UDC 34.047/34.096 (043.2)

Cristani F., PhD., REEEC Virtual Open Research Laboratory Associate, University of Illinois, USA

ECONOMIC CYBER-ESPIONAGE IN THE (POST-)COVID-19 ERA IN EUROPE: WHICH (NEW) CHALLENGES?

The present paper offers a reflection on the (new) challenges to economic cyber-espionage that have emerged in the (post-)COVID-19 period in the European region.

1. Economic cyber-espionage in Europe. 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 destabilization. By 2021, experts estimate that cyberattacks will cost the world $6 trillion per year. Among the cyber challenges 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).

Europe is a particularly exposed region, because of the advanced know-how of the companies based therein, as testified by a study prepared in 2018 for the European Commission by PricewaterhouseCoopers, which confirmed that there is limited qualitative and quantitative information available on cyber theft of trade secrets and calls for a more appropriate regulatory framework in the field [9].

Under international law, there exist no uniform approach to the matter [6; 10, p. 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», the United Nations report of the same year does not include economic cyber-espionage among possible States behaviour in the cyberspace [5]. Moreover, it is not clear whether the Agreement on Trade-Related Aspects of Intellectual Property Rights of the World Trade Organization – which includes the commitment to protect certain types of intellectual property rights, including trade secrets - can be applied in case of economic cyberespionage [1, p. 143]. Also at the European Union (EU) level, the legal framework appears rather fragmented: while there is a quite robust regulatory framework dealing with cybersecurity (e.g. Regulation 2019/881 and the 2020 EU NIS Cooperation Group's report on Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures), there is no specific act addressing the issue of economic or industrial cyberespionage. Also at the national level, each country has adopted its own cybersecurity regulation [7]. The question of economic cyber-espionage is also interlinked with the protection of national

security: many countries consider economic cyber-espionage an important element for the national security and economic development.

2. Economic cyber-espionage in the (post-)covid-19 era. The COVID-19 pandemic have opened up new opportunities for cyber-threats and cyber-espionage operations, because of the increasing dependence by states and private businesses on digital technologies: we call briefly recall episodes of ransomware attacks on national health facilities (like in Czech Republic and France during March and April 2020) and cyber espionage against vaccine research organizations [4]. In May 2020, UK and USA released a joint statement warning of a rise in cyberespionage against pharmaceutical firms, research institutes and universities, and healthcare institutions [8]. Also ENISA has highlight how «[t]he threat landscape is becoming extremely difficult to map. Not only attackers are developing new techniques to evade security systems, but threats are growing in complexity and precision in targeted attacks» [2, p. 13].

Some concluding remarks. As it has been rightly stated «[t]he ways that COVID-19 highlights many cybersecurity problems invites re-consideration of cybersecurity strategies and policies» [3]. As already pointed out in the PricewaterhouseCoopers's study, there is growing need of cross-border cooperation among all interested stakeholders. There have been already suggestions to use international trade law as a vehicle to mitigate cyberattacks and «better protect trade secrets» [9, p. 45]. The EU can take a leading role in acting as a coordinator in this regard and «providing a concerted solution to a shared problem» [9, p. 52].

Literature

1. Buchan R. Cyber Espionage and International Law, 2018.

2. ENISA. From January 2019 to April 2020. The year in review. ENISA Threat Landscape. 20 October 2020. URL: https://www.enisa.europa.eu/publications/year-in-review

3. Fidler D.P. Cybersecurity in the Time of COVID-19. Council on Foreign Relations Blog. 30 March 2020. URL: https://www.cfr.org/blog/cybersecurity-time-covid-19

4. Fidler D.P. 2020 in Review: The COVID-19 Pandemic and Cyberspace. Council on Foreign Relations Blog. 14 December 2020. URL: https://www.cfr.org/blog/2020-review-covid-19-pandemic-and-cyberspace

5. Janárková T., Minárik T. Scenario 09: Economic cyber espionage. Cyber Law Toolkit. 2019. URL: https://cyberlaw.ccdcoe.org/wiki/Main_Page

6. Lotrionte C. Countering State-Sponsored Cyber Economic Espionage Under International Law. North Carolina Journal of International Law and Commercial Regulation. 2015. N 40. P. 443-541.

7. Meltzer J.P. Cybersecurity and digital trade: What role for international trade rules?. Global Economy & Development Working Paper. November 2019. N 132. URL: https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-and-digital-trade_-What-role-for-international-trade-rules.pdf

8. Oxford Analytica. COVID-19 alters focus of cyberespionage. Daily Brief. 11 June 2020. URL: https://dailybrief.oxan.com/Analysis

9. PricewaterhouseCoopers. Study on The scale and impact of industrial espionage and theft of trade secrets through cyber. Prepared for the European Commission. 18 December 2018. URL: https://ec.europa.eu/docsroom/documents/34841

10. Schmitt M.N., Vihul L. Tallinn Manual 2.0 on the international law applicable to cyber operations. 2017. URL: https://ccdcoe.org/research/tallinn-manual/

UDC 347(043.2)

Šimkutė Laura, Master in Law graduate
from the Vytautas Magnus University in Lithuania, judicial assistant
in the District Court of Panevėžys, Lithuania

DIGITAL AGE AND DIGITAL PRIVACY

Currently law is challenging of regulation protection of the main currency – information [1]. Vast amount of significant as well as sensitive information is being collected cheaply and efficiently stored and analysed. Law has to comply with technological changes and human rights. It becomes more and more difficult for law-makers to follow technology changes and ensure that law is effective in securing the right to privacy, to protect personal data and the freedom of expression.

Today's era of social transformation also includes living in a digital age, which relates in particular to the use of computer technology [2]. According to the Internet World Stats Data, in 1995 there were 16 million Internet users, 0.4% of World's Population, in 2017 51.7% of the world's population were internet users and in October 2020 there were 4,929 billion Internet users, 63.2% of World's Population [3]. The numbers have expanded in a short time and the internet continues to grow day by day. Internet users openly create profiles, provides sensitive personal information, i.e. marital status, sexual orientation, and reveal their locations. They pay for seemingly free services with their data and trade privacy for services.

Privacy is the state or condition of being free from being observed or disturbed by other people [4]. The right to privacy is established in Article 17 of International Covenant on Civil and Political Rights [5]. Privacy was already known in the 19th century: "The right to be left alone" [6] – as defined by Brandeis and Warren is "the person's right to lead his life the way he wants without any interference" [7]. According to Alan Westin: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [8]. As scholar Robert C. Post explains: „[p]rivacy is a value so complex, so entangled