and other espionage. Employing international investment law by the use of BITs indicates one factor of this development.

The accurate magnitude of digital crime is not known, but it has been estimated that the losses sustained from such attacks amounted to about \$1 trillion just for 2010, com-

¹ Jeswald Salacuse, *The Law of Investment Treaties*, (OUP 2010) para 210; R. Dolzer and C. Schreuer, *Principles of International Investment Law* (OUP 2008) para 149; M. Sornarajah, *The International Law on Foreign Investment* (OUP 2010) para 359.

² *LFH Neer and Pauline Neer v United Mexican States*, [1926] US-Mexican General Claims Commission, Decision, 4 UNRIAA 60; *ADF Group Inc v US* ICSID Case No. ARB(AF)/00/1 (NAFTA), Award, 9 January 2003, para 179.

³ *ADF Group Inc v US* (n 2) para 179.

⁴ See Thomas Rid, *Cyber War Will Not Take Place* (OUP 2013) paras. 37-38; Paolo Passeri, 'What is a Cyber Weapon?' (Hackmsgedon, 22 April 2012), <<http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit>> accessed 12 April 2023.

⁵ See e.g., Jonathan B. Wolf, "War games Meets the Internet: Chasing 21 Century Cybercriminals with Old Laws and Little Money" (2000) AM. J. CRIM. L. 95, 96; Debra Wong Yang and Brian M. Hoffstadt, "Countering the Cyber-Crime Threat" (2006) AM. CRIM. L. REV 201, 201-02; BBC, 'Cybercrime Threat on the Rise, Says PwC Report', *BBC News* (26 March 2012) <<http://www.bbc.co.uk/news/business-17511322>> accessed 12 April 2023.

elling Sheldon Whitehouse, a US senator, to insinuate that “the US and the entire world are experiencing what is possibly the greatest transfer of resources through theft and piracy in the entire evolution of humanity”.⁶ Furthermore, some countries are involving in cyber surveillance otherwise known as espionage, encompassing trade secrets theft,⁷ causing the contemplation of new approaches to combat cyber-crime. One such master plans of enhancing protection against cyber-crime is by using international investment and trade law and especially BITs as a mechanism to reduce cyber threats and better secure and safeguard trade secrets, that by estimation accordingly, “contained a means of two-third of the worth of corporations’ data portfolios.”⁸ It is as a result of the fact that cyber-attacks have multiplied in vast number, sophistication and worldliness, and extremity in the past years that have led some countries to announce proposals to begin brokering a deal for an extensive bilateral investment treaty which will comprise the problematic issue of combating bilateral cyber offence.⁹ Indeed, the application of cyber security to BITs, especially under the provision of full protection and security standard could be instrumental in passing laws of cyber-attack protection akin to that of the armed war threshold, encompassing the law of neutrality.¹⁰

To apply the standard of FPS in this manner would be difficult since it is not a host State that has control over a digital network in their territory of jurisdiction. Moreover, it will be difficult for a host State to fulfil its obligation in a BIT because the security guarantee might be more than its economic volume, particularly in respect to developing nations, where cyber harms are presumed to be rampant.

In this study, it will be looked beyond the full protection and security standard that was customarily held to oversee the material and physical protection of tangible assets of foreign investors to the need of modifying the standard as to fit the sophisticated kind of cyber security threats that are being faced globally by investments and their owners in this 21st Century, especially the structural stability of digital ventures such as investments that involve a system of interconnected computers and websites against attacks that wage war either through or against the internet. To apply the full protection and security standard

⁶ Sheldon Whitehouse, ‘U.S. Sen., Sheldon Speaks in Senate on Cyber Threats, (White House.senate, 27 July 2010) <<http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats>> accessed 12 April 2023; see also Peter Mass and Megha Rajagopalan, ‘Does Cybercrime Really Cost \$1 Trillion?, (Propublica, 1 August 2012) <<http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion>> accessed 12 July 2023. (critiquing various estimates of cybercrimes-base losses).

⁷ See Clay Wilson, ‘Cyber Crime’, in Franklin D. Kramer et al (eds), *Cyberpower and National Security* (NDU 2009) 415, 424-26; Ramona R. Rantala, ‘Bureau of Justice Statistics, U.S. Dep’t of Justice NO. NCJ 221943, *Cybercrime against Business*, 2005 1, 3 (2008) available at: <<http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf>>

⁸ Kurt Calia, John Veraneau and David Fagan et al, ‘Economic Espionage and Trade Secret Theft: An Overview of the Legal Landscape and Policy Responses’ [2013] Covington & Burling LLP 3. <<https://bpb-us-e2.wpmucdn.com/wordpress.auburn.edu/dist/8/7/files/2021/01/economic-espionage-and-trade-secret-theft.pdf>> accessed 12 April 2023.

⁹ See Annie Lowrey, ‘U.S. and China to Discuss Investment Treaty, but Cyber Security Is a Concern’ *New York Times* (12 July 2013) <<https://www.nytimes.com/2013/07/12/world/asia/us-and-china-to-discuss-investment-treaty-but-cybersecurity-is-a-concern.html>> accessed 15 April 2023.

¹⁰ See Scott J. Shackelford, “From Nuclear War to Net War: Analogizing Cyber Attacks in International Law” [2009] *BERKELEY J. INT’L L.* 192, 231. (Proposing international law implementation atop and beneath the armed conflict standard; above the standard is the stage that the regulation of war is triggered).

in this way might be challenging due to the sort of control that States keep in monitoring digital assets specifically, and supervising cyber security generally, and coupled with the dearth of uniformity of international law in this milieu. The study elucidates on the cyber threats that have engulfed and proliferated in number and severity in the world today by considering some of these so-called cyber-attacks that have taken place in recent times. Also, the study will also look at the rules and commentary from Tallinn Manual on International law applicable to cyber warfare by groups of experts that have interpreted the applicable standards in the cyber environment in the following characteristics: sovereignty; jurisdiction; States control of cyber facilities; and countries legal responsibility in relation to cyber threats. It explores the applicability of BITs, and the topographical and multilateral agreements to reduce cyber-attacks. The study will be rounded up by analysing the employability of BITs and trade agreements to promote global cyber security via the lens of polycentrism of governance.

2. STATES AND COMPUTER NETWORK

There are sets of rules of a traditional international legal existence describing the linkage between countries, computer network infrastructure, and computer network activities. Phraseology is absolutely necessary in order to get a correct comprehension of this section of this article. ‘Computer network infrastructure’ represents the transmissions, storing, and computing facilities by which data mechanisms function (glossary).¹¹ To a degree countries can apply supervision concerning cyber infrastructure. They support some rights and duties as an affair under international law. The phrase ‘cyber operation’ describes the application of cyber capacities with the main aim of reaching objectives by the application of cyberspace (glossary).¹² In international law, countries could be accountable for cyber-attacks (if it causes any adverse effects) which the country or their entities transmit, or in other words as regarded as being caused by the States by the strength of the law on State responsibility. Conducts of third party actors might as well be ascribed to countries. This section will be determined by rules and report from Tallinn Manual under the international law employable to cyber warfare as outlined in principles ruling of such issues and describing how the Groups of Experts defined applicable concepts in the cyber atmosphere, and indicates any differences within the group as to each rule’s accomplishment.

2.1. TALLINN MANUAL RULE 1: SOVEREIGNTY

Under Rule 1 of Tallinn Manual rule, a country could apply control on the subject of cyber infrastructure and operations in its sovereign jurisdiction. This rule highlights the reality that despite the fact that no country may allege autonomous concerning cyberspace *per se*, countries could exercise independence rights regarding any cyber infrastructure situated on their region, including activities that are linked to that cyber facility.

The recognised interpretation of ‘sovereignty’ has been outlined in the arbitral award

¹¹ See in the glossary in Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013) 257-262.

¹² *ibid.*

of 1928 in *Island of Palmas*,¹³ where it was stipulated that ‘Sovereignty in the connections between countries indicates independence. Independence with reference to a part of the sphere is the prerogatives to employ in that respect, to the exception of every other country, the tasks of a country.’¹⁴ It is as a result of the independence that a country benefit concerning jurisdiction that grants it the prerogative to monitor cyber infrastructure and cyber operations in the borders of its jurisdiction. Consequently, cyber infrastructure sited in the State’s territorial land, national rivers, territorial ocean waters, island waters, or State air space is affected by the independence of the regional country.¹⁵ Sovereignty signifies that a country could control access to its region and universally possesses and benefits, inside the restriction outlined by agreement and traditional international law, the full prerogative to use power and control on its region. A country’s sovereignty concerning cyber infrastructure in its region has two repercussions. Firstly, cyber infrastructure is likely to be affected by legal and supervisory monitoring by the country.¹⁶ Secondly, the country’s regional sovereignty safeguards cyber infrastructure, regardless of if it is owned by the State or individual bodies or private third parties. In the cases of cyber-attacks initiated from abroad to another country, for example, China, United States, or Russia, some of these cyber-attacks reportedly originated from servers network situated in these countries. A cyber activity by a country launched against cyber infrastructure situated in another country may breach that country’s sovereignty which it was directed against. It surely does if there are damages done as a consequence of the launch. The International Group of Experts of the Tallinn Manual who came out with these rules could not reach to any agreement concerning whether the installation of malware which is specifically designed to disrupt or damage a computer system which does not cause physical damage (as with malware used to control operations) amounts to a breach of sovereignty or independence. If that sort of cyber activities are aimed to pressurise the State and are not in other respects allowed within international law, the activity may amount to a forbidden ‘intervention’.¹⁷ With this reasoning in mind on sovereignty over control of infrastructure on its region, one would argue that any cyber-attack which emanates either from outside or within a sovereign State which causes devastating damage to investment may be attributable to that State for their failure to have prevented the damage from happening.

However, the rules on sovereignty permits a country to, amongst other things, limit or protect either partially or in wholly the access to the internet work, without being bias to

¹³ *Island of Palmas (Netherlands v US)* [1928] RIAA Vol. II 829, 838.

¹⁴ *ibid.*

¹⁵ On independence concerning seas and aerospace above seas, see United Nations Convention on the Law of the Sea, Art. 2; on independence concerning over aerospace, see Convention on International Civil Aviation (also known as Chicago Convention), Arts. 1-3. Concerning cyber facilities within outer space, see Rules 3 and 4 and following report in Michael N Schmitt (n 11) 21-23.

¹⁶ In the 1949 Corfu Channel case, Judge Alejandro Alvarez added a different view where he stipulated: ‘By sovereignty, we infer all the areas of prerogatives and qualities that a country has in its region, to the exception of every other country, and as well in its connections with other country. Sovereignty accords prerogatives on countries and enforces duties upon states’ *Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*, [1949], I.C.J. Rep, 4, 43 (Individual opinion by Judge Alvarez).

¹⁷ UN Charter, Art. 2(1).

relevant international law, like human rights or other international communication law.¹⁸ Even if cyber infrastructure situated in a particular country's region is associated with the international communications network, still it cannot be read as an abandonment of such sovereignty prerogatives concerning that infrastructure. In spite of the fact that countries may not be able to exercise sovereignty on cyberspace *per se*, countries could use their region in relation to computer network offences and some other operations of a computer network nature in conformity with the concepts of jurisdiction acknowledged under international law (Rule 2).¹⁹

Customarily, the concept of the contravention of sovereignty was restricted to activities being handled by, or ascribable to States. Nevertheless, there are some underdeveloped opinions presented by some academics that computer network attacks conducted by non-State participants will also breach a country's sovereignty, especially in part of its territorial unit. This will be addressed later in this article below.

2.2. TALLINN MANUAL RULE 2: JURISDICTION

Rule 2 of the Tallinn Manual stipulates that, 'without being bias to relevant international duties, that a country may use its jurisdiction and control: (a) over individual involved in cyber operations on its territorial region; (b) over cyber infrastructure situated on its territorial zone; and (c) extraterritorially, according to international law'.²⁰

The phrase 'jurisdiction' includes the power to stipulate, implement, and judge. It expands to all issues, encompassing the ones that are non-criminal (civil matters), criminal matters and managerial in human kindness and existence. The main reason for a country to use its jurisdiction is bodily or lawful presence of an individual (*in personam*) or thing like object (*in rem*) on its territorial domain. For example, in accordance with the State's *in personam* jurisdiction a country can endorse legislations and statutes controlling the cyber operations of persons on its region. It can as well control the actions of individually owned' companies incorporated within its jurisdiction but bodily functioning overseas, like internet service providers (ISP). Concerning the *In rem* jurisdiction, it would permit it to accept legislations controlling the activities of cyber infrastructure on its country.

It may be challenging to ascertain jurisdiction inside the cyberspace since cloud or internet network distributed mechanisms could cross State boundaries, as may the replication (the action of copying or reproducing data) including the constant movement of data processing. This causes it difficult at any point in time to establish where the whole of the user's information and operating data programme are situated because such information may have been resided in various parts of the jurisdictions concurrently. These technological complexities do not prevent a country of its legitimate prerogative to use jurisdiction concerning individuals and cyber infrastructure situated on its borders. In respect of jurisdiction depended on territoriality, it should be observed that while persons using data and transmitting

¹⁸ E.g., 1992 International Telecommunication Union Constitution.

¹⁹ See e.g., Council of Europe, Convention on Cybercrime, 23 November 2001, Eur. T.S. No. 185. <<https://rm.coe.int/1680081561>> accessed 20 May 2023.

²⁰ See Rule 2 in Michael N Schmitt (n 11) 18.

scientific knowledge have a particular physical site, the site of mobile appliances can move or switch off at computing activities. For example, an individual using some mobile computing gadgets like tablets and smart phones can open various database challenges or upgrades for processing by a digital data storage service. As those challenges and upgrades occur, the operator of the phone may switch to another site. Any country where the person has operated the phone from benefits jurisdiction since the person, and the associated gadgets, were situated on its jurisdiction when they were used.

Surprisingly, with scientific knowledge like mobile digital data storing computer services, the gadgets from which the user is opening an instruction to provide information or perform another function may be geo-located; and software services and computer database applications could follow the geographical coordinates of the computer gadgets, such as Wi-Fi connection position or the gadget's global positioning system (GPS). Therefore, it is likely under particular conditions for somebody that does not want to be traced to spoof- (interfere with radar or signals so as to make them useless) the geographical-coordinates publicised by that person's computing mechanism. It is as well likely that the user-location could potentially not be made accessible by the infrastructure or those that provide the service, or by the computer programming, or even by the gadget itself. Real physical existence is needed and is adequate for jurisdiction based on territoriality; spoofed (interfere with radar or signals so as to make them useless) existence is not enough.

The territorial jurisdiction has resulted to the development of two unoriginal or imitative kinds of jurisdiction, namely: subjective territorial jurisdiction and objective territorial jurisdiction.²¹ The first one includes the use of the legislation of the country applying jurisdiction to a particular occurrence which is generated inside its region but accomplished in some other place (or State). It relates even if the criminal cyber-attacks or operation have not impacted negatively in the country exercising this jurisdiction. Otherwise, objective territorial jurisdiction provides jurisdiction on persons to the country where the specific occurrence has impacted negatively despite the fact that the activity started outside the jurisdiction.²² Objective regional jurisdiction is of specific importance to cyber activities. For instance, Estonia in 2007 was attacked by cyber-attacks that were launched from overseas. As for those conducts which contravened Estonian legislation, the State of Estonia would at least have been qualified to use jurisdiction on the persons, wherever situated, who launched the attacks. Especially, Estonian jurisdiction would possibly have been vindicated since the activities had considerable negative impacts on Estonian region, like intrusion

²¹ The ECJ Attorney General has expressed the notion as following: Territoriality ... has produced two different rules of jurisdiction: (i) *subjective* Territoriality, that allows a country to confront conducts emanated from inside its region, although these may have been completed overseas, (ii) *objective* territoriality, that, contrarily, allows a country to confront actions that emanated from overseas but were completed, to an extent partially, inside its own region ... [from the rules of objective territorialism] is obtained the effects notion, that, for the purpose of confronting the impacts at issue offers jurisdiction on a country despite the possibility that the act which generated them was not taken place within its region.' Opinion of Mr Advocate General Darmon, Joined Cases 89, 104, 114, 116, 117, and 125-9; *Osakeyhtiö and Others v Commission [in re Wood Pulp Cartel]* paras 20-1. 1994 E.C.R. I-100.

²² Whereas the effects idea has extended to a general standard of approval, its use in many circumstances has resulted to dispute. American Law Institute Third Restatement of Foreign Relations Law Section 402(1) (C) (1987).

in the system of its banks and State tasks. At the same vein, non-combatant implicated in cyber activities against Georgia during that country's international arms confrontation in 2008 with Russian government could have been under the control of Georgian jurisdiction due to consequential intrusion on websites and disturbance of cyber transmission in breach of State of Georgian law.²³ The State of Estonia should have used jurisdiction to bring the perpetrators of these acts to book, especially if there had been a uniformity of international law that safeguards actors from cyber-attacks.

Other acknowledged grounds concerning this extraterritorial jurisdiction, despite some limitations, encompass: (i) country of the wrongdoers; (ii) country of the individuals harmed by the operation; (iii) danger to national security of the country; and (iv) contravention of a general concept in international law, like commission of war crime. For instance, any important cyber intrusion with a country's military protective framework such as an air defence and early warning radars) amounts to a danger to State security and as a result is included in the defensive concept.

Considering the variation of jurisdictional positions under international law, two countries, even more can frequently benefit from jurisdiction on the same individual or thing in regards to the same occurrence. An example of this would be an insurgent organisation that stages a computer network attack or activities from the region of country A fashioned to inflict physical harm to country B's power generation facilities. The insurgents used a cyber-arsenal against the factory's control mechanisms, causing a detonation that caused harms to personnel. Inmates of the prison are from several different countries. Country A may assert jurisdiction on the premises that the activity happened there. Country B could as well assert jurisdiction based on the footing of the nationality of the victim known as passive personality and objective regional jurisdiction. Some countries possess jurisdiction on the basis of an attacker's citizenship. Considering these circumstances one would argue that it is not easy for a sovereign State to exonerate itself from cyber-attacks based on jurisdiction, especially where such cyber-attacks are launched from inside its borders.

The term 'without bias to relevant international duties' is incorporated to acknowledge that, in some situations, international law might successfully restrict the use of jurisdiction upon some individuals or things of objects on a Country's region. Instances encompass exemption (e.g., military and consular exemption) and the provision of main jurisdiction to one country out of two countries benefitting simultaneously jurisdiction about an individual or specific crime, for example by the employment of a Status of Forces Agreement).

2.3. TALLINN MANUAL RULE 5: STATE CONTROL OF COMPUTER NETWORK INFRASTRUCTURE

Rule 5 of Tallinn Manual on the international law applicable to cyber warfare that is initiated from abroad stipulates that 'a country must not wilfully permit the computer network infrastructure situated in its region or directly within its complete and individual State supervision to be used for conducts which unfavourably and illegally upset or damage

²³ Non-combatants do not have the right for combatant exemption within the armed conflict law and consequently are completely vulnerable to the customary foundation of jurisdiction confronted here.

another country'.²⁴ If a country is not deliberately allowing that computer network infrastructure situated in its region to be exercised against other countries disadvantageously and illicitly, that would mean that, a State should not also intentionally permit such cyber infrastructure within its State control be used against alien investments within the region of its own country in the case of international investment law.

This principle creates a guideline of conduct for countries in the context of two classes of computer network infrastructure: (i) any computer network infrastructure be it State agency in essence or not, situated on their border; and (ii) computer network infrastructure sited in some other places but upon which the country at issue has either *de jure* (entitlement or claim by legal right) or *de facto* (whether by legal right or not) total and individual control. It is applicable to each other notwithstanding of the ascription of the conducts at issue to a country.²⁵ The duty of State equality demands an obligation of every country to accord due deference for the territorial independence of another country. In *Nicaragua v United States*²⁶, it was ruled by the ICJ that, 'amongst autonomous countries, deference for territorial sovereignty is a crucial basis of global relationships.'²⁷ The duty for deference to the independence of other countries, as observed in the ICJ case of *Corfu Channel*,²⁸ indicates that a country should not 'permit wilfully its jurisdiction to be taken as a location for activities against the rights of another country'.²⁹ Therefore, countries are necessitated to employ reasonable measures to shield those rights within international law.³⁰ This could be regarded as the same reasonable steps of measures of due diligence that a country is mandated to maintain in safeguarding the investments of foreign investors in its territory under FPS clauses in BITs in international investment law. These duties do not just cover unlawful conducts that are damaging to another country, but as well, for instance, actions that impose severe harm, or conducts that have the possibility to cause such harm, on individuals (investors) and objects (investments) protected by the regional sovereignty of the focus country,³¹ such as the ones posed by international computer network threats that have allegedly originated from China, Russia and United States to other countries. Therefore, if it is true that there have been serious computer network attacks against a vast number of corporations in foreign countries from network servers situated in China and the US as has been alleged, that would mean that China, Russia and United States have failed to accord due respect for the regional independence of those countries it launched such computer network attacks against.

²⁴ See, Rule 5 in Michael N Schmitt (n 11) 26.

²⁵ *ibid* Rules 6 & 8.

²⁶ *Military and Paramilitary activities against Nicaragua, (Nicaragua v United States of America)* [1986] I. C. J. Rep. 14.

²⁷ *ibid* para 202.

²⁸ *Corfu Channel Case*, (n 16).

²⁹ *ibid* para 22.

³⁰ *Case Concerning United States Diplomatic and Consular Staff in Tehran (US v Iran)* [1980] I.C.J Rep. 3 paras 67-68.

³¹ See, *Trail Smelter Case*, the Adjudicators, quoting the Switzerland's Federal Court, observed that, 'The prerogative of sovereignty comprises ... not just the seizure and application of sovereign prerogatives ... but as well a real intrusion that could bias the real utilisation of the region and the liberty of movement of their citizens.' *Trail Smelter Case (US v Canada)* [1941] RIAA Vol. III 1905, 2963.

However, these necessities are complex by the existing kind of damaging computer network activities, particularly time and room compression of data, and their frequently uncommon nature. There could be situations to which it cannot be possible for a country to thwart damage to another country. For instance, country A might be aware that a damaging computer network operation is being made ready and is going to be activated from its region against country B. But, since it has not known the striker's accurate identity and schedule time, the only successful choice might be to separate the computer connection that will be employed in the strike from that particular internet. By doing so, it will frequently result in the country A denying that it provided the service for the attack against country B. The kind, level and ambit of the possible damage to both countries must be evaluated to consider whether this corrective step is necessitated. The yardstick in such conditions is one of reasonableness. The same thing will be applicable to where an infrastructure sited within a country's territory or under its complete governmental control is to be used for activities that unfavourably and illegally affect investors and investments within the host country under the obligation of FPS of BIT in international investment law.

As to the ambit of implementation, this Rule relates to all the activities that are illegitimate and which have harmful impacts on another country, notwithstanding if those damaging that it impacts happened on another country's region or occurred on objects that are protected in international law. The phrase unlawful has been applied within this Rule to indicate a conduct which is against the lawful prerogatives of the negatively impacted country. The International Experts of this Tallinn Manual intentionally decided not to restrict the prohibition of this rule to narrower notions, like the using of force in Rule 11³² or armed attack in rule 13,³³ as to highlight that the disallowance expands to every computer network operation from one country's region that impact the prerogatives of another country and have negative damage on another country's region. Especially, there can be no necessity that the computer network activity at issue ends in physical harm to objects or damages to persons; it requires only causation of adverse impact.

The Rule deals with circumstances to which the applicable operations are in progress. For example, a country that permits computer network infrastructure on its borders to be engaged by an insurgence organisation to launch a cyber-attack against other countries would invariably be in contravention of this Principle, as also would a country that is warned by another country that a computer network is being prepared and omits to take adequate possible steps to prevent the action. This approach is in consonance with or would be likened to *Bernhard v Zimbabwe*³⁴ and *MNSS v Montenegro*³⁵ cases on FPS obligation in international investment law, where the two states' authorities in the respective cases were forewarned about imminent attacks against the respective investors and yet they did nothing to prevent those attacks from happening.

The Experts of this Manual could not reach consensus on whether circumstances to which

³² See, Rule 11 in Michael N Schmitt (n 11) 45.

³³ *ibid* Rule 13.

³⁴ *Bernhard von Pezold and others v Republic of Zimbabwe* [2015] ICSID Case No. ARB/10/15 para 597.

³⁵ *MNSS B.V. and Recupero Credito Acciaio N.V. v Montenegro* [2016] ICSID Case No. ARB (AF) 12/8 para 356

the applicable actions are merely possibly are included in this Rule. A large number of these experts of this Rule took the stance that countries should employ necessary steps to avert them. Few others insinuate that no obligation of thwart exists, especially not in relation to internet crime, considering the challenges of organising inclusive and successful protections against all feasible attacks. The Rule as well is used in relation to activities against international law initiated from internet infrastructure that is in the complete supervision of a State. It makes mention to circumstances where the infrastructure is situated externally out of the individual country's region, but that country, nonetheless, apply complete control upon it. Such instances encompass a military infrastructure in an alien country subject to entirely transmitting country control in accordance with a basing (more than one) agreement, State podiums on top of the high oceans or in global aerospace, or consular establishments.

This Rule is used if the applicable corrective computer network activities can be tackled by country corpuses or by persons under country control. Experts of this Manual as well reached consensus that where a corrective step could only be executed by a personal organisation, like individual Internet service supplier, the country would be mandated to employ every avenue within its reach to mandate that organisation to apply the steps reasonable to bring to an end such activity. This Rule is used if a country is truly aware of the conducts at issue. A country will be assumed of having real awareness if, for instance, country corpuses, like its intelligence bodies have discovered a computer network threats being masterminded or launched from its region, or where the country has obtained reliable information tip-off that a computer network operational attack is imminent from within its borders.

The international Experts on this Rule could not reach agreement if this Rule can be used as well if the individual country has just constructive ('should have known') awareness.³⁶ To put it differently, it is not explicit if a country breaches this Rule when it omits to apply duty of due diligence in monitoring computer network operations within its region accordingly being ignorant of the conducts at issue. Even if constructive awareness is adequate, the standard of duty of due diligence and care is unknown in the computer network surroundings because of elements like problem of causation, the difficulties of connecting different collections of occurrences as a portion or a division of an interrelated and disseminated attack on a particular or more victims or directions, and the simplicity with which fraud can be organised through computer network infrastructure.

Again, the Experts could not reach agreement if this Rule is as well applicable to countries through which computer network activities are dispatched. Many of the Experts on this Rule took the stand that to the degree that a country of transit is aware of a wrongful activity and also have the capability to prevent it, the country must act accordingly so. They also acknowledged, accordingly, of the uniqueness of dispatching mechanisms of computer network communications. For example, should a communication be obstructed at one junction of internet connection, it will generally be re-sent through a separate communication route, frequently via another country. In that kind of situation, these Experts accepted that the country of passage has no duty to carry out any action, since by doing so can hardly have any significant impact on the result of the activities.

³⁶ Rule 11 in Michael N Schmitt (n 11) 45.

Other Experts position themselves differently stating that the Tallinn Rule is only applicable to the region of the country from where the activity originated or the region under its total control and monitor. They either asserted that the lawful rule did not expand to other region in *abstracto* (ordinary negligence arising from the failure to exercise the very degree of care that every prudent person would exercise under all circumstances) or defend their viewpoint on the ground of the individual challenges of employing the Rule in the computer surroundings. The International Group of Experts' disagreement on certain issues on internet attacks one would argue must have come as a result of a gap in the general cyber international law protection. To put it differently, it is as a result of failure to have one uniform international law that protects against computer network offences, and this loophole makes way for the inclusion of cyber security protection on FPS clauses of BITs under international investment law.

2.4. TALLINN MANUAL RULE 6: COUNTRIES LEGAL RESPONSIBILITY ON COMPUTER NETWORK THREATS

Under Rule 6 of the Tallinn Manual, 'a country carries legal responsibility internationally for a computer network activity imputable to that country and which amounts to a contravention of international duty'.³⁷ This Rule basically is on the premises of traditional international law of State responsibility, which is widely shown on the Articles on State Responsibility by the International Law Commission. The typical rule under international law prescribes that country shoulder responsibility for a conduct when: (i) the conduct at issue is ascribable to the country in international law; also (ii) it amounts to a contravention of international legitimate duty relevant to that country either by any treaty or by tradition international law.³⁸ This sort of contravention can comprise of commission or inaction.³⁹ In the sphere of cyberspace (the notional environment in which transmission over computer networks occur) any international unlawful conduct can comprise, among other things, of a breach of the United Nations Charter, for instance, a use of force perpetrated via cyber mechanism under Rule 10, or as well, a contravention of the law concerning the arm conflict duty, for example, a computer network attack launched against non-combatants objects, Rule 37) ascribable to the country at issue.⁴⁰

State responsibility law expands only to a commission, or omission to take measures, that breaches international law. To put it differently, an action perpetrated by a country's entity, or on the other hand, ascribable to that State, can only constitute an 'international unlawful conduct' where the act is against international law.⁴¹ The law concerning State responsibility

³⁷ See, Rule 6 (1) in Michael N Schmitt (n 11) 29.

³⁸ Draft articles on responsibility of States for internationally wrongful acts, Text adopted by the International Law Commission at its fifty-third session [2001] YILC Vol II Part 2, Articles 1-2. [ARSIWA]

³⁹ *ibid* Art. 2.

⁴⁰ See, Thomas Rid (n 4) paras 37-38; Paolo Passeri (n 4).

⁴¹ This standard is a strict necessity because, as was devised by the International Court of Justice. '*It is wholly likely for a specific conduct ... not to breach international law in the absence of certainly amounting to the use of a prerogatives granted by it*'. *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* [2010] I.C.J. Rep. 403 para 56.

would not be complex if countries undertake in other conducts which are either allowed or uncontrolled under international law.⁴² International law for instance, has not confronted the issue of espionage *per se*. Therefore, any State's responsibility concerning an operation of computer network espionage committed by a corpus of the country in cyberspace can not to be connected as an issue under international law except specific areas of the cyber espionage contravenes particular international lawful disallowances, for example, where computer network surveillance is containing consular transmissions under Rule 84.⁴³

The attribution of harm cannot be a prerequisite to the classification of a cyber-activity for an international unlawful conduct on the law of State responsibility.⁴⁴ Although the principle at issue might comprises harm as a vital component. In such situations, harm can be regarded as a *conditio sin qua non* (indispensable and essential, condition or ingredient) of the extension and connection of country responsibility. Example, in a traditional principle in international law, countries are forbidden from causing crucial harm on another country through operations on its own regions (Rule 5).⁴⁵ This same principle applies to international investment law, since FPS obligation in BIT forbids States not to cause harm to foreign investors and their investments in their region as seen in many case law. And that includes in this case computer network attacks that can cause devastating damages to an investor and its investment if initiated within the region of the host State against the foreign investor. In the dearth of such harm there will be no responsibility attributes to States except another principle not including a component of harm has been contravened. Furthermore, to a State being responsible internationally, a conduct ought to be ascribable to a country in order to fall in the scope of this particular Rule. Every commission and inactions of country's entities are certainly and inevitably ascribable to that country.⁴⁶ The notion of corpuses of a country' under State liability law is wide. All individuals or organisations which have that standing in the State's domestic law must be grouped as an entity of the country in spite of their purpose or position within the governmental classification.⁴⁷ Any cyber operation handled by the armed forces, intelligence, national security, customs and exercise, or other governmental organisations will connect to State responsibility in international law particularly, if it contravenes an international legitimate responsibility that applies to that country. It is immaterial whether the entity at issue acted in accordance with, extensively, or with lack of any orders. When perpetrated by a corpus of the country, as long as that corpus is reacting in a seemingly representative position,⁴⁸ even the supposed ultra-virus conducts activate a country's international lawful responsibility provided they violate international

⁴² *ibid* para 84; *Case of the S.S. "Lotus" (France v Turkey)* [1927] P.C.I.J. Judgement Series A, No 10.

⁴³ See, Rule 84 in Michael N Schmitt (n 11) 233.

⁴⁴ Report of the International Law Commission on the Work of its Fifty-third Session, Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, [2001] YILC Vol. II Part 2, commentary of the Article 2 [ARSIWA Commentary].

⁴⁵ See, Rule 5 in Michael N Schmitt (n 11) 26.

⁴⁶ ARSIWA (n 38) Art. 4(1).

⁴⁷ *ibid* Art. 4(2).

⁴⁸ See, Articles on State Responsibility, para 13 of report following, Art. 4.

duties.⁴⁹

For the reasons concerning the law on State's responsibility, individuals or entities that are not entities of the government of a country, that are particularly permitted by its national law to use 'governmental powers' are regarded to be a State entity.⁵⁰ When functioning in that position, their commissions, as with country entities, are ascribable to that country. Instances encompass an individual company which has been accorded the power by State government to carry out hostile cyber activities against other countries or against its own citizens. Likewise, as an individual organisation authorised to participate in computer network intelligence information collection. It is vital to highlight that responsibility of State is on interconnected when the organisation at issue is applying components of governmental power. For instance, countries may have laws empowering individual department like Computer Emergency Response Teams (CERTs) to undertake computer network protection of government internet connections. During the time of the performance, their operations automatically interconnect the responsibility of their financing and equipping State. Still, there will be no connection or attraction of the responsibility of a State when an individual department CERT is executing data security works for individual corporations. In some situations, the action of private performers may be ascribable to a country and cause the country's international law responsibility.⁵¹ Article 8 on State Responsibility, stipulates again more clearly traditional international law, it observed that 'the action of an individual or a set of individuals shall be regarded as a conduct of a country by international law where the individual or a set of individuals is in reality acting to the commands of, or in the instruction of that country in executing the action'.⁵² This standard is specifically applicable in the computer network sphere. For instance, countries could have a written an undertaking with an individual corporation to handle computer network activities. In the same vein, countries have accountably requested individual nationals to launch computer network attacks against other countries or other focused areas overseas, or even within its own jurisdiction, (essentially, like cyber come forward).

The ICJ has ruled, in respect to military activities that, a country is liable for the actions of the none-State (individual or organisation that has significant political influence but not allied to any particular country or state) participants if it has 'official or operative control' on such participants.⁵³ For example, the equipment rendered by a country of computer

⁴⁹ ARSIWA (n 38) Art. 7.

⁵⁰ ARSIWA Commentary (n 44) commentary of the Article 5.

⁵¹ In the Articles 9 and 10 of the ARSIWA, the Tallinn Experts came to the reasoning that it is presently problematic to think of a setting to which Art. 9 gives rise to State Responsibility because of its necessity that the act be conducted in the absenteeism or failure of the legal authorities. They were not sure if Art. 10, that deals with the acts of a revolutionary and other organisation that turns to a regime, correctly reflects traditional international law.

⁵² ARSIWA (n 38) Art. 8. 'In respect of Art. 8, the three phrases "instruction", "direction" and "control" are lacking connection and consistency; it is enough to prove any one of the three. Simultaneously, it has been made obvious that the instructions, directions or control should link to the act that is interpreted to have constituted to internationally illegitimate act.'

⁵³ The Court articulated the effective control standard for the first time in the *Military and Paramilitary activities against Nicaragua* (n 26) para 115. See also e.g., *Genocide Judgement (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] I.C. J. Rep 43 paras 399-401.

network prowess at the time of the arrangement of a particular computer network attacks could, according to how extensive the participation goes, provokes State responsibility concerning any unlawful conducts perpetrated by those non-State participants. It is occasionally argued that unpredictability surrounds the magnitude of control necessitated for a private person or non-State participant's action to be ascribable to the country. In *Tadic* case, the tribunal for the one-time State of Yugoslavia supported the 'overall control' standard – a lower strict test, in respect of private wrongdoing responsibility for the aim of considering the nature concerning the armed dispute.⁵⁴ Nevertheless, during the *genocide* ruling, the ICJ differentiated such an assessment from that held for the intent of proving State responsibility.⁵⁵ Notwithstanding, even by looking at the 'overall control' threshold, the required control must extend to more than 'the mere funding and providing of those military and encompassing as well involvement in the organising and controlling of military activities'.⁵⁶ Additionally, even if this lesser 'overall control' criterion were to be embraced, it cannot be used for private persons or State's unrepresented groups.⁵⁷

These circumstances must be differentiated from the ones by which individual nationals, on their own action, carried out computer network activities (known as 'hacktivists' or 'patriotic hackers').⁵⁸ The material ambit to be applied to Article 8 is comparatively strict for the fact this is restricted to orders, managements or supervision. The country must have given special orders or managed or supervised a specific activity to become involved in State responsibility.⁵⁹ Solely promoting or in other respects, showing encouragement for the individualistic action of a third person or a non-State participant will not meet the test of Article 8.

The location where the action at issue was carried out, or the place where the participants that are associated with the action are situated, does not impact on the consideration of whether country responsibility is involved. Just for illustration purposes, for example, think of a bunch of people in country A that takes information from computers that are situated in country B in its botnet (a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g., to send spam). Those people operate the botnet and overwork the computer system in country C dependent on the orders given by country D. In the law of State responsibility, the action is ascribable to country D. It should be acknowledged that country A cannot be assumed liable merely on the ground that this bunch of people was based there, neither would it be assumed that country B shoulder the responsibility for this people's action just on the fact of the position of the bots (internet program on network which can interact with systems or users) in its border.

⁵⁴ *Prosecutor v Dusko Tadic a.k.a. "Dule"* [1997] International Criminal Tribunal for Former Yugoslavia, IT-94-1-T paras 131 and 145.

⁵⁵ *Genocide Judgement* (n 53) paras 403-405.

⁵⁶ *Prosecutor v Dusko Tadic* (n 54) para 145.

⁵⁷ *ibid* para 132.

⁵⁸ Michael N Schmitt (n 11) 33.

⁵⁹ ARSIWA Commentary (n 44) commentary of the Article 8.

This principle is only relevant to ascription for the determination in regards to State responsibility. Nevertheless, a country's connection with non-State participant could in itself amount to international law contravention, even in matters where the activities of the private persons who participated cannot be ascribed to the country. For example, If Country A supplied hacking apparatus which is later used by a rebel or terrorist organisation by its own plan against country B (for instance, the organisation is not operating under the supervision of country A), the sole supplying of these devices is enough to ascribe the organisation attacks to country A. However, such help can itself amount to a contravention under international law.⁶⁰

Even in a situation where Article 8 terms are originally met, actions which took effect from a date in the past may be ascribable to the country. In accordance with the Articles on State Responsibility, under Article 11, 'action that is ascribable to a country under the foregoing articles shall nonetheless be regarded an action of that country in international law where and to the degree that the country recognises and approves the action at issue as their own.'⁶¹ For example, think about computer network activities carried out by non-State participant (third party) against a country. If another country over time indicated approval for them and employs its computer network skills to defend the non-State participant against counter-computer network activities, State responsibility would be linked with those activities and any associated successive activities of the group. It is useful to acknowledge that this plan or measure is barely used. Not solely are the terms of 'acknowledgement' and 'adoption' progressive, they as well necessitate more than trivial support or implied approval.⁶²

Considering all the aforementioned, it is worth saying that any computer network attack that is initiated from a particular jurisdiction to another jurisdiction that causes adverse and unlawful effects to the other jurisdiction and its nationals undoubtedly breaches international law on State Responsibility. Also, any computer network attack that causes harm to investments that is initiated within the State might also breach the law on Articles on State Responsibility whether the action emanate from the country's entities or from the non-State participants. However, based on control elements, ascription of State responsibility to a country for computer network attacks that emanate within a country might be difficult to achieve since country do not manage computer network connectivity. To this end therefore, it seems unfeasible to attribute responsibility of cyber offences on digital investments to a host country since internet suppliers are more often left in the hands of individual corporations and its connectivity is not linked with the State government and as such the government do not have management and control over it.

Relating the issue of control and territory of digital assets to BITs, it is well known that BIT obligations are usually limited to investments that were entered in the region by

⁶⁰ *Military and Paramilitary activities against Nicaragua* (n 26) para 242.

⁶¹ ARSWIA (n 38) Art. 11.

⁶² ARSIWA Commentary (n 44) commentary of the Article 11.

the individual contracting members.⁶³ This custom comes into being since investments are supposed to strengthen the host country's economy, by either yielding capital flows or by generating new employments opportunities⁶⁴ in such a way that simply buying and selling goods and services cannot create. On this note, territoriality is undoubtedly a more complicated quality to attribute to internet website, which may merely be available by customers within the host country as a method of advertising overseas products and services. This kind of singly on-line publicity could still be adequate, if the firm can establish of its physical existence in the region, like a managerial office, or a plant, or any establishment. In that sense, the centre of the evaluation to ascertain the territoriality cannot be the area where the internet website is situated⁶⁵ but instead the site of the corporation that it was linked to. For the interest of investment treaty security and of international investment law, therefore, it is possible that the excellence assertion that an internet is inside the region of a country is when or where the website is stored through a server which is physically situated inside the host country, which would seem to support the basic comprehension of internet territoriality.⁶⁶ Accordingly, as a result of the logical contemplation of the ruling in case of *SGS v Pakistan* by the tribunal, it might help the investor's assertion of territoriality when the proof of disbursement to form the business inside the host country could be cited as evidence.⁶⁷ Therefore, a foreign investor can prove that it made payment to a domestic internet storing firm to store its website or data in a server or computer in the jurisdiction, or prove that it bought or rented resident premises to store the pertinent server. On the other hand, where the website merely was available in the territory via the internet, its link to the region would supposedly be very weak, particularly if the firm do not have physical existence in that jurisdiction. It is probably clearer and better to claim that any computer network that belongs to an organisation which is physically situated within the host country jurisdiction, like the internet keeping the operation of a mining firm, would meet the territorial prerequisite since they are clearly within the boundaries of that party country and therefore must have had territorial and jurisdictional control and links to the host State.

⁶³ See, Bilateral Investment Treaty between Canada and Peru, (Investment Policy Hub, 20 June 2006) Article 1. <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/626/download>> accessed 21 May 2023.

⁶⁴ Salacuse (n 1) para 169.

⁶⁵ See e.g., M. Susan, 'The Critical Challenge from International High-Tech and Computer Related Crime at the Millennium' [2009], *Duke Journal of International and Comparative Law* 451; Ray August, 'International Cyber-Jurisdiction: A Comparative Analysis' [2002] *American Business Law Journal* 531; D Powers, 'Cyber law: The Major Areas, Development and Information Security Aspects' in H. Bidgoli (ed), *Global Perspectives in Information Security* (John Wiley and Sons Inc. 2009). See Rule 2 above on Jurisdiction in Michael N Schmitt (n 11) 18, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (n 11) 18.

⁶⁶ *ibid.*

⁶⁷ *SGS Societe Generale de Surveillance SA v Islamic Republic of Pakistan* [2003] ICSID Case No. ARB/01/13, 13, under the Swiss-Pakistan BIT (entered into force 6 May 1996).

3. ARE DIGITAL ASSETS CLASSIFIED AS INVESTMENTS?

For aliens' digital assets like internets and websites to get protection under the FPS standard from its home country's investment agreement obligations, it should first be demonstrated whether digital assets fall within the ambit of the definition of "investment" in the applicable treaty. For it to fall under investment definition would be based to some degree on the particular terminology that the BIT at issue used, as some general rules come from treaty custom. In series of BITs, there is a common phraseology that defines investments as comprising "every asset", "all kinds of assets" or "every kind of asset,"⁶⁸ followed by catalogue of instances. This phrase is appropriate for the intentions of websites including various computer information networks where a treaty agreement makes mention of 'intangible assets including movable and intellectual property'.⁶⁹ Digital asset like websites may be classified under intellectual property provided they are created out of technical perception and frequently inventive innovation. For example, the Argentina-US BITs incorporate the extensive definition: 'inventions in all fields of human endeavor' and 'confidential business information' when defining intellectual property.⁷⁰ Also, the Ukraine-Denmark BIT stated investment to signify all kinds of assets linked to economic affairs for the intention of creating long period of time profitable connection.⁷¹ This appears to include computer networks and websites and in as much as they are linked with a profit-oriented business with a long period of plan, not just a few simple business deals.

The early BITs brokered by the US did not demand for the inclusion of any specific intellectual property rights. They solely requested that host country expand to alien investors whatever intellectual property safeguards that exist in its national laws.⁷² Nevertheless, the United States-Poland BIT created a special set of prerogatives and duties concerning intellectual property.⁷³ Additionally, the BIT outlines under Annex 3 that the fundamental rule for the security of propriety data, necessitating Poland to "provide adequate and effective protection for proprietary information, which includes any formula, device, compilation of

⁶⁸ See, United Nations, 'Scope and Definition' [2011] UNCTAD Series on Issues in International Investment Agreements II 24 <http://unctad.org/en/Docs/diaeia20102_en.pdf> accessed 17 April 2023.

⁶⁹ R. Dolzer and C. Schreuer (n 1) para 63; Salacuse (n 1) para 160. Instance of such interpretation is in article 1(6) of the European Energy Charter Treaty; also Art. 1(1) of the 2001 Germany and Bosnia Herzegovina. Bilateral Investment Treaty between Germany and Bosnia and Herzegovina 2001. (Investment Policy Hub, 11 November 2007) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bit/606/bosnia-and-herzegovina---germany-bit-2001->> accessed 14 April 2023.

⁷⁰ Bilateral Investment Treaty between Argentina and United States of America 1991 (Investment Policy Hub, 20 October 1994) article 1 (IV) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/127/download>> accessed 20 June 2023.

⁷¹ Bilateral Investment Treaty between Ukraine and Denmark, (Investment Policy Hub, 29 April 1994) Article 1. <<https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bit/1291/Denmark---ukraine-bit-1992->> accessed 21 May 2023.

⁷² Kenneth J. Vandeveld, *U.S. International Investment Agreement* (OUP 2009) 762-763.

⁷³ The U.S.-Poland BIT 1990 establishes: a non-exhaustive, illustrative list of specific steps that each part agrees to take in order to establish protection of intellectual property rights, see Art. IV, Poland and United States of America 1990 (Investment Policy Hub, 6 August 1994) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5339/download>> accessed 20 July 2023.

information, computer program, pattern, technique or process that is used or could be used in the owner's business and has actual or potential economic value from not being generally known."⁷⁴ Such data, whether practical or businesslike, must be safeguarded as far as it satisfies three tests - it "(i) has actual or potential commercial value from not being known to the relevant public; (ii) is not readily accessible; lastly, (iii) has been subject to reasonable efforts, under the circumstances, by the rightful proprietor to maintain the secrecy."⁷⁵

For the reason that digital assets have been established as part of intangible assets and intangible assets fall under the definition of investment, there is no doubt that digital assets are protected by FPS standard. In *Siemens v Argentina*, the Tribunal held that the duty to accord FPS can be expanded further than physical protection and security, especially since the 'interpretation of investment encompasses tangible and intangible assets, though it is hard to see how physical security can be accorded to intangible investment'.⁷⁶

Since digital assets can be classified as tangible and intangible assets, the best security to be afforded to this type of investment under the obligation of FPS standard is to accord to it both legal protection and physical protection. Salacuse argued by saying that these kinds of wide and open-ended interpretation are aimed to accord as broad variety of investment kinds as feasible.⁷⁷ It does not matter if a computer networks or websites is not classified in the listed group catalogued under any treaty, it could without doubt still be as eligible for the protection of BIT as any kind of asset except if it is grouped within a classification of scenarios that are completely outside of investment, like the extension of credit and claims to money, like it was expressed under the NAFTA.⁷⁸

Considering the wide phraseology that is used to interpret investments in treaty application, digital asset like websites coupled with internets must without doubt be seen as investments and accordingly be protected by BIT clauses, but only where they are specifically used for commercial purposes, and also if it has a serious jurisdictional control and connection to that of the host country. Digital investments may in supposition magnetise the security of FPS clauses that feature in standard investment treaties in a host State's jurisdiction.

4. CYBER ATTACKS ON CORPORATE ENTITIES

There are so many academic legal literatures that raise concerns against attacks committed via the internet, known as 'cyber-attacks'.⁷⁹ It is a well-established fact in this modern technological era that the examples of computer network attacks generally against companies and State's classified information are rampant as the proportion of sophistication of spiteful software mechanisms grows. There have been instances of highly descriptive accounts

⁷⁴ U.S.-Poland BIT 1990, Annex 3, <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5339/download>> accessed 20 July 2023.

⁷⁵ *ibid* Annex 3, para 1.

⁷⁶ *Siemens v Argentina* [2007] ICSID Case No. ARB/02/6 para 303.

⁷⁷ Salacuse (n 1) para 162.

⁷⁸ Art. 1139 of North American Free Trade Agreement between Canada, The United States and Mexico (NAFTA) (entered into force 1 January 1994).

⁷⁹ In order to examine the most probably the excellent current instance concerning a treatment over this subject in one capacity look Indiana Carr (ed), *Computer Crime* (Ashgate 2009). See also D Powers (n 65).

of internet attacks today in the world. In the beginning of 2010, three US oil firms, encompassing Exxon Mobil, has in quick succession suffered cyber-attack from an internet servers that was situated in China, where the sole motive was getting information about the area and exact worth of oil findings. On 12 January, 2010, Google announced that cyber-attacks reportedly invented from around China was focused at thieving the intellectual property of Google together with information that belongs to various numbers of other corporations.⁸⁰ These attacks which were nicknamed “Operation Aurora” according to the cyber protection company McAfee, created partially a sophisticated economic espionage crusade.⁸¹ The threats were unique in part considering the kind of intellectual property information that was taken: that is, the corporation’s proprietary information source secret language, which is exactly its main trade confidential.⁸² The degree of sophistication used in this cyber-attack made the Vice President of MacAfee, Dmitri Alperovitch who was in charge of threat research to stipulate that, “the country has never ever, apart from in the field of defence, found business industrial corporations on that scale of sophisticated attack.”⁸³ Attacks like Aurora had been tagged “advanced persistent threats” (APTs)⁸⁴, and company corpuses have as well become focus of APTs as demonstrated by Operation Aurora.⁸⁵ Furthermore, Aurora was specifically remarkable because the crusade showed the scope to which country-sponsored attacks, concerning this matter reportedly originating from China, are focusing on corporations” trade confidential.⁸⁶

It is not just Google that is facing computer attacks in the world today. In 2013, Apple, Microsoft and Facebook, together with about who is who Fortune 500 corporations, were harmed or endangered, in various cases several times.⁸⁷ Organised crusade like that of Operation Aurora are as well rapidly increasing in number. For instance, about seventy various States and entities, encompassing the UN, International Olympic Committee, India, and other defence including security companies, were all the focus of computer network attacks

⁸⁰ See e.g., Kim Zetter, ‘Google Hack Attack Was Ultra Sophisticated, New Details Show’ (Wired, Jan. 14, 2010) <<http://www.wired.com/threatlevel/2010/01/operation-aurora/>> accessed 15 April 2023.

⁸¹ See Michael Joseph Gross, ‘Enter the Cyber-Dragon’ (Vanity Fair, Sept. 2011) <<https://www.vanityfair.com/news/2011/09/chinese-hacking-201109>> accessed 16 April 2023; Brian Grow and Mark Horsenball, ‘Special Report: In Cyberspy v Cyberspy, China Has the Edge’ (Reuters, Apr 14 2011), <<http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTR73D24220110414>> accessed 18 April 2023; Kim Zetter (n 81).

⁸² See e.g., Kim Zetter, ‘Google Hack Attack Was Ultra Sophisticated, New Details Show’ (Wired, Jan. 14, 2010) <<http://www.wired.com/threatlevel/2010/01/operation-aurora/>> accessed 16 April 2023.

⁸³ *ibid.*

⁸⁴ McAfee, ‘Protecting Your Critical Assets: Lessons Learned from: Operation Aura’ [2010] McAfee Labs and McAfee Foundstone Professional Services 3. <http://www.wired.com/images_blogs/threatlevel/2010/03/operationaura_wp_0310_fnl.pdf> accessed 25 April 2023.

⁸⁵ See *ibid.*

⁸⁶ See U.S.-China Economic and Security Review Commission (2012) <https://www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf> accessed 20 June 2023.

VERIZON, 2023 Data Breach Investigations Report <<https://www.verizon.com/business/resources/reports/dbir/>> accessed 20 June 2023.

⁸⁷ See Damon Poeter, ‘Microsoft Joins Ranks of the Tragically Hacked’ (PCMAG, 22 February 2013) <www.pcmag.com/article2/0,2817,2415787,00.asp> accessed 29 April 2023.

that was nicknamed in 2011, by McAfee as “Operation Shady RAT”. It was alleged that this crusade was funded by China, though it was difficult to pinpoint exactly who carried out this particular crusade.⁸⁸ The truth of the matter is that cyber-attacks on both private and government corporations are increasing rapidly all over the world today either by States or third parties. Also, in the same year in August 2013, Syrian Electronic Army reportedly staged computer network attacks directed at the *New York Times* newspaper including Twitter amid other channels, the biggest computer network attacks in recent history directed at China, and recent reports loomed concerning the National Security Agency’s (NSA) reconnaissance activities.⁸⁹ In March 2014, NSA hacked into Huawei’s computer systems, prompting the Chinese government representatives to cry out demanding for an end to cyber espionage.⁹⁰

The United States’ ambitions of overseeing international endeavours to protect cyber-attack security sustained a significant difficulties after it came into the open that NSA infiltrated into the telephones and internet transmission networks of millions of people.⁹¹ Dilma Rousseff, the President of Brazil, had to cancel a visit to the US in reaction to accounts that NSA was spying on her including Petrobras, a Brazilian government oil firm.⁹² In Germany the company executives have also cried out reaffirming President Rousseff’s anxiety that the US surveillance program “may have been employed to thief trade confidential”⁹³ after obtaining information that the US NSA had spied on Angela Merkel, the German Chancellor. Germany in this regard said: “that powerful countries want to steal their highest valued confidential and this information must accordingly be protected by all means.”⁹⁴ These are all cyber-attacks that emanate from actions of the government or its organs that have caused adverse effects to investments. Actually, 20th EY Global Information Security Survey (GISS) conducted a survey in 2017 and reached the conclusion that business or

⁸⁸ See Dmitri Alperovitch, ‘Reveal: Operation Shady Rat’ (McAfee, 6 Sep. 2011), <<http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>> accessed 2 May 2023.

⁸⁹ See Dave Lee, ‘New York Times and Twitter Struggle After Syrian Hack’ *BBC News* (28 Aug. 2013) <<http://www.bbc.co.uk/news/technology-23862105>> accessed 2 May 2023; BBC, ‘China Hit by “Biggest Ever” Cyber-Attack’ *BBC News* (27 Aug. 2013), <<http://www.bbc.co.uk/news/technology-2385041>> accessed 2 May 2023; Karen McVeigh, ‘NSA Surveillance Program Violates the Constitution, ACLU Says’ *Guardian* (27 August 2013), <<http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit>> accessed 2 May 2023.

⁹⁰ See Andrew Jacobs, ‘After Reports on N.S.A, China Urges End to Spying’ *N.Y. Times* (24 Mar. 2014) <<https://www.nytimes.com/2014/03/25/world/asia/after-reports-on-nsa-china-urges-halt-to-cyberspying.html>> accessed 2 May 2023.

⁹¹ James Ball, Julian Borger and Glenn Greenwald, ‘Revealed: how US and UK spy agencies defeat internet privacy and security’, *The Guardian* (6 September 2013) <<https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>> accessed 25 June 2023; Ben Deighton and Annika Breidhardt, ‘EU confronts U.S. over reports it spies on European allies’, *Reuters* (30 June 2013) <<https://www.reuters.com/article/uk-usa-eu-spying-idUKBRE95S0B720130630>> accessed 25 June 2023.

⁹² Jonathan Watts, ‘Brazilian president postpones Washington visit over NSA spying’, *The Guardian* (17 September 2013) <<https://www.theguardian.com/world/2013/sep/17/brazil-president-snub-us-nsa>> accessed 25 June 2023.

⁹³ Ibid.

⁹⁴ Chris Bryant, ‘NSA Claims Put German Business on Guard’, *FIN. TIMES* (1 Nov. 2013) at 4.

commercial espionage including data theft posed a danger to companies.⁹⁵ In this milieu, a serious predicament may arise if digital assets are not accorded investment protection befitting of it under FPS obligation in BITs under international investment law. These aforesaid cyber-attacks which reportedly originated from different regions to other countries is truly a contravention of traditional international law under the State Responsibility because countries are forbidden from causing crucial damages on another country region through actions that emanate from their own regions. (Rule5).⁹⁶

Statistically, on February, 2010, about 2,800 company computers were violated by fraudulent ‘hackers’ situated within Europe, authorising them entrance to delicate individual records, encompassing the intrusion of that of the clients. An Australian mega financial corporation whose name was not disclosed for security reason was attacked via the internet in 2010, presumably from around China, incapacitated that corporation’s Server for many hours.⁹⁷ In October 2015, the telecommunication company Talk-Talk was violated by criminal hackers and approximately 4,000 personal customers’ records were stolen, although this time the hacking was launched within the UK. There are also similar attacks that have happened not long ago that have originated from contaminated computers situated in countries like Egypt, Turkey, China, Saudi Arabia, and Mexico, where the possibility of identifying such attacks by governments is considered to be at its lowest ebb.⁹⁸ On 12 May, 2017, a cyber-attack that was nickname ‘operation Ransomware’ was launched from unknown destination by unknown persons hitting about 150 countries globally, causing a huge devastating and catastrophic effects to the UK’s NHS computer systems, and hence bringing the services of many UK hospitals to standstill. The Hackers demanded that some ransoms must be paid before they would unlock the computers that were infected with the virus. It was because of the weight of the devastation that it has caused that prompted the Europol and European Law enforcement Agency to state that; global computer attack is of an unprecedented scale’.⁹⁹ ‘It was one of the swiftest-spreading and possible harmful cyber-attacks acknowledged to date’.¹⁰⁰ Furthermore, it was alleged by Financial Times Newspapers that ‘the arsenal that was used in the hacking was stolen from the United States National Security Agency (NSA)’.¹⁰¹ Nigeria is well known for using computers to scam

⁹⁵ 20th Global Information Security Survey 2017–18, Cybersecurity regained: preparing to face cyber attacks, <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/digital/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf> accessed 20 June 2023.

⁹⁶ See Rule 5 in Michael N Schmit (n 11) 26.

⁹⁷ Rohan Sullivan, ‘Company: Chinese Cyber-attack targets Australia’ *SMH* (15 April 2010).

<<https://www.smh.com.au/technology/company-chinese-cyberattack-targets-australia-20100415-sh1d.html>> accessed 2 May 2023.

⁹⁸ S. Gorman, ‘Broad New Hacking Attack Detected’ *Wall St. Journal* (18 Feb. 2010) <<https://www.wsj.com/articles/SB10001424052748704398804575071103834150536>> accessed 2 May 2023.

⁹⁹ BBC, “NHS cyber-attack: GPs and hospitals hit by ransomware” *BBC News* (13 May, 2017) <<https://www.bbc.com/news/health-39899646>>

¹⁰⁰ See Sam Jones, Sarah Nevile, Jim Pickard, Joshua Chaffin, ‘NHS Hackers Used Stolen Cyber Weapons from US Spy Agency’ *Financial Times FT Weekend* (13 May 2017) <<https://www.ft.com/content/e96924f0-3722-11e7-99bd-13beb0903fa3>> accessed 20 June 2023.

¹⁰¹ *ibid.*

companies both within and outside its borders with such illegal activity being nicknamed ‘419’. In fact according to reports, Nigeria is ranked third amongst all other States identified and associated with cyber-crime and fraud in the world.¹⁰² Cyber-attacks are not frequently associated with the stealing of data, but they could be merely aimed to destroy property, perhaps for so many reasons, such as governmental or dogmatically reasons, for example, like the alleged ‘cyber terrorism’.

As has been mentioned earlier, there were high profile published cyber-attacks that were directed at Estonia in 2007 and against Georgia in 2008 respectively, from Russia, causing the internet to malfunction and crash, and bringing some neighbourhood of these two States to a halt. The success of these attacks was as a result of both the growing sophisticated nature of cyber insurgent methods and also due to the impromptu and unsettled position of the Georgian and Estonian regimes.¹⁰³ Politically inspired cyber-attacks may as well be aimed against business or many other investment organisations. Probably, the greatest renowned catastrophic computer network attack against a corporation as mentioned earlier was launched in the beginning of 2010 against Google in China from hacker criminals inside the State, supposedly aiming to incapacitate the Human Rights nonconformists e-mail accounts.¹⁰⁴ This situation could best be described as physical destruction in the practice of the standard of FPS to commercial investments, particularly where the consequence is an epidemic one, intruding with the real operation of a significant element of the secular community.

Another clear risk created by a cyber-attack on essential infrastructural systems is that this computer network attacks is highly exorbitant to individual parties, like alien investors who are based inside the contaminated region. If websites are interrupted, it could cost providers to loose their contracts and also cause destruction to their reputations and that of the investors. For example, some Talk–Talk customers who were affected as a result of the cyber-attack terminated their contracts with the telecommunication company. Intrusion to computer networks or machines could incapacitate manufacturing and at the same time can harm associated physical properties. Alien investors may be specifically endangered considering the magnitude of fund dedications comparative to dividend in the starting years of a foreign country investment scheme. A United States Congressional Research Service that was published in US learnt that cyber infiltration or attacks on computer networks caused a normal shareholder financial reduction for privately traded companies about US\$50 mil-

¹⁰² See The Cable, ‘Nigeria ranks third in global internet crimes’ *The Cable* (23 August 2017) <<https://www.thecable.ng/ncc-nigeria-ranks-third-global-internet-crimes>> accessed 20 July 2023.

¹⁰³ E. MacAskill, ‘Countries Are Risking Cyber Terrorism: Security Expert Tells World Summit’ *The Guardian* (5 May 2010) <<https://www.theguardian.com/technology/2010/may/05/terrorism-uksecurity>> accessed 2 May 2023; see further S. Shackelton, ‘Estonia Three Years Later: A Progress Report on Combating Cyber Attacks’ [2010] *Journal of Internet Law* 22.

¹⁰⁴ A. Jones and M Helft, ‘Google, Citing Attack, Threatens to Exit China’ *New York Times* (12 January 2010) <<https://www.nytimes.com/2010/01/13/world/asia/13beijing.html>> accessed 2 May 2023. Commercial surveillance was regarded to be an intention behind that hacking on Google’s activities in China, A Eunjung Cha and E. Nakashima, ‘Google China Attack Part of Vast Espionage Campaign’ *NBC News* (14 January 2010) <<https://www.nbcnews.com/id/wbna34855470>> accessed 20 June 2023.

lion to \$200 million.¹⁰⁵ And this number excludes the damage imposed on a corporation name because of the internet attack that may be seriously and grossly harmful, for instance, in the banking department where the protection of consumer's identities or details is a vital element of the work. Without doubt, alien investors are potentially vulnerable to suffering huge financial deprivations from internet-based unlawful harm against digital investments such as websites and the computer sets itself.

It was as a consequence of the internet attacks infiltration against private entities and State classified information, which has also caused huge financial deprivation to companies, that has led the U.S and China to propose for an extensive US-China BIT that will incorporate trade secret theft and enhance bilateral cyber protection so as to prevent any cyber threats against the private sector. This move seems to be a step in the right direction in order to assist host States to thwart cyber-attacks that pose threat to digital assets of foreign investors inside their borders either caused by the host country itself or caused by private parties.

Accordingly, Charles E. Schumer stated concerning the proposed extensive US-China BIT that, “[t]o not confront matters like intellectual property theft [during brokering of a BIT between U.S.-China] . . . can be a significant error.”¹⁰⁶ Also, previous leading government representatives in charge of international investment and trade affairs, in 2013 wrote that “most importantly, the complicated and governmentally alleged cracks over commercial cyber-espionage, if it is not tackled, jeopardise development on every front.”¹⁰⁷ Furthermore, in July 2013, the United States and China, instantly after re-agreeing on the both governments’ aims to broker an expansive bilateral investment treaty, “China and the United States pledged to accord robust security and application of trade confidential, and to intensify policies and solutions by applying the law.”¹⁰⁸ This United States and China proposal that will be announced for brokering an extensive BIT which will supposedly incorporate the problematic matter of intensifying bilateral cyber security¹⁰⁹ can a be starting point of addressing this issue globally.

If China and the United States would accept the incorporation of cyber threats clause and not just trade secret theft clause in their proposed BIT for the purpose of the prevention of damage to digital assets, and will consider a matter such as this which affects foreign investors and investments perpetrated or deliberately disregarded by States corpuses through extra-legal governmental takings, and which falls under the ambit of full protection and security standard. Not just to insert the provision to BITs, if this provision can be app-

¹⁰⁵ B. Cashell, WD Jackson, M. Jickling and B. Webel, ‘The Economic Impact of Cyber-Attacks Congressional Research Service, the Library of Congress’ [2004] CRS Report for Congress <<https://sgp.fas.org/crs/misc/RL32331.pdf>> accessed 18 May 2023.

¹⁰⁶ Ian Talley and William Mauldin, ‘U.S., China to Pursue Investment Treaty’ *WALL ST. J* (11 July 2013), <<http://online.wsj.com/news/articles/SB10001424127887324425204578599913527965812>> accessed 4 May 2023.

¹⁰⁷ Daniel M. Proce and Michael J. Smart, ‘BIT by BIT: A Path to Strengthening US-China Economic Relations’ [2013] 1 < <https://www.paulsoninstitute.org/wp-content/uploads/2016/07/BIT-by-BIT-English.pdf>> accessed 4 May 2023. <<http://www.paulsoninstitute.org/wp-content/uploads/2016/07/BIT-by-BIT-English.pdf>> accessed 4 May 2023

¹⁰⁸ U.S. Department of Treasury, ‘U.S.-China Joint Fact Sheet on Strategic and Economic Dialogue’ (12 July 2013). <<https://home.treasury.gov/system/files/136/SEDjointeconfactsheet072910.pdf>> accessed 20 June 2023.

¹⁰⁹ See Annie Lowrey (n 9).

lied by contracting State parties, then this problem of cyber-attacks may at least start to ease. The advice also is that the proposed US/China BIT should include general cyber security protection and not just limit it to trade secrets theft. Other countries must now follow suit to include in their BITs provision that will enhance cyber security so as to thwart any cyber threat against private and foreign investments. More importantly, a perfect BIT would also warrant such matters to be settled by international arbitral tribunals, such as ICSID, which also would provide an important forum to settle these kinds of disputes.

5. APPLYING INVESTMENT TREATY ADJUDICATION TO REDUCE CYBER ATTACKS

Expanding the application of mandatory permits necessitates a demand for a firmer regulation to tarpaulin trade secrets theft and all cyber-attacks.¹¹⁰ The illegalisation of such operation and the intensification of legal proceedings against persons are significant tools against cyber threats by persons or commercial rivals. Nevertheless, legal proceedings will suffer a setback when the wrongdoer is the country itself. The general security of cyber-attack will only happen when State participants are as well involved in the cyber protection. This matter is brought within intensive relation as the cyber attackers become stronger within the international cyber community. There is an anxiety among commercial amalgamation which is at the very heart of cyber security and BIT. William Burns who was Deputy Secretary of State for the United States highlighted on the US-China BIT the “necessity to get a shared comprehension of the principles about the road” in computer network.”¹¹¹ The necessity to generate a principle about the road for cyber protection is big, if not a bigger concern, as various countries and commercial investors are confronted with cyber threats, encompassing industrial espionage and BITs could be a channel to galvanise such ideas. The employment of bilateral investment treaties in this way gives two major components that are frequently absent in other investment protective mechanism like TRIPS: claims that occur within the scope of a bilateral investment treaty can not only be initiated by a person but as well may be settled in an internationally agreed arbitration framework. The application of arbitration renders many benefits, like the employment of a neutral surrounding for determination of their claims, a well-established principle of adjudication and implementation of award settlements,¹¹² and admission of and the application of firmly established investor-dispute concentrated arbitration bodies. Moreover, initiating a proceeding at ICSID within a BIT contract permits an alien investor to initiate a lawsuit against that particular host nation within investor-State adjudication without the necessity to request from its

¹¹⁰ Scott J. Shackelford and et al, ‘Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties’ (2015) 52 (1) *American Business Law Review* 1-74.

¹¹¹ See Paul Eckert and Anna Yukhananov, ‘U.S., China Agree to Restart Investment Treaty Talks’, *Reuters* (12 July 2013). <<https://www.reuters.com/article/uk-usa-china-dialogue-trade-idUKBRE96B04F20130712>> accessed 4 May 2023.

¹¹² Certainly, this is an indicator of adjudication as settlements are absolute and irrevocable on the parties to the contract, in both trade and investment associated disputes, see ICSID Convention, Rules and Regulation 2006 <<https://icsid.worldbank.org/sites/default/files/ICSID%20Convention%20English.pdf>> accessed 20 June 2023.

national government to lodge disagreement resolution proceedings.¹¹³ Unlike its precursor FCN, BITs are established to be less complicated and more restrictedly concentrated. Transparency in the ICSID mechanism must be encouraged for it to be a successful framework in building a regulation of cyber security as this article has already addressed. The dearth of transparency and inconsistency of interpretation of claims by ICSID arbitral tribunals is an increasing concern within the world community because investor-State adjudication rates have amplified, however positive measures have been taken in this respect that ought to be strengthened in subsequent BITs.¹¹⁴ Nevertheless, some anonymity is necessary in these lawsuits, if that happens parties who are involved will be confident bringing disputes that could in other respects remain unsettled in that tribunal. It is better left for negotiators in the proposed China-United States BITs to endeavour to thread this needle¹¹⁵ (to strike a balance between the conflicting forces).

Furthermore, multilateral mechanism may as well be used to fill the vacuum left by BITs. However, the TRIPS mechanism has its own flaws and has been condemned for numerous reasons, especially for having an ambiguous definition. In the same vein, although countries frequently observe WTO rulings, however, it has “*no jailhouse, no bail bondsmen, no blue helmet, and no truncheons or tear gas.*”¹¹⁶ This is so because the rules of the organisation are not being applied or followed properly, and the violators of its rules do not face stringent penalties. And it could also perhaps be that the WTO has been overshadowed by other international protective investment conventions. Additionally, the WTO up until now has been unsuccessful as a corpus for promoting international cyber security because of State or national security exceptions. For the aforesaid reasons, BITs can be good faith principle catch on if they are made more resilient for cyber security enhancement, but only if it is without national security exceptions. MFN provisions, within the WTO surrounding, are as well restricting factors, because they are included in BITs; however, there is greater ambit within BITs to successfully address this challenging problem. For instance, the MFN provisions under the third batch of Chinese bilateral investment treaties are more restricted in ambit than the second creation.¹¹⁷ The third batch of Chinese’s BITs was aimed to “strike a

¹¹³ See Gaetan Verhoosel, ‘The Use of Investor-State Arbitration Under Bilateral Investment Treaties to Seek Relief for Breaches of WTO Law’ (2003) 6 J. INT’L ECON. L. 493, 495; Resul Habyeyev and Serkan Kaya, *A Critical Role Of Diplomatic Protection In Investor-State Disputes* (On İki Levha 2021).

¹¹⁴ See United Nations General Assembly, Report of the United Nations Commission on International Trade Law, Rep. UN. Doc., A/68/17, On its 46th Sess, 8-26 July (2013) para 116, *available at*: <http://unctad.org/meetings/en/SessionalDocuments/a68d17_en.pdf> accessed 5 May 2023.

¹¹⁵ In its 2013 annual investment report, UNCTAD outlined a series of perceived shortcomings in the ICSID arbitral process.

¹¹⁶ See Judith Hipper Bello, Editorial Comment, ‘the WTO Dispute Settlement Understanding: Less Is More’, (1996) 90 Am. J. INT’L L. 416, 417.

¹¹⁷ See generally, Ton Qui, ‘How Exactly Does China Consent to Investor-State Arbitration: On the First ICSID Case Against China’ (2012) 5 CONTEMPORARY ASIA ARB. J. 265 (emphasising on batches of China BITs and efforts to apply most-favoured nation (MFN) provisions to debate the prerogatives to transfer matters to international adjudication).

better balance at the prerogatives of the host country and the foreign investor.”¹¹⁸ In addition, more supplementary wording may be inserted in BITs, to include computer network security, and cyber security protections in general. Ideally, both bottom-up (progressing from small or subordinate units to larger or more important units, as an organisation or process), e.g., BITs and top-down (situation in which decisions are made by few people in authority rather by the people who are affected by the decisions), e.g., WTO mechanisms have strengths and weaknesses, requiring a polycentric mechanism to promoting cyber security protection and creating a regulation for cyber peace.

BITs may offer a successful path to increase international computer network protection or a general cyber protection, and the extending international investment agreements (IIAs) to a broader investment environment may need to persist to gather approval from major countries internationally. Such an extension of custom BIT security is not in a dearth of precedent since current negotiated IIAs made mention about trade law, including rights to intellectual property, even non-economic matters like environmental protections, and labour rights. The OECD in working paper in 2011 announced that more than one hundred protocols out of a specimen of about 1593 BITs that have been incorporated made reference to climate issues.¹¹⁹ Such references effectively were scarce prior to the middle of 1990s, increased rapidly to being a portion of over eighty per cent of currently negotiated treaties in 2008.¹²⁰ Moreover, all preferential trade and investment agreements (PTIAs) under the OECD example enshrined environmental wording. For example, Japan, has constantly imputed anti-corruption principle in their recent BITs.¹²¹ The US and Canada have started to confront the issue of corporate social responsibility in many of their chapters of PTIA investment.¹²² In line with recent BITs signed by Canada and United States, the Benin-Canada BIT incorporated a provision “calling on the two States to promote their

¹¹⁸ Axel Berger, “Investment Rules in Chinese Preferential Trade and Investment Agreements: Is China Following the Global Trend Towards Comprehensive Agreement?” (2013) 7 *German Dev. Inst.* 1. <http://www.die-gdi/uplots/media/DP_7.2013.pdf> accessed 5 May 2023; Cai Congyan, “China-US BIT Negotiations and the Future of Investment Treaty Regime: A Grand Bilateral Bargain with Multilateral Implications” (2009) 12 *J. INT’L L.* 457.

¹¹⁹ See e.g., Kathryn Gordon and Joachim Pohl, ‘Environment Concerns in International Investment Agreements: A Survey’ 5 (2011) (OECD Working Papers on International Investment No. 2011/1) <https://www.oecd.org/daf/inv/internationalinvestmentagreements/WP-2011_1.pdf> accessed 5 May 2023.

¹²⁰ *ibid.* Other States like Germany including the UK still abstain from incorporating such issues into their protocols on a methodical basis.

¹²¹ See e.g., Agreement between Japan and the Republic of Colombia for the Liberalisation, Promotion and Protection of Investment art. 8 (12 September 2011) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/797/download>> accessed 5 May 2023; Agreement between Japan and the Republic of Peru for the Promotion, Protection and Liberalisation of Investment article 10 (21 Nov. 2008), <<https://www.iisd.org/toolkits/sustainability-toolkit-for-trade-negotiators/wp-content/uploads/2016/06/1733.pdf>> accessed 5 May 2023; see generally Joost Pauwelyn, “Different Means, Same End: The Contribution of Trade and Investment Treaties to Anti-Corruption Policy” in Susan Rose-Ackerman and Paul D. Carrington (eds), *Anti-Corruption Policy: Can International Actors Play a Constructive Role?* (Carolina Academic Press 2013) 247.

¹²² See UNCTAD, ‘World Investment Report 2011: Non-Equity Modes of International Production and Development’ (2011) 119-20, <https://unctad.org/system/files/official-document/wir2011_en.pdf> accessed 5 May 2023.

investors to comply with international recognised standard of corporate responsibility.”¹²³ All of these examples help as a reminder that broader regulatory objectives, encompassing cyber security, can be faced up to and deal with the rules of investment protections, especially under the obligation of the standard of FPS in BITs of international investment law.

6. FEW LEADING ARBITRAL DECISIONS THAT MAY BE APPLIED TO DIGITAL ASSETS

A few arbitral rulings can be greatly vital in the application of FPS to cyber security, especially digital assets, although the wording of any BIT cannot be a determinant factor in comprehending the purview of applying the standard.¹²⁴

In *ATM v Zaire*,¹²⁵ a claim started under the US-Zaire BIT for the assertion of Zaire’s omission to shield a US corporation from sustaining harms to its investment as a consequence of operations of the Zairian military forces in the State. Zaire argued that it did not breach the FPS obligations since AMT was not given a less favourable treatment than it gave to other national investors, encompassing its own. The ICSID tribunal ruled that the State of Zaire had contravened the FPS clause since it did not take any steps at all to guarantee the security of AMT’s investment and the reality that the Zaire as well was unable to safeguard the other investor was immaterial. What was of great significance to the arbitral tribunal was that the damages AMT incurred were as a consequence of the activities of the Zaire’s military operating personally and without in their collective authorised position as Zairian forces, and for that reason, their activities failed to be classified under the battle activities exception of this principle of FPS obligation, enshrined under the BIT. Like in this case, FPS provisions under investment treaties could incorporate some in-built exceptions in the favour of the host country, like warfare or an announcement of an urgency circumstances due to national security attacks. Lack of internet control by a State could emerge at a time of severe computer network attacks against a State, which may possibly avert the host country from fulfilling its FPS duties.

Another FPS case that may be applied to digital assets is *AAPL v Sri Lanka*,¹²⁶ where the arbitral tribunal assessed the principle of FPS provision under a UK-Sri Lanka BIT, and which concerned the damage sustained by the owner of shrimp farm at a time of clash between Tamil Tiger rebels and the Sri Lanka military Task Force. It was decided by the tribunal that the term full protection and security that was incorporated under a BIT supposed not to suggest that the principle is by any means greater than the international standard of minimum treatment necessitated under traditional international law. During the period of civil unrest, there was an obligation on the host country’s side to accord proper security to alien investors’ investments and that any omission to afford such security will

¹²³ See Lorenzo Cotula, ‘Is the Tide Turning For The Africa’s Investment Treaties?’ (IEDD, 8 March 2013) <<http://www.iied.org/tide-turning-for-africa-s-investment-treaties>> accessed 5 May 2023.

¹²⁴ See G. Cordero Moss, ‘Full Protection and Security’ in August Reinisch (ed), *Standards of Investment Protection* (OUP 2008) 134-135.

¹²⁵ *AMT v Democratic Republic of Congo*, ICSID Case No. ARB/93/1, Award, 21 February 1997 paras 6.05-6.06

¹²⁶ *Asian Agricultural Products v Republic of Sri Lanka* (1990) ICSID case No. ARB/87/3. Final Award para. 77.

attract the culpability of the country, specifically, to recompense the alien investor against any harm that the investor might have incurred. This duty that exists autonomously of the phrase FPS was breached by the Sri Lankan State. The standard of FPS clause in this matter was neither helpful nor beneficial to the claimant, since it was incorporated with a broad exception: there is no recompense that will be outstanding to be paid if the harm ensued from reasonable battle operation engaged by the military forces of the host country, which encompassed the activity that was undertaken by the forces against the insurgents. To avoid such exception and exclusion of compensation for the obligation of an FPS clause in a BIT such as the one in the AAPL case, such clauses should be carefully drafted by respective States to a BIT so as to give contracting parties and their digital assets adequate protection where an operation has resulted in digital investment damage from an attack.

In *Noble Ventures v Romania*,¹²⁷ the ICSID tribunal took almost the same approach that an FPS provision must not be perceived to be broader in ambit than the customary obligation to accord FPS to alien citizens found under traditional international law of foreigners. It was also stipulated by the tribunal that, for FPS to be claimed there is the need to show that the action that the host country has applied that attributed the harm was aimed particular against a specific investor because of its citizenship.¹²⁸ To bring this particular case in the context of cyber security protection, therefore, if every investor is to sustain injury at the time of a prevalent attack against a particular State itself, then the obligation of FPS may not be an attractive option, because the attack affected other nationalities. To put it differently, that would mean that any cyber-attack against a website and computer in the host State's territory would not be attributed to that host State so long as such an attack affected other nationalities.

However, there could be a glimmer of hope for investors on FPS obligation in this regard as it was in the *Wena Hotel v Egypt* case.¹²⁹ The principle received some contemplation when a claim was initiated by a British corporation against Egypt Republic for the State's inability to thwart an attack against Wena Hotels. Visitors that were at the hotel at the time of the raid were forcefully ejected and properties were damaged because of civil disobedience. It does not matter to the tribunal whether the host country did not really take part in that attack against the hotel. However, it was still concluded by the tribunal that Egypt was responsible for the violation of the obligation of FPS standard since Egypt knew about the attack and yet it did nothing to avert it. In this regard therefore, where a host State is aware of an imminent cyber-attack against investor's digital assets, for example computers and websites, and yet did nothing to prevent the attack from happening, such a State would be held liable for such failure.

In *Azurix v Argentina*,¹³⁰ there was a contravention of water and underground conduit drainage compromise agreements that was permitted by the State of Argentina district that benefitted a US firm. Nervousness erupted amid the populace when an eruption of an

¹²⁷ *Noble Ventures Inc. v Romania* (2005) ICSID Case No. ARB, Award, 12 October 2005.

¹²⁸ *ibid* at 111.

¹²⁹ *Wena Hotels v Egypt* (2002) ICSID Case No. ARB/98/4, Award, 8 December 2002, 41 I.L.M. 896.

¹³⁰ *Azurix and Argentina* (2006) ICSID Case No. ARB/01/12, Award, 14 July 2006.

algae ensued, resulting the public to cancel their contract agreements that was entered with the water providing company. In finding a violation of the standard of FPS for Argentina's action in omission to finish labour on systems dangerous to algae eradication, also as worsening the citizens' reaction to the occurrences, the arbitral tribunal accounted that even though some arbitral tribunals explicitly had restricted the standard of FPS to a minimum degree of physical protection, it may well be expanded in the relevant BIT between US-Argentina. Above all, FPS concerned not merely physical security but as well incorporate an additional obligation that the host States warranty the 'stability of secure environment',¹³¹ notwithstanding that the exact characteristic of the particular BIT which gave rise to this interpretation was not examined. It is worth noting that the claim of Azurix occurred prior to the State of Argentina suffered economic emergency and thus had no bearing on any urgency action exercised by the country in respect of that. The interpretation seems to mean that if there is a cyber-attack that has affected the digital assets, and which led to investors' contracts to be terminated based on the attack, for instance, where the investor failed to complete its work based on the host State's inaction to prevent the attack, the State would be held liable for it. This is so, because the host State is obligated to provide foreign investors 'stability for a secure investment environment both, politically, economically and socially for its investment'.¹³²

Lastly, in *Pantechniki v Albania*,¹³³ where riots were initiated by Albanian nationals owing to the breakdown of a State managed programme that destroyed the investor's road work scheme, demonstrates that there is a component of proportionality that is needed when evaluating breaches of the principle of FPS. Proportionality is required since, contrary to denials of justice that arise from a deliberate absence of due diligence in relation to administration, an omission to provide FPS is possibly to emerge from:

An unforeseeable example of public disobedience that may have been easily contained by a strong nation but which overcomes the restricted capability of a country that is deprived and vulnerable. There is no concern of motivation and deterrent in respect to unpredictable disintegration of civil unrest. It appears hard to state that a regime suffers international obligation for omission to prepare for extraordinary disturbance of extraordinary scale in extraordinary places.¹³⁴

It may be said that as a result of this decision a host country may have been issued with a ticket not to shoulder international obligation for its omission to react to an intense occurrence, a cyber-attack that is wholly unprecedented in nature and scale since the connectivity and control of internet services is not in the hands of the host State. Therefore, under the standard of FPS the host country ought to apply due diligence measure required of a State in the same circumstances, a characteristic that would be applicable when employing the principle to less-developed countries below.

¹³¹ *ibid* para 408.

¹³² *ibid*.

¹³³ *Pantechniki Contactor & Engineers v Albania*, (2009) ICSID Case No. ARB/07/21, Award, 30 July 2009.

¹³⁴ *ibid* para 77.

7. HOST STATES' DUTY TO PREVENT CYBER-ATTACKS ON FOREIGN INVESTOR'S DIGITAL INVESTMENTS

Focusing more on computers and websites, there may be a suggestion that the host state is obligated under full protection and security to avert attack imposed on digital investments or properties as the case may be, by rendering a secure online atmosphere, that is, one that weakens the capability of computer network perpetrators to initiate attacks effectively to investments. In a situation that the Server which provides an alien investor's website is situated inside the region and not outside the jurisdiction of the host State, it may be asserted that the State that host the server would be responsible to ascertain that the websites that are within its territory are protected from cyber-attacks. With this type of reasoning, scholars have recommended that computer connections security must be comprehended as a commodity of the public¹³⁵ which connotes that this is a useful and standard characteristic of workable community. This important feature is particularly relevant for the fact that host countries attempt to accord a stable, secure atmosphere to alien investors and their investments as a way of increasing the States' economic standing as stated by the tribunal in *Azurix v Argentina*¹³⁶ case. Viewing it in this sense, computer network protection can be regarded as a method in which the strength of economic wealth mechanism of the country is reached, encompassing that framework's capability to entice foreign capitals flows into the host State. A stable, secure and friendly investment atmosphere is provided to foreign investors in a swap for the trade, industry, and the creation of wealth benefits that it attracts.

The maintenance of a reasonable degree of security against internet offences that would appear under international legal document such as BITs could be argued to be a suggestive of what an adequate protected digital atmosphere ought to be for the sole aim of creating the standard of full protection and security, or minimum standard of treatment of international law. That would be precisely what full protection and security would be taken to mean.

Aside from BITs, computer network security has also become a vital subject in regional and global trade negotiations. The 2002 OECD Guidelines concerning the Security of Information Systems and Networks proposed that countries must apply swift and successful collaboration to thwart any computer network offensive attacks that emerge from internet on-line atmosphere.¹³⁷ The United Nations as well has promulgated propositions with the intention of reducing terrorist operations incited via the internet, the type that may harm the operation of computer systems.¹³⁸ The United State and European Union business discussions have been modelled at least in the beginning by worries over NSA reconnaissance

¹³⁵ J. Trachtman, 'Global Cyber terrorism, Jurisdiction and International Organisation' in Mark F. Grady and Francesco Paris (eds), *The Law and Economics of Cybersecurity* (Cambridge, 2006) 271.

¹³⁶ *Azurix Corp v Argentine Republic* (n 131) para 408.

¹³⁷ Organisation for Economic Co-operation and Development (OECD), 2002, Art. III.3. <<https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm>> accessed 20 June 2023.

¹³⁸ UN General Assembly Resolution (1997) 51/210 (16 January 1997); UN Security Council Resolution 1373 (2001) S/RES/1373 (28 September 2001).

activities, including intellectual property (IP) security;¹³⁹ the recommended Trans-Pacific Partnership (TPP) as well as general cyber security protection components;¹⁴⁰ and the WTO uses implementation framework that may be pertinent to computer network attacks if national security is perturbed could be defeated.¹⁴¹ All in all, those investment and commercial schemes could give a support for the promotion of bilateral and territorial team-work to strengthen internal internet protection generally and improve the security of computer systems to be specific at a period of gradual development on national and multinational advancement on cyber security strategy making.¹⁴² It is worthy of saying that applicability of those schemes to cyber security has failed to be valued sufficiently high in written works till today.¹⁴³ The international trade and investment community is still in a dearth of a consistent international framework for the security of alien investments and computer network protection, i.e. cyber security in general. Therefore, BITs may be influential in strengthening a legislation of this desperately required cyber peace relevant below the armed conflict maximum level.¹⁴⁴ Taking into consideration of these mechanisms, the indication will be that in the acknowledgement of full protection and security duty in any BIT, those host countries have assumed the commitment to offer internet or cyber protection to a level acknowledged as required by the global community such as to avert harm against websites (a set of related web pages located under a single domain name) and the computers machines itself of alien investors which could emanate direct or indirect from consequences of a well organised computer aggression or attack. Assumption of such obligation by a State would fall below the standard of the traditional international law requirements since this would necessitate that countries have participated in this conduct because of their perception of

¹³⁹ See e.g. Doug Palmer, 'US, EU start free-trade talks despite spying concerns', *Reuters* (9 July 2013), <<https://www.reuters.com/article/us-usa-eu-trade/us-eu-start-free-trade-talks-despite-spying-concerns-idUSBRE96704F20130708>> accessed 20 June 2023; but see James Fontanella-Khan, "Brussels Opposes German Data Protection Push" *FIN. TIMES* (5 November 2013).

¹⁴⁰ See Kevin Collier, 'Sen. Ron Wyden on the Problems with the Trans-Pacific Partnership', *DAILY DOT* (19 September 2012) <<http://www.dailydot.com/politics/ron-wyden-trans-pacific-partnership/>> accessed 5 May 2023.

¹⁴¹ Allan A. Friedman, 'Cybersecurity and Trade: National Policies, Global and Local Consequences' (2013) Brookings Inst. 10-11 available at: <<https://www.brookings.edu/wp-content/uploads/2016/06/BrookingsCybersecurityNEW.pdf>> accessed 5 May 2023; Mark L. Mossman, 'Essay, Enforcement of WTO Rulings: An Interest Group Analysis' (2013) 32 *HOFSTRA L. REV.* 1, 1-2; James A. Lewis, 'Conflict and Negotiation in Cyberspace' (2013) *CTR. STRATEGIC & INT'L STUD.* 49-51 (discussing the applicability of the WTO dispute resolution processes to help manage cyber espionage). This restriction in the World Trade Organisation composition emphasises the necessity for bilateral and territorial methods to promoting cyber security.

¹⁴² See e.g., Scott J. Shackelford, 'In Search of Cyber Peace: A Response to the Cyber security Act of 2012', (2012) 64 *STAN. L. REV. ONLINE* 106 <<http://www.stanfordlawreview.org/online/cyber-peace>> accessed 6 May 2023; Tom Greaten, 'Seeing the Internet as an "Information Weapon,"' (NPR, 23 September 2010) <<http://www.npr.org/templates/story/story.php?storyId=130052701>> accessed 6 May 2023 Emphasising the reality that UN-sponsored cyber reduction talks have been taking place from 1990s but have been futile since then.

¹⁴³ cf Steven E. Feldman and Sherry L. Rollo, 'Extraterritorial Protection of Trade Secret Rights in China: Do Section 337 Actions at the ITC Really Prevent Trade Secret Theft Abroad?' (2012) 11 *J. Marshall REV. INTELL. PROP. L.* 523, 525; Gerald O'Hara, 'Cyber-Espionage: A Growing Threat to the American Economy' (2010) 19 *CommLaw CONSPECTUS* 241, 253-54; Peter Swire and Kenesa Ahmad, 'Encryption and Globalisation' (2012) 13 *COLUM. SCI. & TECH. L. REV.* 416, 475-76.

¹⁴⁴ See Scott J. Shackelford (n 10) 231.

legal responsibility and that is not obvious from the mechanisms stated.

Nevertheless, it seems improbable that a duty may be imposed on a host country's administration for the protection of private investors' websites against any designated cyber-attacks. It is due to this fact that the provision of internet services is overseen by individual corporations. It is not in the tradition of most regimes of controlling or keeping servers that store websites. It is mostly the field of individual telecommunications firms, such as Internet Service Providers (ISPs), especially in most developed countries where the governments have privatised such companies to provide these services. Permits may be given by host countries to ISPs who sell internet networks and those governments can render some level of supervision, but this supervision does not expand to practical management or control of the operation and protection of the internet network or personal web-pages that emerge on it. With this explanation, it is very challenging to recommend significant and serious State control or supervision of a website than it is likely to be in the issue of, for instance, a plant, where the law enforcement agents like the police may generally have entrance and interfere if there is a cyber-attack occurrence. Accordingly, there is virtually the certainty for an inadequate measure of State supervision to ascribe any protection negligence or omission in respect of particular website to the countries on the ground of full protection and security obligation. Instead, individual groups like ISP suppliers could fit in as the major credible players with regards to avoiding subsequent damage.¹⁴⁵ Ascribing liability to the country could be more easily created in non-market system economies where the government does keep first-hand control upon the internet.

It could be just to claim that an extensive degree of internet security problems, for instance the wholeness of a country's internet infrastructure generally, and the steadiness of transmission computer networks that trouble so many subscribers like those impacting on the provision of utilities, must remain under the control of the State¹⁴⁶ as it is or used to be in most developed and developing countries before the surge of corporation privatisation. Internet construction and planning is progressively an essential element of workable society, and as such it must be regarded as under the domain of a State's obligation to its nationals, even where many crucial amenities like internet network, energy generation and water supplies, are directly distributed by an individual corporation. Nevertheless, in some developing countries energy and water supplies is still being control and supervised by the government and is still left in the hands of the State for distribution. Disruptions of internet infrastructure would place adverse effects to foreign investments upon which the full protection and security is based, and would equally amount to a violation of full protection and security standard. For this reason, culpability for property harmed, even if it comes as an indirect result of the chaos affecting the wider system, could possibly be the liability of the government. On this viewpoint, foreign corporations functioning inside the territory of a host State could have asked for compensation from the authority of that country for the breakdown in the network, especially if the internet disruption resulted from mistake

¹⁴⁵ See D. Littman and E. Posner, 'Holding Internet Service Providers Accountable' in Mark F. Grady and Francesco Paris (eds), *The Law and Economics of Cybersecurity* (Cambridge University Press 2006).

¹⁴⁶ See Trachtman (n 136) para 270.

or negligence on the side of the State, particularly where there are no governmental agencies that monitor the activities of the individual internet providers. This reasoning must be mitigated with possible impromptu or urgency situation justification which the State could claim, like the ones found in *AMT* case.¹⁴⁷ FPS provisions in investment protocols may incorporate some exceptions that could favour the host country, like warfare. Likewise, an announcement of an urgency situation that threatens national security, which probably will emerge at a time of a severe attack against a State's network, could possibly preclude the host country from its duty of an FPS standard. As the internet structure is in the hands of the government, the graver the attack on the government computer system, the more the likelihood that the country is capable of claiming that the actions it took was taken as a result of the emergency of the circumstances surrounding it. It must be said that, in a situation whereby the host country played a direct part in financing or organising the computer network attack on an alien investor's website that has investment or business existence in its territory, full protection and security obligation to prevent harm would clearly be breached.¹⁴⁸

7.1. INVESTORS' DUE DILIGENCE FOR THE PROTECTION OF CYBER ATTACKS

With regards to any evaluation of the obligation to accord due diligence to a foreign investor that a State owe under the standard of FPS provision, this must be weighed against the adequate steps which the foreign investor ought to have anticipated to enforce to safeguard their own investments, extent as the foreign investor would be anticipated to secure their business building with locks at night, especially in the location where the computer system is kept. Or better still, to employ security guards to watch the premises to avoid any unwanted intruders breaking in to their business premises. If the investor fails to abide by the necessary basic standard of protection concerning its individual on-line presence can very possibly reduce any host country of culpability and aggravate the investor's loss on this issue, or at minimum, minimise the amount of payment granted by an arbitral tribunal if the tribunal ruled in the claimant's favour. Like Trachtman asserted, corporations must be accountable for the rudimentary protection about their own gadgets, like firewalls protection against e-mail spam, including preserving their anti-virus computer software, since they are capable of preventing such damages at minimal cost.¹⁴⁹ However, the above rudimentary level of security cannot be achieved in most developing States, for instance in some States where law and order are in disarray, where legislation, the law enforcement agencies and judiciary care relatively little about their own inhabitants.

7.2. COMPENSATION FOR CYBER ATTACKS

If peradventure a contravention of an FPS provision is found in respect of a computer network attack against investors' digital asset, arbitral adjudication undoubtedly would be left with a challenging task of evaluating a suitable amount of payment due for such investor. Assessing compensation for damage for contravention of investment agreement stan-

¹⁴⁷ *AMT v Democratic Republic of Congo* (n 126).

¹⁴⁸ See Shackelford (n 10) 235.

¹⁴⁹ See Trachtman (n 136) para 270.

dards of security can be famously a complex matter under international law.¹⁵⁰ The “Hull Principle” necessitates “immediate, sufficient and successful” payment.¹⁵¹ In reality, when one contemplates about cyber-attack damage, the concern becomes what will the full compensation be? This question is an especially hard one to provide an answer to taking into consideration of the protracted effect on the company’s reputation, together with business disruption and interference, it might be hard to ascertain and quantify. Arbitral tribunal seems to be having problems with this notion in the area of FET. The case of *Chorzow Factory* assists to lay down the criterion: “Compensation must, to the extent that is possible, remove all the results of unlawful conduct and re-create the circumstances which may, in all possibility, have occurred if that action had not been perpetrated.”¹⁵² In reference to cyber-attack, especially on computers or websites, there seldom is the likelihood to place the foreign investor back in the level that he would have been had the conduct not been perpetrated, given that computers or websites are frequently at the central of the business. The expectation is that injuries for the omission to apply preventable computer network attack on investor’s investment would possibly comprise some mixture of the loss of investment or financial lost at the time that the web-page or the computer system itself broke down in case of physical damage, the repairing expenses or the replacement cost of related harmed physical property, like the equipment including the computer hardware. The level of the harm available could depend on the measure Remoteness that involved with the loss and the related foreseeability of damage as a result of the government’s or State’s negligence to avert the action. On this note, contracting parties to a treaty must consent on the current fair and equitable compensation mechanism for cyber security protections, and may as well need to come to an agreement on a technique or principle to accord for adequate recompense when cyber-attack occurs.

7.3. AVAILABILITY OF FUNCTIONAL LEGAL SYSTEM TO CONTROL CYBER THREATS

The use of the duty of FPS standard to cyber-attacks would undoubtedly need the offering of a workable legal mechanism that can control and implement legislations against the execution or perpetration of damage on computers equipment and some other different digital properties belonging to alien investors. First off, the wholeness of the country’s legal framework in regards to the identification and bringing proceedings against cyber perpetrators may be seen as a collection of processes characteristic by the host country atmosphere and accordingly would be more properly grouped under the standard of FET. However, seeking the investigation under the standard of FPS, while the prompt instituting of a legal proceeding against the offenders based on actual results rather than predictions could pro-

¹⁵⁰ See further I. Marble, *The Calculation of Compensation and Damages in International Investment Law* (OUP 2009).

¹⁵¹ See Ronald Charles Wolf, *Trade, Aid, and Arbitrate: The Globalisation of Western Law* (Ashgate 2004) 26 (citing Cordell Hull, the United States’ Secretary of State (quoting 3 Green Haywood Hachworth, ‘Digest of International Law’ 658-59 (1942) (and following text); UNCTAD, ‘Taking of Property’ (2002) 13-14 *available at*: <<http://unctad.org/en/Docs/psiteiitd15.en.pdf>> accessed 5 May 2023 See World Bank Guidelines on the Treatment of Foreign Direct Investment s. IV (1999) *available at*: <<http://italaw.com/documents/WorldBank.pdf>>

¹⁵² *Factory at Chorzow (Germany v Poland)* (1928) P.C.I.J, Merits, (ser. A) No. 17, 13 September 1928 para 47.

vide an effective legal reaction to the cyber offences to placate affected investors and may prevent subsequent computer network attacks, and decrease the possibility that such offences will reoccur.¹⁵³ The offenders who committed the cyber crimes could not probably have done so if they fright that they would be caught by the law and be punished accordingly for committing such a crime. Where a State did not succeed in preventing cyber-attack, it must at least apprehend and punish those that perpetrated the act.¹⁵⁴ This will serve as a deterrent to other future criminals to refrain from such act.

Yet, legislations that associate with the ultimate importance of digital assets or cyber investments might not be uniform in international investment law, but they are familiar under international law and therefore may fall under an appropriate degree of protection offered by the FPS standard. For instance, the World Trade Organisation in 1994 extended the area of business confidential (trade secrets) that can be covered for protection from business in commodities and business in other services to a description of rights of intellectual property also.¹⁵⁵ Recognised as TRIPS, the multilateral treaty, under its Article 39, makes mention of trade secret as the security against any unjust competition under the Convention of Paris.¹⁵⁶ Some Parties members to the World Trade Organisation are bound under the trade confidential measures obligated by TRIPS, for instance, China, unlike many States, where there are frequently no laws that are particularly focused on the security of trade confidential.¹⁵⁷ Additionally, the WTO Trade Related Measures of Intellectual Property Agreement orders for a minimum degree of security for the rights of intellectual property to be accorded to the WTO party States' local legal mechanisms, that may help where trade useful digital properties, like client record data are duplicated and in other respect stolen at the time of a computer network attack. Article 5 of the Council of Europe Convention on Cybercrime necessitates that members must legally take lawful steps to create as an unlawful crime the hampering of computer system operation by deliberately inserting and loading, transferring, destroying, removing, degenerating, changing or concealing of com-

¹⁵³ See W. McGauran, 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 *Tulane Journal of Technical and Intellectual Property* 259.

¹⁵⁴ *Sergei v Government of Mongolia* (2011) Award on Jurisdiction and Liability, 28 April 2011 para 323. <<https://jsumundi.com/fr/document/decision/en-sergei-paushok-cjsc-golden-east-company-and-cjscvostokneftegaz-company-v-the-government-of-mongolia-award-on-jurisdiction-and-liability-thursday-28th-april-2011>> accessed 5 May 2023.

¹⁵⁵ Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organisation (Marrakesh, Morocco 15 April 1994), available at: <https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm>

¹⁵⁶ *id.* section 7, art. 39(1) ("during the period of undergoing lawful security from unfair competition like it is accorded under Article 10bis of the Convention of Paris . . . , Parties must protect confidential data . . ."). The Paris Convention necessitates Parties "to ensure to citizens of those States legal security from unfair competition." Paris Convention for the protection of Industrial Property art. 10bis (1) (1979), available at: <http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html#p213_35515> In addition, it reads unfair competition like "[a]ny conduct of competition against impartial applications in factory or business issues". *Id.* Art. 10bis (2).

¹⁵⁷ See Shan Hailing, *The Protection of Trade Secrets in China* (2nd edn, Kluwer Law International 2012) 27. (European States have often used a different type of laws and encompass trade confidential legislations in respect of their civil laws, business laws, and other different legislations, and they never have given a particular law or a one code for national trade confidential security.)

puter information.¹⁵⁸ Various other domestic legitimate frameworks as well keep regulations which were promulgated to bring legal proceedings against cyber-attack offenders for offences against computer equipment, like attacks on business websites. For example, ‘Canada’s Criminal Code establishes an unlawful crime for damaging, changing or intruding with the utilisation of information’.¹⁵⁹ Section 16 (3) of the Nigerian Cybercrimes (Prohibition, Prevention, Etc.), Act 2015, ‘necessitates as an unlawful crime the hampering of the operation of a computer sets by inserting or loading,, transferring, destroying, removing, degenerating, changing or concealing computer information or any kind of intrusion with the computer equipment’.¹⁶⁰ These aforementioned legislations are proof of country approach that support protection against attacks to computer connected businesses and assets,¹⁶¹ and as a result should provide a comprehension surrounding the level of due diligence measures of legitimate security against computer network attacks that could be linked with the standard of FPS guarantee.

It would be challenging to assert if the host country was responsible to initiate legal proceedings against cyber perpetrators that had staged a cyber-attack away from the country’s territory since the country is not supposed to have the legal right to rule on the case, except the offenders are citizens that come from the host country.¹⁶² The Council of Europe Convention that deals with computer network offences only stipulates that ‘jurisdiction can only be shown where the crime takes place, amongst other things, in the region of a country’¹⁶³ providing no direction on how it will be interpreted. Traditionally, the principle of FPS is involved in a situation where harm is sustained inside the borders of a host country, a circumstance that has been mentioned earlier and would possibly be fulfilled when the server of the website or the computer device itself was situated inside its territory. However, it is never obvious that international tradition concerning computer offence implementation is conclusive enough to the extent that it might form a standard. Various scholars have condemned the dearth of international legislations for offences committed on

¹⁵⁸ Council of Europe Convention on Cybercrime, Budapest 23. XI.2001, *European Treaty – No. 185*, Art. 5. In 2006 the treaty got 28 signatory countries, and 15 out of the 28 had endorsed it. The Convention got accolade from scholars like M. Miquelon Weismann. See M. Miquelon Weismann: ‘The Convention on Cybercrime: A Harmonised Implementation of International Penal Law: What Prospect for Procedural Due Process’ in Indiana Carr (ed), *Computer Crime* (Ashgate 2009).

¹⁵⁹ See, Criminal Code of Canada s. 430(1.1). See also Title 18 ch. 47 United States Code s. 1030, reporting the illegitimate crimes of deliberately gaining entrance to computer with lack of permission to access data or generate harm. In *Cyber Law and Security in Developing and Emerging Economies* (Edward Elgar 2010), authors ZK Shalhoub and SL AI Qasimi stated that it just 26 States worldwide that have created some regulation that deals with cyber matters, at 224.

¹⁶⁰ Section 16 (3) of the Nigerian Cybercrimes (Prohibition, Prevention, Etc.), Act 2015.

¹⁶¹ R. Garnet and P. Clarke, ‘Cyber terrorism: A New Challenge in International Law’ in A Bianchi (ed), *Enforcing International Law Norms against Terrorism* (Hart 2004) 477.

¹⁶² *R v Graham Waddon*, 2000 WL 41456 (2 April 2000), in that regard as far as webs sites can be gaining entrance to in the host country, they have jurisdiction over the case. Nonetheless, Appeal Court of the UK ruled that criminal regional jurisdiction can be created in the area that the websites material may be entered and copied

¹⁶³ European Convention on Cybercrime (Budapest Convention 2001) Article 22.1(a), <<https://rm.coe.int/1680081561>> accessed 5 May 2023.

the sphere of internet,¹⁶⁴ like those that can possibly harm the worth of a corporation's trade investments. It is particularly the situation in less-developed countries, where these kinds of commercially protective legislations do not exist, or are not implemented at all if such laws do exist, that will thus necessitate a contextual amendment of the standard of FPS. This will only happen if wording, to prevent cyber harms that will impact on foreign investors' investments, are inputted in Full protection and security clauses in BITs just as the United States and China BITs have proposed in their future BIT.

8. LESS DEVELOPED STATES AND THE FULL PROTECTION AND SECURITY STANDARD

It is well known that half of the overall global FDI presently goes to the less-developed world,¹⁶⁵ where the judicial and governmental situations are frequently and obviously more unstable compared to the countries from where the capital emanates from. Many scholars caveat that it is not all State governments that are able to provide for the capital that is required to manage operational computer connections, let alone avert harmful activities against them.¹⁶⁶ Additional to substandard degrees of internet connection system,¹⁶⁷ and related absence of technological understanding or technical know-how to avert cyber-attack, only a small number of less-developed countries have promulgated regulations to confront these pressing problems and have as a result been unable to bring legal proceedings against the offenders.¹⁶⁸ Even in few underdeveloped States where such legislations have been enacted, implementations of such regulation are far from the reality. Damaging cyber-attacks can be more widespread in countries in which there is the existence of a general deficiency of trustworthiness in the administration and where a few number of individuals with restricted wealth can be emancipated by the use of anonymity and damaging capability of destroying the internet.¹⁶⁹ These States frequently have creaking infrastructure or are incapacitated to react to the protection of internet attacks matters when it arises. Those circumstances outline a handful number of those States that are capital-importing countries of the less-developed world that have finalised BITs just for the single intention of quelling the anger and winning over foreign investors. The action of taking up protective steps that are reasonable to avert cyber-attack on computer machines in these States is described as occurring at

¹⁶⁴ Ugo Draetta, 'The Internet and Terrorist Activities' in A Bianchi (ed) (n 161); In *Cyber Law and Security in Developing and Emerging Economies* (Edward Elgar, 2010), authors ZK Shalhoub and SL AI Qasimi stated that it just 26 States worldwide that have created some regulation that deals with cyber matters, at 244; See W. McGauran (n 153) 259.

¹⁶⁵ UNCTAD, 'World Investment Report' (2010) <https://unctad.org/system/files/official-document/wir2010_en.pdf> accessed 5 May 2023

¹⁶⁶ See, Trachtman (n 135) 273.

¹⁶⁷ See further R. Kariyawasam, *International Economic Law and Digital Divide: A New Silk Road* (Edward Elgar, Publication 2007).

¹⁶⁸ Shalhoub and AI Qasimi quote the instance concerning the Philippines that had proof of the people that are liable regarding the 'Love Bug' infection in 2000 that cost the State over \$10 billion in compensation but was powerless to bring legal proceedings due to a defective legal mechanism.

¹⁶⁹ Ronald D. Crelinsten, 'Terrorism and Counter-Terrorism in a Multi-Centric World: Challenges and Opportunities' in M. Taylor and J. Hogan (eds), *The Future of Terrorism* (Routledge 2006).

irregular intervals and only in a few places, with innumerable less-developed States having shortcomings in the maintenance of adequate preventive actions.¹⁷⁰

There is no way a foreign investor ought to anticipate the same degree of internet protection from all countries where it invests, because protection against cyber offences can be exorbitant and definitely would necessitate a great degree of technological or occupational professionalism encompassing human capital wealth which most developing States are lacking at the moment.¹⁷¹ This is the expression of Jan Paulsson obiter dicta in *Pantechniki* case: “an unforeseeable exemplification of public disobedience that surpasses the restricted capability of a country that is in abject poverty and is susceptible.”¹⁷² This maxim could arguably be far from universal especially in some of the more wealthy developing countries whose technical proficiency has been crippled due to endemic corruption and not because of poverty. Having said that, it is prudent to accept the ruling in this case that an extremely poor host country must not shoulder international obligation where it failed to act to threats of a cyber-attack which is beyond its control and is extraordinary in kind and magnitude. Therefore, under FPS a host country ought to take a reasonable measure of care of a State in a very much alike situation, a characteristic that is suitable at employing the FPS standard to the less-developed countries.

As for the expression of ‘due diligence’ in the standard of FPS as it is given by *APPL v Sri Lanka*, it as well implies that foreign investors ought to have a less anticipation in less developed countries. The duty of ‘due diligence’ signifies necessary steps of deterrence that a good-ruling and organised State might be anticipated to apply under the same situations.¹⁷³ Whereas a proper standard of governance can be anticipated, this ought to be weighed against the situation by which the occurrences have happened. Sornarajah stated that, “this should comprise the strength of the contention and wealth which possibly could be redirected for the aim of security”.¹⁷⁴ Additional to the intensity, likely referring in this context, to the several of persons injured, this balancing must encompass the kind of the adverse effects. David Collins stated that “countries which have a substandard internet connection will unavoidably get a poorer quality capacity to confront greatly technological disruptions like that of computer network attacks.”¹⁷⁵ This statement is correct, because the developing States’ lack of technological know-how will serve as an impediment in addressing such a problem. He further stated that, “this is because the wealth to confront the extent of such computer network contention

¹⁷⁰ Centre for Strategic and International Studies (CSIS) and McAfee Inc. Australia, China, the UK, and the US have the excellent history of keeping protection of computer networks. See S. Baker, S. Waterman and G. Ivanov, ‘In the Crossfire: Critical Infrastructure in the Age of Cyber War’ < <https://www.govexec.com/pdfs/012810j1.pdf> > accessed 13 July 2023.

¹⁷¹ *ibid.*

¹⁷² *ibid.* 77

¹⁷³ See Salacuse (n 1) para 132. This phrase is itself a quote from AV Freeman, *Responsibility of States for Unlawful Acts of their Armed Forces* (1956) 88 *Recueil des Cours* 261.

¹⁷⁴ *ibid.* 135.

¹⁷⁵ David Collins, “Applying the Full Protection and Security Standard of International investment Law to Digital Assets” (2011) 12 *Journal of World Investment and Trade* 225, 242.

in those countries is minimal".¹⁷⁶ The second viewpoint seems not to be completely correct because some of these developing States as stated before have enough resources to address such problems but failed to do so because of the corruption that has eaten deep into the fabric of those nations. For instance, a country such as Nigeria with plentiful resources cannot be said to lack the financial resources needed to confront the volume of cyber threats in its territory. It would fail to do so because of the unquenchable thirst for siphoning the country's wealth to private overseas bank accounts by its government officials. This factor has led to misappropriation of funds and misplacement of its priorities.

This adaptability including the danger it poses to foreign investors indicates the procedural benefit provided by less developed countries. A lack of enabling environment, such as creaking and frail infrastructures with feeble governance could be possibly the exact rationale behind why a foreign country can provide cheap manufacturing prices that are significantly tempting to alien investors. Developing States may offer lesser production rates to foreign investors which may be counterbalanced or be balanced in excessive charges for PRI – (Political Risk Insurance). Nevertheless, the World Bank's Multilateral Investment Guarantee Agency's Guidelines (MIGA) have not made reference of host country internet connection or interconnection, neither did it make mention of any legislations of cyber-attacks in existence as at the time it was creating the levels of the indemnity charges for PRI candidates,¹⁷⁷ connoting that the peril of cyber threats against foreign investors has still not entered into the procedural argumentation of development organisations. It ought to be made reference of that a few less developed countries, such as India and Peru for example, have indicated a significant preparedness to fight computer attack offences than many other developing countries¹⁷⁸ and the enhancements in that respect are not merely a concern of technical prowess, but it as well comprises community and societal aspects, encompassing the necessity of higher internet connection and the inclusion of domestic satisfaction.¹⁷⁹

9. BILATERAL INVESTMENT TREATIES AND POLYCENTRIC REGIME MECHANISM

A new ideological mechanism is needed to examine the part that an international framework of bilateral investment treaties plays in enhancing cyber protection. One such possibility is polycentric regulation, which is a method that visualises "a communal of wholly and partly and ungraded systems" that differ in scale and motive.¹⁸⁰ Academics from a

¹⁷⁶ *ibid.*

¹⁷⁷ MIGA gives PRI to qualified alien investors who are investing in less developed countries. It is notable that although MIGA does issue warranty against conflict and public unrest, it only protect losses sustained from tangible properties or where the business had been interrupted completely. It could be the same case when an important computer system becomes non-operational. See, Multilateral Investment Guarantee Agency, 'Investment Guarantee Guide' <<http://www.miga.org/documents/IGGenglish.pdf>.> accessed 5 May 2023.

¹⁷⁸ T. Tripathy, 'India Restricts Telecom Suppliers, carriers' *The National Post (Canada)* (29 July 2010); Shalhoub and Al Qasimi, in *Cyber Law and Security in Developing and Emerging Economies*, (Edward Elgar 2010), 227.

¹⁷⁹ *ibid* 217.

¹⁸⁰ Kal Raustiala and David G. Victor, "The Regime Complex for Plant Genetic Resources" (2004) 58 INT'L ORG. 277, 277

different branch of knowledge have devised the idea of polycentric regime, which could be contemplated as a regulatory regime, something that is regarded and called “regime complex”,¹⁸¹ i.e., “*identified by various ruling powers at diverge degrees instead of a monocentric component*,” as stated by Professor Elinor Ostrom.¹⁸² As time goes by, this multistage, multifaceted, “multifunction, and multi-industrial”¹⁸³ framework indicates the advantages of self-organisation, networking governances “at multiple levels”¹⁸⁴ and the extent to which citizens and individual management can sometimes exist together with collective governance. Rather than top down - (a system of regulation or supervision that actions and policies are initiated at the highest level) State-imposed laws, analysts discovered that small sets of people across an arrangement of subjects do actually collaborate and can create the correct motivation and atmosphere for the best and most favourable communal work.¹⁸⁵ An obstinate, comprehensive government then can truly suppress transformation by changing small-scale endeavours.¹⁸⁶ This is partly why Professor Ostrom has argued that polycentric regulation is “*the foremost method to confront across-border issues ... for the reason that the perplexity of these difficulties contributes to itself better to various little, specific issue units working independently partly of a system that is confronting communal action issues. It is a use of the adage, ‘think internationally, but act domestically.’*”¹⁸⁷

Nonetheless, polycentric systems are far from flawless. They are, for instance, likely to be influenced or harmed by organisational breakdowns and deadlock, that developed from partly or wholly coinciding of control which, as stated by Professors Robert Keohane and David Victor, must nevertheless still meet the principle of consistency, successfulness and

¹⁸¹ See e.g., Daniel H. Cole, “From Global to Polycentric Climate Governance” (2011) 2 CLIMATE L. 395, 412 (debating system composite from the viewpoint of environmental Change). For more argument on employing polycentric governance to present-day cyber protection and computer connection governance difficulties, see Scott J. Shackelford, “Towards Cyber Peace: Managing Cyber Attacks through Polycentric Governance” (2013) 63 AM. U.L. REV. 1273 (employing polycentric control to the cyber protection surroundings), and Scot J. Shackelford, *Managing Cyber Attacks in International Law, Business and Relations: In Search of Cyber Peace*, (Cambridge University Press 2014).

¹⁸² Elinor Ostrom, “Polycentric Systems for Coping with Collective Action and Global Environmental Change”, (2010) 20 GLOBAL ENVIL. CHANGE 550, 552.

¹⁸³ The “fundamental notion” of polycentric control or rule “is that whatever set of persons confronting few collective challenges must be capable of tackling such difficulties in any way they best deem fit.” Michael D. McGinnis, ‘Costs and Challenged of Polycentric Governance: An Equilibrium Concepts and Examples from U.S. Health Care’ (2011) 1, available at <<http://ssrn.com/abstract=2206980>> accessed 6 May 2023. This may encompass the employment of existing governance arrangement, or crafting of a brand new framework ibid 171-172.

¹⁸⁴ Vicente and Elinor Ostrom Workshop in Political Theory and Policy Analysis, (2011) Working Paper No. W11-3, available at: <<http://ssrn.com/abstract=2206980>> 1, 3.

¹⁸⁵ See Elinor Ostrom (n 184) 8-10; Elinor Ostrom, *Public Entrepreneurship: A case Study in Ground Water Basin Management* (1965) (unpublished Ph.D. dissertation, Univ. Of Calif., Los Angeles); Elinor Ostrom and Harini Nagendra, ‘Insights on Linking Forests, Trees, and People from the Air, on the Ground, and in the Laboratory’ (2006) 103 PROC. NAT’L. ACAD. SCL 19224-25.

¹⁸⁶ See e.g., Elinor Ostrom, ‘Beyond Markets and States: Polycentric Governance of Complex Economic System’ (2010) 100 AM. ECON. REV. 641, 656.

¹⁸⁷ Interview with Elinor Ostrom, Distinguished Professor, Indiana University-Bloomington, in Bloomington, Ind. (13 October 2010).

maintainability.¹⁸⁸ In other words, for the fact that no particular corpus or corpuses is in charge of this system, hesitation and procrastination may be the order of the day,¹⁸⁹ which is in the area of cyber security can have notable and consequential adverse network results. There are as well ethical and diplomatic difficulties to consider. First, polycentric regime may ensue in what Professor Garrett Hardin named “lifeboat ethics” which supports the theory that in circumstances where it is hard and unfeasible to conserve access to the commoners, the poor are frequently abandoned.¹⁹⁰ In the context of cyber-attacks, this may take the shape of developing State corporations being powerless to safeguard their websites or investments because of a dearth of beneficial BITs absent of a multilateral investment mechanism, as well as some cyber super-power nations being reluctant to broker a deal on cyber security matters in a small assembly due to their present unequal advantages, like the United States and China. That is the reason it is crucial to combine multilateral advancement with bottom-up - (proceeding from the bottom or beginning of a hierarchy or process upwards; non-hierarchical) schemes to successfully control international collective-action difficulties such as cyber threats.

Yet, many of the BITs signed around the world contain a changeable system of investor security which in some manner could be regarded as comparable to, or even illustrative of, polycentric regime, particularly when combined with local, territorial, and multilateral laws. Instead of a reincarnation of the Hull Rule or creation of a new multilateral treaty on investor security that may congest the original and new bottom-up most excellent practices, bilateral investment treaties may well offer a helpful channel for promoting cyber protection that protects websites and computers by assisting to discovering and applying domestic most excellent methods resulting to useful network effects¹⁹¹ like beefing up cyber-attack protection. As time goes by, this kind of polycentric process may even accelerate to the birth of a brand new traditional international law that offers foreign investors rights that contains resilient cyber security and protection if it is continuously practiced and adopted.

10. CYBER SECURITY AND TRADITIONAL INTERNATIONAL LAW OF INVESTMENT DISAGREEMENT

BITs depict a reliable commitment due to the scope of actual result costs that they produce, encompassing political, independent, adjudication, and reputational harms associated in their performance and breach. Has the accumulative effect of many thousands of BITs now established a brand-new rule of traditional international law to replace the disused

¹⁸⁸ See Robert O. Keohane and David G. Victor, “The Regime Complex for Climate Change” (2011) 9(1) *Perspective on Politics* 19.

¹⁸⁹ See Elinor Ostrom (n 182) 554-55 (reassessing few of the purposes to depending on polycentric rule to tackle international environmental change, encompassing “leakage, unstable strategies, improper certification, gaming the mechanism, including free riding”).

¹⁹⁰ See Garrett Hardin, ‘Lifeboat Ethics: The Case Against Helping the Poor’ (1974) *PSYCHOL, TODAY, SEPT.* at 38.

¹⁹¹ cf Neal K. Kayal, ‘The Dark Side of Private Ordering: The Network/Community Harm of Crime’ in Mark F. Grady and Francesco Paris (eds), *The Law and Economics of Cybersecurity* (Cambridge University Press 2006) 193, 193-94.

Hull Rule? Taking into account the enormous number of BITs now in operation in the world, one would ask, how connected and general is BIT membership? Do investors at the present days fail to appreciate the value of these principles of BITs to such an extent too, as they failed to appreciate during the time of Hull Rule?

Few have claimed that this link has accelerated to the development of a traditional international law in investment. For instance, Professor Bernard Kishoiyan, has argued that “every bilateral investment treaty is nothing less but a *lex specialis*” - (law governing a specific subject matter) “among parties fashioned to establish a reciprocal system of investment security.”¹⁹² On the other hand, in the viewpoint held by Professor Asoka Gunawardana, he states that, “despite the fact that the clauses of bilateral investment promotion and security treaties might not have reached the position of traditional international law, undoubtedly they have a role to play in this aspect.”¹⁹³ This leads to the posing of a question drawn from a ruling in one particular ICJ decision. Can there be any sense at present of legitimate duty, and practice, suggestive of such a duty? In answering this question, the ICJ stated in *North Sea Case*, as follows:

“Not only should the conducts concerned constitute a settled custom, but they should as well be the type, or be commissioned in the type of manner, as to be evidence of a conviction that this practice is provided mandatorily through the existence by a particular principle of law necessitating it... The countries affected should accordingly perceive that they really are complying with what constitutes to a legal duty.”¹⁹⁴

The regularity or even customary nature of the conducts is not by itself sufficient.¹⁹⁵ As this has been indicated previously, the content of Bilateral Investment Treaties can differ broadly, particularly in respect to the insertion of cyber security protection, making it improbable that there is yet enough State custom to point to a developing traditional international concept of cyber security protection. However, the signed BITs that are already in existence may be a starting point to start making a law regarding cyber-attacks and cyber security protection generally, for example, the proposed BIT between the United States and China should endeavour to incorporate it.

11. ADVANTAGES AND DISADVANTAGES OF EMPLOYING INTERNATIONAL INVESTMENT LAW TO MAKING LAW OF CYBER SECURITY PROTECTION

The need to promote cyber security to the global community can never be downplayed or underrated. Actually, in 2013, associates of the Wassenaar Arrangement - a union of forty one Western countries (encompassing the US) that was formed to limit the escalation

¹⁹² Bernard Kishoiyan, ‘The Utility of Bilateral Investment Treaties in the Formulation of Customary International Law’ (1994) 14 Nw. J. INT’L L. & BUS 327, 329.

¹⁹³ Asoka de Z. Gunawardana, ‘The Inception and Growth of Bilateral Investment Promotion and Protection Treaties’ (1992) 86 AM. Soc’v INT’L L. PROC. 544, 550.

¹⁹⁴ *North Sea Continental Shelf (Federal Republic of Germany v Denmark; F.R.G. v Netherlands)* (1969) I.C.J. Rep. 3, 44.

¹⁹⁵ Oscar Schachter, Editorial Comment, “Compensation for Expropriation” (1984) 78 AM. J. INT’L L. 121, 126 (“As a common principle, the tautology of general provisions in BITs does not establish or promote an inference which those provisions express traditional law. To continue with such an assertion of practice one ought to demonstrate that aside from the convention itself, the principles in the provisions are contemplated mandatory.”).

of possibly perilous goods and technology - recommended “a treaty that was supposed to put delicate cyber security scientific knowledge on equal footing with regular weaponry.”¹⁹⁶ The requirement for cross-border extraterritorial collaboration in enhancing cyber security turns even more importance considering the international amalgamation of economic projects joined with the swift development of scientific transformation. In a nutshell, the function of data management appears growingly bigger in the commercial growth of respective States. “If it may be stated that during the 19th century the general nationwide power of a State depended on the gold it reserves, it means during the 21st century the general nationwide power of a State depends on the scale by which intellectual property prerogatives”-cum general cyber security- “rights are benefitted by its populace and its companies.”¹⁹⁷

Investment law creates an important basis for the necessitated legislation of cyber peace appropriate beneath the limit, which is the armed threat margin. Whilst a lot of work seems to have been carried out to explain the meaning of international law operating in the department of armed conflict law, relatively scanty work has been carried out to influence or pressurise international law into supervising the increasing regularity of global cyber-attacks, encompassing websites and computers. This is a shocking exclusion or unfilled gap considering the proliferation of helpful comparable schemes which may be applied to promote cyber protection. Bilateral investment treaties and international law indicates a possible untapped means to start the exercise of building a regulation of cyber security in generality.

Generally, “Bilateral investment treaty-making pursuit skyrocketed within 1990s”¹⁹⁸ and “reached the lowest bottom in 2012.”¹⁹⁹ In spite of the dwindling number of fresh BITs, the amount of investor cum State arbitrary litigation has risen. For example, in 2012, fifty eight of these types of claims were lodged representing “the biggest digit of familiar ... application ever lodged in a single year and reaffirming alien investors’ heightened tendency

¹⁹⁶ Sam Jones, ‘Cyber security Exports to Face Same Controls as Weapon Sale’ *FIN. TIMES*. (5 December. 2013), at 1 (“Cyber protection software and hardware can be one of the most rapidly growing fields of the protection industry however the transactional disposal and employment of various individually-developed scientific knowledge has till today merely been supervised on an ad hoc position by respective States.”).

¹⁹⁷ Shan Hailing (n 157) 13. After three former employees of a U.S. corporation, Eli Lilly, were charged on a federal inducement of dispatching trade confidential owned by the medicinal drug corporation to a rival Chinese firm, the United States lawyer dealing with the lawsuit “assert the stealing as an offence against the country.” The Herald-Times ‘Indictment: Ex-Lilly Workers Sold Company Secrets to China’, *Bloomington Herald-Times* (10 October 2013), <<https://www.heraldtimesonline.com/story/news/2013/10/10/indictment-ex-lilly-workers-sold-company-secrets-to-china/47390995/>> accessed 20 July 2023.

¹⁹⁸ See UNCTAD, World Investment Report 2013: Global Value Chains: Investment and Trade for Development 108 (2013), available at: <http://unctad.org/en/publicationsLibrary/wir2013_en.pdf> accessed 20 July 2023.

¹⁹⁹ See Reuters, ‘US Charges Chinese Wind Company with Stealing Trade Secrets’, (CNBC, 27 June 2012), <<http://www.cnbc.com/id/100851053>> accessed 20 July 2023 (Just 20 bilateral investment treaties were finalised in 2012, that was the least figure within the last quarter century).

to use investor-State adjudication²⁰⁰ The growing number of arbitrary petitions shows the significance of an incessant use of BITs as a component of the polycentric legal method to enhance cyber security and encourage investor-State adjudication as a medium to resolving disagreement and delivering

12. CONCLUSION

This article has analysed the development of BITs which has emerged out of the need to accord multilateral investment protection to cyber security in general and digital assets in particular. It seems that interpreting a responsibility on the host countries side to afford cyber protection to foreign investors in respect of digital assets, especially website and computer systems, by applying the standard of FPS standard into a bilateral investment treaty will be hard to achieve considering the explained factors above. Whilst the State may have some obligations to control the stability of fundamental cyber security mechanisms within its territory, it is arguable that this could be expanded to protection for specific servers and websites that are being monitored by private or individual service providers (non-governmental) or which is being controlled by investors, and sudden crisis peculiarities could invalidate State culpability for such big magnitude cyber-attacks. A nation's duty to initiate proceedings against cyber offenders can arguably be said to be more probable, nevertheless legislation of this kind is not common, and even non-uniform, and as a result it is going to be extremely hard to match this duty in the environmental sphere of the principle of FPS that has appeared under international law with remedial recompense, that kind of an omission is likely to be challenging. Even in a situation where the FPS principle would be used to accord digital investment security upon cyber-threats, modern day tribunal rulings have suggested that the obligations of FPS is associated with the scale of advancement or development existing in the host country, and also the type of attacks that happens. Since it is only a small number of less developed countries that have an improved standard of global computer network connection systems, it is unlikely that foreign investors would anticipate an intensive degree of cyber protection in these countries.

Explicitly, FPS provision ambit will base its exact phraseology on the BIT legal document where it emerges. A particular reference to computer and websites networks in the definition of covered investment in a BIT where the provision relates to it, or reference to cyber security in general would help an arbitral tribunal in upholding whether the host nation had contravened its FPS responsibilities in a situation where digital assets have been stolen or harmed because of an organised cyber operation. Again, it would be sensible for domestic countries of where the foreign investors hail to impute a clear mention to protection against cybercrime or threats on data networks in their BITs. Considering the growing threat of cyber based attacks on computers and websites against companies and governments, ter-

²⁰⁰ See Andrew T. Guzman, 'Why LDCs Sign Treaties That Hurt Them: Explaining the Popularity of Bilateral Investment Treaties' (1998) 38 VA. J. INTL L. 639, 649-50, ("By the last quarter of 2012, entire figure of renowned cases (finalised, awaiting or withdrawn) amount to 514, including the entire number of States which have answered to a single or more than one Investment-State Dispute Settlement (ISDS) allegations skyrocketed to 95. The huge bulk of cases persisted to accumulate within the ICSID Protocol including the ICSID Additional Facility Rules (314 claims) and within UNCITRAL Rules (131).

minology of this kind is reasonable and should appear more conspicuously in future BITs, especially in the proposed US-China BIT if it is to succeed. It should also be included in BITs with developing States, if not foreign investors would be left with no judicial remedy and host States attracting investors will bear the large brunt of the risk. Essentially, proving States' accountability in this way must be seen in the guise of optimism in the technological development of less developed countries which presently experience a low intensity of global computer network connection systems and an equally low scale of internet protection and cyber protection in general. There is also some discussion concerning whether BITs protection has attained the level of customary international law. Notwithstanding though, the confluence of these two forces indicate the necessity to attain a new agreement on investor cyber security protection from the bottom-up, which may be comprehended within a polycentric mechanism. To achieve this there is the need to move towards a greater transparency of interpretation that spotlights the possibility of using BITs to protect all bytes and cyber security in general, most especially digital assets in the form of computer systems and websites.

Ideally, the article has found that there is every need to advance the concept of FPS to cover the epidemic of cyber-attacks that besiege investments nowadays due to the threats imposed by advancing technology. The interpretation of FPS standard needs to be amended in order to face up with the challenges that go with the existence of attacks that foreign investors have to confront with in the twenty-first century, especially the unity of digital businesses like computer systems including websites against threats imposed upon the internet connections, also otherwise known as cyber security. Since a digital asset is classified as an investment therefore it should be covered under the protective umbrella of FPS. Again, as it has been depicted by case law, that customary international law is not stagnant in time and minimum international law does develop. For this reason, it is imperative to apply the standard of FPS to provide protection to investment that goes beyond physical protection to providing protection to digital security and cyber threats in generality.

As the study has often stated, the extent of digital offence is great and has been statistically put at the approximate loss of a trillion US dollars. However, having surveyed the threat of cyber security, and especially on how digital assets is managed and controlled generally, imposing FPS obligation on host country for the security of foreign investors' cyber protection, especially in the field of digital asset protection, will be very hard to achieve. This is so because, although government may have some part to play in maintaining the solidarity of hidden internet infrastructure within its domain, it is not feasible that this could be broadened to protection for a particular server or to a website as these are left in the hands of private service providers and governments do not have power or control over its management. Unless the infrastructure like internet servers is left in the hands of the states for them to have control over their management. Even at that, an emergency exception could exonerate country liability for any big scale attack on foreign investors' digital investments. Also, a host country's duty to initiate proceedings against cyber perpetrators will be very little because the legislation in this environment is universally scarce in international law and as a result it will be hard to attach this duty within the purview nature of FPS principle,

unless the obligation is inserted in FPS standard in BITs.

This article has laid down some ground rules on how to tackle cyber criminality on digital investment and cyber security in general. One of the ways to provide security to digital assets under the clause of FPS in BITs is the expansion of the application of mandatory permits that necessitates stronger regulation to tarpaulin cyber threats. The criminalisation of this type of conduct and the heightening of lawsuits against persons are all important apparatus against computer attacks by private persons or business opponents that engage themselves in cyber threats. However, this method will suffer a hiccup when the perpetrator is the country itself. For this reason, the solution to solving this problem will be to engage in a commercial and economic integration which is at the heart of cyber protection and BITs in the relevant of FPS which will channel and galvanise such a concept. The employment of BITs in this manner enables claims of cyber-attacks not only be initiated by foreign investors but also can be settled in international arbitration bodies. The employment of adjudication offers advantages, like the use of an impartial setting for rulings of cases, well-established rules of arbitration and implementation of awards, and access to and application of well-created investor-dispute focused arbitration organisations. Additionally, initiating the claim at ICSID under a BIT agreement permits a foreign investor to start an arbitral claim upon the host country within investor-State adjudication without the need to appeal to its State government to start dispute settlement proceedings. Moreover, a more addictive phrase could be inserted in the standard of FPS obligation under BITs, to cover computer attacks security protections necessitating a polycentric principle to enhancing cyber protection and building a legislation of international cyber protection.

BIBLIOGRAPHY

- 20th Global Information Security Survey 2017–18, Cybersecurity regained: preparing to face cyber attacks, <https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/digital/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf> accessed 20 June 2023
- Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* [2010] I.C.J. Rep. 403
- ADF Group Inc v US* ICSID Case No. ARB(AF)/00/1 (NAFTA), Award, 9 January 2003
- Agreement between Japan and the Republic of Colombia for the Liberalisation, Promotion and Protection of Investment (12 September 2011), <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/797/download>> accessed on 5 May 2023
- Agreement between Japan and the Republic of Peru for the Promotion, Protection and Liberalisation of Investment article 10 (21 Nov. 2008), <<https://www.iisd.org/toolkits/sustainability-toolkit-for-trade-negotiators/wp-content/uploads/2016/06/1733.pdf>> accessed on 5 May 2023
- Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organisation, (Marrakesh, Morocco 15 April 1994), *available at*: <https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm>
- Agreements II 24. <http://unctad.org/en/Docs/diaeia20102_en.pdf> accessed on 17 April 2023
- Alperovitch D., ‘Reveal: Operation Shady Rat’ (McAfee, 6 Sep. 2011), <<http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf>> accessed 2 May 2023
- American Law Institute Third Restatement of Foreign Relations Law Section 402(1) (C) (1987)
- AMT v Democratic Republic of Congo*, ICSID Case No. ARB/93/1, Award, 21 February 1997
- Asian Agricultural Products v Republic of Sri Lanka*, (1990) ICSID case No. ARB/87/3. Final Award

- August R., 'International Cyber-Jurisdiction: A Comparative Analysis' (2002), *American Business Law Journal* 531
- Azurix and Argentina* (2006), ICSID Case No. ARB/01/12, Award, 14 July 2006
- Baker S., Waterman S. and Ivanov G., 'In the Crossfire: Critical Infrastructure in the Age of Cyber War' <<https://www.govexec.com/pdfs/012810j1.pdf>> accessed 13 July 2023
- Ball J., Borger J. and Greenwald G., 'Revealed: how US and UK spy agencies defeat internet privacy and security', *The Guardian* (6 September 2013) <<https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>> accessed 25 June 2023
- BBC, 'China Hit by "Biggest Ever" Cyber-Attack' *BBC News* (27 Aug. 2013), <<http://www.bbc.co.uk/news/technology-2385041>> accessed 2 May 2023
- BBC, 'Cybercrime Threat on the Rise, Says PwC Report', *BBC News* (26 March 2012) <<http://www.bbc.co.uk/news/business-17511322>> accessed 12 April 2023
- BBC, 'NHS cyber-attack: GPs and hospitals hit by ransomware' *BBC News* (13 May 2017) <<https://www.bbc.com/news/health-39899646>>
- Bello J.H., *Editorial Comment*, 'The WTO Dispute Settlement Understanding: Less Is More', (1996) 90 *Am. J. INT'L L.* 416
- Berger A., 'Investment Rules in Chinese Preferential Trade and Investment Agreements: Is China Following the Global Trend Towards Comprehensive Agreement?' (2013) 7 *German Dev. Inst.*, 1. <http://www.die-gdi/uplots/media/DP_7.2013.pdf> accessed on 5 May 2023
- Bernhard von Pezold and others v Republic of Zimbabwe* [2015] ICSID Case No. ARB/10/15, para. 597
- Bilateral Investment Treaty between Argentina and United States of America 1991 (Investment Policy Hub, 20 October 1994) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/127/download>> accessed 20 June 2023
- Bilateral Investment Treaty between Canada and Peru, (Investment Policy Hub, 20 June 2006), Article 1. <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/626/download>> accessed 21 May 2023
- Bilateral Investment Treaty between Germany and Bosnia and Herzegovina 2001. (Investment Policy Hub, 11 November 2007) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bit/606/bosnia-and-herzegovina---germany-bit-2001->> accessed on 14 April 2023
- Bilateral Investment Treaty between Poland and United States of America 1990 (Investment Policy Hub, 6 August 1994) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5339/download>> accessed 20 July 2023
- Bilateral Investment Treaty between Ukraine and Denmark, (Investment Policy Hub, 29 April 1994) <<https://investmentpolicy.unctad.org/international-investment-agreements/treaties/bit/1291/Denmark---ukraine-bit-1992->> accessed 21 May 2023
- Bryant C., 'NSA Claims Put German Business on Guard', *FIN. TIMES* (1 Nov. 2013) at 4
- Calia K., Veraneau J. and Fagan D. et al., 'Economic Espionage and Trade Secret Theft: An Overview of the Legal Landscape and Policy Responses', (2013), Covington & Burling LLP, 3. <<https://bpb-us-e2.wpmucdn.com/wordpress.auburn.edu/dist/8/7/files/2021/01/economic-espionage-and-trade-secret-theft.pdf>> accessed on 12 April 2023
- Carr I. (ed), *Computer Crime* (Ashgate 2009)
- Case Concerning United States Diplomatic and Consular Staff in Tehran (US v Iran)* [1980], I.C.J Rep. 3, paras 67-68
- Case of the S.S. 'Lotus' (France v Turkey)* [1927], P.C.I.J Judgement Series A, No 10
- Cashell B., Jackson WD., Jickling M., and Webel B., 'The Economic Impact of Cyber-Attacks Congressional Research Service, the Library of Congress' (2004), CRS Report for Congress. <https://sgp.fas.org/crs/misc/RL32331.pdf> accessed 18 May 2023
- Cha A. E. and Nakashima E., 'Google China Attack Part of Vast Espionage Campaign' *NBC News* (14 January 2010) <<https://www.nbcnews.com/id/wbna34855470>> accessed 20 June 2023

- Cole D. H., 'From Global to Polycentric Climate Governance' (2011) 2 *CLIMATE L.* 395
- Collier K., 'Sen. Ron Wyden on the Problems with the Trans-Pacific Partnership', *DAILYDOT* (19 September 2012) <<http://www.dailydot.com/politics/ron-wyden-trans-pacific-partnership/>> accessed on 5 May 2023
- Collins D., 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' (2011) 12 *Journal of World Investment and Trade* 225
- Congyan C., 'China-US BIT Negotiations and the Future of Investment Treaty Regime: A Grand Bilateral Bargain with Multilateral Implications' (2009) 12 *J. INT'L L.* 457
- Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)* [1949] I.C.J. Rep, 4
- Cotula L., 'Is the Tiding Turning for The Africa's Investment Treaties?' (IEDD, 8 March 2013) <<http://www.iied.org/tide-turning-for-africa-s-investment-treaties>> accessed on 5 May 2023
- Council of Europe Convention on Cybercrime, Budapest 23. XI.2001, *European Treaty – No. 185*
- Council of Europe, Convention on Cybercrime, 23 November 2001, Eur. T.S. No. 185. <<https://rm.coe.int/1680081561>> accessed 20 May 2023
- Crelinsten R. D., 'Terrorism and Counter-Terrorism in a Multi-Centric World: Challenges and Opportunities' in M. Taylor and J. Hogan (eds), *the Future of Terrorism* (Routledge 2006)
- Deighton B. and Breidhardt A., 'EU confronts U.S. over reports it spies on European allies', *Reuters* (30 June 2013) <<https://www.reuters.com/article/uk-usa-eu-spying-idUKBRE95S0B720130630>> accessed 25 June 2023
- Dolzer R. and Schreuer C., *Principles of International Investment Law* (OUP 2008)
- Draetta U., 'The Internet and Terrorist Activities' in A Bianchi (ed), *Enforcing International Law Norms against Terrorism* (Hart 2004)
- Draft articles on responsibility of States for internationally wrongful acts, Text adopted by the International Law Commission at its fifty-third session [2001] YILC Vol II Part 2, Articles 1-2. [ARSIWA]
- Eckert P. and Yukhananov A., 'U.S., China Agree to Restart Investment Treaty Talks', *Reuters* (12 July 2013) <<https://www.reuters.com/article/uk-usa-china-dialogue-trade-idUKBRE96B04F20130712>> accessed 4 May 2023
- European Convention on Cybercrime (Budapest Convention 2001) <<https://rm.coe.int/1680081561>> accessed 5 May 2023
- Factory at Chorzow (Germany v Poland)* (1928) P.C.I.J, Merits, (ser. A) No. 17, 13 September 1928, para. 47
- Feldman S. E. and Rollo S. L., 'Extraterritorial Protection of Trade Secret Rights in China: Do Section 337 Actions at the ITC Really Prevent Trade Secret Theft Abroad?' (2012) 11 *J. Marshall REV.INTELL. PROP. L.* 523
- Khan J. F., 'Brussels Opposes German Data Protection Push' *FIN. TIMES* (5 November 2013)
- Freeman A.V., 'Responsibility of States for Unlawful Acts of their Armed Forces' (1956) 88 *Recueil des Courts* 261
- Friedman A.A., 'Cybersecurity and Trade: National Policies, Global and Local Consequences' (2013) *Brookings Inst.* <<https://www.brookings.edu/wp-content/uploads/2016/06/BrookingsCybersecurityNEW.pdf>> accessed 5 May 2023
- Garnet R. and Clarke P., 'Cyber terrorism: A New Challenge in International Law' in A Bianchi (ed), *Enforcing International Law Norms against Terrorism* (Hart 2004)
- Genocide Judgement (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] I.C. J. Rep 43
- Gordon K. and Pohl J., *Environment Concerns in International Investment Agreements: A Survey 5* (2011) (OECD Working Papers on International Investment No. 2011/1) <https://www.oecd.org/daf/inv/internationalinvestmentagreements/WP-2011_1.pdf> accessed 5 May 2023
- Gorman S., 'Broad New Hacking Attack Detected' *Wall St. Journal* (18 Feb. 2010) <<https://www.wsj.com/articles/SB10001424052748704398804575071103834150536>> accessed 2 May 2023
- Gross M. J., 'Enter the Cyber-Dragon' (Vanity Fair, Sept. 2011) <<https://www.vanityfair.com/news/2011/09/chinese-hacking-201109>> accessed on 16 April 2023

- Grow B. and Horsenball M., 'Special Report: In Cyberspy v Cyberspy, China Has the Edge', *Reuters* (Apr 14 2011), <<http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTR73D24220110414>> accessed 18 April 2023
- Gunawardana A. Z., 'The Inception and Growth of Bilateral Investment Promotion and Protection Treaties' (1992) 86 AM. Soc'v INT'L L. PROC. 544.
- Guzman A.T., 'Why LDCs Sign Treaties That Hurt Them: Explaining the Popularity of Bilateral Investment Treaties' (1998) 38 VA. J. INTL L. 639.
- Habyeyev R. and Kaya S., *A Critical Role of Diplomatic Protection in Investor-State Disputes* (On İki Levha 2021)
- Hailing S., *The Protection of Trade Secrets in China*, (2nd edn, Kluwer Law International 2012)
- Hardin G., 'Lifeboat Ethics: The Case Against Helping the Poor' (1974) PSYCHOL. TODAY SEPT.
- ICSID Convention, Rules and Regulation 2006, <<https://icsid.worldbank.org/sites/default/files/ICSID%20Convention%20English.pdf>> accessed 20 June 2023
- Interview with Elinor Ostrom, Distinguished Professor, Indiana University-Bloomington, in Bloomington, Ind. (13 October 2010)
- Island of Palmas (Netherlands v US)* [1928] RIAA Vol. II, 829, 838
- Jacobs A., 'After Reports on N.S.A, China Urges End to Spying' *New York Times* (24 March 2014) <<https://www.nytimes.com/2014/03/25/world/asia/after-reports-on-nsa-china-urges-halt-to-cyberspying.html>> accessed 2 May 2023
- Jones A. and Helft M., 'Google, Citing Attack, Threatens to Exit China' *New York Times* (12 January 2010) <<https://www.nytimes.com/2010/01/13/world/asia/13beijing.html>> accessed 2 May 2023
- Jones S., Nevile S., Pickard J. and Chaffin J., 'NHS Hackers Used Stolen Cyber Weapons from US Spy Agency', *Financial Times, FT Weekend* (13 May, 2017) <<https://www.ft.com/content/e96924f0-3722-11e7-99bd-13beb0903fa3>> accessed 20 June 2023
- Jones S., 'Cyber security Exports to Face Same Controls as Weapon Sale', *FIN. TIMES* (5 December 2013)
- Kariyawasam R., *International Economic Law and Digital Divide: A New Silk Road* (Edward Elgar 2007)
- Kayal N. K., 'The Dark Side of Private Ordering: The Network/Community Harm of Crime' in Grady M. F. and Francesco P. (eds), *The Law and Economics of Cybersecurity* (Cambridge University Press 2006)
- Keohane R. O. and Victor D. G., 'The Regime Complex for Climate Change' (2011) 9(1) *Perspective on Politics* 19
- Kishoiyian B., 'The Utility of Bilateral Investment Treaties in the Formulation of Customary International Law' (1994) 14 Nw. J. INT'L L. & BUS 327
- Lee D. 'New York Times and Twitter Struggle After Syrian Hack', *BBC News* (28 Aug. 2013) <<http://www.bbc.co.uk/news/technology-23862105>> accessed 2 May 2023.
- Lewis J. A., 'Conflict and Negotiation in Cyberspace' (2013) CTR. STRATEGIC & INT'L STUD 49
- LFH Neer and Pauline Neer v United Mexican States*, [1926] US-Mexican General Claims Commission, Decision, 4 UNRIAA 60
- Littman D. and Posner E., 'Holding Internet Service Providers Accountable' in Grady M. F. and Francesco P. (eds), *The Law and Economics of Cyber Security* (Cambridge University Press 2006)
- Lowrey A., 'U.S. and China to Discuss Investment Treaty, but Cyber security is a Concern', *New York Times* (12 July 2013), <<https://www.nytimes.com/2013/07/12/world/asia/us-and-china-to-discuss-investment-treaty-but-cybersecurity-is-a-concern.html>> accessed 15 April 2023
- MacAskill E., 'Countries Are Risking Cyber Terrorism: Security Expert Tells World Summit', *The Guardian* (5 May 2010) <<https://www.theguardian.com/technology/2010/may/05/terrorism-uksecurity>> accessed 2 May 2023
- Marble I., *The Calculation of Compensation and Damages in International Investment Law* (OUP 2009)
- Mass P. and Rajagopalan M., 'Does Cybercrime Really Cost \$1 Trillion?', (Propublica, 1 August 2012) <<http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion>> accessed 12 July 2023
- McAfee, 'Protecting Your Critical Assets: Lessons Learned from: Operation Aura' [2010], McAfee

- Labs and McAfee Foundstone Professional Services, 3. <http://www.wired.com/images_blogs/threatlevel/2010/03/operationaura_wp_0310_fnl.pdf> accessed 25 April 2023
- McGauran W., 'Intended Consequences: Regulating Cyber Attacks' (2009) 12 *Tulane Journal of Technical and Intellectual Property* 259
- McGinnis M. D., 'Costs and Challenged of Polycentric Governance: An Equilibrium Concepts and Examples from U.S. Health Care' 1, <<http://ssrn.com/abstract=2206980>> accessed 6 May 2023
- McVeigh K., 'NSA Surveillance Program Violates the Constitution, ACLU Says' *Guardian* (27 August 2013) <<http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit>> accessed 2 May 2023
- Military and Paramilitary activities against Nicaragua, (Nicaragua v United States of America)* [1986] I. C. J. Rep. 14
- MNSS B.V. and Recupero Credito Acciaio N.V. v Montenegro* [2016] ICSID Case No. ARB (AF) 12/8, para 356
- Moss G. C., 'Full Protection and Security' in August Reinisch (ed), *Standards of Investment Protection* (OUP 2008) 134
- Mossman M. L., 'Essay, Enforcement of WTO Rulings: An Interest Group Analysis' (2013), 32 *HOFSTRA L. REV.* 1
- Multilateral Investment Guarantee Agency, 'Investment Guarantee Guide' <<http://www.miga.org/documents/IGGenglish.pdf>> accessed 5 May 2023
- Noble Ventures Inc. v Romania* (2005) ICSID Case No. ARB, Award, 12 October 2005
- North Sea Continental Shelf (Federal Republic of Germany v Denmark; F.R.G. V Netherlands)* (1969) I.C.J. Rep. 3
- O'Hara G., 'Cyber-Espionage: A Growing Threat to the American Economy' (2010) 19 *CommLaw CONSPECTUS* 24
- Opinion of Mr Advocate General Darmon, Joined Cases 89, 104, 114, 116, 117, and 125-9
- Organisation for Economic Co-operation and Development (OECD), 2002, Art. III.3 <<https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm>> accessed 20 June 2023
- Osakeyhtiö and Others v Commission [in re Wood Pulp Cartel] paras 20-1. 1994 E.C.R. I-100*
- Ostrom E. and Nagendra H., 'Insights on Linking Forests, Trees, and People from the Air, on the Ground, and in the Laboratory' (2006) 103 *PROC. NAT'L. ACAD. SCL* 19224.
- Ostrom E., 'Beyond Markets and States: Polycentric Governance of Complex Economic System' (2010) 100 *AM. ECON. REV.* 641.
- Ostrom E., 'Polycentric Systems for Coping with Collective Action and Global Environmental Change' (2010) 20 *GLOBAL ENVIL. CHANGE* 550.
- Ostrom E., *Public Entrepreneurship: A case Study in Ground Water Basin Management* (1965) (unpublished Ph.D. dissertation, Univ. Of Calif., Los Angeles)
- Palmer D. 'US, EU start free-trade talks despite spying concerns' *Reuters* (9 July 2013), <<https://www.reuters.com/article/us-usa-eu-trade/us-eu-start-free-trade-talks-despite-spying-concerns-idUSBRE96704F20130708>> accessed 20 June 2023.
- Pantehniki Contactor & Engineers v Albania* (2009) ICSID Case No. ARB/07/21, Award, 30 July 2009
- Paris Convention for the protection of Industrial Property (1979), *available at*: <http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html#p213_35515>
- Passeri P., 'What is a Cyber Weapon?' (Hackmsgedon, 22 April 2012), <<http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit>> accessed 12 April 2023
- Pauwelyn J., 'Different Means, Same End: The Contribution of Trade and Investment Treaties to Anti-Corruption Policy' in Susan Rose-Ackerman and Paul D. Carrington (eds), *Anti-Corruption Policy: Can International Actors Play a Constructive Role?* (Carolina Academic Press 2013)

- Poeter D., 'Microsoft Joins Ranks of the Tragically Hacked', (PCMAG, 22 February 2013,) <www.pcmag.com/articl2/0,2817,2415787,00.asp> accessed 29 April 2023
- Powers D., 'Cyber law: The Major Areas, Development and Information Security Aspects' in H. Bidgoli (ed), *Global Perspectives in Information Security* (John Wiley and Sons Inc. 2009)
- Proce D. M. and Smart M. J., 'BIT by BIT: A Path to Strengthening US-China Economic Relations' [2013] 1 <<http://www.paulsoninstitute.org/wp-content/uploads/2016/07/BIT-by-BIT-English.pdf>> accessed 4 May 2023
- Prosecutor v Dusko Tadic a.k.a. 'Dule'* [1997] International Criminal Tribunal for Former Yugoslavia, IT-94-1-T
- Qui T., 'How Exactly Does China Consent to Investor-State Arbitration: On the First ICSID Case Against China' (2012) 5 CONTEMPORARY ASIA ARB. J. 265
- R v Graham Waddon*, 2000 WL 41456 (2 April 2000)
- Rantala R. R., Bureau of Justice Statistics, U.S. Dep't of Justice NO. NCJ 221943, *Cybercrime against Business*, 2005 1, 3 (2008), available at: <<http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf>>
- Raustiala K. and Victor D. G., 'The Regime Complex for Plant Genetic Resources' (2004) 58 INT'L ORG. 277
- Report of the International Law Commission on the Work of its Fifty-third Session, Commentary to the Articles on the Responsibility of States for Internationally Wrongful Acts, [2001] YILC Vol. II Part 2. [ARSIWA Commentary]
- Reuters, 'US Charges Chinese Wind Company with Stealing Trade Secrets', (CNBC, 27 June 2012), <<http://www.cnbc.com/id/100851053>>
- Rid T., *Cyber War Will Not Take Place* (OUP 2013)
- Salacuse, J., *The Law of Investment Treaties* (OUP 2010)
- Schachter, O., Editorial Comment, 'Compensation for Expropriation' (1984) 78 AM. J. INT'L L. 121
- Schmitt M. N., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013)
- Sergei v Government of Mongolia* (2011) Award on Jurisdiction and Liability, 28 April 2011. <<https://jsumundi.com/fr/document/decision/en-sergei-paushok-cjsc-golden-east-company-and-cjstvostokneftegaz-company-v-the-government-of-mongolia-award-on-jurisdiction-and-liability-thursday-28th-april-2011>> accessed 5 May 2023
- SGS Societe Generale de Surveillance SA v Islamic Republic of Pakistan* [2003] ICSID Case No. ARB/01/13, 13, under the Swiss-Pakistan BIT (entered into force 6 May 1996)
- Shackelford S. J., *Managing Cyber Attacks in International Law, Business and Relations: In Search of Cyber Peace* (Cambridge University Press 2014)
- Shackelford S. J., 'In Search of Cyber Peace: A Response to the Cyber security Act of 2012', (2012), 64 STAN. L. REV. ONLINE 106 <<http://www.stanfordlawreview.org/online/cyber-peace>> accessed 6 May 2023
- Shackelford S. J., 'From Nuclear War to Net War: Analogizing Cyber Attacks in International Law', (2009), BERKELEY J. INT'L L. 192
- Shackelford S. J., 'Towards Cyber Peace: Managing Cyber Attacks through Polycentric Governance' (2013) 63 AM. U.L. REV. 1273
- Shackelford S. J. and et al, 'Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties' (2015) 52 (1) American Business Law Review 1
- Shackkelton S., 'Estonia Three Years Later: A Progress Report on Combating Cyber Attacks' [2010] Journal of Internet Law 22
- Shalhoub Z. K. and Al Qasimi S.L., *Cyber Law and Security in Developing and Emerging Economies* (Edward Elgar Publishing 2010)
- Siemens v Argentina* [2007] ICSID Case No. ARB/02/6
- Sornarajah M., *The International Law on Foreign Investment* (OUP 2010)

- Sullivan R., 'Company: Chinese cyberattack targets Australia' *SMH* (15 April 2010 <<https://www.smh.com.au/technology/company-chinese-cyberattack-targets-australia-20100415-sh1d.html>> accessed 2 May 2023
- Susan M., 'The Critical Challenge from International High-Tech and Computer Related Crime at the Millennium' (2009) *Duke Journal of International and Comparative Law* 451
- Swire P. and Ahmad K., 'Encryption and Globalisation', (2012), 13 *COLUM. SCI. & TECH. L. REV.* 416
- Talley I. and Mauldin W., 'U.S., China to Pursue Investment Treaty' *WALL ST. J* (July 11, 2013) <<http://online.wsj.com/news/articles/SB10001424127887324425204578599913527965812>> accessed 4 May 2023
- The Cable, 'Nigeria ranks third in global internet crimes' *The Cable* (23 August 2017) <<https://www.thecable.ng/ncc-nigeria-ranks-third-global-internet-crimes>> accessed 20 July 2023
- The Herald Times 'Indictment: Ex-Lily Workers Sold Company Secrets to China', *BLOOMINGTON HERALD-TIMES* (10 October 2013) <<https://www.heraldtimesonline.com/story/news/2013/10/10/indictment-ex-lilly-workers-sold-company-secrets-to-china/47390995/>> accessed 20 July 2023
- Tom G., 'Seeing the Internet as an "Information Weapon"' (NPR, 23 September 2010) <<http://www.npr.org/templates/story/story.php?storyId=130052701>> accessed 6 May 2023
- Trachtman J., 'Global Cyber terrorism, Jurisdiction and International Organisation' in M. Grady and Paris (eds), *The Law and Economics of Cyber Security* (Cambridge 2006)
- Trail Smelter Case (US v Canada)*, [1941], RIAA Vol. III, 1905, 2963
- Tripathy T., 'India Restricts Telecom Suppliers, carriers' *The National Post (Canada)* (29 July 2010)
- U.S.-China Economic and Security Review Commission (2012) <https://www.uscc.gov/sites/default/files/annual_reports/2012-Report-to-Congress.pdf> accessed 20 June 2023
- U.S.-China Joint Fact Sheet on Strategic and Economic Dialogue, U.S. DEP'T OF TREASURY (12 July 2013). <<https://home.treasury.gov/system/files/136/SEDjointefactsheet072910.pdf>> accessed 20 June 2023
- U.S.-Poland BIT 1990, Annex 3, <<https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5339/download>> accessed 20 July 2023
- UN General Assembly Resolution (1997) 51/210 (16 January 1997)
- UN Security Council Resolution 1373 (2001) S/RES/1373 (28 September 2001)
- UNCTAD, 'Taking of Property', (2002) *available at*: <<http://unctad.org/en/Docs/psiteitd15.en.pdf>> accessed on 5 May 2023
- UNCTAD, 'World Investment Report 2011: Non-Equity Modes of International Production and Development' (2011) <https://unctad.org/system/files/official-document/wir2011_en.pdf> accessed 5 May 2023
- UNCTAD, 'World Investment Report', (2010)
- UNCTAD, World Investment Report 2013: Global Value Chains: Investment and Trade for Development 108 (2013), *available at*: <http://unctad.org/en/publicationsLibrary/wir2013_en.pdf>
- United Nations General Assembly, Report of the United Nations Commission on International Trade Law, Rep. UN. Doc., A/68/17, On its 46th Sess, 8-26 July, (2013) <http://unctad.org/meetings/en/SessionalDocuments/a68d17_en.pdf> accessed 5 May 2023
- United Nations, 'Scope and Definition', [2011] UNCTAD Series on Issues in International Investment
- United Nations, UN World Investment Report 2010 <https://unctad.org/system/files/official-document/wir2010_en.pdf> accessed 5 May 2023
- Vandeveld K. J., *U.S. International Investment Agreement* (OUP 2009)
- Verhoosel G., 'The Use of Investor-State Arbitration Under Bilateral Investment Treaties to Seek Relief for Breaches of WTO Law' (2003) 6, *J. INT'L ECON. L.* 493
- VERIZON, 2023 Data Breach Investigations Report, <<https://www.verizon.com/business/resources/reports/dbir/>> accessed 20 June 2023
- Vicente and Elinor O. Workshop in Political Theory and Policy Analysis (2011) Working Paper No. W11-3,

- , available at: <<http://ssrn.com/abstract=2206980>> At 1, 3
- Watts J., 'Brazilian president postpones Washington visit over NSA spying', *The Guardian* (17 September 2013) <<https://www.theguardian.com/world/2013/sep/17/brazil-president-snub-us-nsa>> accessed 25 June 2023
- Weismann M. M., 'The Convention on Cybercrime: A Harmonised Implementation of International Penal Law: What Prospect for Procedural Due Process' in Indiana Carr (ed) *Computer Crime* (Ashgate 2009)
- Wena Hotels v Egypt* (2002) ICSID Case No. ARB/98/4, Award, 8 December 2002, 41 I.L.M. 896
- Whitehouse S., 'U.S. Sen., Sheldon Speaks in Senate on Cyber Threats', (White House.senate, 27 July 2010), <<http://www.whitehouse.senate.gov/news/speeches/sheldon-speaks-in-senate-on-cyber-threats>> accessed 12 April 2023
- Wilson C., 'Cyber Crime' in Franklin D. Kramer et al (eds), *Cyberpower and National Security* (NDU 2009)
- Wolf R.C., *Trade, Aid, and Arbitrate: The Globalisation of Western Law* (Ashgate 2004)
- Wolf J. B., 'War games Meets the Internet: Chasing 21 Century Cybercriminals with Old Laws and Little Money' [2000] AM. J. CRIM. L. 95
- World Bank Guidelines on the Treatment of Foreign Direct Investment s. IV (1999), available at: <<http://italaw.com/documents/WorldBank.pdf>>
- Yang D.W and Hoffstadt B. M., 'Countering the Cyber-Crime Threat' (2006) AM. CRIM. L. REV, 201
- Zetter K., 'Google Hack Attack Was Ultra Sophisticated, New Details Show' (Wired, 14 January 2010) <<http://www.wired.com/threatlevel/2010/01/operation-aurora/>> accessed 15 April 2023