Designing a Governance System for Cybersecurity of Foreign Investment in Europe[1]

Senior researcher PhD**. Federica CRISTANI**[2]

Abstract

Increased global digitalisation has brought both economic benefits as well as cybersecurity challenges; more and more companies around the world are becoming the target of cyberattacks. The consequences of cyberattack have ranged from money losses and information theft to infrastructure destabilization. Companies face different types of cyber-attacks. In the last years, the most frequent (documented) cyber-threats have been: malware; phishing attacks; spam; denial of service; ransomware; insider threat; data breaches; information leakage; cryptojacking and cyber espionage. In the context of investment protection, cyberattacks may have different targets: data on foreign investments and/or foreign investors that are available in digital forms (including trade secrets) and data related to investment arbitration. While the consequences of cyberattacks are clear, less clear is how to deal this problem at the international (and European) regulatory level. This paper deals with the question of how foreign investment can be secured from cyberattacks within the investment law framework, both at the international and the European law levels. The focus is on which international and European actors are involved in cybersecurity and investment protection policies; the aim is to design a 'map of relevant actors' – by using the social network analysis method – and highlight the relevant relationships.

Keywords: *cybersecurity, foreign investment, European Union, cyber-attacks.*

JEL Classification*:* K22, K24, K33

1. Cybersecurity challenges of foreign investment: an overview

Increased global digitalisation has brought both economic benefits as well as cybersecurity challenges;[3] more and more companies around the world are becoming the target of cyberattacks.[4]

---

[1] The author is very grateful to Dr. Gustavo Prieto and Prof. Daniele Butturini for invaluable comments and suggestions on previous drafts of this paper. All errors remain the author's responsibility.

[2] Federica Cristani - Head of the Centre for International Law at the Institute of International Relations in Prague, Czech Republic; Co-Chair of the Coordinating Committee of the Interest Group on International Economic Law of the European Society of International Law (ESIL), cristani@iir.cz.

[3] UNCTAD, *World Investment Report 2017. Investment and the Digital Economy* (UNCTAD, 2017), 187, http://unctad.org. There is no commonly adopted definition of cybersecurity, cyberattack and cybercrime at the international level. According to the European Union (EU), 'Cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure' (European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication on *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final (7 February 2013), 3).

[4] According to the definition adopted by the EU, 'Cybercrime commonly refers to a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences

In May 2017, the WannaCry ransomware in few hours affected 200,000 computers and the security of hospitals (NHS), public transport (Deutsche Bahn), banks (Deutsche Bank), service providers (Telefónica), delivery services (FedEx), and businesses across the globe.[5] This incident was not an isolated case; cyberattacks to businesses worldwide appear in the news every day.[6]

The consequences of cyberattack have ranged from money losses and information theft to infrastructure destabilization.[7] Companies face different types of cyber-attacks, including: malware; web-based attacks; phishing attacks; spam; denial of service; ransomware; insider threat; data breaches; information leakage; crypto jacking and cyber espionage.[8] In the context of investment protection, cyberattacks may have different targets:[9] data on foreign investments and/or foreign investors that are available in digital forms (including trade secrets)[10] and data related to investment arbitration.[11]

While the consequences of cyberattacks are clear, less clear is how to deal this problem at the international (and European) regulatory level. Overall, the approach to cybersecurity issues appears rather fragmented; one reason could be the difficulty in defining the manifold types of cyber-threats that develop over time.

The following paragraphs deal with the question of how foreign investment can be secured from cyberattacks within the investment law framework, both at the international and the European law levels. The focus is on which international and European actors are involved in cybersecurity and investment protection policies; the aim is to design a 'map of relevant actors' – by using the social network analysis method – and highlight the relevant relationships.

2. Building up a governance system of cybersecurity of foreign investment (?)

At the international level, the challenges posed by cybersecurity in the digital economy have been widely recognized. On 4 September 2019 the United Nations Conference on Trade and Development (UNCTAD) released its first-ever Digital

unique to computers and information systems (e.g. attacks against information systems, denial of service and malware)' (European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication, cit., 3). According to the Tallinn Manual 2.0, "[…] A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects. […]" (Rule 92). See Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press, 2017, p. 132.

[5] I. Tasheva, 'European cybersecurity policy – Trends and prospects' *European Policy Centre – Policy Brief* (8 June 2017), 1, https://www.epc.eu/pub_details.php?cat_id=3&pub_id=7739.

[6] Id., 1. For a timeline of the most significant cyber incidents since 2006, see https://www.csis.org/programs /technology-policy-program/significant-cyber-incidents.

[7] J. Chaisse, C. Bauer, 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' 21 *Vanderbilt Journal of Entertainment & Technology Law* 3 (2019), 577.

[8] ENISA (EU Agency For Network and Information Security), *ENISA Threat Landscape Report 2018* (ENISA, January 2019), 26, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

[9] S. Magen, 'Cybersecurity and Economic Espionage: the Case of Chinese Investments in the Middle East' 1 *Cyber, Intelligence and Security* 3 (December 2017), 3- 18.

[10] M.E. Stanley, 'From China with Love: Espionage in the Age of Foreign Investment' 40 *Brooklyn Journal of International Law* 3 (2015), 1033-1079.

[11] M. Piers, C. Aschauer (eds.), *Arbitration in the Digital Age*, Cambridge University Press, 2018, p. 95.

Economy Report 2019[12], which made it clear that „[t]he digital economy has […] created new risks [such as] cybersecurity breaches […]. Governments, civil society, academia, the scientific community and the technology industry must work together to find new solutions".[13]

The digital economy has important implications for investment,[14] as also outlined by the 2017 UNCTAD's *World Investment Report*.[15]

At the international level, the only binding instrument to date on cybercrime is the Convention on Cybercrime of the Council of Europe (the Budapest Convention),[16] which focuses on infringements of copyright, computer-related fraud, child pornography and violations of network security. It has been ratified to date by 64 States.[17] The Convention does not include an express reference to protection of foreign investment;[18] however, States are committed to adopt national measures in order to criminalize computer-related offences and engage in international cooperation and mutual assistance.[19] Overall, the Budapest Convention has been used as a guideline for developing domestic legislation in the field.[20]

There are also a number of multilateral initiatives addressing cybersecurity at the international level, like the work of the G7 Cyber Expert Group,[21] the Council of Europe,[22] the G20[23], the United Nations,[24] the Organisation for Economic Cooperation and Development (OECD),[25] the Organisation for Security and Cooperation in Europe

[12] UNCTAD, *Global efforts needed to spread digital economy benefits, UN report says* (4 September 2019), https://unctad.org/en/pages/newsdetails.aspx?OriginalVersionID=2175&utm_source=CIO+-+General+public&utm_campaign=8646ae5dad-EMAIL_CAMPAIGN_2019_05_17_11_42_COPY_01&utm_medium=email&utm_term=0_3d334fa428-8646ae5dad-70467333

[13] UNCTAD, *Digital Economy Report 2019* (UNCTAD, 2019), iv.

[14] UNCTAD, *World Investment Report 2017. Investment and the Digital Economy* (UNCTAD, 2017).

[15] Id., 209.

[16] Convention on Cybercrime of the Council of Europe (CETS No.185), signed on 23 November 2001 and entered into force on 1 July 2004, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

[17] See the relevant information at the Council of Europe's official website https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[18] Chaisse, Bauer, cit., 581

[19] Article 25 of the Budapest Convention.

[20] A. Seger, 'Enhanced cooperation on cybercrime: a case for a protocol to the Budapest Convention' *ISPIonline Commentary* (16 July 2018), https://www.ispionline.it/en/pubblicazione/enhanced-cooperation-cybercrime-case-protocol-budapest-convention-20964.

[21] It was established in November 2015, with the aim to identify the main cyber security risks in the financial sector and propose relevant actions. The Group published the "G7 Fundamental Elements of Cybersecurity for the Financial Sector" (October 2016) and the "G7 Fundamental Elements for Effective Assessment of Cybersecurity" (October 2017), https://www.banque-france.fr/en/economics/international-relations/international-groups-g20g7/focus-g7-cyber-expert-group.

[22] The Council of Europe has launched the 'Action against Cybercrime', which helps to protect societies worldwide from the threat of cybercrime (https://www.coe.int/en/web/portal/coe-action-against-cybercrime).

[23] See the G20 Leaders' Communiqué (15–16 November 2015), https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf.

[24] See the Global Programme on Cybercrime carried out within the framework of the United Nations Office on Drugs and Crime (UNODC), https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

[25] Through the Cybercrime Law project (https://www.cybercrimelaw.net/OECD.html).

(OSCE)[26] and NATO.[27] Worth mentioning are also private codification initiatives like the Tallinn Manual, which deals with international law applicable in case of cyber war.[28]

Overall, the existing international legal framework is rather fragmented and does not address expressly the question of cybersecurity of foreign investment. Accordingly, the question arises whether the investment law framework can properly address the challenges of cybersecurity.

2.1. (Cyber)securing foreign investment through international investment agreements: the role of States…

To date, large part of IIAs and BITs, which were mostly concluded before the emergence of digitalization, do not address the specificities of the digital economy:[29] for example, provisions of these treaties are not clear in identifying cryptocurrency as a form of investment;[30] on the other hand, there might be possible grounds for cyber-related claims under the treaty provisions of fair and equitable treatment and full protection and security.[31]

As regards the question whether and to what extent digital assets can be qualified as 'investment' under the IIAs and BITs,[32] it should be recalled that under international investment law there is no uniform definition of 'investment'. The definition of 'investment' is provided by the applicable IIA/BIT, which includes the definition of 'investment' for the scope of the agreement itself.[33]

Many treaties provide a non-exhaustive list of examples of investment, including a reference to 'every kind of asset'.[34] For example, the Bulgaria - Republic of Korea BIT (2006), in its definition of 'investment' in article 1 states as follows: „For the purposes of this Agreement: 1. The term "investments" shall mean *every kind of asset* invested by an investor of one Contracting Party in the territory of the other Contracting Party and shall include in particular, *though not exclusively*: (a) movable and immovable property as well as any other related property rights such as mortgages, liens, pledges and similar

[26] See the official webpage https://www.osce.org/secretariat/cyber-ict-security. Worth recalling is the Permanent Council Decision No. 1106 of 3 December 2013 establishing *Initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies*, https://www.osce.org/pc/109168.

[27] NATO adopted a Policy on Cyber Defence in September 2014. Moreover, through the NATO Industry Cyber Partnership (NICP), NATO and its Allies are working to reinforce their relationships with industry (https://www.nato.int/cps/en/natohq/topics_78170.htm#).

[28] Cooperative Cyber Defense Center of Excellence, *Tallinn Manual on the International Law applicable to Cyber Warfare* (CUP, 2013) and *Tallinn Manual 2.0* (CUP, 2017), https://ccdcoe.org/research/tallinn-manual.

[29] UNCTAD, *World Investment Report 2017. Investment and the Digital Economy*, 187.

[30] P. Simsive, 'Investing in Cryptocurrencies under the Existing Investment Arbitration Regime' *Kluwer Arbitration Blog* (19 May 2015).

[31] Chaisse, Bauer, cit., 553.

[32] See most recently in this topic, E. Horváth, S. Klinkmüller, "The Concept of 'Investment' in the Digital Economy: The Case of Social Media Companies" *Journal of World Investment & Trade* 20 (2019), 577–617.

[33] Id., 555.

[34] S.J. Shackleford, E.L. Richards, A.H. Raymond, A.N. Craig, 'Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties'52 *American Business Law Journal* 1 (2015), 60.

rights; (b) shares in, stocks and debentures of, and any other form of participation in a company or any business enterprise and rights or interest derived therefrom; (c) claims to money or to any performance having an economic value associated with an investment; (d) intellectual property rights, including copyrights, trademarks, patents, industrial designs, technical processes, know-how, trade secrets, trade names and goodwill; (e) any right conferred by law or under a contract and any licenses and permits pursuant to law, including the right to explore, extract, cultivate or exploit natural resources […] [emphasis added]".[35]

Relying on UNCTAD's IIA Mapping Project and its online database[36] to get an overview of the types of definitions of investment included in IIAs/BITs,[37] it appears that 2493 investment treaties (around 75% of overall number of investment treaties currently in force) cover 'every kind of asset' or 'any kind of asset'. According to UNCTAD – based on the relevant investment arbitration interpretation – 'every kind of asset' may 'embrace […] everything of economic value, virtually without limitation'.[38] This suggests that digital assets could also fall within this broad type of investment definition.[39]

However, also as regards the concept of 'digital asset' there is no international agreed definition. In general terms, we can define a digital asset as 'an electronic record in which an individual has a right or interest',[40] which may include software, source codes, data packages, email accounts, domain names, databases, designs, trade secrets, and digital currency.[41] Accordingly, if States wish to include 'digital assets' in the definition of 'investment' of the relevant IIAs/BITs, they should also consider which kind of assets they want to refer to.

To the extent that investment definitions are drafted broadly in IIAs and BITs, we may argue that digital assets could fall within most definitions of a 'investment';[42] and in support of this, it can be recalled that recently, investment arbitral tribunal have been in favour of including non-expressed kind of investment within the scope of application of the relevant BIT.[43] If qualified as an international 'investment', digital assets can be granted the relevant protection of the applicable IIA/BIT.

As regards the question of cybersecurity of foreign investment (also in the form of digital asset, when considered as 'investment'), it has been argued that the fair and equitable treatment (FET) and the full protection and security (FPS) standards included

---

[35] Bulgaria - Republic of Korea BIT (2006).

[36] See the official website https://investmentpolicy.unctad.org/international-investment-agreements/iia-mapping.

[37] The IIA Mapping Project has mapped 2571 treaties, out of the 3317 IIAs concluded so far (UNCTAD, *World Investment Report 2019. Special Economic Zones* (UNCTAD, 2019), 99).

[38] UNCTAD Series on Issues in International Investment Agreements II. *Scope and Definition (A sequel)*, UNCTAD/DIAE/IA/2010/2 (1 Mar 2011), 24.

[39] Chaisse, Bauer, cit., 558

[40] J. Bick, 'All Digital Assets Are Not Legally Equal' *Law Journal Newsletters* (November 2017), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/11/01/all-digital-assets-are-not-legally-equal.

[41] Chaisse, Bauer, cit., 560. See 'Digital Asset' *Techopedia*, https://www.techopedia.com/definition/23367/digitalasset and J. Spacey, '11 Examples of Digital Assets' *Simplicable* (9 March 2017), https://simplicable.com/new/digital-asset.

[42] Chaisse, Bauer, cit., 568.

[43] UNCTAD, 'Review of ISDS Decisions in 2018: Selected IIA Reform Issues' *IIA Issues Note* 4 (July 2019), 3-4.

in IIAs/BITs may have a role to play.

The FET standard requires that the host state provides fair and equitable treatment to foreign investors. This kind of provisions are very common in IIAs/BITs (according to the database of the UNCTAD's IIA Mapping Project, 2440 out of 2571 mapped treaties include a FET provision – around the 73% of the overall number of treaties) and are drafted, with some variation in the wording, like the following: „Article 2 (Promotion and Protection of investments) […] (4) Each […]Party shall at all times ensure fair and equitable treatment of the investments made by investors of the other […] Party and shall not impair the management, maintenance, use, enjoyment or disposal thereof through unjustified or discriminatory measures".[44]

FET provisions may allow investors to pursue cyber claims where, for example, the host state implements new regulations,[45] such as source code disclosure requirements or changes that impact cross-border dataflows or data localization requirements. While changes to cyber regulations can be justified on the ground of public policy objectives, they can also favour domestic industries at the expense of foreign investors and may undermine the value of their investment.[46]

Also, the FPS provision included in IIAs/BITs may grant protection to digital assets, when qualified as international investment under the applicable IIA/BIT. The FPS provision is very common in IIAs and BITs (according to the database of the UNCTAD's IIA Mapping Project, 1972 out of 2571 mapped treaties include a FPS provision – around the 59% of the overall number of treaties) and is generally drafted like the following: „Article 4 (1) Investments by investors of either Contracting State shall enjoy full protection and security in the territory of the other Contracting State […]".[47]

The interpretation of the FPS provision has traditionally addressed physical protections from army, militants, and rioters.[48] During the years, the security obligation included in the FPS provision has evolved in the interpretation of the investment arbitral tribunals to include also the reference of a 'safe' investment environment.[49] Accordingly, if a host state fails to provide a safe investment environment in relation to cybersecurity (e.g., it lacks cybercrime laws, or it does not prevent damage to the assets of foreign investors or fails to prosecute cyber criminals),[50] the breach of the FPS obligation may be claimed.[51]

Lack of insufficient cybersecurity protection within the regulatory framework of the host State leave companies more vulnerable to cyberattacks (since the State is not legally equipped to prevent and prosecute such crimes).[52] However, the FPS standard

---

[44] Argentina - Bulgaria BIT (1993).

[45] It has been questioned whether '[a] digital services tax could also raise issues under the FET obligation in Australia's investment treaties', in relation to the fact that Australia is considering implementing a tax on digital services. A.D. Mitchell, T. Voon, J. Hepburn, 'Taxing Tech: Risks of an Australian Digital Services Tax under International Economic Law' 20 *Melbourne Journal of International Law* (2019), 33.

[46] Chaisse, Bauer, cit., 570.

[47] Afghanistan - Germany BIT (2005).

[48] Chaisse, Bauer, cit., 578

[49] *Azurix Corp. v. Argentine Republic*, ICSID ARB/01/12, Award (14 July 2006), paras 406, 408; *Compañía de Aguas del Aconquija, S.A. v. Argentine Republic*, ICSID ARB/97/3, Award (21 November 2000), p. 1.

[50] D. Collins, 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' 12 *Journal of World Investment and Trade* 2 (2011), 19 f.

[51] Chaisse, Bauer, cit., 579.

[52] Id., 580.

should not be interpreted as a strict liability standard; States are required to exercise due diligence in order to prevent harm to the foreign investment. For example, they could amend their cybercrime national regulations in accordance with the Budapest Convention.[53] However, the principle of proportionality applies:[54] if foreign investors invest in less developed countries, they cannot expect cybersecurity protections equivalent to those applicable in developed countries.[55]

When dealing with cyberattacks to foreign investment, also the key question of the attribution of the cyber intrusion arises. This question is still debated under international law,[56] but surely it should be dealt with in the framework of cyber-related claims before an investment arbitral tribunal, in order to ascertain whether the host State may be held responsible for breaches of obligations under the applicable IIA/BIT - both in the case of cyberattacks from third parties that the host State was not able to prevent and in the case the cyber intrusion is attributable directly to the host state.[57] Also, host states may invoke national security reasons – and the relevant provisions included in the applicable IIA/BIT - in response to alleged cyber espionage or when changing cybersecurity national regulations to the detriment of foreign investors.[58]

As the above quick overview has shown, it might be quite challenging to bring a cyber-related claim under the current international investment legal framework. In order to avoid uncertainty, states could proactively address these issues by updating their BIT language to include express reference to cyber risk.[59]

In the field of international investment promotion and protection, it is also worth recalling the contribution of non-state actors, whose soft law instruments and activities in the field help raising awareness, sharing knowledge and best practices and fostering international cooperation. Worth mentioning is the work of the OECD,[60] the United Nations Commission on International Trade Law (UNCITRAL) Working Group III,[61] OSCE[62] and UNCTAD.[63]

---

[53] Id., 582.

[54] The tribunal in *Pantechniki v. Albania* explained that the duty for a state to comply with FPS is relative to the resources available to it. *Pantechniki S.A. Contractors (Greece) v. Republic of Alb.,* ICSID ARB/07/21, Award (30 July 2009), para 76.

[55] Chaisse, Bauer, cit., 582.

[56] See C. Antonopoulos, 'State responsibility in cyberspace', in N. Tsagourias (ed.), *Research Handbook on International Law and Cyberspace* (EE Publishing, 2015), 62-65.

[57] Chaisse, Bauer, cit., 586.

[58] Ibid., 587 and Shackleford et al., cit.

[59] Chaisse, Bauer, cit., 587.

[60] The 1967 *OECD Draft Convention on the Protection of Foreign Property*, though never entered into force, influenced the next model BITs of States. More generally, the OECD work is aimed at advancing investment policy reform and international co-operation in the field (http://www.oecd.org/investment).

[61] The UNCITRAL Working Group III began its work in November 2017 with the mandate to identify the concerns regarding investor-State dispute settlement and draft relevant reform proposals (https://uncitral.un.org/en/working_groups/3/investor-state).

[62] OSCE supports sustainable economic growth and international economic co-operation on a variety of issues, including improvement of investment climates in several countries (https://www.osce.org/economic-activities).

[63] UNCTAD's Investment Policy Hub, https://investmentpolicy.unctad.org.

2.1.1. … and cybersecurity concerns in international (investment) arbitral proceedings

To date, there is no documented instance of international investment arbitration case dealing with cyberattacks (and cyberespionage) to foreign investment.

On the other hand, there are some instances (1) in which investment arbitral tribunals have dealt with WikiLeaks diplomatic cables as evidence brought by one of the parties and (2) where international arbitral proceedings have been compromised because of cyber intrusion during the proceedings themselves.

Indeed, digitalization has created opportunities to illegally obtain private or privileged information.[64] In the international investment case *ConocoPhillips v. Venezuela*,[65] Venezuela challenged the Decision of the arbitral tribunal and used WikiLeaks diplomatic cables containing confidential communications between ConocoPhillips' counsel and representatives from the US Embassy. The tribunal rejected the request of Venezuela,[66] however, it did not mention the US diplomatic cables and their admissibility as evidence in the arbitral proceeding,[67] thus leaving the question of their admissibility open – it should be recalled that international arbitrators have a broad power to determine the admissibility of privileged or confidential evidence.[68]

Again, in *OPIC Karimum Corporation v Venezuela*, OPIC Karimum relied on WikiLeaks cables detailing Venezuelan government information to support its request to disqualify an arbitrator;[69] similarly, in *Kiliç İnşaat İthalat İhracat Sanayi Ve Ticaret Anonim Şirketi v. Turkmenistan*, Kiliç relied on WikiLeaks cables introduced by Turkmenistan to support its argument that recourse to Turkmenistan's courts was futile:[70] in both cases, the tribunals failed to address the question of their admissibility as evidence.[71]

In another case, the arbitral tribunal reached an admissibility decision. Caratube International Oil Company and American-national Devincci Salah Hourani, who were suing Kazakhstan, brought to the tribunal as evidence a number of leaked documents that had become publicly available on WikiLeaks.[72] The Tribunal reasoned that, since the documents were relevant to the dispute and that were in the public domain - and thus they have lost their privileged and confidential character - , they could be admitted as

---

[64] R. Calvillo Ortiz, 'Admissibility of Hacked Emails as Evidence in Arbitration' *Blogs Law NYU - Transnational Notes* (14 May 2018), https://blogs.law.nyu.edu/transnational, J.O. Ireton, 'The Admissibility of Evidence in ICSID Arbitration: Considering the Validity of WikiLeaks Cables as Evidence' 30 *ICSID Review* 1 (2015), 231–242 and B. John, 'Admissibility of Improperly Obtained Data as Evidence in International Arbitration Proceedings' *Kluwer Arbitration Blog* (28 September 2016).

[65] *ConocoPhillips Petrozuata BV, ConocoPhillips Hamaca BV and ConocoPhillips Gulf of Paria BV v. Venezuela*, ICSID ARB/07/30, Decision on Jurisdiction and the Merits (3 September 2013).

[66] Decision on Respondent's Request for Reconsideration of 10 March 2014 and Interim Decision (17 January 2017).

[67] Ireton, cit., 240.

[68] Id., 238.

[69] *OPIC Karimum Corporation v Venezuela*, ICSID ARB/10/14, Decision on The Proposal to Disqualify Professor Philippe Sands (5 March 2011) paras 11 and 23.

[70] *Kiliç İnşaat İthalat İhracat Sanayi Ve Ticaret Anonim Şirketi v. Turkmenistan*, ICSID ARB/10/1, Award (2 July 2013) paras 4.1.1 and 4.3.16.

[71] Ireton, cit., 240

[72] Calvillo Ortiz, cit.

evidence in the proceedings.[73]

Overall, the question of admissibility of this kind of evidence seems to be left to the discretion of the single arbitral tribunal. In this respect, a more specific drafting of the relevant investment agreements might help tribunals in achieving a uniform approach on this question.

As regards the issue of cyber intrusions during an international arbitration proceeding, the most remarkable example happened in July 2015, when the website of the Permanent Court of Arbitration in The Hague was hacked during a hearing of a maritime border arbitration between China and the Philippines.[74]

In order to address the challenges of cyber intrusions during international arbitration proceedings, the International Council for Commercial Arbitration, the New York City Bar Association and the International Institute for Conflict Prevention & Resolution set up a Working Group on Cybersecurity in International Arbitration, which released the *Cybersecurity Protocol for International Arbitration* in November 2019.[75] The Protocol aims at offering a series of recommended standards that the parties can agree to adopt during international arbitration proceedings.[76]

The Protocol is a very interesting document also as regards the history of its drafting. The first consultation paper was launched at the ICCA Congress in Sydney in April 2018 and opened for public consultations until December 2018; additionally, the Working Group held public workshops in different countries to discuss the Draft.[77] This cooperation method in drafting the document could serve also as a model for possible future documents in this field.

2.2. Addressing cybersecurity and foreign investment protection at the EU level: the state of play

Focusing on the European Union (EU) level, it is worth recalling that the 2009 Lisbon Treaty has included foreign direct investment in the exclusive competence of the EU; this means that the EU can now conclude international investment-related agreements with third countries and may decide to approach cybersecurity concerns in the framework of such agreements.

The following paragraphs delineate the current EU cybersecurity regulatory framework and its approach to cybersecurity in international investment agreements.

---

[73] *Caratube International Oil Company LLP v. The Republic of Kazakhstan*, ICSID ARB/08/12, Tribunal's Decision on the Claimants' Request for the Production of "Leaked Documents" (27 July 2015) – unpublished and reported in Calvillo Ortiz, cit.

[74] J. Fernández-Samaniego, G. Hierro, 'The Draft ICCA-CPR-New York City Bar Association Protocol for Cybersecurity in Arbitration: A Leading Light, at Least' 16 *Transnational Dispute Management - Special Issue on Cybersecurity in International Arbitration* 3 (May 2019).

[75] See the official webpage of the Working Group on Cybersecurity in International Arbitration https://www.arbitration-icca.org. For a preliminary comment, see Fernández-Samaniego et al., cit.

[76] "Although the Protocol is drafted with international commercial arbitrations in mind, Arbitral Participants may find it a useful starting point for domestic arbitration matters and/or investor-state arbitrations" (Section III. Purpose of the Cybersecurity Protocol, point G).

[77] See https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html, consulted on 1.03.2023.

2.2.1. The EU cybersecurity regulatory framework

The EU has been always aware of the challenges of cybercrime to economic activities: the 2013 Cybersecurity Strategy of the EU[78] made it clear that „[t]he EU economy is already affected by cybercrime activities against the private sector and individuals. Cybercriminals are using ever more sophisticated methods for intruding into information systems, stealing critical data or holding companies to ransom. The increase of economic espionage and state-sponsored activities in cyberspace poses a new category of threats for EU governments and companies".[79]

In May 2017, the Commission expressly included cybersecurity as one of the three emerging challenges in its Digital Single Market Strategy mid-term review[80]. And in the last years, cybersecurity has been at the heart of manifold EU regulations and policies.[81]

At the EU level, different players and institutions are involved in addressing cybersecurity:

- the European Parliament and the Council;
- the European Commission: the main Directorates-General (DG) responsible for cybersecurity policy are DGs CNECT and HOME; DG DIGIT is responsible for the IT security of the Commission's own systems;
- EU agencies:
    - the EU Network and Information Security Agency (ENISA), which will be updated with a new EU cyber security agency, according to the most recent Cybersecurity Act;[82] it works with EU member states and private sector giving advice and support in the development of the National Cybersecurity Strategies and in the implementation of EU policies;
    - the Europol's European Cybercrime Centre (EC3), which supports member states law enforcement operations in response to cybercrime and coordinates prevention and awareness measures. Each year, EC3 publishes the *Internet Organised Crime Threat Assessment* (IOCTA) Report, which highlights the emerging threats and developments in cybercrime and provides recommendations to policy makers;[83]
    - the Computer Emergency Response Team (CERT-EU), for the support of EU institutions, agencies and bodies;[84]
    - the European Defence Agency (EDA), which supports EU member

[78] European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication, cit.
[79] Id., 3.
[80] European Commission, Communication *on the Mid-Term Review on the implementation of the Digital Single Market Strategy a Connected Digital Single Market for All*, COM/2017/0228 final (10 May 2017).
[81] European Court of Auditors, 'Challenges to effective EU cybersecurity policy' *Briefing Paper* (March 2019), 11-12.
[82] See the official website https://www.enisa.europa.eu/about-enisa/regulatory-framework, consulted on 1.03.2023.
[83] See the official website https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3; https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assess ment, consulted on 1.03.2023.
[84] See the official website https://cert.europa.eu/cert/plainedition/en/cert_about.html, consulted on 1.03. 2023.

states in the development of their cyber defence capabilities;[85]

- the European External Action Service (EEAS), which deals primarily on cyber defence and cyber diplomacy measures.

It is worth recalling that in 2018, ENISA, EDA EUROPOL-EC3 and CERT-EU signed a Memorandum of Understanding, which aims at promoting cooperation and coordination among them in the field of cybersecurity and cyberdefence.[86]

As regards the EU legal framework on cybersecurity, a series of legal acts have been adopted in order to protect electronic communications networks:

- the 2016 Directive on Security of Network and Information Systems (NIS Directive),[87] which introduced commitments for member states on security measures and incident notifications in a number of sectors such as energy, transport, drinking water supply and distribution, banking, financial market infrastructures, healthcare, digital infrastructure;[88]

- the 2016 General Data Protection Regulation (GDPR),[89] which has introduced the figure of the Data Protection Officer (DPO), who coordinates and controls the compliance with data protection regulations;[90] according to the Regulation, all companies should take measures to enhance data security and notify regulatory authorities, and potentially consumers of any significant breach of the data (which may well include any form of cyber intrusion).[91] The GDPR applies to every organization that handles data belonging to EU citizens and residents, also outside the EU territory;[92]

- the 2018 Directive establishing the European Electronic Communications Code,[93] according to which member states should ensure the security of public communications networks;

- the 2019 Cybersecurity Act,[94] which has introduced:

  - a system of EU certification for information and communications

---

[85] See the official website https://www.eda.europa.eu/Aboutus/Missionandfunctions. The Agency signs also Administrative Arrangements with non-EU members in order to enhance cooperation on EDA's projects and programmes.

[86] Point 1 of the Memorandum. See "Four EU cybersecurity organisations enhance cooperation" Europol - Press Release (23 May 2018), https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation. For the text of the Memorandum see https://www.eda.europa.eu/docs/default-source/documents/mou---eda-enisa-cert-eu-ec3---23-05-18.pdf.

[87] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 *concerning measures for a high common level of security of network and information systems across the Union*.

[88] See Fernández-Samaniego, Hierro, cit. and Chaisse, Bauer, cit., 584.

[89] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

[90] Fernández-Samaniego, Hierro, cit.

[91] Articles 5 and 33 of the GDPR Regulation. See P. Beshar, 'Cybersecurity and the EU General Data Protection Regulation: The Time for Action Is Now' *Marsh Report* (2017), https://www.marsh.com/uk/insights/research/cybersecurity-and-the-EU-general-data-protection-regulation-the-time-for-action-is-now.html.

[92] Article 3 of the GDPR Regulation (https://gdpr.eu/companies-outside-of-europe).

[93] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 *establishing the European Electronic Communications Code* (OJ L 321, 17.12.2018, p. 36).

[94] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 *on ENISA (the EU Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013* (Cybersecurity Act).

technology (ICT) products, services and processes that would be recognised in all EU member states;[95]

- an EU cyber security agency that will upgrade ENISA: the new agency will have a stronger role of support in the area of European cybersecurity.[96]

The Cybersecurity Act was proposed as part of the cybersecurity package that the European Commission presented on 13 September 2017; the package outlined several measures aimed at strengthening cybersecurity in the EU, including a blueprint for rapid emergency response[97] - which sets out the objectives and modes of cooperation between the member states and EU institutions in responding to large scale cross-border cyber incident or crisis.

In the field of cyberdefence, in 2017 the *Joint EU Diplomatic Response to Malicious Cyber Activities*[98] (the so-called *cyber diplomacy toolbox*) was developed, based on the Council conclusions on cyber diplomacy.[99] As the Council recognized: „cyberspace offers significant opportunities, but also poses continuously evolving challenges for EU external policies, including for the Common Foreign and Security Policy".[100]

The toolbox allows the EU and member states to implement a diplomatic response to malicious cyber activities through the means of the Common Foreign and Security Policy. These can include preventive (e.g. awareness-raising, capacity-building), cooperative, stability and restrictive measures (e.g. travel bans, arms embargoes, freezing funds).[101]

As part of the EU cyber diplomacy toolbox, in May 2019 the Council established also a '[…] framework for targeted restrictive measures to deter and respond to cyber-attacks with a significant effect which constitute an external threat to the Union or its Member State […] against third States or international organisations […]', when such measures are deemed necessary to achieve the objectives of the Common Foreign and Security Policy.[102]

All the above-mentioned initiatives and regulations are aimed at guaranteeing a safe cyber regulatory environment in the EU.

---

[95] European Commission, *The EU cybersecurity certification framework* (2019), https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

[96] European Council, *Cybersecurity in Europe: stronger rules and better protection* (11 July 2019), https://www.consilium.europa.eu/en/policies/cybersecurity/.

[97] Commission Recommendation (EU) 2017/1584 of 13 September 2017 *on coordinated response to large-scale cybersecurity incidents and crises*, C/2017/6100.

[98] Council of the European Union, *Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*, 9916/17, 7 June 2017.

[99] Council of the European Union, *Council Conclusions on Cyber Diplomacy*, 6122/55, 11 February 2015.

[100] Council of the European Union, *Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*, 7923/2/17 REV 2 (7 June 2017), para 1.

[101] Council of the European Union, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.

[102] Council Decision *concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 7299/19 (4 May 2019), para 7.

2.2.2. Protecting foreign investment through international investment agreements (?): the EU approach

It remains to be seen whether the EU has also included cybersecurity aspects in international investment-related agreement that has negotiated so far. To date, the EU already included investment provisions in its new trade agreements with Canada (provisionally entered into force on 21 September 2017)[103] and Vietnam (trade and investment agreements were signed on 30 June 2019)[104] and is also negotiating investment rules as part of its trade agreements with other third countries.[105]

The Canada - EU CETA includes a broad definition of investment, which might also include digital assets,[106] and also includes FET and FPS standards of protection. However, the FET and FPS standards have been drafted including a rather closed list of measures amounting to a breach of such obligations; article 8.10 (Treatment of investors and of covered investments) – also the most recent EU - Viet Nam Investment Protection Agreement includes a quite similar provision – reads as follows:

„*1. Each Party shall accord in its territory to covered investments of the other Party and to investors with respect to their covered investments fair and equitable treatment and full protection and security […].*

2. A Party breaches the obligation of fair and equitable treatment referenced in paragraph 1 if a measure or series of measures constitutes:

(a) denial of justice in criminal, civil or administrative proceedings;

(b) fundamental breach of due process, including a fundamental breach of transparency, in judicial and administrative proceedings;

(c) manifest arbitrariness;

(d) targeted discrimination on manifestly wrongful grounds, such as gender, race or religious belief;

(e) abusive treatment of investors, such as coercion, duress and harassment; or

(f) a breach of any further elements of the fair and equitable treatment obligation adopted by the Parties in accordance with paragraph 3 of this Article.

3. The Parties shall regularly, or upon request of a Party, review the content of the obligation to provide fair and equitable treatment. The Committee on Services and Investment, established under Article 26.2.1(b) (Specialised committees), may develop recommendations in this regard and submit them to the CETA Joint Committee for decision.

4. When applying the above fair and equitable treatment obligation, a Tribunal may take into account whether a Party made a specific representation to an investor to induce a covered investment, that created a legitimate expectation, and upon which the investor relied in deciding to make or maintain the covered investment, but that the Party subsequently frustrated.

5. For greater certainty, "full protection and security" refers to the Party's

---

[103] Comprehensive Economic and Trade Agreement (CETA), https://ec.europa.eu/trade/policy/in-focus/ceta/.

[104] EU - Viet Nam Investment Protection Agreement (2019), https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5868/download.

[105] For the update list of on-going negotiations with third countries, see http://trade.ec.europa.eu/doclib/docs/2006/december/tradoc_118238.pdf.

[106] Article 8.1 of CETA.

obligations relating to the physical security of investors and covered investments […]".

Under this article, it seems quite difficult for a foreign investor to pursue cyber claims where the host state implements new regulations on cybersecurity that the investor considers discriminatory or arbitrary – unless there is a recommendation on this point brought by the Committee on Services and Investment or in the case of a 'legitimate expectation' upon which the investor had relied. Moreover, the article has limited the FPS standard of protection to 'physical security', making its application to digital assets quite problematic.

The possibility to challenge a host State's measure is further restricted in the case of CETA by the fact that investment claims will be heard before an ad hoc multilateral investment tribunal and appellate mechanism,[107] which „[…]shall apply this Agreement [the CETA] […and] shall not have jurisdiction to determine the legality of a measure, alleged to constitute a breach of this Agreement, under the domestic law of a Party. […]".[108]

Also, in the case of the EU - Viet Nam Investment Protection Agreement, the investment tribunal system set up by the Agreement provides that „[…] the Tribunal and the Appeal Tribunal shall apply the provisions of […] this Agreement, as applicable […and they do] not have jurisdiction to determine the legality of a measure, alleged to constitute a breach of this Agreement, under the domestic laws and regulations of the disputing Party […]".[109]

3. A 'mapping exercise' through the social network analysis

As the previous paragraphs have shown, different actors have a role to play in either cybersecurity and/or investment protection policies at the international and European levels. In order to have a clear visual map of the actors and their relations, we have applied the method of social network analysis.[110]

The aim of this visualization is twofold: (1) to 'put on the table' the main actors involved in both cybersecurity and investment protection policies; (2) to understand the relationships among all the actors involved.

The first step of this visualization exercise has been the drafting of a matrix of actors: the following table lists the key (institutional) actors at the European and international level that are active in the field of (1) foreign investment protection and/or (2) cybersecurity. Since the focus of this paper is the governance system at the international and particularly at the EU level, for the national level only the role of the States – more in particular, of EU member States - has been indicated (without going into detail as regards which institutions/agencies play a role in this respect). This table does not aim to include *all* the actors involved at the international and European level: the aim is to indicate the ones that can play a more relevant role in building up a

[107] Article 8.29 of CETA.
[108] Article 8.31 of CETA.
[109] Article 3.42 of the EU - Viet Nam Investment Protection Agreement.
[110] A. Cheevers, "An Introduction to Social Network Analysis" *The Social and Psychological Underpinnings of Commercial Arbitration in Europe* (22 January 2019), https://commercialarbitrationineurope.wordpress.com/2019/01/22/an-introduction-to-social-network-analysis/. For a brief overview on the application of the social network analysis to the study of law, see S. Puig, "Social Capital in the Arbitration Market" *European Journal of International Law* 25 (2014) 2, 387–424.

governance system in this area. Furthermore, the table focuses on institutional actors, as a starting step to understand whether and to what extent a governance system among these players is possible.

Table 1

Actors	Active in the field of **FOREIGN INVESTMENT PROTECTION**	Active in the field of **CYBERSECURITY**
EU MEMBER STATES	✓	✓
EUROPEAN LEVEL		
CERT-EU		✓
Council of the European Union	✓	✓
European Parliament	✓	✓
European Commission	✓	✓
EDA		✓
EEAS		✓
ENISA		✓
EUROPOL EC3		✓
High Representative of the EU for Foreign Affairs and Security Policy		✓
INTERNATIONAL LEVEL		
Council of Europe		✓
G20	✓	✓
G7 Cyber Expert Group		✓
ICCA - NYC Bar-CPR Working Group on Cybersecurity in International Arbitration	✓	✓
Investment arbitral tribunals	✓	

NATO		✓
NATO Cooperative Cyber Defence Centre of Excellence		✓
OECD	✓	✓
OSCE	✓	✓
UNCITRAL	✓	
UNCITRAL Working Group III	✓	
UNCTAD	✓	✓
WTO[111]	✓	✓

From this table, the following visualization has been developed, using NodeXL:[112] the actors listed in the above table have been inserted as vertices; the edges represent the relationships between the nodes. In this visualization, the edges among the nodes have been drawn taking into account the *interaction* between the actors: we have considered as an interaction the occurrence of at least one of these factors: (1) co-drafting of documents (e.g. joint communications); (2) documents directly addressed to one or more actors; (3) contribution to the development of some policies in the field.

We have used different colours for the edges following these criteria:

1. ORANGE: when the interaction occurs only in the field of cybersecurity;

2. LIGHT BLUE: when the interaction occurs only in the field of investment promotion and protection;

3. GREEN: when there are interactions in both fields of cybersecurity and investment promotion and protection (even though the interactions do not occur simultaneously in both fields)

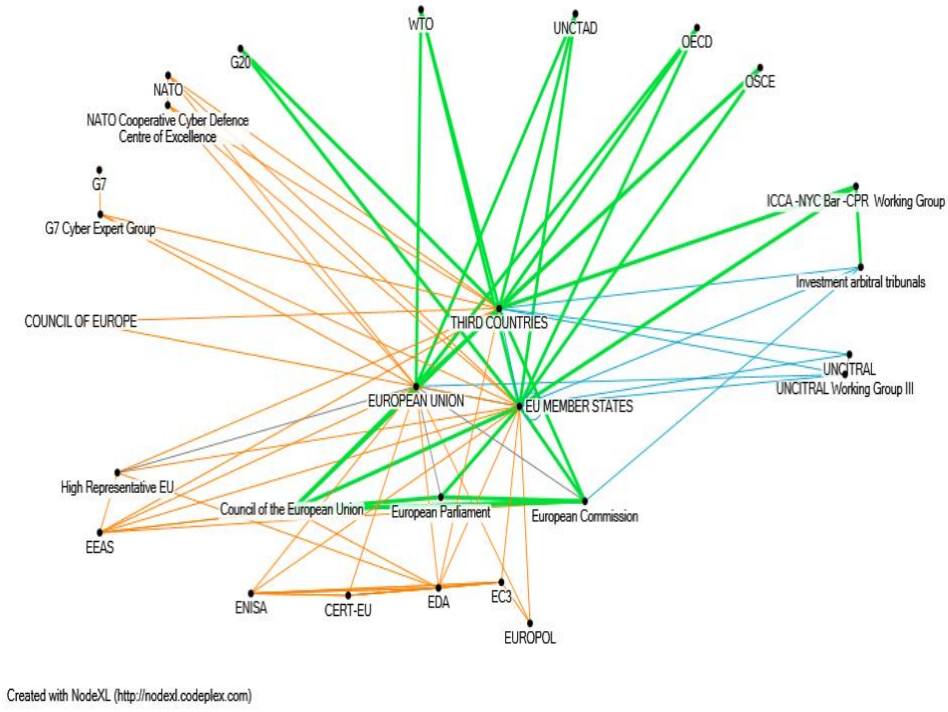
The following picture visualizes the set of nodes and edges that make up the network of actors in the field of cybersecurity and investment promotion and protection.[113]

[111] As regards the WTO (eventual) involvement in cybersecurity, even though it could be argue that the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of the World Trade Organization (WTO) - which includes the commitment to protect certain types of intellectual property rights, including trade secrets, within the territory of the member States - can be applied to protect trade secrets against (cyber) economic espionage (Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C to the Agreement Establishing the World Trade Organization (signed on 15 April 1994), 1869 UNTS 299.), there is no international consensus on this point to date.

[112] NodeXL allows to visualize network graphs by using Microsoft Office Excel sheets. For more information, see the official website https://nodexl.com.

[113] This visualization uses the Fruchterman-Reingold layout algorithm. See D.L. Hansen, B. Shneiderman, M.A. Smith, *Analyzing social media networks with NodeXL: insights from a connected world* (Elsevier, 2010), 96, 170-171.

Figure 1



From the graph we can infer two main observations:

- EU institutions have links with almost all the actors involved at the international level in cybersecurity and investment protection;

- International and EU actors have already interactions on both the topics of cybersecurity and investment protection. The green edges highlight that key players are already in contact in both fields of action. However, only in the case of the ICCA -NYC Bar -CPR Working Group on Cybersecurity in International Arbitration there is a unique document which deals on cybersecurity that could be applied in investment arbitration (even though it deals only with cybersecurity issues connected with arbitration proceedings). Nevertheless, it is a starting point for building up integrated approaches on cybersecurity and investment protection among the relevant actors.

Unfortunately, the list of stakeholders that have engaged in the public consultation with the ICCA -NYC Bar - CPR Working Group on Cybersecurity in International Arbitration is not available for the public (thus, the graph is incomplete in this respect); it would have been interesting to check whether some of the actors displayed in the graph have contributed with comments to the Protocol.

4. Some concluding remarks

The EU has already remarked that „the Commission, the High Representative and the Member States should articulate a coherent EU international cyberspace policy, which will be aimed at increased engagement and stronger relations with key international partners and organisations, as well as with civil society and private sector.

[…] To address global challenges in cyberspace, the EU will seek closer cooperation with organisations that are active in this field […]".[114]

This is in line with the *Paris call for trust and security in cyberspace* launched by the UNESCO Internet Governance Forum on 12 December 2018 and supported by more than 50 States, 90 non-state actors and 130 corporations and groups at the international level, which called for „[..] collaboration among governments, the private sector and civil society to create new cybersecurity standards that enable infrastructures and organizations to improve cyber protections […]".[115]

At the EU level, a quite robust regulatory cybersecurity framework has been developed. Accordingly, foreign investors in the EU area may benefit from several measures aimed at guaranteeing a safe cyber environment. On the other hand, a number of questions still need to be addressed at both international and EU level.

As the last paragraph has shown, EU institutions have already built up a robust network of relationships with other international players, with whom have already engaged in discussions on either cybersecurity and/or investment promotion and protection. This should serve as a starting point to enhance such dialogues in a more integrated way (also including private stakeholders and the academia) [116].

As the NATO Secretary General Jens Stoltenberg recalled at the Cyber Defence Pledge Conference in London on 23 May 2019, '[…i]t takes just a 'click' to send a cyber virus spreading across the globe. But it takes a global effort to stop it from inflicting chaos […]'.[117]

Bibliography

1. Antonopoulos, C., 'State responsibility in cyberspace', in N. Tsagourias (ed.), *Research Handbook on International Law and Cyberspace* (EE Publishing, 2015), 62-65.
2. Bick, J., 'All Digital Assets Are Not Legally Equal' *Law Journal Newsletters* (November 2017), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/11/01/all-digital-assets-are-not-legally-equal.
3. Calvillo Ortiz, R., 'Admissibility of Hacked Emails as Evidence in Arbitration' *Blogs Law NYU - Transnational Notes* (14 May 2018), https://blogs.law.nyu.edu/transnational.
4. Chaisse, J. & Bauer, C., 'Cybersecurity and the Protection of Digital Assets: Assessing the Role of International Investment Law and Arbitration' 21 *Vanderbilt Journal of Entertainment & Technology Law* 3 (2019), 549-589.
5. Cheevers, A., "An Introduction to Social Network Analysis" *The Social and Psychological Underpinnings of Commercial Arbitration in Europe* (22 January 2019), https://commercialarbitrationineurope.wordpress.com/2019/01/22/an-introduction-to-social-network-analysis/.
6. Collins, D., 'Applying the Full Protection and Security Standard of International Investment Law to Digital Assets' 12 *Journal of World Investment & Trade* 2 (2011),

[114] European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication, cit., 15.

[115] "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace" *France Diplomatie - Ministry for Europe and Foreign Affairs* (12 December 2018), https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[116] They have not been included in the mapping exercise of paragraph 3, since the kind of interaction with institutional actors are diverse in nature and should deserve a separate visualization.

[117] For the full text, see https://www.nato.int/cps/en/natohq/opinions_166039.htm, consulted on 1.03.2023.

225-255.
7. Fernández-Samaniego, J. & Hierro, G., 'The Draft ICCA-CPR-New York City Bar Association Protocol for Cybersecurity in Arbitration: A Leading Light, at Least' 16 *Transnational Dispute Management - Special Issue on Cybersecurity in International Arbitration* 3 (May 2019), https://www.transnational-dispute-management.com/article.asp?key=2645.
8. Hansen, D. L., Shneiderman, B. & Smith, M.A., *Analyzing social media networks with NodeXL: insights from a connected world* (Elsevier, 2010).
9. Horváth, E. & Klinkmüller, S., "The Concept of 'Investment' in the Digital Economy: The Case of Social Media Companies" *Journal of World Investment & Trade* 20 (2019), 577–617.
10. Ireton, J. O., 'The Admissibility of Evidence in ICSID Arbitration: Considering the Validity of WikiLeaks Cables as Evidence' 30 *ICSID Review* 1 (2015), 231–242.
11. John, B., 'Admissibility of Improperly Obtained Data as Evidence in International Arbitration Proceedings' *Kluwer Arbitration Blog* (28 September 2016), https://arbitrationblog.kluwerarbitration.com/2016/09/28/admissibility-of-improperly-obtained-data-as-evidence-in-international-arbitration-proceedings/.
12. Magen, S., 'Cybersecurity and Economic Espionage: the Case of Chinese Investments in the Middle East' 1 *Cyber, Intelligence and Security* 3 (December 2017), 3- 18.
13. Mitchell, A. D., Voon, T. & Hepburn, J., 'Taxing Tech: Risks of an Australian Digital Services Tax under International Economic Law' 20 *Melbourne Journal of International Law* (2019), 1-33.
14. Piers, M. & Aschauer, C. (eds.), *Arbitration in the Digital Age* (Cambridge University Press, 2018).
15. Puig, S., "Social Capital in the Arbitration Market" *European Journal of International Law* 25 (2014) 2, 387–424.
16. Schmitt, M. N. (ed.), *Tallinn Manual 2.0 on the international law applicable to cyber operations*, (Cambridge University Press, 2017).
17. Seger, A., 'Enhanced cooperation on cybercrime: a case for a protocol to the Budapest Convention' *ISPIonline Commentary* (16 July 2018), https://www.ispionline.it/en/pubblicazione/enhanced-cooperation-cybercrime-case-protocol-budapest-convention-20964
18. Shackleford, S. J., Richards, E.L., Raymond, A.H. & Craig, A.N., 'Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties'52 *American Business Law Journal* 1 (2015), 1-74.
19. Simsive, P., 'Investing in Cryptocurrencies under the Existing Investment Arbitration Regime' *Kluwer Arbitration Blog* (19 May 2015), https://arbitrationblog.kluwerarbitration.com/2015/05/19/investing-in-cryptocurrencies-under-the-existing-investment-arbitration-regime/.
20. Stanley, M. E., 'From China with Love: Espionage in the Age of Foreign Investment' 40 *Brooklyn Journal of International Law* 3 (2015), 1033-1079.
21. Tasheva, I., 'European cybersecurity policy – Trends and prospects' *European Policy Centre – Policy Brief* (8 June 2017), 1, https://www.epc.eu/pub_details.php?cat_id=3&pub_id=7739.
22. UNCTAD, *Digital Economy Report 2019* (UNCTAD, 2019).
23. UNCTAD, *World Investment Report 2017. Investment and the Digital Economy* (UNCTAD, 2017).