Economic Cyber-Espionage in the Visegrád Four Countries: a Hungarian Perspective

FEDERICA CRISTANI

sciendo

Politics in Central Europe (ISSN: 1801-3422)
Vol. 17, No. 4
DOI: 10.2478/pce-2021-0037

Abstract: *This article explores the regulatory framework of reference of economic cyber-espionage in Europe, with a particular focus on the V4 region (comprising Slovakia, Hungary, Poland and the Czech Republic) and taking Hungary as a case study. Europe Union member states, including the V4 countries, are particularly exposed to economic cyber-espionage, because of the advanced know-how of the companies based therein. Under international law, there exists no uniform approach to the matter; also at the European Union level, the legal framework appears rather fragmented and the same holds true at the national level and within the V4 group, where each country has adopted its own relevant regulation. After a general overview of the relevant international and EU regulatory framework of reference, this article overviews the modus operandi of the V4 and examines its approach to economic cyber-espionage, with a special focus on Hungary as case study. As already remarked at the European and international levels, cybersecurity policies and regulations, including those regarding economic cyber-espionage operations, should be drafted in coordination among states; the V4 group can become a privileged platform of discussion to advance in the regulatory harmonisation of the issues at stake.*

Keywords: ***economic cyber-espionage; Visegrád Group; Hungary; cyber-security; governance***

Introduction

More and more companies around the world and in Europe are becoming the target of cyberattacks, whose consequences have ranged from money losses and information theft to infrastructure destabilisation. Among the cyber chal-

lenges that the economic sector faces (e.g. phishing attacks, ransomware and cryptojacking), economic cyber-espionage is a crucial one, namely the attempt to acquire trade secrets held by companies by the state where they are based or third states or by other (non-governmental) companies – in the latter case, it is more common to talk about 'corporate' or 'industrial' cyber-espionage (UNODC 2018).

Europe is a particularly exposed region, because of the advanced know-how of the companies based therein (PricewaterhouseCoopers 2018). In particular, Central European countries, including the Visegrád Four (or V4) countries (comprising Slovakia, Hungary, Poland and the Czech Republic), have experienced several (economic) cyber-espionage incidents: in 2013, CrySyS Lab, a Hungarian cyber laboratory discovered a near decade-long cyber espionage operation that was targeting several public and private entities, mainly in Eastern European countries – the so-called TeamSpy operation (Lennon 2013); in 2019, a Slovakian cybersecurity firm, ESET, unmasked an espionage operation ongoing since about 2013 and targeting public institutions of Central European countries (Wielgos 2019). 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' (Legal Week Intelligence – CMS 2018). Most recently, the COVID-19 pandemic and the relevant increasing dependence on digital technologies have created additional opportunities for cyber-incidents (Fidler 2020a): as regards the V4 region, we can briefly recall the ransomware attack on national health facilities in the Czech Republic in April 2020 (Fidler 2020b), and the cyber-attack against the national vaccine registration website in Hungary in February 2021 (Eder 2021).

Hungary in particular, can be considered a very interesting case study in this respect: it was one of the first countries in Central Europe to formulate its national cybersecurity strategy; even though it is quite difficult to find official and public data and information on economic cyber-espionage operations, it seems to be a particularly vulnerable country because of its weak security systems (around 50 % of large companies in Hungary have addressed cyber security issues in the last years), and because of the recent Chinese economic interests in the region, it risks to become 'a Trojan horse for Chinese [...] influence' (Panyi 2021b).

When talking about cyber threats 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's (PRI)[1] Report, *Stepping up governance on cyber security* (Ravishankar – Mooney – Hader 2018), while there is increasing awareness of companies about cyber risks and the need to deal with them, still there is a general lack

1 PRI is an investor initiative in partnership with UNEP Finance Initiative and the UN Global Compact.

of information publicly disclosed on cyberattacks. Companies generally do not disclose to the public either the cyberthreats they have been victim of, nor the measures they adopt to deal with cyber challenges – due to a number of reasons, including the fear of bad reputation in case of disclosure of cyberattacks or the fear of becoming a target or vulnerable to hackers (PRI 2018). On the other hand, companies recognise the need to cooperate in order to deal with cyber challenges and the advantages of sharing knowledge and best practices also with national institutions (PRI 2018).

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: in Slovakia, the website of National Cyber Security Centre SK-CERT[2] and the annual report of the national CSIRT.SK;[3] in the Czech Republic, the website of the National Cyber Security Centre[4] and the Cyber Security Status Reports and Security Incidents Reports;[5] in Poland, the incident reports prepared by CERT Polska;[6] while in Hungary we can rely on the website of the National Institute of Cyber Defense (NKI) of the National Security Service.[7]

Moreover, we can rely on reports and data published by private companies and institutions.[8]

Overall, the lack of clear and comprehensive (and harmonised) data 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[9] confirmed that there is limited qualitative and quantitative information available on cyber theft of trade secrets (PricewaterhouseCoopers 2018: 15) and calls for a more appropriate regulatory framework in the field (PricewaterhouseCoopers 2018: 42).

2 See the official website of SKCERT at <https://www.skcert.sk/en/statistics/index.html> accessed 31 May 2021.

3 See the latest report of CSIRt.SK, *Report 2016* (2016) <https://www.csirt.gov.sk/doc/CSIRT-SK-Report-2016.pdf> accessed 31 May 2021.

4 See the official website of the National Cyber Security Centre (NCSC) at <https://www.govcert.cz/cs/informacni-servis/hrozby> accessed 31 May 2021.

5 Ibid.

6 See the official website of NASK CERT Polska at <https://www.cert.pl/en/> accessed 31 May 2021.

7 See the official website of the National Cyber Security Center at <https://nki.gov.hu> accessed 31 May 2021.

8 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 by sending information about known cyber-incidents. The initiative is carried out within the US-based Council on Foreign Relations think tank. See all the relevant information at the official website at <https://www.cfr.org/interactive/cyber-operations#CyberOperations> accessed 31 May 2021.

9 European Commission, *Trade secrets* <https://ec.europa.eu/growth/industry/intellectual-property/trade-secrets_en> accessed 31 May 2021.

Turning to the regulatory framework of reference, which (legal) instruments do states have to address the challenges of economic cyber-espionage? The regulatory picture today is highly fragmentated. Before illustrating it in detail, it is necessary first to briefly consider the theoretical framework of reference for economic cyber-espionage, as the following paragraph explores.

Building up a(n international) theoretical framework for economic cyber espionage.

Economic espionage can be defined as 'the act of acquiring trade secrets [...] without the permission of the owner of the information' (Hua 2015: 67); as it has been rightly affirmed, it is

> a less visible but more widespread form of attack that is conducted by employees against their own employers, by competing private companies, and by governments seeking to protect or expand their national economies (Van Arnam 2001: 95).

Although the phenomenon of economic espionage and – with the widespread utilisation of cyberspace – economic *cyber*-espionage, are constantly increasing, and although espionage is often referred to as the 'world's second oldest profession' (Reynolds 2004), there is still little data about it, as already outlined in the previous paragraph.

All businesses can become the target of economic (cyber-)espionage: suffice it to recall that, in 2000, the network of Microsoft was put under attack by hackers allegedly based in Russia (Van Arnam 2001: 96); in 2017, the cyber group APT28 targeted several countries across Europe and the Middle East, stealing passwords and credentials from the networks of the healthcare sector (PricewaterhouseCoopers 2018: 25); also in 2017, the WannaCry ransomware in just a 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 (Tasheva 2017: 1). When we consider the V4 region, in particular, it is worth recalling that in Slovakia, according to the November 2019 report of the IT provider GAMO, up to 53 % of companies in Slovakia have experienced cyber incidents;[10] in the Czech Republic, the Czech Statistical Office reported that one in five domestic companies faced a cyberattack in 2018 (Kenety 2020); 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 cyber-

10 GAMO, Vzdelávajte sa v téme kyberbezpečnosti (12 November 2019) <https://www.gamo.sk/novinky/vzdelavajte-sa-v-teme-kyberbezpecnosti> accessed 3 September 2021.

attacks;[11] and in Hungary, around 50 % of large companies have addressed cyber security issues, as reported by EURACTIV Slovensko (Zachová *et al.* 2018). As reported by ENISA, '[i]n 2019, the number of nation-state-sponsored cyberattacks targeting the economy increased and it is likely to continue this way'.[12]

But is economic (cyber-)espionage lawful under international law? The answer is not clear. Indeed, while some scholars affirm that economic espionage during peacetime violates international law – considering the activity of economic espionage as a form of invasion on the territorial integrity and sovereignty of a state (Garcia-Mora 1964) – others support the idea that the widespread use of economic espionage during peacetime has rendered it accepted and lawful under international law (McDougal 1973).

The same considerations apply also to economic *cyber*-espionage. In such cases, we should add to the theoretical picture the cyberspace element: globalisation has made the international economy widely interconnected and at the same time vulnerable to possible cyber-threats (Magen 2017: 4).

In any case, it is true that, to date, the activity of espionage is not prohibited by any international conventions; on the other hand, misappropriation of trade secrets has started to be dealt with by international, regional and national regulations, as the following paragraphs analyse in more detail.

Economic Cyber-Espionage: the Legal Framework of Reference at the International Level…

Under international law, there exists no uniform approach to and no unique instrument for dealing with economic cyber-espionage (Lotrionte 2015; Schmitt – Vihul 2017: 170): while the G20 Leaders' Communiqué of 2015 stated that 'no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets',[13] the United Nations report of the same year does not include economic cyber-espionage among states' possible behaviour in cyberspace (Jančárková – Minárik 2019).[14]

When it comes to the international regulation of cybersecurity, the only binding instrument to date is the Convention on Cybercrime of the Council of Europe,[15] which focuses on infringements of copyright, computer-related fraud

11 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> accessed 3 September 2021.

12 ENISA, Threat Landscape 2020. Cyber espionage (20 October 2020) <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage> accessed 3 September 2021.

13 G20 Leaders, Communiqué of 2015, para 26 <http://www.g20.utoronto.ca/2015/151116-communique.html> accessed 31 May 2021.

14 UNGA Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015, A/70/174.

15 Budapest Convention, CETS No.185, signed on 23 November 2001 and entered into force on 1 July 2004.

and violations of network security. It has been ratified to date by 64 states and has been used as a guideline for developing domestic legislation in the field.

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,[16] the Council of Europe,[17] the G20, the United Nations,[18] the Organisation for Economic Cooperation and Development (OECD),[19] the Organisation for Security and Cooperation in Europe (OSCE)[20] and the North Atlantic Treaty Organization (NATO).[21]

Worth mentioning are also private codification initiatives like the Tallinn Manual 2.0, which deals with international law applicable to cyber operations, and which includes Rule 32 (Peacetime cyber espionage), according to which '[a]lthough peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so'. The Commentary to Rule 32 makes it clear that 'customary international law does not prohibit espionage per se. [...] On the contrary, a number of States have by domestic law authorised their security services to engage in espionage, including cyber espionage' (Schmitt – Vihul 2017: para. 5); on the other hand, '[d]espite the absence of an international law prohibition of espionage, states are entitled to, and have, enacted domestic legislation that criminalises cyber espionage carried out against them' (Schmitt – Vihul 2017: para. 17).

16 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). More information is available at the website <https://www.banque-france.fr/en/economics/international-relations/international-groups-g20g7/focus-g7-cyber-expert-group> accessed 31 May 2021.

17 The Council of Europe has launched the *Action against Cybercrime*, which helps to protect societies worldwide from the threat of cybercrime. See all relevant information at the official website <https://www.coe.int/en/web/portal/coe-action-against-cybercrime> accessed 31 May 2021.

18 The UN introduced cybersecurity in its agenda after 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). See the UNODC official website at <https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html> accessed 31 May 2021.

19 Through the Cybercrime Law project. See all relevant information at the official website <https://www.cybercrimelaw.net/OECD.html> accessed 31 May 2021.

20 See the official webpage at <https://www.osce.org/secretariat/cyber-ict-security> accessed 31 May 2021. Worth recalling is the Permanent Council Decision No. 1106 of 3 December 2013 establishing the *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> accessed 31 May 2021.

21 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. See all relevant information at the official website <https://www.nato.int/cps/en/natohq/topics_78170.htm#> accessed 31 May 2021.

Taking into account, more in particular, the international economic law framework, it is worth recalling the Paris Convention for the Protection of Industrial Property[22] and the Agreement on Trade-Related Aspects of Intellectual Property Rights of the World Trade Organization (WTO TRIPS)[23] as possible international instruments that can apply in case of economic cyberespionage (Buchan 2018: 143). Actually, even though they do not specifically regulate economic (cyber)espionage, they include some provisions that WTO member states are likely to breach in case they carry on economic (cyber) espionage operations against companies located in the territory of other WTO member states (Buchan 2018: 130). Indeed, according to article 10bis of the Paris Convention for the Protection of Industrial Property '[…] countries […] are bound to assure […] effective protection against unfair competition […]', which might also include operations of economic cyberespionage; also article 39.2 of WTO TRIPS provides that '[i]n the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention […] Members shall protect undisclosed information […]'. In this respect, we might recall the *Guidelines and Objectives by the European Community for the Negotiations on Trade-Related Aspects of Substantive Standards of Intellectual Property Rights*, according to which '[t]rade secrets and business secrets shall be protected by law at least by providing their proprietor the right to prevent these secrets from becoming available to, or being used by, others in a manner contrary to honest commercial practices'.[24] Accordingly, one may argue that the WTO TRIPS and the Paris Agreement can cover instances of economic cyber-espionage; however, there has been no relevant inter-state claim so far under such agreements.

Also free trade agreements (FTAs) can add some elements to the regulatory framework of economic cyber-espionage. We can briefly recall in this respect the recent United States-Mexico-Canada Agreement (USMCA), according to article 20.69 (Protection of Trade Secrets):

> [i]n the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention, each Party shall ensure that persons have the legal means to prevent trade secrets lawfully in their control from being disclosed to, acquired by, or used by others (including state-owned

22 Paris Convention for the Protection of Industrial Property (as amended on 28 September 1979), entered into force on 3 June 1984 <https://wipolex.wipo.int/en/treaties/textdetails/12633> accessed 31 May 2021.

23 Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed on 15 April 1994, <https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm> accessed 31 May 2021.

24 Guidelines and Objectives by the European Community for the Negotiations on Trade-Related Aspects of Substantive Standards of Intellectual Property Rights, MTN.GNG/NG11/W/26 (7 July 1988), 10.

enterprises) without their consent in a manner contrary to honest commercial practices.[25]

The PricewaterhouseCoopers study report prepared for the European Commission in 2018 considered the USMCA as a model in this respect (PricewaterhouseCoopers 2018: 48); we can also recall the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which includes a trade secrets discipline, requiring the availability of criminal procedures and penalties for unauthorised and wilful misappropriation of a trade secret.[26] In this respect, some scholars have suggested, more generally, using international trade law and particularly bilateral investment treaties (BITs) 'to help build out a customary international law of cyber norms designed to protect intellectual property' (Shackelford *et al.* 2015: 53).

Finally, with reference to inter-state agreements, it is worth recalling the practice of concluding bilateral cooperation commitments in order to refrain from economic cyber-espionage activities. In this regard, we can mention the USA–China Commitment (25 September 2015), according to which

> The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors [...]. (Kolbasuk McGee 2015)

We can also mention the UK–China Joint Statement of 22 October 2015 (Abott 2015) and the Australia-China Joint Statement of 21 April 2017 (Cowan 2017).

Overall, though the existing international legal framework is rather fragmented, we can infer that the trade-related regulatory framework seems the most suitable to be applied in case of economic cyber-espionage operations. This is also true when considering the European Union (EU) law, as the following paragraph illustrates.

25 United States–Mexico–Canada Agreement, signed on 30 November 2018 and entered into force on 1 July 2020 <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/fact-sheets/modernizing> accessed 31 May 2021.

26 Article 18.78, para 2 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), between Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore and Vietnam. The CPTPP was signed on 8 March 2018 and entered into force on 30 December 2018. The full text is available at <https://www.dfat.gov.au/trade/agreements/not-yet-in-force/tpp/Pages/tpp-text-and-associated-documents> accessed 31 May 2021.

…at the EU Level…

Also at the European Union (EU) level, while there is a quite robust regulatory framework dealing with cybersecurity,[27] there is no specific act addressing the issue of economic (or industrial) cyberespionage. However, the EU has been always aware of the challenges of cybercrime to economic activities: the 2013 Cybersecurity Strategy of the EU 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.[28]

In May 2017, the Commission expressly included cybersecurity as one of the three emerging challenges in its Digital Single Market Strategy mid-term review[29] and in October 2017, the European Parliament affirmed that '[…] the lines between cybercrime, cyber espionage, cyber warfare, cyber sabotage and cyber terrorism are becoming increasingly blurred; […] cybercrimes can […] cover a wide range of offences, including […] espionage […]'.[30]

Most recently, and as part of the intellectual property (IP) 2020 action plan, the Commission announced that it 'will, together with the EUIPO Member States and the business community, develop awareness tools and targeted guidance that will increase the resilience of EU businesses (and SMEs in particular) against cyber theft of trade secrets'.[31] Moreover, the Commission restated that '[i]n terms of foreign policy [it] will, in cooperation with the High Representative and Member States, stand ready to use the restrictive measures available to

27 E.g. 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) and the EU NIS Cooperation Group, Cybersecurity of 5G networks. The EU Toolbox of risk mitigating measures (2020), published on 29 January 2020 <https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5 g-networks-eu--toolbox-risk-mitigating-measures> accessed 31 May 2021.

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 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).

30 European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI)).

31 European Commission, Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience, COM(2020) 760 (25 November 2020), para. 5 <https://ec.europa.eu/docsroom/documents/43845> accessed 31 May 2021.

counter private and government-sponsored cyber espionage aimed at acquiring cutting-edge European IP assets'.[32]

When it comes to the protection of trade secrets, we should recall Directive 2016/943 *on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*, which states that '[…] businesses are increasingly exposed to dishonest practices aimed at misappropriating trade secrets, such as theft, unauthorised copying, economic espionage […] whether from within or from outside of the Union […]'.[33] The Directive does not refer to cases of economic *cyber*-espionage; however, we might argue that it covers also such instances of 'misappropriation' of trade secrets. In any case, it should be noticed that, such as any EU Directive, it should be translated for the different EU member states; accordingly, it does not offer a homogenous regulation of the issue – indeed, we have 27 different national provisions that have implemented the Directive. Moreover, as the Directive points out:

> there are important differences in the Member States' legislation as regards the protection of trade secrets against their unlawful acquisition, use or disclosure by other persons. For example, not all Member States have adopted national definitions of a trade secret or the unlawful acquisition, use or disclosure of a trade secret, therefore knowledge on the scope of protection is not readily accessible and that scope differs across the Member States.[34]

It follows that:

> [t]he differences in the legal protection of trade secrets provided for by the Member States imply that trade secrets do not enjoy an equivalent level of protection throughout the Union, thus leading to fragmentation of the internal market in this area and a weakening of the overall deterrent effect of the relevant rules.[35]

As regards the international economic law framework, we can recall that the EU and its member states are signatories to the WTO Agreement including the

32 European Commission, Making the most of the EU's innovative potential – An intellectual property action plan to support the EU's recovery and resilience, COM(2020) 760 (25 November 2020), para. 6 <https://ec.europa.eu/docsroom/documents/43845> accessed 31 May 2021. See also the Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 *concerning restrictive measures against cyber-attacks threatening the Union or its Member States*.

33 Preamble (4).of the Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

34 Preamble (6).of the Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

35 Preamble (8).of the Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

TRIPS Agreement; therefore, they are also obliged to comply with article 39 of the TRIPS Agreement (Kaan Pehlivan 2019: 98).

Moreover, provisions on trade secrets are starting to be included in international economic agreements with third countries: we can recall the EU and Japan's Economic Partnership Agreement, which entered into force on 1 February 2019 and which includes in its Chapter 14 (Intellectual property) two specific subsections on 'Trade secrets and undisclosed test or other data' (Sub-section 7) and on 'Enforcement of protection against misappropriation of trade secrets' (Sub-section 3). In particular, according to article 14.36, '[e]ach Party shall ensure in its laws and regulations adequate and effective protection of trade secrets in accordance with paragraph 2 of Article 39 of the TRIPS Agreement', while article 14.50 states that '[e]ach Party shall provide for appropriate civil judicial procedures and remedies for a trade secret holder to prevent, and obtain redress for, the acquisition, use or disclosure of a trade secret whenever carried out in a manner contrary to honest commercial practices'.[36] We can find similar provisions also in the Trade and Cooperation Agreement between the EU and UK,[37] in the New EU-Mexico Agreement in Principle[38] and in the EU's proposals for the EU-Australia FTA[39] and for the EU-New Zealand FTA.[40] Even though such texts do not mention (cyber) espionage operations, we may argue that such provisions might also cover this kind of situation.

Following the trend at the international level, at the EU level the economic legal framework seems the most suitable one (at least, it is the most used by countries) to deal with economic (cyber) espionage.

The following paragraph offers an overview of the situation at the EU national level, with a special focus of the V4 countries and Hungary in particular.

36 Article 14.36(1) and Article 14.50(1) of the EU-Japan Economic Partnership Agreement. See the EU Commission website for the text of the agreement <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1684> accessed 31 May 2021.

37 See Article IP.34 (Protection of trade secrets) of the Trade and Cooperation Agreement between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part, OJ L 444 (31 December 2020) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2020.444. 01. 0014.01.ENG> accessed 31 May 2021.

38 See Article X.48 (scope of protection of trade secrets) of the Modernisation of the Trade part of the EU-Mexico Global Agreement, agreed in principle on 21 April 2018 <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1833> accessed 31 May 2021.

39 See Article X.43 (scope of protection of trade secrets) of the EU proposal for the EU-Australia FTA of 13 June 2018. On 18 June 2018, the EU and Australia officially launched negotiations for an FTA <https://trade.ec.europa.eu/doclib/press/index.cfm?id=1865> accessed 31 May 2021.

40 See article X.43 (scope of protection of trade secrets) of the EU proposal for the EU-New Zealand FTA of 13 June 2018 <https://ec.europa.eu/trade/policy/in-focus/eu-new-zealand-trade-agreement/> accessed 31 May 2021.

…and at the National Level: the V4 Countries

When it come to the national level of the V4 countries, it should be recalled that the Czech Republic, Slovakia, Poland and Hungary, as EU member states, implement the relevant EU Directives and Regulations described in the previous paragraph (Zachová *et al.* 2018). Moreover, at the international level, all V4 countries are part of the Budapest Convention, the WTO and the major international *fora* discussing cybersecurity issues like NATO, OSCE and the UN (Górka 2018).

When it comes to the national regulatory framework of reference, each V4 country has its own cybersecurity-related regulation: the Czech Republic adopted its National Cyber Security Strategy in 2021[41] and the Cybersecurity Act in 2014;[42] Hungary adopted the National Cyber Security Strategy in 2013;[43] Poland adopted the Cybersecurity Strategy in 2019[44] and the National Cybersecurity Act in 2018;[45] and Slovakia adopted its National Cyber Security Strategy in 2021[46] and the Act on cybersecurity in 2018.[47]

However, none of the four countries has adopted an *ad hoc* regulation on economic cyber-espionage, even though they all envisage provisions on trade secrets misappropriation in their national unfair competition-related laws (European Union Intellectual Property Office 2018: 5–6). In the Czech Republic, the main provisions for the protection of trade secrets from unfair competition can be found in the Labour Code,[48] the Civil Code[49] and the Criminal Code;[50] in

41 National Cyber Security Strategy of the Czech Republic for the period from 2021 to 2025 (18 March 2021) <https://www.nukib.cz/en/cyber-security/strategy-action-plan> accessed 31 May 2021.

42 Act No 181/2014 Coll. of 23 July 2014 on Cyber Security and Change of Related Acts <https://nukib.cz/en/cyber-security/regulation-and-audit/legislation/> accessed 31 May 2021.

43 Government Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Hungary> accessed 31 May 2021.

44 Cybersecurity Strategy of the Republic of Poland for 2019–2024 <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Poland> accessed 31 May 2021.

45 Act on the National Cybersecurity System, 5 July 2018 <https://www.cybsecurity.org/pl/act-on-the-national-cyber-security-system/> accessed 31 May 2021.

46 National Cyber Security Strategy of the Slovak Republic 2021–2025 <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map?selected=Slovakia> accessed 31 May 2021.

47 Act No. 69/2018 Coll on cybersecurity of 30 January 2018 <https://www.nbu.gov.sk/wp-content/uploads/legislativa/EN/Act_Cybersecurity.pdf> accessed 31 May 2021.

48 Labour Code No. 262/2006 Coll. <https://www.mpsv.cz/documents/625317/625915/Labour_Code_2012.pdf/a66525f7-0ddf-5af7-4bba-33c7d7a8bfdf> accessed 31 May 2021.

49 Civil Code, Law No 89/2012 of 3 February 2012 <http://obcanskyzakonik.justice.cz/images/pdf/Civil-Code.pdf> accessed 31 May 2021.

50 Criminal Code, Law No 40/2009, of 8 January 2009 <http://www.ejtn.eu/PageFiles/6533/Criminal%20Code%20of%20the%20Czech%20Republic.pdf> accessed 31 May 2021.

Hungary, the protection of trade secrets is regulated in various legislative acts covering a wide range of fields of law, including the Civil Code, the Competition Act, the Criminal Code, the Labour Code, the Information Act and the Public Procurement Act;[51] in Poland, trade secrets are regulated under several laws, including the Act on Combating Unfair Competition,[52] the Labour Code,[53] the Civil Code[54] and the Criminal Code;[55] on the other hand, in Slovakia the main sources for trade secrets protection are the Criminal Code,[56] the Competition Act[57] and the Commercial Code.[58] Overall, at the national level the legal picture is rather fragmented and not homogeneous among the four countries. In the next paragraph we get an insight into the relevant national regulation in Hungary; even though each one of the four V4 countries presents its unique national regulatory framework, the Hungarian case is quite paradigmatic in demonstrating how the four countries tend to treat economic cyber-espionage operations from a regulatory perspective.

Taking a Hungarian Perspective

Hungary was one of the first countries in Central Europe to formulate its national cybersecurity strategy in 2013; nevertheless, it has not regulated economic cyber-espionage in an *ad hoc* document. Indeed, we find several provisions protecting trade secrets in different national regulations: the Hungarian Civil Code[59] includes a definition and protection of 'trade secret';[60] additional provisions for the protection of trade secrets can be found in the Hungarian Competition Act,[61]

51 See the following paragraph.

52 Act on Counteracting Unfair Competition of 16 April 1993, Journal of Laws 2003, No 153, Item 1503 <http://www.wipo.int/wipolex/en/text.jsp?file_id=195378> accessed 31 May 2021.

53 Labour Code of 23 December 1997, Journal of Laws of 1998, No 21, Item 94 <https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=&p_isn=49416 & p_classification=01.02> accessed 31 May 2021.

54 Civil Code of 23 April 1964, Journal of Laws 1964, No 16, Item 93 <http://www.polishlaw.com.pl/pdf/act01b_new.pdf> accessed 31 May 2021.

55 Criminal Code, Act of 6 June 1997, Journal of Laws No 88, Item 553 <https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=&p_isn=43864 & p_classification=01.04> accessed 31 May 2021.

56 Criminal Code, Law No 300/2005 of 20 May 2005 <http://www.legislationline.org/documents/section/criminal-codes/country/4> accessed 31 May 2021.

57 Slovak Competition Act, Law No 136/2001 of 27 February 2001 <http://www.antimon.gov.sk/data/files/163_act-no-136-2001-on-protection-of-competition-amended-by-387-2011.pdf> accessed 31 May 2021.

58 Commercial Code, Law No 513/1991 of 5 November 1991 <https://is.muni.cz/el/1422/jaro2013/SOC038/um/Obchodny_zakonnik_513_1991_v_anglickom_jazyku.pdf> accessed 31 May 2021.

59 Hungarian Civil Code, Act V of 2013, available at <http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/96512/114273/F720272867/Civil_Code.pdf> accessed 31 May 2021.

60 Article 2: 47(1) of the Hungarian Civil Code

61 Hungarian Competition Act, Act LVII of 1996 on the Prohibition of Unfair Market Practices and Unfair Competition <https://www.gvh.hu/pfile/file?path=/en/legal_background/rules_for_the_hungarian_

the Hungarian Criminal Code,[62] the Hungarian Labour Code,[63] the Information Act[64] and the Public Procurement Act.[65] Accordingly, there are no specialised courts dealing with trade secrets violations: depending on the circumstances and the type of provisions that come into play, civil courts, or criminal courts, or the Hungarian Competition Authority might be competent (European Union Intellectual Property Office 2018: 210).

Hungary has been reported to be particularly vulnerable to industrial and economic espionage because of its weak security systems (Nasheri 2003: 26). This has led Hungary to cooperate with other countries, especially with the United States: back in October 1998, the United States and Hungary entered a joint initiative with the aim to fight organised crime, including cyber-crime, in Central and Eastern Europe (Nasheri 2003: 27). However, there is not much documented information regarding Hungary-USA agreements or joint public statements on the topic.

Moreover, it is hard to find data and cases of economic cyber-espionage; one of the most notable and well-documented ones seems to be a cyber-espionage operation discovered in 2013 by CrySyS Lab, a Hungarian cyber laboratory, which revealed a near decade-long cyber espionage operation that was targeting several public and private entities, mainly in Eastern European countries – the so-called TeamSpy operation (Lennon 2013). However, there is no information on the legal and/or judicial consequences (at the national, EU or international level) of such an operation. This confirms the fact that when it comes to economic cyber-espionage, one of the main problems is the lack of relevant data on the operations that are discovered and, accordingly, the lack of relevant legal and judicial information, which makes it quite difficult to assess whether the current regulatory framework in force is the most suitable (and efficient) one to deal with this kind of operations.

Nevertheless, Hungary remains a very interesting case study especially with the growing Chinese economic interests in the country. Most recently, news spread that Hungary is 'considering taking a huge, opaque and disadvantageous Chinese loan to pay for the construction of Fudan University's new Budapest campus' (Panyi 2021b), which would make Hungary become 'a Trojan horse for

market/competition_act/competition-act-documents/jogihatter_tpvt_hataly_20190101_a & inline=true> accessed 31 May 2021.

62 Hungarian Criminal Code, Act C of 2012 on the Criminal Code <http://www.legislationline.org/documents/section/criminal-codes/country/25> accessed 31 May 2021.

63 Hungarian Labour Code, Act I of 2012 <http://www.ilo.org/dyn/travail/docs/2557/Labour%20Code.pdf> accessed 31 May 2021.

64 Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information <https://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf> accessed 31 May 2021.

65 Public Procurement Act, Text No 2015 CXLIII <http://ilo.org/dyn/natlex/natlex4.detail?p_lang=en & p_isn=102840> accessed 31 May 2021.

Chinese [...] influence' (Panyi 2021b); indeed, is has been reported that 'Chinese [...] spies have been the second-most active in [Hungary] since 2016–17' (Panyi 2021b) with a 'growing number of Chinese citizens and companies [operating] in Hungary for intelligence tasks' (Panyi 2021a).

Accordingly, (cyber)espionage operations are likely to increase in the near future; it would be interesting to follow the regulatory developments in this respect. This is also true when it comes to the other three V4 countries; in this respect, it is also quite difficult to gather official and public data and information on economic cyber-espionage, its regulation and cooperation with other (non)EU countries in this field.

The V4 Group: Which Role for the Sub-Regional Level?

Generally, platforms of discussion can help in harmonising regulations and policies, as in the case of sub-regional groups, that may serve at the same time as a platform of discussion for countries and as a privileged channel for advocating national interests at the (next) regional (and international) level(s). Indeed, in contrast to international organisations, regional and more in particular sub-regional organisations 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 in which to discuss national, regional and international issues; exchanges of best practices, experiences and knowledge might work better within a small(er) group of countries.[66]

Back in 1997, James Crawford, former Judge at the International Court of Justice, wrote:

> 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. (Crawford 1997: 101)

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

66 For an emphasis 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 organisations in implementing UN Security Council Resolution 1540, described in the paper by Johan Bergenas (2008).

framework of reference. This can be particularly helpful when it comes to dealing with policies that are not (yet) harmonised, as in the case of economic cyber-espionage.

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 historical experiences since the late 1980s (Gebhard 2013: 26). Today, a number of sub-regional groupings of states exists, such as Benelux,[67] the Nordic Council,[68] the Central European Initiative[69] and the Baltic cooperation,[70] just to name a few (Rudka 1997: 196–197).

Especially in Central and Eastern Europe, almost every country is involved in at least one of sub-regional groupings (Cabada 2018); one of the most significant examples in this respect is the V4 (Gebhard 2013: 26).

The Visegrád group was established as a forum for sub-regional cooperation on 15 February 1991, when the heads of governments of Czechoslovakia (now the Czech Republic and Slovakia), Hungary and Poland signed the Declaration of Visegrád (Wołek 2013: 88). One of the first aims of the V4 was '[...the] full involvement in the European political and economic system [...]'.[71]

The V4 is 'weakly' institutionalised – the only organisations being the International Visegrád Fund[72] and the Visegrad Patent Institute[73] – 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.[74]

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.[75] Worth recalling are also the joint declarations of the

67 The Benelux Union includes Belgium, The Netherlands and Luxembourg. See the official website at <https://gouvernement.lu/en/dossiers/2018/benelux.html> accessed 31 May 2021.

68 It includes 87 members, from Denmark, Finland, Iceland, Norway, Sweden, the Faroe Islands, Greenland and Åland. See the official website at <https://www.norden.org/en/nordic-council> accessed 31 May 2021.

69 It is a regional organisation 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 at <https://www.cei.int> accessed 31 May 2021,

70 It includes Estonia, Latvia and Lithuania. For more information visit <https://vm.ee/en/baltic-cooperation> accessed 31 May 2021.

71 Visegrád declaration, 15 February 1991 <http://www.visegradgroup.eu/documents/visegrad-declarations/visegrad-declaration-110412> accessed 31 May 2021.

72 Established in 2000. See the official website at <https://www.visegradfund.org> accessed 31 May 2021.

73 Operating from 2016. See the official website at <http://www.vpi.int/index.php/en> accessed 31 May 2021.

74 For information on the work and activities of the V4 group, see the official website at <http://www.visegradgroup.eu> accessed 31 May 2021.

75 They all can be accessed (in the English version) at the official website at <http://www.visegradgroup.eu/documents/official-statements> accessed 31 May 2021.

ministers of the V4 countries on European Commission communications,[76] EU proposals for regulations[77] or on EU Directives.[78] The V4 has also drafted letters addressed to the European Commission.[79] The topics addressed during these meetings may range from agriculture, renewable energy, migration, financial and labour issues, to name a few (Strážay 2018).

When it comes to the issue of economic cyber-espionage, it should be noted that to date there has been no significant joint document in this regard issued by the V4; however, we find some programmatical references in a number of documents related to the more general issues of cyber-security and/or cyber--threats. Indeed, cybersecurity has been referred to in V4 Presidency Programs, with a call to strengthen cooperation,[80] and in the 2011 Bratislava Declaration on the occasion of the 20th anniversary of the Visegrad Group, according to which:

> 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 [...].[81]

And, more recently, in the Visegrad Group Joint Declaration on Mutual Cooperation in Digital Projects – adopted on 17 February 2021 at the meeting of the prime ministers of the V4 on the occasion of the 30th anniversary – which underlined 'the importance of cybersecurity and digital technologies in ensuring the economic growth in the V4 countries'.[82]

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

76 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.

77 E.g., Joint declaration of the Ministers of the interior on the proposal for a Regulation on the European border and coast guard, 16 October 2018.

78 E.g., Joint declaration of the Agricultural Ministers of Visegrád group, Bulgaria and Romania on the renewable energy Directive after 2020, 21 September 2017.

79 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.

80 It is worth recalling the recent 2020/2021 Polish Presidency 'Back on Track' <https://www.visegradgroup.eu/documents/presidency-programs/2020-2021-polish> accessed 31 May 2021. See also the 2018/2019 Slovak Presidency 'Dynamic Visegrad for Europe', the 2017/2018 Hungarian Presidency Program, the 2016/2017 Polish Presidency Program, the 2015/2016 Czech Presidency Program, the 2014/2015 Slovak Presidency Program, the 2013/2014 Hungarian Presidency Program, the 2012/2013 Polish Presidency Program and the 2007/2008 Czech Presidency Presidential Program, all available at <https://www.visegradgroup.eu/> accessed 31 May 2021.

81 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).

82 Visegrad Group Joint Declaration on Mutual Cooperation in Digital Projects (17 February 2021) <https://www.gov.pl/attachment/71bfd2d2-1d0a-4460-8479-8c9caea10fad> accessed 31 May 2021.

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-economy of the coming digital age. [...] A good and trusted blueprint of cyber-security cooperation at V4+ level should be followed [...].[83]

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

> The 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 [...].[84]

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 programme as well the EDA-led Cyberdefence Project Team [...].[85]

It is also worth recalling that in June 2020, a V4 document also made reference for the first time to 'intelligence activities' as one of the 'methods' that have been used to undermine the security of the countries: according to the *Long Term Vision of the Visegrad Group Countries on Their Defence Cooperation*, '[...] both state

83 Joint Declaration of the Ministers of Economic Affairs of the Visegrad Group Countries on the Future of Economic Cooperation (19 April 2018).

84 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).

85 Joint statement of the V4 ministers of defence (4 June 2013).

and non-state actors increasingly use unconventional and hybrid methods to exploit our vulnerabilities [...] includ[ing], among others, cyber-attacks [...] and increased intelligence activities'.[86]

Cybersecurity has also been 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',[87] 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 to 'take action on issues including [...] cybersecurity as well as digital skills'[88] 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'.[89]

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.[90]

In this respect, it is very interesting to highlight that the previous 2020/2021 Polish Presidency Programme 'Back on Track', in the section dedicated to the 'Initiatives in the cyber security area' listed, among others, the need for

> [c]onsultations with a view of finding topics of mutually beneficial cooperation in cyber security. These consultations will primarily take place through

86 Long Term Vision of the Visegrad Group Countries on Their Defence Cooperation (24 June 2020) <https://www.visegradgroup.eu/documents/official-statements/the-long-term-vision-of> accessed 31 May 2021.

87 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).

88 Joint Statement of the Ministers of Foreign Affairs of the Visegrad Group, Austria, Croatia and Slovenia (10 July 2017).

89 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).

90 See the description of the CECSP at the official website of the National Security Authority of Slovakia at <https://www.nbu.gov.sk/en/cyber-security/partnership/central-european-platform-for-cybersecurity/index.html> accessed 31 May 2021.

established channels, especially the Central European Cyber Security Platform, and may include [...] international law applicable to cyberspace operations.[91]

Accordingly, the V4 can make use of the already existing technical cooperation within the CECSP in order to also advance on coordination and (possible) harmonisation of the (national, European and international) regulatory framework applicable to cybersecurity-related operations, including economic cyber-espionage ones.

Conclusion

Globalisation and increasing economic interconnections, together with technology developments and the use of cyberspace in economic relations have brought up new challenges in protecting trade secrets (PricewaterhouseCoopers 2018: 22). Cyber security, including cyber-espionage, has become a key component of security strategies of countries. As it has been rightly affirmed, 'if a nation wants to be a great cyber power, it must elaborate a comprehensive national cyber strategy that will encompass the changes brought out by cyber capabilities and interconnected networks' (Joubert 2010: 111). Accordingly, states have started to elaborate regulations in order to deal with such a phenomenon. However, the relevant regulatory picture is still rather fragmented. Indeed, cyber threats know no boundaries; accordingly, national-oriented solutions are not sufficient.

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.[92]

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 organisations 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

91 2020/2021 Polish Presidency 'Back on Track' <https://www.visegradgroup.eu/documents/presidency-programs/2020-2021-polish> accessed 31 May 2021.

92 European Commission, High Representative of the EU for Foreign Affairs and Security Policy (n 50) 15.

new cybersecurity standards that enable infrastructures and organizations to improve cyber protections'.[93]

Today, the V4 has become a 'recognised' voice in international fora. Also EU institutions more and more tend to mention the V4 in press releases that report some of their meetings.[94] The ability to talk with one voice through the V4 platform has been labelled as the 'soft power' of the V4 (Strážay 2011); also in the field of cybersecurity in general, and of economic cyber-espionage in particular, the V4 may use its soft power to advocate sub-regional interests at the EU, as well as at the international level (Wielgos 2019), in order to influence in a positive way future law- and policy-making in the field.

As already stressed in the 2020 *Visegrad Group Joint Statement on the Future of the Eastern Partnership*, '[h]ybrid threats including cyber-attacks need to be addressed in a collaborative way through activities aimed at strengthening resilience'.[95] Finding a common way to deal with economic cyber-espionage operations at the V4 level, taking advantage of the platform of discussion and collaboration that already exists among the four countries, may provide a first step (and best practice) towards a more European (and international) approach to the issues at stake. In this regard, Hungary can have a key role in this respect since it has taken up the current round of the V4 presidency for 2021/2022: according to the Hungarian Presidency Program 2021/2022, *Recharging Europe*:

> the Hungarian Presidency will continue V4 coordination related to [...] cyber issues on the EU agenda. Cooperation between national cyber-security organizations and network security centres aimed at strengthening the resilience of critical infrastructures, especially in the health sector, and detecting and countering risks and attacks from cyberspace are important goals.[96]

93 '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> accessed 31 May 2021.

94 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> accessed 31 May 2021 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> accessed 31 May 2021.

95 The Visegrad Group Joint Statement on the Future of the Eastern Partnership; Prague, April 8, 2020 <https://www.visegradgroup.eu/documents/official-statements/the-visegrad-group-joint-200409> accessed 31 May 2021. See also the Speech given by the Czech Prime Minister in Warsaw on the occasion of the accession of the Visegrad Group countries to NATO (10 March 2019) <https://www.vlada.cz/en/clenove-vlady/premier/speeches/speech-given-by-the-czech-prime-minister-in-warsaw-on-the-occasion--of-the-accession-of-the-visegrad-group-countries-to-nato-173699> accessed 31 May 2021.

96 Hungarian Presidency Program 2021/2022, Recharging Europe (2021), 12 <https://v4.mfa.gov.hu/> accessed 3 September 2021.

As we have seen, economic cyber-espionage raises several points that deserve further research and discussion among all stakeholders, starting from the definition of the phenomenon, the collection of a database of relevant cases at the international level, and an appropriate regulatory framework of reference at any level of regulation. Discussions among stakeholders may well start among neighbour countries, on the appropriate instruments to use in order to address such activities. In this respect, the V4 group can become a privileged platform of discussion to advance in the regulatory harmonisation of the issues at stake.

References

Abott, Rich (2015): U.K. Agrees With China Not To Support Cyber Theft Of Intellectual Property, *Defense Daily* (29 October): available at https://www.defensedaily.com/u-k-agrees-with-china--not-to-support-cyber-theft-of-intellectual-property-2/uncategorized/ (31 May 2021).

Bergenas, Johan (2008): *The role of regional and sub-regional organizations in implementing UN Security Council Resolution 1540: a preliminary assessment of the African continent:* available at http://www.vertic.org/media/assets/nim_docs/background%20articles/UNIDIR%20Scheinman%201540%20pdf2-act341.pdf (31 May 2021).

Buchan, Russell (2018): *Cyber Espionage and International Law*, Hart Publishing.

Cabada Ladislav (2018): Visegrad Group in the Context of Other Central European Cooperation Formats. *Politics in Central Europe*, Vol. 13, No. 2, 165–179.

Cowan, Paris (2017): Australia, China agree to oppose cyber IP theft, *IT News* (24 April): available at https://www.itnews.com.au/news/australia-china-ink-agreement-to-stop-industrial--hacking-459387#:~ (31 May 2021).

Crawford, James (1997): Universalism and regionalism from the perspective of the work of the International Law Commission, in United Nations, ed., *International Law on the Eve of the Twenty-fist Century. Views from the International Law Commission*, 99–122, United Nations.

Eder, Marton (2021): Hungary says vaccine registration website under cyber attack, *Bloomberg Blog* (19 February): available at https://www.bloomberg.com/news/articles/2021-02-19/hungary-says-vaccine-registration-website-under-cyber-attack (31 May 2021).

European Union Intellectual Property Office (2018): *The baseline of trade secrets litigation in the EU member states*, EUIPO: available at https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States_EN.pdf (31 May 2021.)

Fidler, David P. (2020a): Cybersecurity in the Time of COVID-19, *Council on Foreign Relations Blog* (30 March): available at https://www.cfr.org/blog/cybersecurity-time-covid-19 (31 May 2021).

Fidler, David P. (2020b): 2020 in Review: The COVID-19 Pandemic and Cyberspace, *Council on Foreign Relations Blog* (14 December): available at https://www.cfr.org/blog/2020-review--covid-19-pandemic-and-cyberspace (31 May 2021).

Garcia-Mora, Manuel R, (1964: Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition, *U. PITT.L. REV.* 26 (65): 79–80.

Gebhard, Carmen (2013): Sub-Regional cooperation in Central Europe – past, present and future, *AARMS* 12 (1): 25–38.

Górka, Marek (2018): The Cybersecurity Strategy of the Visegrad Group Countries, *Politics in Central Europe* 14 (2): 75–98.

Hua, Jian (2015): Industrial Cyber Espionage, *Journal of Management Systems* 25 (3): 67–81

Jančárková, Taťána – Minárik, Tomáš (2019): Scenario 09: Economic cyber espionage, *Cyber Law Toolkit*: available at https://cyberlaw.ccdcoe.org/wiki/Scenario_09:_Economic_cyber_espionage (31 May 2021).

Joubert, Vincent (2010): Getting the essence of cyberspace: a theoretical framework to face cyber issues, in Czosseck – Podins, eds, *Conference on Cyber Conflict. Proceedings 2010,* 111–124, CCD COE Publications.

Kaan Pehlivan, Oğuz (2019): *Confronting Cyberespionage Under International Law*, Routledge.

Kenety, Brian (2020): ČSÚ: nearly 1 in 5 Czech companies faced cyberattack in 2018, *Radio Prague International* (13 January): available at https://www.radio.cz/en/section/business/csu-nearly-1-in-5-czech-companies-faced-cyberattack-in-2018 (3 September 2021).

Kolbasuk McGee, Marianne (2018): U.S., China Reach Cyber Agreement, *Bank Info Security* (25 September): available at https://www.bankinfosecurity.com/us-china-a-8553 (31 May 2021).

Legal Week Intelligence – CMS (2018): *The Cybersecurity Challenge in Central and Eastern Europe. Are multinational companies prepared?*, CMS Publication: available at https://cms.law/en/hun/publication/the-cybersecurity-challenge-in-central-and-eastern-europe (31 May 2021).

Lennon, Mike (2013): TeamSpy – A Decade-long Cyber Espionage Operation Targeting Eastern Europe, *Security Week* (20 March): available at https://www.securityweek.com/teamspy--decade-long-cyber-espionage-operation-targeting-eastern-europe (31 May 2021).

Lotrionte, Catherine (2015): Countering State-Sponsored Cyber Economic Espionage Under International Law, *North Carolina Journal of International Law and Commercial Regulation* 40: 443–541.

Magen, Sharon (2017): Cybersecurity and Economic Espionage: The Case of Chinese Investments in the Middle East, *Cyber, Intelligence, and Security* 1 (3): 3–18.

Nasheri, Hedieh (2003): The Intersection of Technology Crimes and Cyberspace in Europe: The Case of Hungary, *Information & Communications Technology Law* 12 (1): 25–48.

Panyi, Szabolcs (2021a): How Orbán's Eastern Opening brought Chinese spy games to Budapest, *Direkt36* (14 March): available at https://www.direkt36.hu/en/kemjatszmakat-hozott--budapestre-orban-kinai-nyitasa/ (31 May 2021).

Panyi, Szabolcs (2021b): Hungary could turn into China's trojan horse in Europe, *Reporting Democracy* (9 April): available at https://balkaninsight.com/2021/04/09/hungary-could-turn--into-chinas-trojan-horse-in-europe (31 May 2021).

PRI (2018): Investor-company dialogue on cyber security: five emerging findings, *PRI - Governance Issues* (24 September): available at https://www.unpri.org/governance-issues/investor--company-dialogue-on-cyber-security-five-emerging-findings/3664.article (31 May 2021).

PricewaterhouseCoopers (2018): Study on the scale and impact of industrial espionage and theft of trade secrets through cyber, *Study prepared for the European Commission* (18 December): available at https://ec.europa.eu/docsroom/documents/34841 (31 May 2021).

Ravishankar, Vaishnavi – Mooney, Olivia – Hader, Nora (2018): *Stepping up governance on cyber security. What is corporate disclosure telling investors?*, Principles for Responsible Investment, UNEP Finance Initiative, UN Global Compact: available at https://www.unpri.org/download?ac=5134 (31 May 2021).

Reynolds, Paul (2004): The World's Second Oldest Profession, *BBC News* (26 February): available at https://perma.cc/B9KM-E5E5 (3 September 2021).

Rudka, Andrzej (1997): Central Europe: regional cooperation and beyond, in Hayashi, Tadayuki, ed., *The emerging new regional order in Central and Eastern Europe*, 193–209, Hokkaido University.

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

Schmitt, Michael – Vihul, Liis (2017): *Tallinn Manual 2.0 on the international law applicable to cyber operations*, Cambridge University Press.

Strážay, Tomas (2011): Visegrád – arrival, survival, revival. Selected V4 Bibliography, *Visegrad Group*: available at http://www.visegradgroup.eu/documents/bibliography/visegradarrival--survival-120628 (31 May 2021).

Strážay, Tomas (2019): When pragmatism wins: Slovakia in the Visegrád group, in Brezáni, Peter, ed., *Yearbook of Slovakia's foreign policy 2018*, 67–74, Research Center of the Slovak Foreign Policy Association.

Tasheva, Iva (2017): European cybersecurity policy. Trends and prospects, *European Policy Centre – Policy Brief* (8 June): available at https://www.epc.eu/pub_details.php?cat_id=3 & pub_id=7739 (3 September 2021).

UNODC (2018): Cyberespionage, *E4J University Module Series: Cybercrime:* available at https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html (31 May 2021).

Van Arnam, Robert C. (2001): Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection, *North Carolina Journal of International Law* 27: 95–139.

Wielgos, Alexander (2019): V4 in Changeful Espionage, *The Warsaw Institute Review* (4 November) available at https://warsawinstitute.org/v4-changeful-espionage (31 May 2021).

Wołek, Artur (2013): Precipices beneath summits? The Visegrád cooperation seen from middle policy levels, in Marušiak, Juraj *et al.,* eds., *Internal cohesion of the Visegrád group*, 86–99, VEDA.

Zachová, Aneta *et al.* (2018): Is Visegrad group ready for cyber-attacks?, *Visegrad.info* (7 May): available at https://visegradinfo.eu/index.php/collaborative/560-is-visegrad-group-ready-for-cyberattack (31 May 2021).

Federica Cristani *is a senior researcher at the Centre for International Law at the Institute of International Relations in Prague (CZ). She earlier worked as a post-doctoral researcher at the World Trade Institute of the University of Bern (CH), and at the University of Verona (IT), and has been a visiting scholar in different universities and research centres in Europe. E-mail: cristani@iir.cz.*