Cybersecurity of foreign investment in the Visegrád Four (V4) countries: designing a governance model with(in) Europe

*Federica Cristani**

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.

Starting from an analysis of the most relevant cybersecurity challenges to foreign companies and their regulatory protection at the international, European, Visegrád Four (V4) sub-regional and national levels – especially in Slovakia –, this paper aims at identifying which are the actors involved in the governance of cybersecurity of foreign investment.

This paper questions whether – and to what extent – it is possible to frame a governance system for cybersecurity of foreign investment at the regional level in the EU and at the sub-regional level in the V4 countries, with a special focus on Slovakia

* *2019 Think Visegrad Non-V4 Expert Fellow* at the Research Center of the Slovak Foreign Policy Association, Bratislava (Slovakia), *Visiting Professor* in the Jean Monnet Module "Foreign Policy of EU" at the School of International Economic Relations and Travel Business of the V.N. Karazin Kharkiv National University (Ukraine) and *co-editor* of the ENTER *Policy Brief Series*, an output of the COST Action CA17119 - *EU Foreign Policy Facing New Realities: Perceptions, Contestation, Communication and Relations*.

The author would like to express her gratitude to all the government officials and experts met in Bratislava for their time and interest in the research project, to Prof. Tomas Strazay and Prof. Alexander Duleba for the enriching talks about the research, to all the team members of the Research Center of the Slovak Foreign Policy Association for their warm welcome and outstanding support during the research stay and to all the participants at the public presentation of the research at the premises of the International Visegrad Fund for the insightful discussion. Sole liability of this analysis rests with the author and Think Visegrad - V4 Think-Tank Platform is not responsible for any use that may be made of the information contained therein.

This analysis was produced within the Think Visegrad Non-V4 Fellowship programme.

Contents

Executive Summary

(FOREIGN) COMPANIES/INVESTORS AND CYBERSECURITY CHALLENGES

More and more **companies** around the world are becoming the **target of cyberattacks** (e.g. in Slovakia, according to the IT provider GAMO, up to 53% of companies experienced cyber incidents in 2018). Also, more and more investors are including the evaluation of cyber-risks of their investment.

However, **we still lack**: (1) **relevant detailed public data** about cyber incidents (foreign) companies are victims of; and (2) a **harmonized terminology** at the international, European and national level on cybercrime and cybersecurity. Also within the V4 Group, each country has adopted different definitions for these concepts.

A MULTI-LEVEL AND MULTI-STAKEHOLDER APPROACH TO CYBERSECURITY OF FOREIGN INVESTMENT: THE V4 SUB-REGIONAL CONTEXT

We witness a **multi-level** and a **multi-stakeholder** approach to the topic of cybersecurity and investment protection, which has led to a fragmentation of the relevant regulations.

*Platforms of discussion can help in harmonizing regulations and policies; the **sub-regional context** may have a greater role in in this respect, serving at the same time as platform of discussion for countries and as a privileged channel for advocating national interests at the (next) regional (and international) level.*

THE LEGAL FRAMEWORK OF REFERENCE AT THE INTERNATIONAL LEVEL…

A the **international level**, there is no unique instrument dealing with **cybersecurity and cybercrime**; there exist a number of international organizations and multilateral initiatives dealing with this issues.

With respect to the **investment law framework,** large part of international investment agreements (IIAs) and bilateral investment treaties (BITs) have been concluded before the emergence of cybersecurity concerns. An update in the language of IIAs and BITs is required in order to expressly refer to cybersecurity challenges.

In the field of **international trade law**, specific provisions on cybersecurity have started to be included in free trade agreements (FTAs): e.g. Article 19.15 of the U.S.-Mexico-Canada trade agreement.

…AT THE EU LEVEL…

Different EU institutions are involved in **cybersecurity** issues: the European Parliament and the Council; the European Commission; EU agencies (the EU Network and Information Security Agency (ENISA); the

Europol's European Cybercrime Centre (EC3); the Computer Emergency Response Team (CERT-EU); the European Defence Agency (EDA)); the European External Action Service (EEAS).

The EU legal framework on cybersecurity includes: the 2016 Directive on Security of Network and Information Systems (NIS Directive); the 2016 General Data Protection Regulation (GDPR); the 2018 Directive establishing the European Electronic Communications Code; the 2019 Cybersecurity Act and the most recent EU toolbox of risk mitigating measures in the field of cybersecurity of 5G networks (adopted on 29 January 2020).

In the field of **cyberdefence**, in 2017 the *Joint EU Diplomatic Response to Malicious Cyber Activities* (the so-called *cyber diplomacy toolbox*) was developed.

As regards **investment protection**, the 2009 Lisbon Treaty has included foreign direct investment in the exclusive competence of the EU; 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. To date, this has never happened.

…AT THE SUB-REGIONAL LEVEL: THE V4 GROUP…

To date there has been no significant joint document on cybersecurity and/or investment protection issued by the V4 group; however, we can find programmatical references in some V4 official documents e.g. in V4 Presidency Programs, in the 2011 Bratislava Declaration on the occasion of the 20th anniversary of the Visegrad Group; as well as during V4+ meetings).

Within the V4 region, worth mentioning is the (technical) cooperation in cybersecurity through the Central European Cybersecurity Platform (CECSP)

Each of the V4 country: (1) has its own cybersecurity-related regulation; (2) has its own investment promotion policy; in the field of investment protection, each country can conclude BITs with non-EU third countries only with the prior authorization of the European Commission

All V4 countries are part of the Budapest Convention and of the major international *fora* discussing cybersecurity issues; they have also acceded the main international economic organizations and treaties.

…AND AT THE NATIONAL LEVEL: SLOVAKIA

The main documents on **cybersecurity** are: the Cyber Security Concept of the Slovak Republic for years 2015-2020 + Action Plan; Act No. 69/2018 Coll on cybersecurity (Cybersecurity Act).

As regards the **organizational framework**, the following governmental institutions are involved in cybersecurity issues: the National Security Authority (NBU) and the National Cyber Security Centre (SK-CERT); the Office of Deputy Prime Minister for Investments and Informatization, with a Government CSIRT; other CSIRTs within the framework of the Ministry of Economy (Industry CSIRT), the Ministry of Defence (CSIRT.MIL.SK), as well as other Ministries (sector CSIRTs).

There exist collaborations with other actors at the international, European and bilateral level with other (non-)EU countries.

Non-institutional actors engaged in cybersecurity and cybercrime issues include: companies (e.g. through platforms like Industry4UM); security service providers.

As regards **investment protection,** one of the most recent acts in Slovakia was the 2018 Act on Regional Investment Aid; the **institutional actors** dealing with foreign investment include: the Slovak Investment and Trade Development Agency (SARIO); the Ministry of Finance.

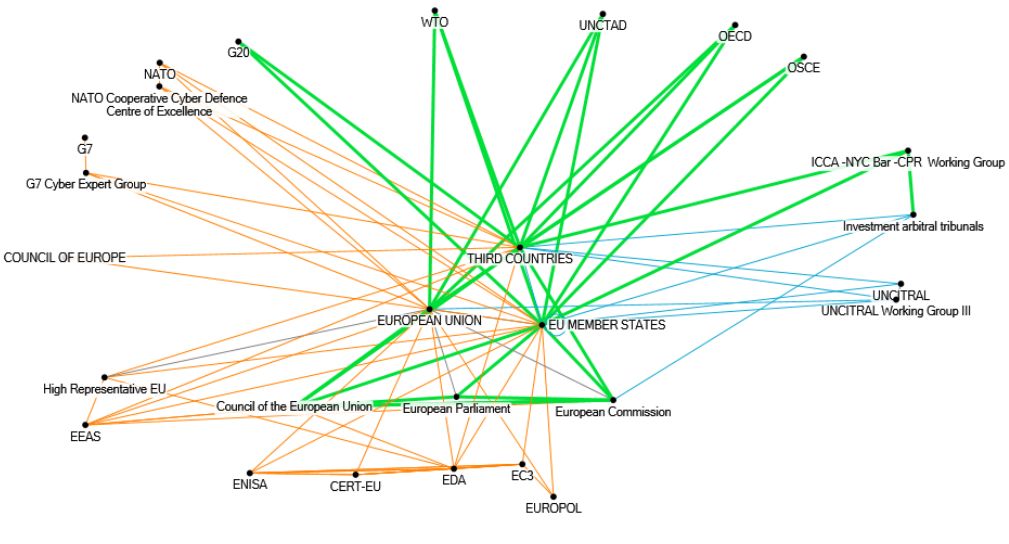
Non-institutional actors supporting the business of foreign investors include: law firms, Chambers of Commerce, the Investment Support Association (ISA).

A MAPPING EXERCISE WITH THE SOCIAL NETWORK ANALYSIS

The **social network analysis** allows: (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.

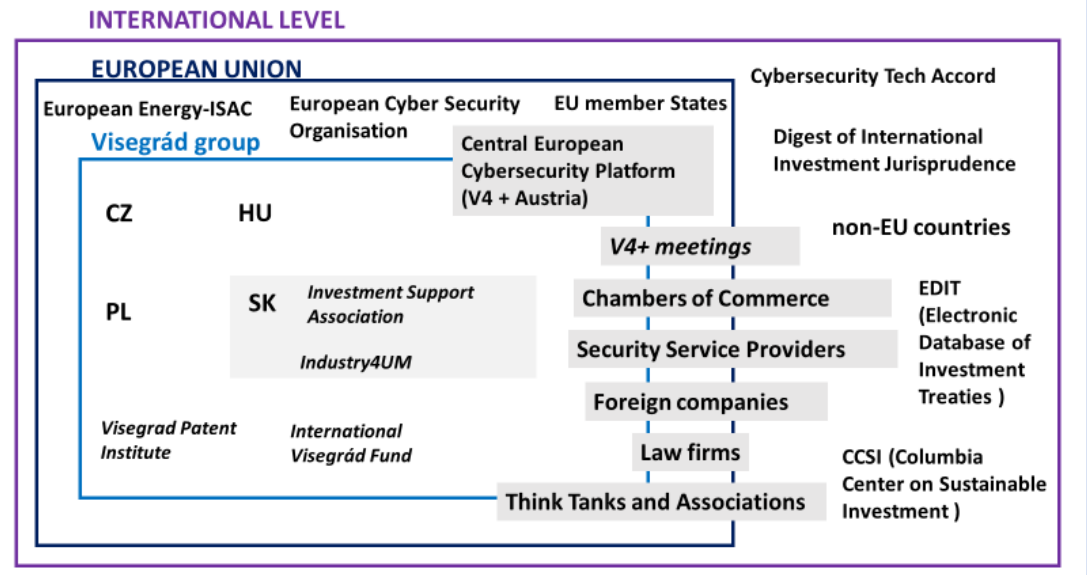
Starting from a matrix of **key (institutional) actors at the European and international level** that are active in the field of (1) foreign investment protection and/or (2) cybersecurity, the following visualization has been developed, using NodeXL.

ORANGE: interaction in the field of cybersecurity;
LIGHT BLUE: interaction in the field of investment promotion and protection;
GREEN: interactions in both fields of cybersecurity and investment protection (even though the interactions do not Occur simultaneously in both fields)



Created with NodeXL (http://nodexl.codeplex.com)

As regards **non-governmental stakeholders and foreign investors**, the following picture summarizes the map of relevant actors, with a focus on the V4 sub-regional framework.



MAIN FINDINGS AND STEPS FORWARD

The following steps should be taken into consideration for a more comprehensive understanding of cybersecurity issues of foreign investment:

- *For national governments*
  - Cooperating for a more harmonized vocabulary on cybersecurity;
  - Introducing cybersecurity concerns in the negotiation tables on international investment protection;
  - Using the existing international platforms of discussion on cybersecurity issue in order to introduce questions related to investment protection;
- *For the Visegrad group*
  - Introducing more comprehensive talks on cybersecurity concerns in investment protection in the V4 agenda;
- *For (foreign) companies*
  - Becoming active players in raising awareness within national, European and international *fora* on cybersecurity investment-related issues;
  - Using existing platforms for discussion in order to engage with national governments in order to bring their vision on cybersecurity investment-related issues.

1. (Foreign) Companies and cybersecurity challenges

Increased global digitalisation has brought both economic benefits as well as cybersecurity challenges;[1] more and more companies around the world are becoming the target of cyberattacks.

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.[2] This incident was not an isolated case; cyberattacks to businesses worldwide appear in the news every day.[3] In Slovakia, according to the report of the IT provider GAMO of November 2019, up to 53% of companies in Slovakia have experienced cyber incidents;[4] in Czech Republic, the Czech Statistical Office reported that 1 in 5 domestic company faced a cyberattack in 2018;[5] the *5th issue of the Global State of Information Security Survey* report drafted by PwC Polska found that 44% of Polish companies suffered financial losses due to cyberattacks;[6] and in Hungary, around 50% of large companies have addressed cyber security issues, as reported by EURACTIV Slovensko.[7] All in all, according to a survey conducted by Legal Week Intelligence and CMS, "CEE companies realise that cyber threats are for real and require effective measures to protect against".[8] Most recently, the World Economic Forum's *Global Risks*

[1] UNCTAD, *World Investment Report 2017. Investment and the Digital Economy* (UNCTAD, 2017), 187, http://unctad.org.

[2] 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.

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

[4] Even though this data could be higher, since companies are not likely to admit this kind of attacks. See GAMO, 'Vzdelávajte sa v téme kyberbezpečnosti' *GAMO* (12 November 2019), https://www.gamo.sk/novinky/vzdelavajte-sa-v-teme-kyberbezpecnosti.

[5] B. Kenety, 'ČSÚ: nearly 1 in 5 Czech companies faced cyberattack in 2018' *Radio Prague International* (13 January 2020), https://www.radio.cz/en/section/business/csu-nearly-1-in-5-czech-companies-faced-cyberattack-in-2018.

[6] PwC Polska, 'Cyber-roulette in Poland. Why do companies try their luck when dealing with cybercriminals?' *5th Issue of the Global State of Information Security Survey* (2018), https://www.pwc.pl/en/services/cyber-security.html.

[7] A. Zachová, E. Zgut, K. Zbytniewska, L. Yar, 'Is Visegrad group ready for cyber-attacks?' *Visegrad.info* (7 May 2018), https://visegradinfo.eu/index.php/collaborative/560-is-visegrad-group-ready-for-cyberattack.

[8] Legal Week Intelligence and CMS, *The Cybersecurity Challenge in Central and Eastern Europe. Are multinational companies prepared?* (November 2018), https://cms.law/en/hun/publication/the-cybersecurity-challenge-in-central-and-eastern-europe.

Report 2019, published on 15 January 2020, highlights that cyber-attacks have become a concern for individuals, governments and businesses.[9]

The consequences of cyberattack have ranged from money losses and information theft to infrastructure destabilization.[10] By 2021, it is estimated that cybercrimes will cost companies around the world about $6 trillion per year.[11]

Companies face different types of cyber-attacks. According to the ENISA's *Threat Landscape Report 2018* – which provides an overview of cyber threats occurred from December 2017 to December 2018 – in 2018 the most frequent (documented) cyber-threats have been: malware; web-based attacks; phishing attacks; spam; denial of service; ransomware; insider threat; data breaches; information leakage; cryptojacking and cyber espionage.[12] Moreover, more and more critical infrastructure — such as telecommunications, transport, and health care — have become the target of cyber-attacks.[13]

1.1. Lack of data on cyber incidents

When talking about cyberattacks to companies, it should be highlighted from the outset the lack of relevant detailed public data about cyber incidents they are victims of. As also affirmed in the 2018 Principles for Responsible Investment (PRI)[14]'s Report, *Stepping up governance on cyber security,*[15] while there is increasing awareness of companies about cyber risks and the need to deal with them, still there is a general lack of information publicly disclosed on cyberattacks. Companies generally do not disclose to the public either the cyberthreats they have been victim of, neither the measures they adopt to deal with cyber challenges (due to a number of reasons, including the fear of bad reputation

[9] World Economic Forum, *The Global Risks Report 2019. 14th Edition* (World Economic Forum, 2020), 16, https://www.weforum.org/reports/the-global-risks-report-2019.
[10] 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.
[11] Id., 551.
[12] 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.
[13] J.P. Meltzer, 'Cybersecurity and digital trade: What role for international trade rules?' *Global Economy & Development Working Paper* 132 (November 2019), 1, https://www.brookings.edu/research/cybersecurity-and-digital-trade-what-role-for-international-trade-rules.
[14] PRI is an investor initiative in partnership with UNEP Finance Initiative and the UN Global Compact.
[15] V. Ravishankar, O. Mooney, N. Hader, *Stepping up governance on cyber security. What is corporate disclosure telling investors?* (Principles for Responsible Investment (PRI), UNEP Finance Initiative, UN Global Compact, 2018), https://www.unpri.org/download?ac=5134.

in case of disclosure of cyberattacks or the fear to become a target or vulnerable to hackers).[16] On the other hand, companies recognize the need to cooperate in order to deal with cyber challenges and the advantages of sharing of knowledge and best practices, also with national institutions.[17] The lack of clear and comprehensive data, however, is surely an obstacle when it comes to understand how to regulate in the most efficient way this phenomenon.

A study that was prepared in 2018 for the European Commission on cyber theft of trade secrets[18] confirmed that there is limited qualitative and quantitative information available on cyber theft of trade secrets[19] and calls for a more appropriate regulatory framework in the field.[20]

At the national level, we can find some data and statistics, but they are generally not comprehensive and detailed. In the V4 region, for example we can rely on the following sources:

- Slovakia: website of National center for cybersecurity SK-CERT[21] and the annual report of the national CSIRT.SK;[22]
- Czech Republic: website of the National Cyber Security Center[23] and the Cyber Security Status Reports and Security Incidents Reports;[24]
- Poland: incident reports prepared by CERT Polska;[25]
- Hungary: website of the National Institute of Cyber Defense (NKI) of the National Security Service;[26]

Moreover, we can rely on reports and data published by private companies and institutions.[27]

---

[16] 'Investor-company dialogue on cyber security: five emerging findings' *PRI (Principles for responsible investment) - Governance Issues* (24 September 2018), https://www.unpri.org/governance-issues/investor-company-dialogue-on-cyber-security-five-emerging-findings/3664.article.

[17] Id.

[18] European Commission, *Trade secrets*, https://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en.

[19] PricewaterhouseCoopers, *Study on The scale and impact of industrial espionage and theft of trade secrets through cyber*, document prepared for the European Commission (18 December 2018), 15 https://ec.europa.eu/docsroom/documents/34841.

[20] Id., 42.

[21] See https://www.skcert.sk/en/statistics/index.html.

[22] See the latest report available https://www.csirt.gov.sk/doc/CSIRT-SK-Report-2016.pdf.

[23] See https://www.govcert.cz/cs/informacni-servis/hrozby.

[24] See https://www.govcert.cz/cs/informacni-servis/publikace.

[25] See https://www.cert.pl/en/news/single/incidents-and-incident-reports-in-2018.

[26] See https://nki.gov.hu.

[27] An interesting initiative in this respect is the Digital and Cyberspace Policy program's cyber operations tracker, a public database of state-sponsored incidents that have occurred since 2005, where anyone can contribute in sending information about know cyber-incidents. The initiative is carried out within the US-based Council on Foreign Relations think tank: https://www.cfr.org/interactive/cyber-operations#CyberOperations.

1.2. Lack of harmonized terminology on cybersecurity and cybercrime

Also as regards the question of terminology, there is no uniformity at the international, European and national level. Actually, 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.[28]

EU's conception of cyber-security is rather broad. On the other hand, according to the Recommendation ITU-T X.1205 of the International Telecommunication Union

> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; confidentiality.[29]

Also at the national level, we may find different definitions; in Poland, for example,

> security of network and information systems" or "cybersecurity" or "ICT security" means the resilience of ICT systems, at a given level of trust, to any actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted, or processed data or the related services offered by, or accessible via, those networks and information systems.[30]

In Slovakia, cybersecurity is defined as

> a state in which the networks and information systems have the capability to resist, at a certain reliability level , against any conduct threatening the availability, authenticity, integrity or confidentiality of the

---

[28] 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

[29] Recommendation ITU-T X.1205 (18 April 2008), https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1205-200804-I!!PDF-E&type=items.

[30] National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022 (2017), 27, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013.

> stored, transferred, or processed data or related services provided and available through these networks and information systems.[31]

In Czech Republic,

> Cyber security comprises a sum of organizational, political, legal, technical, and educational measures and tools aiming to provide a secure, protected, and resilient cyberspace in the Czech Republic for the benefit of both public and private sectors, as well as for the general public. Cyber security helps to identify, evaluate, and resolve cyber threats, to reduce cyber risks and to eliminate impacts of cyber attacks, cyber crime, cyber terrorism and cyber espionage by enhancing confidentiality, integrity, and availability of data, information systems and other elements of information and communication infrastructure. The main purpose of cyber security is protection of cyber space to allow the individuals' right to informational self-determination to be realized.[32]

While in Hungary,

> Cyber security is the continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace.[33]

Also when it comes to cybercrime, the terminology varies. According to 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 unique to computers and information systems (e.g. attacks against information systems, denial of service and malware).[34]

According to the Tallinn Manual 2.0, Rule 92,

> […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. […].[35]

---

[31] Article 3a let g) of the Act on Cybersecurity (30 January 2018), https://www.nbu.gov.sk/en/cyber-security/index.html.

[32] National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020 (2015), 5, https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/czech-republic-national-cyber-security-strategy-2015-2020.

[33] National Cyber Security Strategy of Hungary (2013), para. 5, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy.

[34] European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication, cit., 3

[35] See M.N. Schmitt, L. Vihul, *Tallinn Manual 2.0 on the international law applicable to cyber operations* (CUP, 2017).

In general, a harmonized vocabulary on cybercrime and cybersecurity still lacks at the international, European as well as at the national levels. An effort towards harmonization in this regard would be a first step towards more harmonized policies and regulations on the topics at hand.

1.3. Why should (foreign) investors care about cybersecurity?

More and more investors are including the evaluation of cyber-risks of their investment;[36] in this respect, the World Economic Forum's Centre for Cybersecurity has developed a set of principles and a cybersecurity due-diligence assessment framework that can be used by investors when evaluating their businesses.[37]

One of the most notable (and known) examples of the impact of cybersecurity on an investment is the Marriott/Starwood hack, which was made public in 2018. Before Marriott and Starwood began negotiations on the acquisition, hackers had stolen about 500 million Starwood customer records, including payment information. Marriott unknowingly inherited Starwood's vulnerabilities; when the incident became public, the negative results for Marriott included a reputational damage and a loss in share price. [38]

On the other side, foreign companies and foreign investors should also take into consideration the national cyber-security (related) regulation they should comply with in the host country. For example, foreign companies have been worried about the most recent China's cybersecurity regulation of December 2019, which requires all foreign companies to switch to Chinese service providers; the concern of the companies include the effect this might have, among others, on the secrecy of their trade information.[39]

To date, there is no international regulation that applies in such cases.

---

[36] A. Pipikaite, M. Cheung, 'Investors have a role in securing our shared digital future' (8 July 2019) *World Economic Forum,* https://www.weforum.org/agenda/2019/07/why-cybersecurity-should-be-standard-due-diligence-for-investors.

[37] Id.

[38] S. Boyer, 'Top national cybersecurity expert: Every investment is at risk' *CNBC* (9 July 2019), https://www.cnbc.com/2019/07/09/top-national-cybersecurity-expert-every-investment-is-at-risk.html and J. Finkle, A. Panchadar, 'Marriott's Starwood database hacked, 500 million may be affected' *Reuters* (1 December 2018), https://www.reuters.com/article/legal-us-marriott-intnl-cyber/marriotts-starwood-database-hacked-500-million-may-be-affected-idUSKCN1O02VH.

[39] S. McCarthy, 'Will China's revised cybersecurity rules put foreign firms at risk of losing their secrets?' *South China Morning Post* (13 October 2019), https://www.scmp.com/news/china/diplomacy/article/3032649/will-chinas-revised-cybersecurity-law-put-foreign-firms-risk.

1.4. How international/European/sub-regional/national policies deal with cybersecurity of foreign investment? The focus on the V4 sub-regional context within a multi-level and a multi-stakeholder approach

While the consequences of cyberattacks on (foreign) companies are clear, less clear is how to deal this problem at the regulatory level. Overall, the approach appears rather fragmented at every level of regulation: at the international, European, as well as at the sub-regional and national levels.

In general, we can highlight a constant tension between, on the one hand, the development of cybersecurity concerns that know no borders (any cyber-incident may originate in one country/countries and have effects on other country/countries), and, on the other hand, the adoption of (normative) policies at each level of regulation (international, European, sub-regional and national) that do not seem harmonized. The same holds true when it comes to the field of international investment protection: foreign investors are subject to international agreements, EU-specific policies and regulations (especially from 2009, when the EU gained exclusive competence on foreign direct investment), as well as to the national regulatory environment of the host state.

Moreover, both in the field of cybersecurity and investment protection, different (non-)governmental actors are involved in the definition and implementation of the relevant regulations and policies.

All in all, we witness a multi-level and a multi-stakeholder approach to the topic of cybersecurity and investment protection, which has led to a fragmentation of the relevant regulations.

Platforms of discussion can help in harmonizing regulations and policies; the present paper claims that the sub-regional context may have a greater role in in this respect, serving at the same time as platform of discussion for countries and as a privileged channel for advocating national interests at the (next) regional (and international) level. Indeed, in contrast to international organizations, regional and more in particular sub-regional organizations generally consist of states in close proximity to each other, with similar political, social, economic, cultural, and historic experiences. Accordingly, this kind of *fora* can be an appropriate context where to discuss national, regional and international issues; exchanges of best practices, experiences and knowledge might work better within a small(er) group of countries.[40]

[40] For an empahsis of the role of regional and sub-regional entities in shaping the international agenda, see for example the joint research project carried out by the United Nations Institute for Disarmament Research and the Monterey Institute of International Studies Center for Nonproliferation Studies on the role of (sub-)regional organizations in implementing UN Security Council Resolution 1540, described in the paper by J. Bergenas, 'The role of regional and sub-regional organizations in implementing UN Security Council Resolution 1540: a preliminary assessment of the African continent' (2008),

Back to 1997, James Crawford, current Judge at the International Court of Justice, was writing:

> although the situation of every State or nation may be attributed to its "'place in the world", that "place" tends first of all to be seen in terms of its immediate neighbours and its own region. Moreover in many cases the things which Governments and officials spend most time on, and which they can do most to affect, tend to be issues relating to neighbours or to the region. Even when the focus is on matters of apparently universal concern, the approach of many Governments is likely to be profoundly affected by regional postures and implication.[41]

While Crawford was referring to regional contexts in general, this description seems to fit well also for the sub-regional level, which becomes an important framework of reference.

For the scope of this paper, we have focused the analysis on the sub-regional context – in particular on the sub-regional context in Europe – taken the V4 group as the privileged point of observation.

Europe is a very important actor when it comes to cybersecurity and international investment regulations; as detailed better in the next paragraphs, it has built up a quite robust regulatory framework for cybersecurity and gained more and more importance in investment protection due its exclusive competence in foreign direct investment since the 2009 Lisbon Treaty. Europe includes different sub-regional formations, which have begun to emerge among states geographically close to each other and with similar political, social, economic, cultural, and historic experiences since late 1980s.[42] Today, a number of sub-regional groupings of states exists, such as Benelux,[43] the Nordic Council,[44] the Central European Initiative[45] and the Baltic cooperation,[46] just to name a few.[47]

http://www.vertic.org/media/assets/nim_docs/background%20articles/UNIDIR%20Scheinman%201540%20pdf2-act341.pdf.

[41] J. Crawford, 'Universalism and regionalism from the perspective of the work of the International Law Commission', in United Nations (ed.), *Internationlal Law on the Eve of the Twenty-fist Centuy. Views from the International Law Commission* (United Nations, 1997), 101.

[42] C. Gebhard, 'Sub-Regional cooperation in Central Europe – past, present and future' 12 *AARMS* 1 (2013), 26.

[43] The Benelux Union includes Belgium, The Netherlands and Luxembourg. See the official website https://gouvernement.lu/en/dossiers/2018/benelux.html.

[44] It includes 87 members, from Denmark, Finland, Iceland, Norway, Sweden, the Faroe Islands, Greenland and Åland. See the official website https://www.norden.org/en/nordic-council.

[45] It is a regional organization made up of fifteen members: Albania, Austria, Belarus, Bosnia-Herzegovina, Bulgaria, Croatia, the Czech Republic, Hungary, Italy, Macedonia, Poland, Romania, Slovakia, Slovenia and Ukraine. See the official website https://www.cei.int.

[46] It includes Estonia, Latvia, and Lithuania. For more information visit https://vm.ee/en/baltic-cooperation.

[47] A. Rudka, ‚Central Europe: regional cooperation and beyond', in T. Hayashi (ed.) *The emerging new regional order in Central and Eastern Europe* (Hokkaido University, 1997), 196-197.

Especially in Central and Eastern Europe, almost every country is involved in at least one of sub-regional groupings; one of the most significant examples in this respect is the V4.[48]

The V4 group is of special importance both for investment protection and when it comes to cybersecurity challenges.

The V4 countries attract foreign investments worldwide; according to the Ernst & Young's 2019 *European Attractiveness Survey*, Central and Eastern Europe is perceived as the second most attractive region for foreign investors worldwide, right after Western Europe.[49] They have concluded manifold international investment-related agreements (almost the 18% of the international investment-related agreements that are currently in force worldwide) and are often involved in investment state dispute settlements (almost 12% of the currently known treaty-based investor-state arbitrations have involved either Slovakia, Hungary, Poland or Czech Republic).[50]

The V4 is also an important region when it comes to cybersecurity and each V4 country has been quite active in this respect. Apart from the cybersecurity regulatory policies described in the next paragraphs, suffice to remind that the Polish Kosciuszko Institute Association is the creator of the annual CYBERSEC Forum, an annual public policy conference dedicated to the strategic challenges of cybersecurity, a unique in Central and Eastern Europe,[51] and that the Slovak OSCE Chairmanship organized an OSCE conference on the future of Cybersecurity on 17-18 June 2019 in Bratislava.[52]

Moreover, the V4 group has emphasised in different occasions the importance of cybersecurity, including, among others in the 2011 Bratislava Declaration on the occasion of the 20th anniversary of the Visegrad Group:

> […] The Visegrad Group will actively contribute towards international efforts in combating […] security threats and challenges, including those in the area of *cybersecurity* […]. [emphasis added][53]

The V4 countries are also parties, together with Austria, of the Central European Cybersecurity Platform (CECSP) and adopted the *Warsaw Declaration on mutual co-operation in research, innovation and digital affairs* in 2017, in which

[48] Gebhard, cit. 26.
[49] Ernst & Young, *European attractiveness survey* (2019), https://www.ey.com/en_gl/attractiveness.
[50] For all the data see http://investmentpolicyhub.unctad.org.
[51] See the official website https://cybersecforum.eu/en/poland/organiser.
[52] See the relevant news on the OSCE website https://www.osce.org/chairmanship/422954.
[53] The Bratislava Declaration of the Prime Ministers of the Czech Republic, the Republic of Hungary, the Republic of Poland and the Slovak Republic on the occasion of the 20th anniversary of the Visegrad Group (15 February 2011).

> […t]he Visegrad Group agrees to […] adopt[…] the following Warsaw Declaration on mutual co-operation in research, innovation and digital affairs as follows: […] to work towards *sustainable, efficient, resilient and secure cyber space* based, inter alia, on *timely and proper implementation of the NIS Directive*, allowing the joint internal market *for the high-level cyber security and protection of critical information infrastructures and resources* […]. [emphasis added][54]

It is therefore relevant to understand how cybersecurity concerns of foreign investors can be dealt with not only at the international and EU level, but also at the sub-regional level of the V4. In November 2018, a study on how multinational companies deal with cybersecurity challenges more broadly in the Central and Eastern Europe was carried on by Legal Week Intelligence and CMS; even though the report does not tackle the relationship between cybersecurity challenges and trade and investment policies, it highlights the importance of cybersecurity for businesses in the region.[55]

The following paragraphs analyse how the V4 group discusses and channels these global issues; since the countries are the essential element of each regional and sub-regional group, the analysis would not be complete without reference also to the national level. In this framework, we have chosen Slovakia, as member of the V4 and privileged point of analysis where the research has been based and conducted.

The following paragraphs deal with the question of how cybersecurity concerns relating to foreign investment can be dealt with within the investment and cybersecurity regulatory frameworks, at the international (para 2), European (para 2.1) and sub-regional levels of the V4 group (para 2.2.), as well as at the national level, with a special focus on Slovakia (para 2.3). The attention is on the main actors involved, and the aim is to draw a map of actors by using the social network analysis method (para 3); finally, the main findings and steps forward are presented (para 4).

The choice to deal with each level of regulation from the international to the national one follows the nature of the topics at stakes: both cybersecurity challenges and international investment protection have a global dimension and the aim of this paper is to show how such global topics present also 'regional', 'sub-regional' and 'national' connotations.

[54] Joint Declaration of Intent of Prime Ministers of the Visegrad Group on Mutual Co-operation in Innovation and Digital Affairs - "Warsaw Declaration" adopted at the CEE Innovators Summit in Warsaw on March 28, 2017 (28 March 2017).

[55] See the report by Legal Week Intelligence and CMS, cit.

With respect to the methodology, this paper is based on existing literature, official documents and the thematic analysis of semi-structured interviews conducted during the research period at the Research Center of the Slovak Foreign Policy Association, Bratislava, with various key stakeholders: think tanks and associations, experts in cybersecurity and government officials. The identity of the interviewees and of the institutions have been anonymized.

2. Protection of foreign investment and cybersecurity challenges: the legal framework of reference at the international level…

At the international level, there is no unique instrument dealing with cybersecurity and cybercrime. The only binding instrument to date on cybercrime is the Convention on Cybercrime of the Council of Europe (the Budapest Convention),[56] 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.[57] The Convention does not include an express reference to protection of foreign investment;[58] however, States are committed to adopt national measures in order to criminalize computer-related offences and engage in international cooperation and mutual assistance.[59] Overall, the Budapest Convention has been used as a guideline for developing domestic legislation in the field.[60]

There are also a number of multilateral initiatives addressing cybercrime and cybersecurity issues at the international level, like the work of the G7 Cyber Expert Group,[61] the Council of Europe,[62] the G20[63],

[56] 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.

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

[58] Chaisse, Bauer, cit., 581

[59] Article 25 of the Budapest Convention.

[60] 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.

[61] 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.

[62] 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).

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

the United Nations,[64] the Organisation for Economic Cooperation and Development (OECD),[65] the Organisation for Security and Cooperation in Europe (OSCE)[66] and NATO.[67] Worth mentioning are also private codification initiatives like the Tallinn Manual, which deals with international law applicable in case of cyber war.[68]

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

It should be firstly underlined that large part of international investment agreements (IIAs) and bilateral investment treaties (BITs) have been concluded before the emergence of cybersecurity concerns:[69] for example, provisions of these treaties are not clear in identifying cryptocurrency as a form of investment;[70] 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.[71]

Under international investment law there is no uniform definition of 'investment', which is provided by the applicable IIA/BIT.[72] Many treaties provide a non-exhaustive list of examples of investment,

[64] The UN introduced cybersecurity in its agenda since its 1999 Resolution 53/70 on 'Developments in the Field of Information and Telecommunications in the Context of International Security' and the following 2015 report of the Group of Governmental Experts (UNGGE) on responsible state behaviour in cyberspace. See also 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.

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

[66] 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.

[67] 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#).

[68] 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.

[69] UNCTAD, *World Investment Report 2017*, cit. 187.

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

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

[72] Id., 555.

including a reference to 'every kind of asset'.[73] 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';[74] 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.[75]

As regards the question of cybersecurity of foreign investment, it has been argued that the fair and equitable treatment (FET) and the full protection and security (FPS) standards included 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 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, enioyment or disposal thereof through unjustified or discriminatory measures.[76]

FET provisions may allow investors to pursue cyber claims where, for example, the host state implements new regulations,[77] 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.[78]

Also FPS provisions - very common in IIAs/BITs - may be relevant; FPS provisions are generally drafted like the following:

---

[73] 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.

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

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

[76] Argentina - Bulgaria BIT (1993).

[77] 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. See 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.

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

> Article 4 (1) Investments by investors of either Contracting State shall enjoy full protection and security in the territory of the other Contracting State […][79]

The interpretation of FPS provisions has traditionally included physical protections from army, militants, and rioters.[80] 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.[81] 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 in case of cyberattacks or fails to prosecute cyber criminals),[82] the breach of the FPS obligation may be claimed.[83]

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).[84] However, the FPS standard 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 to the Budapest Convention.[85] However, the principle of proportionality applies:[86] if foreign investors invest in less developed countries, they cannot expect cybersecurity protections equivalent to those applicable in developed countries.[87]

When dealing with cyberattacks to foreign investment, we should also note that host states may invoke national security reasons – and the relevant provisions included in the applicable IIA/BIT - in

[79] Afghanistan - Germany BIT (2005). Looking at BITs concluded, for example, by Slovakia, we can recall the FET and FPS commitments included in the Slovakia-Moldova BIT (2009), article 2(2): "[...] Investments made by investors of each Contracting Party shall be accorded fair and equitable treatment and shall enjoy full protections and security in the territory of the other Contracting Party. Neither Contracting Party shall in any way impair by unreasonable or discriminatory measures the operation, management, maintenance, use, enjoyment or disposal of investments in its state territory by investors of the other Contracting Party".

[80] Chaisse, Bauer, cit., 578.

[81] *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.

[82] 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.

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

[84] Id., 580.

[85] Id., 582.

[86] 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.

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

response to alleged cyber espionage or when changing cybersecurity national regulations to the detriment of foreign investors.[88]

In the field of international trade law, there have been already studies underlying how data-flow restrictions, data-localization requirements, and import restrictions on information technology products may violate various World Trade Organization (WTO) and free trade agreement (FTA) commitments. While also in this case the invocation of the security exceptions included in WTO Agreements and FTAs has been suggested as a possible way of justification, it has also been underlined how such provisions are not appropriately drafted to address cybersecurity issues.[89] Accordingly, more specific provisions and policies are needed.

A first step in this direction would be the inclusion of a specific collaboration commitment on cybersecurity within the FTAs,[90] as already done in the U.S.-Mexico-Canada trade agreement, signed on 30 November 2018 and not yet in force, which comprises a new Chapter on Digital Trade (Article 19) and a provision dedicated to cybersecurity, according to which

> Article 19.15: Cybersecurity
>
> 1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:
>
> (a) build the capabilities of their respective national entities responsible for cybersecurity incident response; and
>
> (b) strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.
>
> 2. Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.[91]

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

[89] J.P. Meltzer, 'Cybersecurity and digital trade: What role for international trade rules?' *Global Economy & Development Working Paper* 132 (November 2019), 16, https://www.brookings.edu/research/cybersecurity-and-digital-trade-what-role-for-international-trade-rules.

[90] Id., 26.

[91] Canada-United States-Mexico Agreement (CUSMA); see the Protocol replacing the North American Free Trade Agreement with the Agreement Between the United States of America, The United Mexican States, and Canada,

This provision undertakes a risk-based approach to cybersecurity, which is tailored to the "evolving nature of cybersecurity threats".

It is also worth noting that during the negotiations of this agreement, 10 major cybersecurity companies in the U.S. sent a letter on 9 August 2017 – which was also made public online -[92] to the United States Trade Representative and the Secretary of Commerce, asking for discussion on "cybersecurity trade issues in the upcoming modernization of the North American Free Trade Agreement"; in particular they were asking for a "discussion of how to work toward global cybersecurity standards and global norms". Though the final text of the agreement does not incorporate all the suggestions put forward by these companies, it did include reference to cybersecurity, which can be regarded as a first step towards (hopefully) a new generation of FTAs.

The U.S.-Mexico-Canada trade agreement is one of very first agreements including a cybersecurity-related provision in its text.[93] To date, only the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), a FTA between Canada and 10 other countries in the Asia-Pacific region: Australia, Brunei, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore and Vietnam,[94] has included a cybersecurity-related provision (in the Chapter dedicated to electronic commerce):

> Article 14.16: Cooperation on Cybersecurity Matters
>
> The Parties recognise the importance of:
>
> (a) building the capabilities of their national entities responsible for computer security incident response; and
>
> (b) using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties.

Other FTAs have included provisions on electronic trade, with some very vague reference to cybersecurity. In the EU region, we can recall the EU-Japan Economic Partnership Agreement

https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/text-texte/toc-tdm.aspx?lang=eng.

[92] See the website https://www.tenable.com/blog/cybersecurity-s-role-in-u-s-trade-agreements-starting-with-nafta.

[93] See also Asia Business Trade Association, 'FTA Digital Trade Regulations Comparison' *Asia Business Trade Association - Issue Paper* 01-19 (June 2019), http://asiantradecentre.org/talkingtrade/comparing-digital-rules-in-trade-agreements.

[94] The FTA was signed on 8 March 2018 and entered into force on 30 December 2018 for Canada, Australia, Japan, Mexico, New Zealand, and Singapore; on 14 January 2019, it entered into force for Vietnam. See official website https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/index.aspx?lang=eng.

(EUJEPA),[95] which includes a call for cooperation and sharing of information and best practices on cybersecurity when it comes to electronic commerce, while at the same time remarking the right of each party to regulate on this topic:

> Article 8.80. Cooperation on electronic commerce
>
> 1. The Parties shall, where appropriate, cooperate and participate actively in multilateral fora to promote the development of electronic commerce.
>
> 2. The Parties agree to maintain a dialogue on regulatory matters relating to electronic commerce with a view to sharing information and experience, as appropriate, including on related laws, regulations and their implementation, and best practices with respect to electronic commerce, in relation to, inter alia: […] (b) cybersecurity […]
>
> CHAPTER 18. GOOD REGULATORY PRACTICES AND REGULATORY COOPERATION
>
> SUB-SECTION 1. General provisions
>
> ARTICLE 18.1. Objectives and general principles
>
> 1. The objectives of this Section are to promote good regulatory practices and regulatory cooperation between the Parties with the aim of enhancing bilateral trade and investment […]
>
> 2. Nothing in this Section shall affect the right of a Party to define or regulate its own levels of protection in pursuit or furtherance of its public policy objectives in areas such as: […] (h) personal data and cybersecurity […]

Since all the above-mentioned FTAs are quite new agreements, it remains to be seen how they will be implemented, especially with respect to the cybersecurity-related provisions.

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.[96]

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

[95] The EU and Japan's Economic Partnership Agreement entered into force on 1 February 2019. See the official website https://ec.europa.eu/trade/policy/in-focus/eu-japan-economic-partnership-agreement.
[96] Chaisse, Bauer, cit., 587.

mentioning is the work of the OECD,[97] the United Nations Commission on International Trade Law (UNCITRAL) Working Group III,[98] OSCE[99] and UNCTAD.[100]

To date, there is no documented instance of international investment arbitration case dealing with cyberattacks (and cyberespionage) to foreign investment.[101]

On the other hand, there are some instances in which investment arbitral tribunals have dealt with the admissibility of leaked documents as evidence in the arbitral proceedings and where international arbitral proceedings have been compromised because of cyber intrusion during the proceedings themselves.

In the international investment case *ConocoPhillips v Venezuela*,[102] 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,[103] however, it did not mention the US diplomatic cables and their admissibility as evidence in the arbitral proceeding,[104] 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.[105] Only in one 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.[106] The Tribunal reasoned that, since the documents were

[97] 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).
[98] 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).
[99] 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).
[100] See UNCTAD's *Investment Policy Hub*, https://investmentpolicy.unctad.org.
[101] Also in Slovakia, as confirmed from an interview with a government official.
[102] *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).
[103] Decision on Respondent's Request for Reconsideration of 10 March 2014 and Interim Decision (17 January 2017).
[104] Ireton, cit., 240.
[105] Id., 238.
[106] Calvillo Ortiz, cit.

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 evidence in the proceedings.[107]

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.[108]

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.[109] The Protocol aims at offering a series of recommended standards that the parties can agree to adopt during international arbitration proceedings.[110]

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.[111] This cooperation method in drafting the document could serve also as a model for possible future documents in this field. However, communication of this instrument should be improved, and address all interested national institutions.[112]

---

[107] *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. and in G. Bertrou, S. Alekhin, 'The Admissibility of Unlawfully Obtained Evidence in International Arbitration: Does the End Justify the Means?' *Cahiers de l'Arbitrage / The Paris Journal of International Arbitration* (2018), 34.

[108] 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).

[109] 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.

[110] "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).

[111] See https://www.arbitration-icca.org/projects/Cybersecurity-in-International-Arbitration.html.

[112] At least in Slovakia, where the Protocol is not well known. From an interview with a government official.

2.1….at the EU level…

At the European Union (EU) level, we witness a rather robust set of regulations dealing with cybersecurity. However, to date there seems to be no comprehensive regulation of cybersecurity of foreign investment.

The EU has been always aware of the challenges of cybercrime to economic activities: the 2013 Cybersecurity Strategy of the EU[113] 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.[114]

In May 2017, the Commission expressly included cybersecurity as one of the three emerging challenges in its Digital Single Market Strategy mid-term review[115].

In the last years, cybersecurity has been at the heart of manifold EU regulations and policies,[116] both in the internal dimension of the EU policies - related to the Internal Market and the Area of Freedom, Security and Justice - and in the external one – related to the foreign and security policy.

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;[117] 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;

[113] European Commission, High Representative of the EU for Foreign Affairs and Security Policy, Joint Communication, cit.
[114] Id., 3.
[115] 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).
[116] European Court of Auditors, 'Challenges to effective EU cybersecurity policy' *Briefing Paper* (March 2019), 11-12.
[117] See the official website https://www.enisa.europa.eu/about-enisa/regulatory-framework.

- 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;[118]
- the Computer Emergency Response Team (CERT-EU), for the support of EU institutions, agencies and bodies;[119]
- the European Defence Agency (EDA), which supports EU member states in the development of their cyber defence capabilities;[120]

- 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.[121]

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),[122] 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;[123]

[118] 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-assessment.
[119] See the official website https://cert.europa.eu/cert/plainedition/en/cert_about.html.
[120] 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.
[121] 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.
[122] 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*.
[123] See Fernández-Samaniego, Hierro, cit. and Chaisse, Bauer, cit., 584.

- the 2016 General Data Protection Regulation (GDPR),[124] which has introduced the figure of the Data Protection Officer (DPO), who coordinates and controls the compliance with data protection regulations;[125] 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).[126] The GDPR applies to every organization that handles data belonging to EU citizens and residents, also outside the EU territory;[127]
- the 2018 Directive establishing the European Electronic Communications Code,[128] according to which member states should ensure the security of public communications networks;
- the 2019 Cybersecurity Act,[129] which has introduced:
    - a system of EU certification for information and communications technology (ICT) products, services and processes that would be recognised in all EU member states;[130]
    - 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.[131]

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[132] - which

[124] 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).
[125] Fernández-Samaniego, Hierro, cit.
[126] 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.
[127] Article 3 of the GDPR Regulation (https://gdpr.eu/companies-outside-of-europe).
[128] 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).
[129] 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).
[130] European Commission, *The EU cybersecurity certification framework* (2019), https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.
[131] European Council, *Cybersecurity in Europe: stronger rules and better protection* (11 July 2019), https://www.consilium.europa.eu/en/policies/cybersecurity/
[132] Commission Recommendation (EU) 2017/1584 of 13 September 2017 *on coordinated response to large-scale cybersecurity incidents and crises*, C/2017/6100.

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.

Just a few days before this policy paper was published, the EU released its toolbox of measures aimed at addressing the cybersecurity risks of 5G networks,[133] at both national and EU levels, building on the Commission Recommendation of 26 March 2019 on "Cybersecurity of 5G networks"[134] and the ENISA's *Threat Landscape for 5G Networks* report of 21 November 2019.[135] Indeed, 5G networks – connecting billions of objects and systems, including critical infrastructures – will bring (new) cybersecurity challenges.[136] The EU toolbox illustrates the series of strategic and technical mitigating measures and the relevant supporting actions. Member states are now required to adopt the first steps to implement the Key measures proposed in the toolbox by April 2020.[137]

With regards to the 5G network, the linkage between cybersecurity and economic matters seems to have raise the attention of the EU: recently, the Director for the Future Networks Directorate of DG CONNECT has remarked that "cybersecurity is not only a security issue, but also an internal market issue" and, accordingly, should be dealt with more comprehensively at the EU level.[138] Moreover, the EU toolbox document clearly states that "[t]he cybersecurity of 5G networks is […] essential to protect our economies […]".[139]

Furthermore, and for the first time in an EU cybersecurity-related document, an express reference is made to the relevance of foreign direct investment regulation in this field, to the extent that

> [i]n the area of trade policy, as of 11 October 2020, the EU's Foreign Direct Investment (FDI) Screening Regulation will provide an instrument to coordinate detection and address potential security risks related to foreign direct investments into the EU, amongst others, in sensitive areas such as critical technologies and critical infrastructures. Applied to the 5G toolbox, and in order to protect key 5G assets and avoid

[133] EU NIS Cooperation Group, *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures* (2020), published on 29 January 2020, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[134] Commission, *Recommendation on 'Cybersecurity of 5G networks'*, 26 March 2019, C(2019) 2335 final.

[135] ENISA, *Threat Landscape for 5G Networks* (21 November 2019), https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

[136] For more detailed information, see https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

[137] For an overview of the timetable of implementation, see the *EU Toolbox for 5G Security. Factsheet* (2020), https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[138] See E. Sánchez Nicolás, 'EU to unveil 5G 'toolbox' to tackle security threats' *EUObserver* (23 January 2020), https://euobserver.com/science/147238.

[139] EU NIS Cooperation Group, cit., 3.

> dependencies, the FDI screening mechanism can provide an important instrument to regularly and better monitor FDI developments into the EU along the 5G value chain […].[140]

According to the EU toolbox document, foreign direct investment regulation could become a useful instrument in guaranteeing cybersecurity of 5G networks within EU.

In the field of cyber-defence, in 2017 the *Joint EU Diplomatic Response to Malicious Cyber Activities*[141] (the so-called *cyber diplomacy toolbox*) was developed, based on the Council conclusions on cyber diplomacy.[142] 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.[143]

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).[144]

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.[145]

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

It remains to be seen whether the EU has also included cybersecurity aspects in international investment-related agreement that has negotiated so far. It is worth recalling that the 2009 Lisbon Treaty has included foreign direct investment in the exclusive competence of the EU; this means that

---

[140] EU NIS Cooperation Group, cit., 7.
[141] Council of the European Union, *Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities*, 9916/17, 7 June 2017
[142] Council of the European Union, *Council Conclusions on Cyber Diplomacy*, 6122/55, 11 February 201
[143] 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.
[144] Council of the European Union, *Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities*, 13007/17.
[145] Council Decision *concerning restrictive measures against cyber-attacks threatening the Union or its Member States*, 7299/19 (4 May 2019), para 7.

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.

To date, the EU already included investment provisions in its new trade agreements with Canada (provisionally entered into force on 21 September 2017)[146] and Vietnam (trade and investment agreements were signed on 30 June 2019)[147] and is also negotiating investment rules as part of its trade agreements with other third countries.[148]

The Canada - EU CETA includes a broad definition of investment, which might also include digital assets,[149] 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.

[146] Comprehensive Economic and Trade Agreement (CETA), https://ec.europa.eu/trade/policy/in-focus/ceta/.
[147] EU - Viet Nam Investment Protection Agreement, https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5868/download.
[148] For the update list of on-going negotiations with third countries, see http://trade.ec.europa.eu/doclib/docs/2006/december/tradoc_118238.pdf.
[149] Article 8.1 of CETA.

> 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 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,[150] 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. […].[151]

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 […][152]

As already recalled, the EU is engaging in the field of cybersecurity of 5G network. Given the importance of the sector for foreign investors (and the uncertainties of some member states whether or not to exclude some foreign investors from national 5G-tenders),[153] it remains to be seen whether EU and member states cybersecurity-related decisions in this field would raise issues (and eventual claims) within the international investment law framework.

---

[150] Article 8.29 of CETA.
[151] Article 8.31 of CETA.
[152] Article 3.42 of the EU - Viet Nam Investment Protection Agreement.
[153] See S. Stolton, 'The Capitals Special: Europe's 5G dilemma' *EURACTIV* (16 December 2019), https://www.euractiv.com/section/5g/news/the-capitals-special-europes-5g-dilemma.

In this regard, it is certainly to welcome the express reference in most recently released EU toolbox on cybersecurity of 5G networks to the role of FDI regulation, especially to the EU FDI screening Regulation,[154] in order to monitor FDI development within the EU territory. On the other hand, even though the FDI screening mechanism is specifically designed for monitoring FDI inflow in the EU on grounds of security or public order, its application might raise concerns as regards the observance of the above-mentioned FET and non-discrimination clauses of foreign investors included in IIAs/BITs.[155] Indeed, while the EU toolbox documents points out the role that the FDI screening regulation may have in guaranteeing cybersecurity of 5G networks within the EU territory, there is no reference to the safeguard of investment protection provisions to incoming FDI. As the cooperation mechanism envisaged by the FDI screening regulation will be operational from 11 October 2020, it remains to be seen how it will be applied, also in conjunction with the EU cybersecurity toolbox for 5G networks. All in all, this may open the way to a new understanding of the relationship between cybersecurity and FDI-related regulations.

2.2. …at the sub-regional level: the regulatory environment in the V4 countries…

Turning to the sub-regional level of the V4 group and the question of cybersecurity and investment protection in this area, it should be firstly recalled that all V4 countries, as EU member states, implement the relevant EU Directives and Regulations described in the previous paragraph within their territories.[156] Moreover, each of the V4 country has its own cybersecurity-related regulation; in the field of investment protection, instead, given the exclusive competence of the EU on foreign direct investment, each V4 country can conclude BITs with non-EU third country – when a relevant IIA does not exist or is under negotiation with the EU - only with the prior authorization of the European Commission. As regards BITs with non-EU countries, to date there is no public information regarding the negotiation of cybersecurity provisions in the relevant agreements or of any investment-related case that also involves cybersecurity questions.[157]

---

[154] Regulation (EU) 2019/452 of 19 March, 2019 *establishing a framework for the screening of foreign direct investments into the Union*.

[155] For a general comment on this, see N. Lavranos, 'Some Critical Observations on the EU's Foreign Investment Screening Proposal' *Kluwer Arbitration Blog* (2 January 2018), http://arbitrationblog.kluwerarbitration.com/2018/01/02/critical-observations-eus-foreign-investment-screening-proposal.

[156] A. Zachová, E. Zgut, K. Zbytniewska, L. Yar, 'Is Visegrad group ready for cyber-attacks?' *Visegrad.info* (7 May 2018), https://visegradinfo.eu/index.php/collaborative/560-is-visegrad-group-ready-for-cyberattack.

[157] At least in Slovakia, as confirmed from an interview with a government official.

All V4 countries have adopted a national cybersecurity strategy, which includes the framework of reference for future regulations and policies in the field:[158]

- Czech Republic: the National Cyber Security Strategy was adopted in 2015,[159] while the Cyber Security Law was issued in 2014 and amended in 2017;[160]
- Hungary: the National Cyber Security Strategy was adopted in 2013[161] and Hungary has implemented the EU NIS Directive in December 2017;
- Poland: the National Cyber Security Strategy was adopted in 2017;[162] Poland implemented the EU NIS directive in 2018;[163]
- Slovakia: the Cyber Security Concept of the Slovak Republic for years 2015-2020 with the accompanying Action Plan was adopted in 2015;[164] on 1 April 2018, Act No. 69/2018 Coll on cybersecurity – which implements the EU NIS Directive - came into force[165] (as described more in detail in the following paragraph).

All in all, the four countries do not present a harmonized regulatory framework as regards cybersecurity; the same holds true when it comes to consider the group in terms of economic environment and attractiveness of FDI. There are still considerable differences among them; suffice to recall, for example, that Slovakia introduced euro in 2009 and has been a member of euro zone since then, while three remaining V4 countries are still outside the euro zone.

At the national level, each V4 country has developed its own investment promotion policy and the four countries appear quite diverse in this respect; the only common feature seems the willingness to

[158] M. Górka, 'The Cybersecurity Strategy of the Visegrad Group Countries' 14 *Politics in Central Europe* 2 (2018), 75.
[159] See the official document at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-of-czech-republic-2011-2015.
[160] See the relevant information at https://www.cybersecurity.cz/basic_en.html.
[161] See the official document at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy.
[162] See the official document at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013.
[163] Zachová et al., cit.
[164] See the official texts, https://www.nbu.gov.sk/en/cyber-security/national-cyber-security-strategy/index.html.
[165] Zachová et al., cit.

attract FDI. And indeed, during the last years, the four countries have adopted policies aimed at increasing FDI in the region:

- Slovakia adopted the Act on Regional Investment Aid in 2018, providing new aids and incentives to investors;[166]
- Czech Republic introduced in 2015 a new amendment law on investment incentives;[167]
- Poland adopted in 2018 a new law on the promotion of investments;[168]
- Hungary established in 2014 an institutional triangle – comprising the Hungarian Investment Promotion Agency, the Hungarian Export Promotion Agency and EXIM Bank – in order to support the foreign trade focused foreign policy of the Hungarian Government, covering the fields of investment promotion, trade development and export financing.[169]

Furthermore, Poland and Czech Republic have created state-owned special economic zones, which are customs free and offer fiscal incentives to foreign investors.[170]

All V4 countries are part of the Budapest Convention and of the major international *fora* discussing cybersecurity issues, like NATO, OSCE and the UN. Within the EU, they collaborate, among others, with Europol, the European Cybercrime Center (EC3) and ENISA.[171]

All V4 countries have also acceded international economic organizations and treaties, like the Organization for Economic Cooperation and Development (OECD),[172] the International Monetary Fund

[166] See 'Slovakia adopted new law in the field of investment aid' *UNCTAD Investment Policy Monitor* (1 April 2018), https://investmentpolicy.unctad.org/investment-policy-monitor/measures/3272/slovakia-slovakia-adopted-new-law-in-the-field-of-investment-aid.

[167] Czech Republic adopted Act No. 84/2015, which entered into force on 1 May 2015, amending Act No. 72/2000 Coll. (Act on Investment Incentives). See 'Amendments to the Investment Incentives Act' *UNCTAD Investment Policy Monitor* (1 May 2015), https://investmentpolicy.unctad.org/investment-policy-monitor/measures/2829/czechia-amendments-to-the-investment-incentives-act.

[168] See 'Poland adopted new law on the promotion of investments' *UNCTAD Investment Policy Monitor* (10 May 2018), https://investmentpolicy.unctad.org/investment-policy-monitor/measures/3244/poland-poland-adopted-new-law-on-the-promotion-of-investments.

[169] For the relevant information see the report prepared by the Hungarian Investment Promotion Agency, *Invest in Hungary* (Hungarian Investment Promotion Agency, 2018), https://hipa.hu/images/publications/hipa-invest-in-hungary_2018_09_20.pdf.

[170] UNCTAD, *World Investment Report 2019. Special Economic Zones* (2019), 153-154, https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2460.

[171] M. Górka, 'The Cybersecurity Strategy of the Visegrad Group Countries' 14 *Politics in Central Europe* 2 (2018), 95.

[172] See https://www.oecd.org/about/members-and-partners.

(IMF),[173] the World Bank[174] and the World Trade Organization (WTO)[175] and are all parties to the Energy Charter Treaty,[176] to the Multilateral Investment Guarantee Agency[177] and to the New York Arbitration Convention on the recognition and enforcement of foreign arbitral awards,[178] while all V4 countries but Poland are part of the Convention on the settlement of investment disputes between states and nationals of other states (ICSID).[179]

And what about the role of the Visegrád group in the field of cybersecurity and international investment protection?

The Visegrád group was established as a forum for sub-regional cooperation on 15 February 1991, when the heads of governments of Czechoslovakia (now Czech Republic and Slovakia), Hungary and Poland signed the Declaration of Visegrád.[180] One of the first aim of the V4 was "[…the] full involvement in the European political and economic system […]".[181]

The V4 is 'weakly' institutionalized - the only organizations being the International Visegrád Fund[182] and the Visegrad Patent Institute[183] - and works according to the principle of cooperation through high-level political summits, expert and diplomatic meetings, activities of non-governmental associations in the region, think tanks and research bodies.[184]

The outcomes of the V4 meetings can be political documents including remarks and reflections on EU legislative acts and proposals, joint declarations or other political statements.[185] Worth recalling are also the joint declarations of the ministers of the V4 countries on European Commission

[173] See https://www.imf.org/external/np/sec/memdir/memdate.htm.
[174] See https://www.worldbank.org/en/about/leadership/members.
[175] See https://www.wto.org/english/thewto_e/countries_e/org6_map_e.htm.
[176] See https://energycharter.org/process/energy-charter-treaty-1994/energy-charter-treaty.
[177] See https://www.miga.org/member-countries.
[178] See http://www.newyorkconvention.org/countries.
[179] See https://icsid.worldbank.org/Pages/PageNotFoundError.aspx?requestUrl=https://icsid.worldbank.org/en/Pages/about/Database-of-Member-States.bak.aspx.
[180] A. Wołek, 'Precipices beneath summits? The Visegrád cooperation seen from middle policy levels', in J. Marušiak J et al. (eds), *Internal cohesion of the Visegrád group* (VEDA, 2013), 88.
[181] Visegrád declaration, 15 February 1991, http://www.visegradgroup.eu/documents/visegrad-declarations/visegrad-declaration-110412.
[182] Established in 2000, https://www.visegradfund.org.
[183] Operating from 2016, http://www.vpi.int/index.php/en.
[184] For information on the work and activities of the V4 group, see the official website http://www.visegradgroup.eu.
[185] They all can be accessed (in the English version) at the official website http://www.visegradgroup.eu/documents/official-statements.

communications,[186] EU proposals for regulations,[187] or on EU Directives.[188] The V4 has also drafted letters addressed to the European Commission.[189] The topics addressed during these meetings may range from agriculture, renewable energy, migration, financial and labour issues, to name a few.[190]

To date there has been no significant joint document on cybersecurity issued by the V4;[191] we can find only some programmatical references in some documents,

Cybersecurity has been referred to in V4 Presidency Programs, with a call to strengthen cooperation,[192] and in the 2011 Bratislava Declaration on the occasion of the 20th anniversary of the Visegrad Group:

> […] The Visegrad Group will actively contribute towards international efforts in combating terrorism, human and drug trafficking, illegal migration, extremism and other security threats and challenges, including those in the area of *cybersecurity*, that jeopardise our values and the freedoms of our citizens […]. [emphasis added][193]

Cybersecurity was among one of the express Strategic Priorities for 2017 of the International Visegrad Fund.[194]

In the field of cybersecurity economic-related issues, it is worth noting the Joint Declaration of the Ministers of Economic Affairs of the Visegrad Group Countries on the Future of Economic Cooperation of 19 April 2018, which included a call on

> […] the importance of arising issues that include *cyber security*, standardization, free flow of non-personal data, scale of data-usage and emerging 5G communication. All these factors will contribute to the data-

[186] E.g., Joint declaration of the Ministers of agriculture of the Visegrád group and Croatia on the Commission Communication on the future of food and farming, 25 January 2018.
[187] E.g., Joint declaration of the Ministers of the interior on the the proposal for a Regulation on the European border and coast guard, 16 October 2018.
[188] E.g., Joint declaration of the Agricultural Ministers of Visegrád group, Bulgaria and Romania on the renewable energy Directive after 2020, 21 September 2017.
[189] E.g., Joint statement and Joint letter to EC prepared during the Summit of 22 June 2012; Joint Letter to High Representative Ashton and Commissioner Füle of 5 March 2013.
[190] T. Strážay, 'When pragmatism wins: Slovakia in the Visegrád group', in P. Brezáni (ed.), *Yearbook of Slovakia's foreign policy 2018* (Research Center of the Slovak Foreign Policy Association, 2019), 67.
[191] As also confirmed during interviews with stakeholders.
[192] See 2018/2019 Slovak Presidency Program; 2017/2018 Hungarian Presidency Program; 2016/2017 Polish Presidency Program; 2015/2016 Czech Presidency Program; 2014/2015 Slovak Presidency Program; 2013/2014 Hungarian Presidency Program; 2012/2013 Polish Presidency Program; 2007/2008 Czech Presidency Program.
[193] The Bratislava Declaration of the Prime Ministers of the Czech Republic, the Republic of Hungary, the Republic of Poland and the Slovak Republic on the occasion of the 20th anniversary of the Visegrad Group (15 February 2011).
[194] See the official website https://www.visegradfund.org/news/02-09.

> economy of the coming digital age. […] *A good and trusted blueprint of cyber-security cooperation at V4+ level* should be followed […]. [emphasis added][195]

It is also worth mentioning the Joint Declaration of Intent of V4 Prime Ministers on Mutual Cooperation in Innovation and Digital Affairs, issued in Warsaw on 28 March 2017, where

> […t]he Visegrad Group agrees to further strengthen its ties by adopting the following Warsaw Declaration on mutual co-operation in research, innovation and digital affairs as follows: […] to work towards *sustainable, efficient, resilient and secure cyber space* based, inter alia, on *timely and proper implementation of the NIS Directive*, allowing the joint internal market for the high-level cyber security and protection of critical information infrastructures and resources […]. [emphasis added][196]

And, in fact, all V4 countries then implemented the NIS Directive within their own regulatory framework. A call on implementing cooperation was also included in the Joint Statement of the V4 Ministers of Defence, issued in Brussels on 4 June 2013:

> […]The V4 countries will tighten their cooperation in countering cyber threats at political and operational level as cyber security becomes extremely vital. Their activities should be closely linked with the NATO Smart Defence Multinational Cyber Capability Development program as well the EDA-led Cyberdefence Project Team.[…][197]

Cybersecurity has been also discussed during V4+ meetings, as highlighted in the Joint Statement from the Annual Summit of the Visegrad Group Prime Ministers and the Prime Minister of the State of Israel released in Budapest on 19 July 2017, where

> […t]he five leaders agreed to explore the possibility of further strengthening joint cooperation in the areas of […] *cyber security* […]. [emphasis added][198]

as well in the Joint Statement of the Ministers of Foreign Affairs of the Visegrad Group, Austria, Croatia and Slovenia issued in Budapest on 10 July 2017, where there was a call on

> […] take action on issues including […] *cybersecurity* as well as digital skills […]. [emphasis added][199]

---

[195] Joint Declaration of the Ministers of Economic Affairs of the Visegrad Group Countries on the Future of Economic Cooperation (19 April 2018).
[196] Joint Declaration of Intent of Prime Ministers of the Visegrad Group on Mutual Co-operation in Innovation and Digital Affairs - "Warsaw Declaration" adopted at the CEE Innovators Summit in Warsaw on March 28, 2017 (28 March 2017).
[197] Joint statement of the V4 ministers of defence (4 June 2013).
[198] Joint Statement on the Occasion of the Annual Summit of the Prime Ministers of the Visegrad Group and the Prime Minister of the State of Israel Benjamin Netanyahu (19 July 2017).
[199] Joint Statement of the Ministers of Foreign Affairs of the Visegrad Group, Austria, Croatia and Slovenia (10 July 2017).

and again in the Joint Statement of Prime Ministers of the Visegrad Group and the President of the Republic of Korea, released in Prague on 3 December 2015, where

> […t]he V4 and the ROK acknowledged the goal to strengthen their cooperation on global issues, including […] *cyber security* […] and agreed to continue close consultations in respective areas […]. [emphasis added][200]

Within the V4 region, worth mentioning is the (technical) cooperation in cybersecurity through the Central European Cybersecurity Platform (CECSP), which was established in 2013 and includes representatives of governmental, national and military CSIRT teams along with the representatives of national security authorities and national centres of cybersecurity from Slovakia, Czech Republic, Poland, Hungary, and Austria. The CECSP facilitates the exchange of information and sharing of know-how among the countries on cybersecurity issues.[201] Another forum for technical cooperation on cybersecurity has been the V4+Austria meetings.[202]

Also when it comes to international investment protection, we could find general references in V4 documents, like in V4 Presidency programs.[203] There is also official record of meetings that have been held at the V4 level on the need of cooperation for exchange data on foreign investments[204] and on the need to cooperate to attract foreign investors in the region.[205] Some V4 Presidency programs have also emphasised the need to present a common position with regard negotiations of international investment agreements at the EU level and at the bilateral level (among V4 countries) with non-EU third countries.[206]

As regards relationship with non-EU third countries, it is worth noting the advocacy role of the V4+ meetings, aimed at, among others, reinforcing cooperation in trade and promotion of investment.

---

[200] Joint Statement on the Occasion of the First Summit of Prime Ministers of the Visegrad Group and the President of the Republic of Korea (3 December 2015).

[201] See the description of the CECSP at the official website of the National Security Authority of Slovakia, https://www.nbu.gov.sk/en/cyber-security/partnership/central-european-platform-for-cybersecurity/index.html.

[202] From an interview with a government official.

[203] E.g., Slovak Presidency program 2018/2019, Czech Presidency program 2011–2012 and Polish Presidency program 2008/2009.

[204] E.g., Joint declaration of the Ministers of economic affairs on the future of economic cooperation, 19 April 2018.

[205] E.g., Memorandum of understanding for regional cooperation in the areas of innovation and startups, 12 October 2015 and Bratislava declaration on the occasion of the 20th anniversary of the Visegrád group, 15 February 2011.

[206] E.g., Czech Presidency program 2015/2016 and Slovak Presidency program 2014/2015.

In some cases, the outcomes of the "V4+" meetings have called for further promotion of economic relationship with the EU, as in the case of the V4+ Japan Joint Statement of 2013, where

> […] The V4 and Japan reaffirmed that a comprehensive Japan-EU Economic Partnership Agreement (EPA) / Free Trade Agreement (FTA) would improve access to markets for Japanese and V4's companies and thus strengthen economic relations between both sides. […][207]

In other cases, the V4+ has served as an opportunity to define the best conditions for implementing existing EU international trade agreements, as in the case of the Joint Statement during the First Summit with South Korea of 2015, according to which

> […] The V4 and the ROK acknowledged the economic effects of the EU–Korea Free Trade Agreement (FTA) and affirmed their readiness to create favorable conditions for the economic development under the framework of the EU–Korea FTA […].[208]

2.3.…and at the national level: a special focus on Slovakia

In 2015, Slovakia adopted the Cyber Security Concept of the Slovak Republic for years 2015-2020 with the accompanying Action Plan,[209] while on 1 April 2018, Act No. 69/2018 Coll on cybersecurity – which implements the EU NIS Directive - came into force (Cybersecurity Act).[210]

At the organizational level, the central state administration body is the National Security Authority (NBU),[211] tasked with the protection of domestic cyber-security, the management of cyber security incidents and the coordination of the response activities at the national level;[212] NBU is also the National Point of Contact for cybersecurity for the EU.[213]

NBU established the Slovak Computer Emergency Response Team (SK-CERT), which became the National Cyber Security Centre SK-CERT on 1 September 2019, which deals with cyber-incidents,

---

[207] Visegrád Group Plus Japan Joint Statement of 16 June 2013. The EU and Japan's Economic Partnership Agreement entered into force on 1 February 2019. See European Commission, *EU-Japan Economic Partnership Agreement*, http://ec.europa.eu/trade/policy/in-focus/eu-japan-economic-partnership-agreement.

[208] Joint Statement on the first summit with the President of the Republic of Korea of 3 December 2015.

[209] See the official texts, https://www.nbu.gov.sk/en/cyber-security/national-cyber-security-strategy/index.html.

[210] Zachová et al., cit.

[211] See the official website https://www.nbu.gov.sk/en/index.html.

[212] See M. Hathaway, F. Spidalieri, A. Kaushik, *Slovak republic. Cyber Readiness at a Glance* (Potomac Institute for Policy Studies, GLOBSEC, April 2019), 16, https://potomacinstitute.org/divisions/36-science-and-technology-policy/cyber-readiness/cyber-readiness-translations/2171-slovak-republic-cyber-readiness-at-a-glance.

[213] See all relevant informatio at the official website https://www.sk-cert.sk/en/about-us/index.html.

analytical activities, cybersecurity awareness building as well as cybersecurity training.[214] It also participates in the Incident Response and Security Teams (FIRST),[215] as well as in in European projects, like the most recent European "CyberExchange" project, co-financed by the Connecting Europe Facility of the European Union: 11 European CSIRT teams participate with the aim to increase cooperation and improve the exchange of experience and knowledge in cybersecurity.[216]

NBU also has also organized public workshops over the implementation of the NIS Directive and the Cybersecurity Act, open to all stakeholders;[217] moreover, SK-CERT regularly holds the so-called "National Table-Top Exercises", which are aimed at verifying the preparedness to cyber threats of target group of participants.[218]

Within the public administration sector, the Office of Deputy Prime Minister for Investments and Informatization is in charge of implementing the national digital investment strategies; within the framework of its office, also a Government CSIRT has been established - which shares cyber information and alerts also with other government agencies. Other CSIRTs are also established within the framework of the Ministry of Economy (Industry CSIRT), the Ministry of Defence (CSIRT.MIL.SK), as well as other Ministries (sector CSIRTs).[219] As regards cyber-defence and cyber-diplomacy measures, the main actor is the Ministry of Foreign and European Affairs.

Slovak experts regularly participate at European and international workshops, trainings and simulations.[220] Moreover, the different offices may be involved in bilateral cooperation with other

[214] It also issues warnings on cybersecurity. See for example the recent warning of a potential increase in harmful cyberspace activities in relation to the Middle East situation issued on 9 January 2020 on the official website of SK-CERT: https://www.sk-cert.sk/sk/varovanie-pred-moznym-zvysenim-skodlivych-aktivit-v-kybernetickom-priestore-v-suvislosti-s-eskalaciou-napatia-na-blizkom-vychode/index.html.

[215] See the official website https://www.first.org/about/mission.

[216] See the relevant news 'SK-CERT – a Part of an International Project 'CyberExchange'' (21 January 2019), https://www.sk-cert.sk/en/sk-cert-a-part-of-an-international-project-cyberexchange/index.html.

[217] See e.g. the workshop, co-organised with ENISA, on the implementation of the NIS Directive held on 17-18 October 2016 in Bratislava (https://www.enisa.europa.eu/news/enisa-news/enisa-in-co-operation-with-the-eu-slovakian-presidency-hosts-key-workshop-on-the-nis-directive-1) and the series of workshops on the Cyber Security Act held in 2018 (https://www.sk-cert.sk/en/the-first-of-a-series-of-workshops-on-cyber-security-act/index.html).

[218] See all the relevant information at the official website https://www.sk-cert.sk/en/sk-cert-is-preparing-another-of-the-series-of-national-table-top-exercises/index.html.

[219] Hathaway et al, cit., 15.

[220] See for example the news 'CyberSOPEx Exercise Tested the Cooperation of National CSIRT Units' (27 May 2019), https://www.nbu.gov.sk/news/cybersopex-exercise-tested-the-cooperation-of-national-csirt-units/index.html.

states, depending on the nature and scope of the cyber-incident; Slovakia has also signed *memoranda* with non-EU countries establishing cooperation on sharing of information (e.g. with the USA, Israel).[221] In 2018, the Slovak Republic ranked first in the National Cyber Security Index (NCSI), while in 2019 was positioned in the 12th place;[222] the Index measures countries' willingness to prevent serious cyber threats and to be prepared for cyber incidents, crimes and major crises. [223]

As regards cybercrime protection, Slovakia ratified the Budapest Convention in 2008. Even though Slovakia has included computer system-related crimes within its domestic legislation and regulations,[224] a specific regulation on cybercrime does not exist to date.[225]

Within the framework of the Presidium of the Police Force, dedicated offices of the National criminal agency (NAKA) deal with operational support to cybercrime investigation, collaborating also with the European Cybercrime Centre (EC3), Europol, and Interpol.[226] They also support *ad hoc* campaign for companies, like the "No more ransom" EU campaign, an initiative of the Europol's European Cybercrime Centre.[227]

Also the General Prosecutor's office regularly cooperates with European institutions. Worth mentioning in this respect is the creation of the National Network of Prosecutors against Cybercrime, for sharing information and providing mutual assistance among the members of the Network, as well as with the National expert group against cybercrime – which includes representatives from General Prosecutor's office, Police, Ministries, National Security offices, as well as private companies.[228]

At the international level, it is worth recalling that Slovakia currently holds the Chairmanship of OSCE, which is focusing on the protection of critical infrastructure by furthering the dialogue and

[221] From an interview with a government official.
[222] See NCSI, 'Slovakia takes first place in index' (28 Mar 2018), https://ncsi.ega.ee/1/slovakia-takes-first-place-in-index. However, it should be noticed that the ranking position differs across different Indexes, according to the different methodologies employed. Eg. Slovakia is 45th in the Global Cybersecurity Index, 46th in the ICT Development Index and 47th in the Networked Readiness Index. See https://ncsi.ega.ee/country/sk.
[223] Zachová et al., cit.
[224] See for example, Section 247 (Harm Done to and Abuse of an Information Carrier) of the Slovak Criminal Code.
[225] Hathaway et al, cit., 21.
[226] From an interview with a government official.
[227] See the official website https://www.nomoreransom.org/it/index.html.
[228] See the document prepared by Slovakia for the 5th meeting of the Open-Ended Intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime (IEG) in March 2019 and published on the official UNODC website, https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Slovakia.pdf. Confirmed also by interviews with government officials.

implementation of the 16 confidence-building measures (CBMs) adopted by OSCE member States and aimed at facilitating exchanges of information and communication among States.[229]

Apart from institutional actors engaged in cybersecurity and cybercrime issues, worth recalling are also non institutional actors that have a role to play in these issues.

In particular, companies are becoming more and more aware and engaged in cybersecurity matters in *ad hoc* platforms, like the Industry4UM, an initiative of industry representatives under the auspices of the Ministry of Economy of the Slovak Republic that provide companies with information and expertise on digital transformation and digital-related issues,[230] including cybersecurity concerns.[231]

It should also be recalled that national and foreign companies in Slovakia need to comply with the relevant regulations; in particular, with respect to the obligations included in the Cybersecurity Act (deriving from the EU NIS Directive), companies providing services in the energy, transport, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure should register into the register of basic service providers, establish an information security system, as well as monitor and report security incidents to the responsible authority. In this respect, security service providers come into play as key actors since they give technical support to national and foreign companies.

Foreign investors in Slovakia have also to comply with national regulations regarding investment protection; the Slovak Investment and Trade Development Agency (SARIO), a governmental investment and trade promotion agency support foreign investors willing to invest in Slovakia with all information regarding their entry into the territory.[232] The Ministry of Finance is in charge with negotiation and conclusion of BITs with non-Eu countries of Slovakia and with regard to international arbitration cases involving Slovakia.[233]

Foreign investors can also rely on a network of non-governmental actors supporting their business, like law firms, Chambers of Commerce based in Slovakia - which serve as a network for (foreign)

[229] Decision No. 1202 OSCE *Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technologies* (10 March 2016), https://www.osce.org.
[230] See the official website https://industry4um.sk/en.
[231] See for example the forthcoming workshop on 'Cyber security of an industrial enterprise', https://industry4um.sk/en/kyberneticka-bezpecnost-priemyselneho-podniku.
[232] See the official website https://www.sario.sk.
[233] See the official website https://www.mfsr.sk/sk/financie/statne-vykaznictvo/medzinarodna-ochrana-investicii.

companies -, and the Investment Support Association (ISA) - an association of corporate entities and companies doing business in Slovakia.[234]

It is worth recalling that the Cyber Security Concept of the Slovak Republic for years 2015-2020 makes a reference to the economic implications of cybersecurity:

> Cyber security is one of the defining elements of the security environment of the Slovak Republic […]. At a state level, it is a system of continuous and planned increasing of political, legal, *economic*, security, defence and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organizational nature in cyber space in order to transform it into a trustworthy environment providing for the *secure operation of* social and *economic processes* at an acceptable level of risks in cyber space. […] Insufficient protection and defence against security incidents creates space for rendering society itself vulnerable, with consequences throughout all social and *economic processes* [emphasis added][235]

This reference could be the starting point for considering including cybersecurity issues also in international trade and investment negotiations.[236]

3. Building up a governance of cybersecurity of foreign investment (?): a mapping exercise with 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, European and national levels. In order to have a clear visual map of the actors and their relations, we have applied the method of social network analysis.[237]

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.

[234] See the official website http://isa-association.sk/en/about.
[235] Cyber Security Concept of the Slovak Republic for years 2015-2020, cit., 6-7.
[236] Hathaway et al., cit., 30.
[237] 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.

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 at the national level each State has a peculiar institutional organization, for the scope of this analysis the following table does not list the governmental units of EU member states (also, the focus here is on EU member states – which of course include all the V4 countries). This table does not aim to include *all* the actors involved: the aim is to indicate the ones that can play a more relevant role in building up a 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. As such, non-governmental stakeholders and foreign investors have not been included in this mapping exercise, since the kind of interaction with institutional actors are diverse in nature.

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[238]	✓	✓

From this table, the following visualization has been developed, using NodeXL:[239] 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;

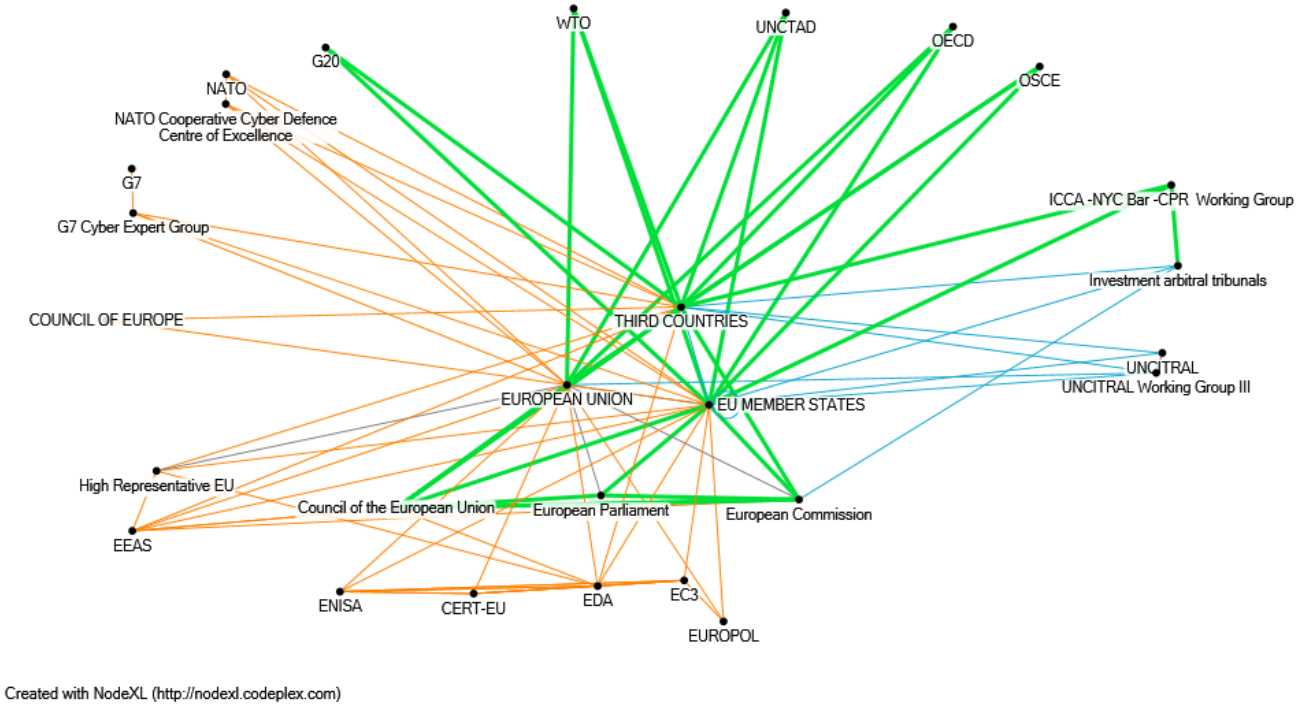
3- GREEN: when there are interactions in both fields of cybersecurity and investment promotion and protection (even though the interactions do not occur simultaneously in both fields)

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.[240]

[238] 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.

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

[240] 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, 201), 96, 170-171.



From the graph we can infer two main observations:

- EU institutions as well as EU member states – and V4 countries - have links with almost all the institutional 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, even though not at the same time and in the same events/meetings. 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. Moreover, the green edges may be used as indicators of existing platforms where discussions over cybersecurity and investment protection may be brought at the same discussion table(s).

As regards non-governmental stakeholders and foreign investors, as already shown in the previous paragraphs, they also have a key role to play in cybersecurity and investment protection matters.

Moreover, they have built relationships with governmental institutions and established several initiatives.

Worth mentioning is the Cybersecurity Tech Accord, signed by global technology companies with the aim to improve the security, stability and resilience of cyberspace;[241] they engage actively with other actors at the international level – e.g. representatives of the accord gathered in New York in December 2019 at UN headquarters for a multi-stakeholder dialogue on promoting international peace and stability in cyberspace with other non-governmental institutions and state representatives.[242]

At the organizational level, we can recall the European Cyber Security Organisation (ECSO), a non-for-profit organisation established in Brussels, which include diverse stakeholders such as large companies, small-medium enterprises, universities, end-users, association as well as European Member State's local, regional and national institutions. The European Commission and the European Cyber Security Organisation (ECSO) signed a Cyber Security contractual Public-Private Partnership on 5 July 2016, in order to foster cooperation between public and private actors in the cybersecurity sector.[243]

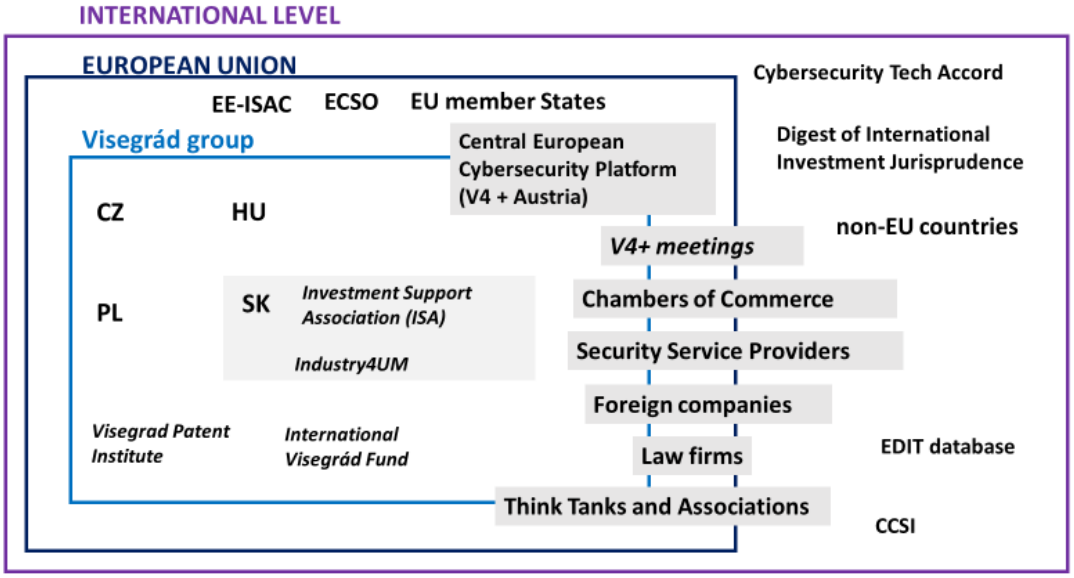
Along the same line, it is also worth mentioning the European Energy - Information Sharing & Analysis Centre (EE-ISAC), an industry-driven network, where private companies and public institutions such as academia, governmental and non-profit organizations (eg. ENISA, the National Cyber Security Centre of The Netherlands, Polskie Sieci Elektroenergetyczne, Enel) share information, data and expertise on cyber security and cyber resilience issues.[244]

We can also recall the above mentioned Industry4UM, which has the support of the Ministry of Economy of the Slovak Republic, or the above mentioned EU-funded projects on cybersecurity which provide opportunities for institutional actors to engage with other non-governmental actors (e.g. the Cyber Crime Training (Slovakia), which was aimed to support the capacity building of the Slovakian Police, in cooperation with the University College Dublin's Centre for Cybersecurity & Cybercrime

[241] See the official website https://cybertechaccord.org/about.
[242] See the news 'Cybersecurity Tech Accord joins the UN dialogue to limit the offensive use of digital technologies' (6 December 2019), https://cybertechaccord.org/cybersecurity-tech-accord-joins-the-un-dialogue-to-limit-the-offensive-use-of-digital-technologies.
[243] See all relevant information at the official website https://ecs-org.eu.
[244] See the official website https://www.ee-isac.eu/about.

Investigation and co-funded by the Prevention of and Fight against Crime Programme of the European Union[245]).

In the field of international investment protection, one of the most important initiative is the Columbia Center on Sustainable Investment (CCSI), a joint center of Columbia Law School and the Earth Institute at Columbia University, is the only university-based applied research center and forum dedicated to the study, practice and discussion of sustainable international investment.[246] The Center works with governments, donors, civil society, and other partners (see for example the online project Negotiation Support Portal, aimed at supporting host countries in their planning, negotiation, conclusion and implementation of complex investment projects[247]). Worth mentioning are also the Digest of International Investment Jurisprudence, a not–for–profit service by the International Investment Law Centre Cologne at the University of Cologne to help scholars and practitioners in their work by providing a systematic collection of statements made by investment tribunals regarding international investment law,[248] as well as other research projects, like Electronic Database of Investment Treaties (EDIT), a database on international investment agreements, which gathers academics and non-governmental stakeholders.[249] The following picture summarize the map of non-governmental actors, with a focus on the V4 sub-regional framework.



[245] See all relevant information at the website https://www.ucd.ie/cci/projects/current_projects/cyber_crime_training_slovakia.html.
[246] See the official website http://ccsi.columbia.edu/about-us.
[247] See the official website http://negotiationsupport.org.
[248] See the official website http://www.investment-law-digest.com/introduction.aspx.
[249] See more information at the website https://www.wti.org/research/res/#open-83222-investment.

4. Main findings and steps forward

As the previous paragraphs have shown, to date there is no unique framework for understanding cybersecurity concerns in international investment protection.[250] Nonetheless, cybersecurity concerns for foreign investors arise; on the other hand, both cybersecurity and investment protection issues have been dealt with in several *fora* at the international, European, V4 sub-regional and national levels with a multi-stakeholder approach.

The EU has already remarked that

> [t]he 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 […].[251]

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 to date by 76 States, 343 organizations and members of civil society and 632 companies and private sector entities 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 […].[252]

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 – most recently, with respects to the role of FDI regulation in the framework of cybersecurity of 5G networks.

As the last paragraph has shown, international, EU and national institutions – including in the V4 countries - have already built up a robust network of relationships with other international players,

---

[250] S. Madnick, S. Johnson, K. Huang, 'What Countries and Companies Can Do When Trade and Cybersecurity Overlap' *Harvard Business Review* (4 January 2019), https://hbr.org/2019/01/what-countries-and-companies-can-do-when-trade-and-cybersecurity-overlap.

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

[252] '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.

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.

Today, the V4 has become a "recognized" voice in international fora: the Slovak Prime Minister Robert Fico in 2012 highlighted that the V4 had "[…] became *trademark* known in Europe, North Atlantic and beyond […]" [emphasis added].[253] Also EU institutions tend to mentioned more and more the V4 in press releases that report some of their meetings.[254]

The ability to talk with one voice through the V4 platform has been labelled as the "soft power" of the V4;[255] also in the field of cybersecurity and investment protection, the V4 may use its soft power to advocate sub-regional interests at the EU, as well as at the international level, in order to influence in a positive way future investment and cybersecurity-related law-making.

Also companies may have a role to play; in this respect, we can recall the above mentioned example of the letter sent by cybersecurity companies to USA representatives in the framework of the negotiation of the U.S.-Mexico-Canada trade agreement. Indeed, companies may have a role in raising awareness of cybersecurity-related issues and bringing their needs to institutional actors.

In particular, the following steps should be taken into consideration for a more comprehensive understanding of cybersecurity issues of foreign investment:

- *For national governments*
    - Cooperating for a more harmonized vocabulary on cybersecurity;
    - Introducing cybersecurity concerns in the negotiation tables on international investment protection;
    - Using the existing international platforms of discussion on cybersecurity issue in order to introduce questions related to investment protection;

[253] Manifesto of the Government of the Slovak Republic, May 2012, http://www.vlada.gov.sk/manifesto-of-the-government-of-the-slovak-republic.

[254] See e.g. the following press releases of the European Commission: 'Future of cohesion policy: Commissioner Hübner to address Visegrád group in Sopot, Poland. European Commission' *Press release* (1 July 2009), https://europa.eu/rapid/press-release_IP-09-1067_en.htm and 'Commissioner Hahn in Bratislava in the run-up to the Eastern Partnership 10th Anniversary. European Commission' *Press release* (3 May 2019), https://europa.eu/rapid/press-release_MEX-19-2390_en.htm.

[255] T. Strážay, 'Visegrád - arrival, survival, revival. Selected V4 Bibliography' *Visegrad Group* (2011), http://www.visegradgroup.eu/documents/bibliography/visegradarrival-survival-120628.

- *For the Visegrad group*
    - Introducing more comprehensive talks on cybersecurity concerns in investment protection in the V4 agenda;
- *For (foreign) companies*
    - Becoming active players in raising awareness within national, European and international *fora* on cybersecurity investment-related issues;
    - Using existing platforms for discussion in order to engage with national governments in order to bring their vision on cybersecurity investment-related issues.

All in all, a multi-stakeholder approach seems the best way to cope with the topics at stake. 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 […]'.[256]

[256] For the full text, https://www.nato.int/cps/en/natohq/opinions_166039.htm.