DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

Mexican Law Review
New Series
XIII-1

CYBERSECURITY AND E-COMMERCE IN FREE TRADE AGREEMENTS

Anahiby Becerril*

Abstract: *We are facing a digital age characterized by constant flows of goods and services, financial assets, people, information and communication. As a consequence, the world economy is increasingly connected, and digitalization has spread to such an extent that today's world economy is a digital one, which has come to break down commercial barriers that the traditional economy and politics were unable to. Security and trade policy concerns are nothing new. However, given the electronic nature of commercial transactions (e-commerce), this has taken on a new and urgent importance. Cyberspace is a space of flows, a virtual space that grows every day with the transactions that take place through the use of ICT. Governments of many countries have begun to develop cybersecurity strategies, while trying to promote the benefits of a hyperconnected and cyber-enabled world. This article analyzes how e-commerce policies promote the protection of cyberspace. Specifically regarding e-commerce, care must be taken so that the cybersecurity strategy does not become an obstacle or constraint to such electronic transactions. The protection of cyberspace must be carried out with a multi-stakeholder approach. These issues are also of public interest since threats to cyberspace can affect entire countries and societies.*

Keywords: *Cyberspace, cybersecurity, e-commerce, treaties.*

Resumen: *Nos enfrentamos a una era digital caracterizada por flujos constantes de bienes y servicios, activos financieros, personas, información y comunicación. Como consecuencia de lo anterior, la economía mundial está cada vez más conectada, y la digitalización se ha extendido hasta tal punto que la economía mundial actual es una economía digital. Esta economía digital ha llegado a romper las barreras comerciales que la economía y la política tradicionales no habían logrado. Las preocupaciones sobre la seguridad y las políticas comerciales no son nuevas. Sin embargo, dada la naturaleza electrónica de las transacciones comerciales (comercio electrónico), esta ha adquirido una importancia nueva y urgente. El ciberespacio es un espacio de flujos, un*

[*] PhD in Law and Globalization, Cybersecurity Law Specialist. Professor at the National Autonomous University of Mexico, UNAM. Email: *anahiby@hotmail.com*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

espacio virtual que crece diariamente con las interacciones que se realizan con el uso de las TIC. Los gobiernos de muchos países han comenzado a desarrollar estrategias de ciberseguridad, mientras intentan promover los beneficios de un mundo hiperconectado y con acceso a Internet. En este artículo analizaremos cómo, a través de las políticas de comercio electrónico, se promueve la protección del ciberespacio. En relación con el comercio electrónico, se debe buscar que una estrategia de ciberseguridad no se convierta en un obstáculo o una barrera para estas transacciones electrónicas. La protección del ciberespacio debe llevarse a cabo con un enfoque de múltiples partes interesadas. Estos temas también son de interés público, ya que las amenazas al ciberespacio pueden afectar a países y sociedades enteras.

Palabras clave: *Ciberespacio, ciberseguridad, comercio electrónico, tratados.*

Table of Contents

I. Introduction

“If you think technology can solve your security problems, then you don’t understand the problems and you don’t understand the technology”.[1]

[1] Bruce Schneier Secrets & Lies, Digital Security in a Networked World, XXII (Wiley Publishing Inc., Indiana) (2004).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

We are facing a digital age characterized by constant flows of goods and services, financial assets, people, information and communication. This global flow is not new; what is new is its exponential growth in recent years, as a result of economic progress, particularly with the massive spread of Information and Communication Technologies (ICTs), specifically the Internet and the accessibility of connected mobile devices (such as smartphones).

The ability to link the physical world with each human activity, through sensors and networks, to obtain knowledge through advanced analysis is — and will undoubtedly continue— transforming our daily lives, as well as the economy and society. The digitalization of things constitutes one of the great phenomena of recent years. Translating everything (documents, music, images, maps, ourselves) into bits transforms the way we understand and interact with the world.[2]

The global economy is increasingly connected, and digitization has spread to such an extent that today's global economy is a digital one. This is nourished to a large extent by the massification of cloud computing, as well as Big Data and advances in the Internet of Things (IoT) and Artificial Intelligence (AI).

Consider the following information: for *The Internet in Real Time*, the amount of data uploaded to the Internet in one second is 24,000 gigabytes (GB).[3] Cisco[4] has estimated that annual global IP traffic will reach 3.3 ZB[5] (1000 Exabytes) by 2021. In 2016, global IP traffic was 1.2 ZB per year or 96 EB[6] (billion GB) per month. By 2021, global IP traffic will reach 3.3 ZB per year, or 278 EB per month. In its *Visual Networking Index: Forecast and Methodology, 2016-2021* report, the Cisco predicts the volume of devices connected to IP networks to be three times greater than the world population. According to their estimates, there will be a 3.5-device-per-capita network by 2021, compared to 2.3 devices per capita in 2016. Accelerated in part by the increase and capabilities of the devices, IP traffic per capita will reach 35 GB in 2021, compared to 13 GB in 2016.

With lower costs and greater connectivity, ICT platforms have allowed goods and services to flow through electronic commerce (e-commerce). The commercial transactions that are reflected in the use of information circulate through this "meta-space that is cyberspace",[7] without having to physically

[2] Anahiby Becerril & Samuel Ortigoza Limón, *Habilitadores tecnológicos y realidades del Derecho Informático Empresarial*, 41, IUS, Revista del Instituto de Ciencias Jurídicas de Puebla 11, 41, January-June (2018).

[3] 1 gigabyte (GB) is an amount of information storage equivalent to 1000^3 (1,000,000,000 or one billion) bytes.

[4] CISCO, *CISCO Visual Networking Index: Forecast and Methodology, 2016-2021*, *https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf*.

[5] 1 zettabyte (ZB) is a storage unit equivalent to 1000^7 (one trillion) gigabytes.

[6] 1 exabyte (EB) is a unit of measurement of data storage that equals 10^{18} bytes.

[7] Concept obtained from the Preamble to the Bill of Rights in Cyberspace, publish-ed by

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

reside in any specific place, as seen in the relocation of the space erected by telecommunications. This has allowed commercial immediacy, which encourages e-commerce.

In 2017, world production of ICT goods and services represented around 6.5% of the world's Gross Domestic Product (GDP).[8] In 2015, worldwide e-commerce sales reached an estimated $25.3 billion US dollars (USD),[9] a figure that continues to increase daily. It is estimated that worldwide e-commerce retail trade for 2017 reached US$2.290 billion,[10] thus representing one tenth of total retail sales worldwide.

According to a study by the Association of Internet.mx, it is estimated that the value of the Mexican e-commerce market for 2017 was USD 396.04 billion, which constitutes a 20.1% increase over the previous year.[11] In this sense, international e-commerce purchases that take place in Mexico constitutes 75% of its total users.[12] With the digitization of everything, ICTs are leading up to an exponential increase in the available volume and types of data, creating countless possibilities to transform society and therefore countries. However, as individuals, governments, companies and societies in general, we are still at a stage of experimentation, innovation and adaptation to this new world of digital interactions, a world where at every moment the data contain greater volume, speed, variety than ever.

The dynamic economic sphere of cyberspace is experiencing great turmoil due to global forces of competition, cooperation and threats to cyberspace. These changes create confusion and uncertainty and can lead to the creation of strategies and policies that become barriers to electronic commerce and the digital economy.

Emilio Suñé Llinas (2013), *http://oiprodat.com/2013/04/21/declaracion-de-derechos-del-ciberespacio/*.

[8] United Nations Conference on Trade and Development (UNCTAD), Informe sobre la economía de la información, 2017. Digitalización, comercio y desarrollo. Panorama general 2 (United Nations, New York) (2017).

[9] Kimberly Boatwright, Sean Doherty, *5 Ways to Make Global E-Commerce Easier for Everyone* (World Economic Forum) (2017), *https://www.weforum.org/agenda/2017/12/ecommerce-trade-wto-growth- opportunity/*.

[10] Emarketer, *Worldwide Retail and Ecommerce Sales: Emarketer's Estimates for 2016-2021* (2017), *https://www.emarketer.com/Report/Worldwide-Retail-Ecommerce-Sales-eMarketers-Estimates-20162021/2002090*.

[11] However, this figure is down from the growth shown in 2016 that was $329.85 million in relation to 2015 which was $257.09 billion USD, which would imply an increase of 28.3% between those years; *see* Asociación de Internet.mx, Estudio de Comercio Electrónico en México 2018, (2018) December, *https://www.asociaciondeinternet.mx/es/component/remository/func-startdown/72/lang,es-es/?Itemid=*.

[12] In 2016, it made up 60%; *see Asociación de Internet.mx, Estudio de Comercio Electrónico en México 2018* (2018) December, *https://www.asociaciondeinternet.mx/es/component/remository/func-startdown/72/lang,es-es/?Itemid=*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

Threats and incidents of digital security have increased in recent years and have had important economic and social consequences for public and private organizations, as well as for people. Some examples include interrupted operations (for example, by *DDoS*[13] or sabotage), direct financial loss, lawsuits, damage to reputation, and diminished competitiveness (as in the case of theft of trade secret), as well as loss of customer trust.

The threats found in cyberspace are different since they do not come only from states, but from people and non-state actors who use it to promote their interests through malicious actions and behaviors.[14] Unlike other domains such as water, land and sea, the purpose of carrying out attacks in cyberspace is not to have a domain over it, but so that, through it, use it to damage people, states and business.

To face risks and threats in cyberspace, most nations have contemplated an international commitment or obligation to cooperate with others and contribute to global cybersecurity. More and more in speeches from all over the world we hear that cooperation is vital to maintaining a secure cyberspace that promotes national security and stability for all users in general. An example of this is found in the Convention on Cybercrime, also known as the Budapest Convention, of the Council of Europe.[15] This document clearly explains the importance of having appropriate legislative measures and international cooperation in the field of cybercrime.

Efforts to address issues related to security have also been carried out by intergovernmental organizations, such as the OAS[16] —Organization of American States—, and the UN —United Nations—.[17] This last one has issued

[13] *Distributed Denial of Service.*

[14] Derek S. Reveron, *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World* (Washington, DC., Georgetown University Press) (2012).

[15] Signed in Budapest in 2001, it came into force in 2004. It has been signed by more than 53 states and is open to accession by countries that are not members of the Union. To date, Mexico has not adhered to this Convention.

[16] With the unanimous approval of the Comprehensive Inter-American Cybersecurity Strategy in 2004, the OAS became the first regional organization to adopt a Cybersecurity Strategy, *see Organization of American States, a Comprehensive Inter-American Cybersecurity Strategy: a Multidimensional and Multidisciplinary Approach for the Creation of a Culture of Cybersecurity* (2004), *http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf*; *The Declaration on Strengthening Cyber Security in the Americas*, *OEA/Ser.L/X.2.12 CICTE/DEC.1/12 rev. 1*, 9 March 2012, *https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/OAS%20-%20STRENGTHENI NG%20CYBERSECURITY%20IN%20THE%20AMERICAS.pdf*; *The Declaration on the Protection of Critical Infrastructure before Emerging Threats, OEA/Ser.L/X.2.15 CICTE/doc.1/15,* 23 March 2015, *https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf*, as well as the OAS Cyber Security Initiative, *https://www.sites.oas.org/cyber/Documents/2015%20 Iniciativa%20de%20Seguridad%20Cibern%C3%A9tica%20de%20la%20OEA.PDF).*

[17] One example, among many others, is the creation of the Group on Information Security and Cybercrime and Cybersecurity.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

several recommendations emphasizing that "the dissemination and use of information technologies and means affect the interests of the entire international community",[18] recognizing that "technologies can also be used for purposes that are inconsistent with the objectives of maintaining international stability and security".

In the same way, we find international institutions that have established formal standards, such as the International Telecommunications Union (ITU), the Internet Corporation for Assigned Names and Numbers (ICANN),[19] the International Organization for Standardization (ISO), and the National Institute of Standards and Technology (NIST), among others.

Along the same strain, military, political and economic organizations such as the North Atlantic Treaty Organization (NATO),[20] the European Union,[21] the Organization for Economic Co-operation and Development (OECD),[22] the Association of Southeast Asian Nations (ASEAN) and the Asia-Pacific Economic Cooperation (APEC), the World Economic Forum (WEF), have also addressed issues of cybersecurity.

Derived from the importance of the global digital economy and market, instead of being treated as technical problems that require technical solutions, the risks in cyberspace must be addressed as economic risks. This is why this article analyzes the importance of cybersecurity for the promotion of e-

[18] "...the dissemination and use of information technologies and means affect the interests of the entire international community"; *see* General Assembly of the United Nations, Preambles of Resolutions A/RES/55/28 November 20, 2000; A/RES/56/19 of November 29, 2001; A/RES/59/61 of December 3, 2004; A/RES/60/45 of December 8, 2005; A/RES/61/54 of December 6, 2006; A/RES/62/17 of December 05, 2007; A/RES/63/37 of December 2, 2008; A/RES/64/25 of December 2, 2009. Preambles of Resolutions A/RES/58/32 of December 08, 2003; A/RES/59/61 of December 3, 2004; A/RES/60/45 of December 8, 2005; A/RES/61/54 of December 6, 2006; A/RES/62/17 of December 5, 2007; A/RES/63/37 of December 2, 2008; A/RES/64/25 of December 2, 2009.

[19] This association is in charge of the administration of the DNS (Domain Name System).

[20] For example, the NATO Defense Center for Cyber Defense (NATO CCDCOE) was established in 2008 in an attempt to improve NATO's cyber defense capability.

[21] The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, presented in 2013, which in addition to establishing the Principles on cybersecurity, states, inter alia, its objective to "safeguard an online environment providing the highest possible freedom and security for the benefit of everyone"; JOIN/2013/01 final, *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001*. Another example is the Directive on the security of network and information systems (NIS), which was introduced to strengthen cooperation among Member States on the subject of cybersecurity, European Parliament and Council of Europe, Directive (EU) 2016/1148, *http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN*, among others.

[22] In 1992, the OECD presented the Guidelines for the Security of Information Systems, *http://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.html*; which were replaced in 2002 by the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, *https://www.oecd.org/sti/ieconomy/15582260.pdf*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

commerce within the framework of free trade agreements. Though cybersecurity policies should be sought in the promotion of e-commerce, cyberspace protection measures and their infrastructures must be analyzed to determine that they do not constitute an obstacle to e-commerce. Therefore, we will first analyze the development of e-commerce as a driving force of the digital economy, mentioning the enablers and technologies that have fostered its development. Later, we will examine cyberspace in the cybersecurity environment to know the efforts that have been carried out for its protection. Through the knowledge of cyberspace and cybersecurity, a framework of cybersecurity will be built up by the countries that make up the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP), as it will be within the framework of the renegotiations of the North American free trade agreement. Lastly, a series of final considerations will be given.

II. Electronic Commerce in the Global Digital Economy

The new economy is global, but also digital; it evolves in real time and without borders. The economy is immersed in a global conversation, or digital interaction. It seems that the world is now united in a single electronic market, just a click away. The basis of commerce that develops in cyberspace is connectivity. The Internet, by its very nature, has knocked down the geopolitical boundaries that traditional commerce could not.

For the World Trade Organization (WTO), e-commerce constitutes: "the production, distribution, marketing, sale or delivery of goods and services by electronic means".[23] While for the OECD this type of commerce constitutes "the sale or purchase of goods or services, performed by computer networks by methods specifically designed for the purpose of receiving or placing of place orders".[24]

In 1996, fulfilling its work of establishing friendly international economic relations, the United Nations Commission on International Trade Law (UNCITRAL) published its Model Law on Electronic Commerce, with Guide to Enactment. With this instrument, UNCITRAL sought to provide legal certainty and unify criteria in transactions that were developed via data messages,[25] with the aim to progressively standardize and unify international

[23] World Trade Organization, *Work Programme on electronic Commerce*, WT/L/ 274 (1998).

[24] Organization for Economic Cooperation and Development (OECD), *Glossary of Statistical Terms*, *https://stats.oecd.org/glossary/detail.asp?ID=4721*.

[25] The Model Law states that data message: "means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy" (Article 2); *see* United Nations Commission on International Trade Law (UNCITRAL), *Uncitral Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 Bis as Adopted in 1998* (United Nations

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

commercial law. In its preamble, the UNCITRAL Model Law[26] refers to "transactions in international trade are carried out by means of electronic data interchange and other means of communication", which "involve the use of alternatives to paper-based methods of communication and storage of information".[27]

In addition to highlighting the importance of e-commerce, the above definitions cover all kinds of commercial electronic transactions, including electronic funds transfers and credit card payments. However, such broad definitions are somehow obsolete as they do not recognize new forms of e-commerce, such as those done through the Internet (open networks) and limited to electronic transactions themselves, without referring to the spirit of this kind of business (cyberspace and virtual market, among others). Therefore, we consider the following, broader definition:

> Electronic commerce includes the set of commercial transactions carried out by electronic or digital means of communication, either through open or closed networks, which is deployed within a global system, using computer and telecommunications networks (mainly the Internet), which create virtual markets of all kinds of products, goods and services in cyberspace.[28]

The economy that takes place in cyberspace groups companies into large networks of interdependent relationships in which these companies share activities and interests.[29] Industrial companies have given their place to technical-scientific companies and to transnational network companies that base their services on software. And in some cases, they have become real-time companies, continuously and immediately adapting to the changing conditions of a new digital or hybrid environment, conditioned by the immediacy of information. An example of this is found in the new models of LegalTech,[30]

Organization, Vienna) (1999), *https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf*.

[26] *Id.* 2.

[27] And while it highlights that many of the discussions are limited to the Internet, as the means with which it is mainly associated, the UNCITRAL Model Law of Electronic Commerce identifies six main instruments through which e-commerce can be carried out: telephone, fax, television, electronic payments and fund transfer systems, EDI and the Internet.

[28] Víctor Manuel Castrillón y Luna & Anahiby Becerril, Contratación Electrónica Civil Internacional. Globalización, Internet y Derecho 167 (Porrúa, México) (2015).

[29] Jeremy Rifkin, La Era del acceso. La revolución de la nueva economía 32 (Paidós, Barcelona) (2013).

[30] Legal Technology, or "Legal Tech", is a term that broadly refers to the use of innovative technology and software to streamline and enhance legal services. Legal Tech companies are generally startups founded for the specific purpose of disrupting the operation of the (traditionally conservative) legal profession. *See* Micha-Manuel Bues & Emilio Matthaei, *LegalTech on the rise: technology changes legal work behaviors, but does not replace its profession*, in Liquid Legal: Trans-

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

RegTech[31] and FinTech,[32] all of which are companies that rely on new technologies like cloud computing, big data, artificial intelligence or blockchain, to create innovative solutions in providing services in their sector, bringing, in turn, more options for their users/customers.

In this way, the business organization has been restructured to adapt and get the most out of ICT. While the proper use of the Internet in companies previously meant a source of competitiveness and productivity, a digital strategy is now a fundamental part of the business plan. Electronic commerce not only benefits business-to-consumer (B2C) or business-to-business (B2B) commerce but has also strengthened consumer-to-consumer (C2C) trade. Platforms like eBay, Mercado Libre, and Amazon, among many others, have allowed small entrepreneurs and basically anyone to participate in international trade.

Another characteristic of this digital economy is the change of "traditional" roles of producers and consumers. By changing from a consumer Internet to a consumer and production Internet, we have become "prosumers".[33] By becoming part of the production process with our knowledge, information and ideas, requesting or designing customized articles, or even uploading content to the network, the gap between consumers and producers is blurred. If the previous decade had brought us an internet of information, we are now witnessing the emergence of the Internet of value, which provides us with tools to achieve more active participation in the processes of services and products.

The rapidity with which this digital economy has developed is the result of the technologies and innovations that drive the Fourth Industrial Revolution. Multiple organizations have classified the technologies that are behind this new Industrial Revolution. However, if we consider that all these new technologies and developments share the key feature of harnessing the power generated by the digitalization of all things and ICT, we should have long

FORMING LEGAL INTO A BUSINESS SAVVY, INFORMATION ENABLED AND PERFORMANCE DRIVEN INDUSTRY (Springer Cham, 2017).

[31] This term, created by the Financial Conduct Authority (FCA) of the United Kingdom, refers to companies that rely on new technologies such as cloud computing, big data or blockchain to create solutions to help companies of all sizes and sectors to comply with regulatory requirements. The FCA defines them as "new technologies to facilitate the delivery of regulatory requirements-so-called RegTech"; *see* FINANCIAL CONDUCT AUTHORITY, "CALL FOR INPUT: SUPPORTING THE DEVELOPMENT AND ADOPTION OF REGTECH", (FCA, UK) (2015), *https://www.fca.org.uk/publication/call-for-input/regtech-call-for-input.pdf*.

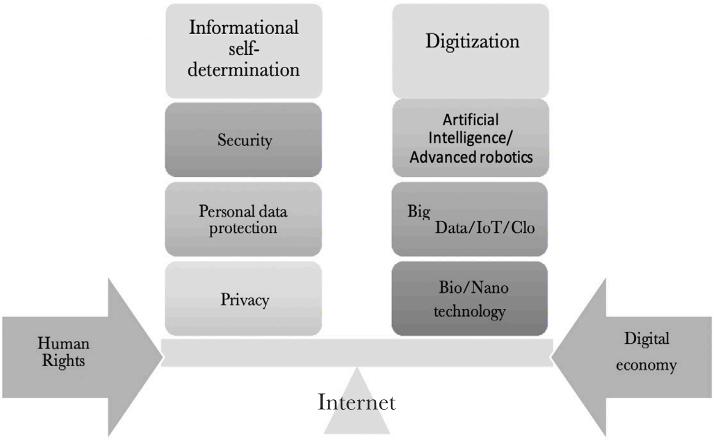
[32] Several international organizations and national authorities have given different definitions to this technological evolution in the financial sector, from Financial Technology or FinTech to the term "technofinance". These concepts are used to describe advances in technology that can transform the provision of financial services and thus promote the development of new business models, applications, processes and products.

[33] "The change of model has empowered users to become producers and, at the same time, consumers of information, services and media, which allows them to become suppliers and co-creators"; *see* ANAHIBY BECERRIL, SAMUEL ORTIGOZA LIMÓN, *supra* note 17.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

ago questioned their safety and resilience. To learn about the challenges on its protection, we will briefly analyze the technologies that we consider are the key in the development of the digital economy.[34]

Figure 1. Enablers and Protections within the Digital Economy



Source: Prepared by the author.

1. *The Digitization of Everything and the Increasing Amount of Information Available*

The data and information that emerge from the digitalization of things have become the raw material for businesses and companies, a vital asset capable of creating a new form of economic value.[35] The implementation of the

[34] UNCTAD recognizes advanced robotics, artificial intelligence, the Internet of Things, cloud computing, big data analysis and three-dimensional (3D) printing, *see United Nations Conference on Trade and Development* (UNCTAD), *Report on the Information Economy, 2017. Digitalization, Trade and Development, General Overview* 2 (United Nations, New York) (2017). The OECD refers to "3D printing, the Internet of Things, advanced robotics, new materials (based on bio or nano technology), as well as new processes (data driven production, artificial intelligence, synthetic biology)", *see Organization for Economic Cooperation and Development* (OECD), *The Next Production Revolution: Implications for Governments and Business* 14 (OECD Publishing, Paris) (2017). For the World Economic Forum, the "megatrends" and the technological engines of the fourth industrial revolution are: physical (autonomous vehicles, 3D printing, advanced robotics, new materials), digital (Internet of Things, blockchain) and biological (synthetic biology), *see* Klaus Schwab, the Fourth Industrial Revolution 17 and ss. (World Economic Forum, Geneva) (2016).

[35] Viktor Mayer-Schönberger & Kenneth Cukier, Big Data. La revolución de los datos masivos (Turner publicaciones S.A., Madrid) (2013).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

DIKW[36] model for knowledge management and the extraction of data value —material premium data— can only be optimized in a coherent data ecosystem that includes software companies, SMEs, data sectors (private and public), researchers, academic institutions and capital providers. This data ecosystem will support the intensification of cooperation among the various groups of stakeholders to work towards achieving mutually reinforcing objectives.

Data economics[37] measures the overall impact of the data market; that is, the market in which digital data are exchanged as products or services derived from raw data, in the economy as a whole. For the European Union, this data economy involves the generation, collection, storage, processing, distribution, analysis, processing, delivery and exploitation of the data that make digital technologies possible.[38]

2. *Artificial Intelligence (AI)*

This is characterized by automatic learning based on data and automated decision-making. In broad terms, AI is a collective term to identify "computer systems that can sense their environment, think, learn and act in response to what they perceive and their objectives".[39] According to the study prepared by PWC,[40] in 2030 the global GDP will be 14% higher as a result of artificial intelligence, which is equivalent to 15 7000 million USD.

3. *Big Data*

If we consider that every day more than 2.5 exabytes (equivalent to 1,000,000 terabytes)[41] are generated in the world, we must consider that, as a result of the digitization of everything, we live in a world of enormous amounts of data. The amount does not define Big Data as it is only an exponential of the amount of information that is generated daily. From a technological point of view, we can understand Big Data as the information or group of data that cannot be stored or visualized with traditional tools due

[36] Data, Information, Knowledge and Wisdom.

[37] If we consider that 70% of the information is generated by us as users of various electronic devices, the foregoing would be equivalent to the "commodification of the self".

[38] European Commission, Smart 2013/0063–Study on a "European Data Market" and Related Services 10, (IDC) (2016), *https://ec.europa.eu/digital-single-market/en/news/smart-20130063-study-european-data-market-and-related-services*.

[39] Anahiby Becerril & Samuel Ortigoza Limón, *supra* note 26.

[40] PWC, *Sizing the prize. What's the real value of AI for your business and how can you capitalise?*, (PWC) (2017), *https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf*.

[41] In terms of bytes: Gigabyte = 10^9 = 1,000,000,000.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

to its high volume, diversity and complexity.[42] Big Data[43] has become a new frontier for innovation, competitiveness and productivity. However, we must consider that data by itself is not valid if it is not converted into information, translated into knowledge and generated into wisdom.[44] Data should lead to the development of actions, processes or even public policies. Big Data is presented as a challenge, but also it provides new opportunities for companies.

4. *Internet of Things (IoT)*

With a market value estimated to exceed one billion euros by 2020, the European Commission[45] identifies the IoT as the next step in the digitalization of society and economy in which people and objects will be interconnected through communication networks that inform on their status and environment. The IoT is made up of a set of sensors[46] that capture information about what happens in their environment. Due to the ubiquitous nature of the objects connected to IoT, it is estimated that by 2020 about 26 billion devices will connect to the Internet. These devices are a source of data collection that grows exponentially and, consequently, can be processed by Big Data systems.

5. *Cloud Computing*

The "cloud", as it is called, is a model that allows ubiquitous access conveniently and on demand network to a set of configurable computing resources, which can be provided quickly with minimal management or interaction with

[42] Javier Puyol Montero, Aproximación jurídica y económica al Big Data 10 (Valencia, Ed. Tirant lo Blanch) (2015).

[43] Regarding the use of Big Data, it should be noted that the large volume of information does not teach computers or devices to "think" as humans do. What it does is apply specific mathematical algorithms to these huge amounts of data to then infer probabilities.

[44] This follows the DIKW model.

[45] European Commission, Definition of a Research and Innovation Policy Leveraging Cloud Computing and Iot Combination. Final Report 10 (European Union) (2014), *https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination*.

[46] Radio frequency or RFID identification system consists of a tag with a microchip. Each tag has a unique code called an EPC (electronic product code). It also contains a reader (consisting of an antenna and a demodulator), which converts analog information into digital information. The converted information is sent through the network to a data center to be captured and in this way to cross-reference the data in a central computer. The EPC connects to the Internet by means of an IP address and a domain name; *see* Susana Navas Navarro & Sandra Camacho Clavijo, Digital Market. Legal Principles and Rules 33 (Tirant lo Blanch, Valencia) (2016).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

the service provider. This model promotes availability with five essential characteristics, three service models and four implementation models.[47] It is a model of ICT services in an ecosystem of technological resources that offers scalable, shared and on demand services in different modalities to different users through the Internet.

6. *Materials Based on "Bio-" or "Nano-" Technology*

Biotechnology and nanotechnology are both enabling technologies that have led to innovations in many industrial sectors, helping to determine broad ranges of economic and social impact. In accordance with ISO / TS 80004-1: 2015,[48] nanotechnology is the application of scientific knowledge to manipulate and control matter at nanoscale, "as well as to make use of size —and structure— dependent properties and phenomena, as distinct from those associated with an individual atoms or molecules or with bulk materials". Meanwhile, biotechnology constitutes the "manipulation[49] of living organisms or their components to produce useful, usually commercial, products".[50]

All these technologies constitute platforms of innovation that permeate all economic sectors. They are possible since they are cultivated and improved through the digitalization of everything. However, the Internet did not succeed because its infrastructure became more secure, but in spite of its inherent insecurity. For the OECD, the nature of the technical vulnerabilities of the information systems interconnected through the Internet have not fundamentally changed. What has changed is that "society and the economy now depend on this fundamentally insecure environment".[51]

As data driven technologies, the issues surrounding privacy, personal data protection, information availability and the security of all of them are some of the main concerns in their being adopted by organizations and companies. With the digitalization of everything enormous volumes of data are generated to constantly feed Big Data, which is stored in the cloud.[52] Hence, this

[47] National Institute of Standards and Technology (NIST), the Nist Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology 2 (2011), *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf*.

[48] International Organization for Standardization/International Electrotechnical Commission, ISO/TS 80004-1:2015, *https://www.iso.org/obp/ui/#iso:std:iso:ts:80004:-1:ed-2:v1:en*.

[49] This can be done through genetic engineering.

[50] *See* Merriam-Webster Dictionary, *https://www.merriam-webster.com/dictionary/biotechnology*.

[51] OCDE, Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy 28, 29 (OCDE) (2012).

[52] The storage of information in the cloud does not exclude the responsibility of organizations to protect both their regulation and reputation. In general, it is often the responsibility of user organizations in the cloud to ensure that personal data are protected and only used in accordance with the law.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

is a potential gold mine for cyberattacks and cybercriminals. In addition to cybersecurity risks of attacks, companies, governments and institutions must be aware of the vulnerabilities associated with ignorance due to breaches of security policies or lawsuits related to data breaches. If you do not have adequate processes, training and technological innovation in cybersecurity in the company, country or institution, you can be plunged in several problems, in addition to the loss of information, financial losses, damage to the brand and reputation, non-compliance with the law (along with fines), as well as the loss of competitive edge and trust.

III. From Cyberspace to Cybersecurity

1. *Cyberspace*

Cyberspace is a space of flows, a virtual space that grows daily with the interactions that are made through ICT. Called the fifth domain with the earth, sea, air and space, cyberspace is a virtual environment in which we carry out most of our daily activities. But unlike the other four domains, it needs permanent attention and human collaboration for it to operate.

Cyberspace is an electronic world, a global common space where people unite to exchange ideas, services and even friendship.[53] It is a kind of nervous system that controls countries and the critical infrastructure that sustains them. Its proper functioning is essential for the economy and national security.[54] It is a worldwide digital environment consisting of computer networks and telecommunications by which people communicate, interact, and are allowed to exercise their rights and freedoms in the same way they do in the physical world.[55] Technically, ISO points out, cyberspace is "a complex environment resulting from the interaction of people, software and services on the Internet through technological devices and networks connected to it, which does not exist in any physical form". The definition of cyberspace is very important to understand what is to be protected. Therefore, there is still no approved concept for it.

Regardless of its definition, cyberspace is the basis by which e-commerce is carried out, as well as the foundation of the digital economy. Consider the daily increase in the creation of services and products, in addition to the

[53] Government of Canada, *Canada's Cybersecurity Strategy. For a stronger and more prosperous Canada*, (2010), *https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx*.

[54] United States Government, *Cyberspace Policy Review. Assuring a Trusted and Resilient Information and Communications Infrastructure*, (2009), *https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf*.

[55] Gobierno de México, *Estrategia Nacional de Ciberseguridad* (2017), *https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberse guridad.pdf*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

technologies that are developed in this space. Nowadays we add information of all kinds that we manage through this virtual flow and the services already connected to it (including critical infrastructure). This results in an increasing dependence on ICT. And to the extent that our dependence on new technologies increases, we become more vulnerable to them,[56] for example we have smart devices, even clothes, and maybe we are not so much.

2. *Cybersecurity*

In May 2017, the WannaCry ransomware hit 150 countries and hundreds of thousands of systems, paralyzing healthcare, production facilities and telecommunications. In 2018, new hardware weaknesses were exposed, and massive data breaches were found: in India's Aadhaar.[57] Considered the world's largest biometric identification system, it suffered breaches that compromised the data of 1,100 million registered citizens. Later that same year, in September, Facebook[58] notified its users of the largest massive data breach it had ever suffered, which came to affect more than 50 million people. And we began 2019 with the "worst attack of computer hacking" Germany has experienced of documents, personal messages, mobile phone numbers, credit card information, addresses, and emails (among others), in this *große Datenleck*. Some of the victims are the German Chancellor and German President Frank-Walter Steinmeier, as well as political parties, journalists and celebrities, among others. Putting this into perspective, one might ask, why worry about the security of cyberspace? Why is it necessary to incorporate it into free trade agreements? In relation to the first question, if the digital economy, like electronic commerce and multiple activities of our daily lives, are currently based on the flow of data and information, we must consider the security of all the infrastructure that contains it. Our critical infrastructure is increasingly connected to the networks that make up said cyberspace. Our daily activities, from com-

[56] Víctor Manuel Castrillón y Luna, & Anahiby Becerril, *infra* 98.

[57] Aadhaar is the database managed by the Unique Identification Authority of India (UIDAI). It provides the UIDAI with a random 12-digit number issued to the residents of India after their complying with the established verification process. In addition to personal and demographic data, it also contains biometric information (ten fingerprints, iris scan of both eyes and a facial photograph). According to the Government: "The Aadhaar identity platform is one of the key pillars of" digital India, "where every resident of the country has a unique identity. The Aadhaar program has already reached several milestones and is, by far, the largest biometric identification system in the world"; *see* Unique Identification Authority of India, "What is Aadhaar?", Government of India, *https://uidai.gov.in/what-is-aadhaar.html*.

[58] According to Facebook, the breach would have happened on the afternoon of September 25. The attackers exploited a feature in the Facebook code to gain access to user accounts and possibly take control of them; *see* Isaac Mike & Frenkel, Sheera, "Facebook Security Breach Exposes accounts of 50 Million Users", The New York Times, September 28, 2018, *https://www.nytimes.com/2018/09/28/technology/facebook-hack-data-breach.html*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

munication to accessing information, work, health and education, are carried out at every moment in that cyberspace. In this way, the Internet and ICTs have become a critical resource in the development of electronic commerce and the digital economy, which has consequences for cybersecurity policies, one of the main ones of which is the adoption of strategies that address the issue of cybersecurity.

And what is cybersecurity? Cybersecurity will strive to deal with the security of this cyberspace. We can interpret the term according to the concepts given by the technical community and those established in national cybersecurity documents. However, we believe that the ITU's definition[59] issued in Recommendation ITU-T X.1209 (12/2019) adequately explains the concept: "3.1.1 Cybersecurity [b-ITU-T X.1205]: 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[60] and organization and user's assets".

Identifying as "assets" the "connected computing devices, the users, the services/applications, the communication systems, the multimedia communications, as well as all the information transmitted and/or stored in the cyber-environment". ITU recognizes that cybersecurity ensures that the security properties of the organization's assets and users are achieved and maintained against the corresponding security risks in the cyber-environment. And refers to the following information properties: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.

Due to its rapid growth in number and sophistication, cyber-attacks[61] are positioned as a critical threat to national security and one of the greatest risk's nations face today. In its "Global Risks Report 2019", the WEF has recognized fraud or massive theft of data and cyber-attacks as two of the five main global risks that countries perceive.[62] While in North America, the risk of

[59] International Telecommunication Union (ITU), Rec. ITU-T X.1209 (12/2019), Capabilities and their context scenarios for cybersecurity information sharing and exchange, ITU-T X-Series Recommendations 1, (ITU) (2010).

[60] ITU does not use the term cyberspace, but refers to the cyber environment to refer to "users, networks, devices, all software, processes, stored information circulating, applications, services and systems that are directly or indirectly connected to networks"; *see* International Telecommunication Union, ITU-T X.1205 *https://www.itu.int/rec/T-REC-X.1205-200804-I/en*.

[61] Although there is no uniform term, we can understand cyber-attacks as: an attack that is perpetrated through cyberspace, aimed at the "use of a company, cyberspace, in order to interrupt, disable, destroy or control maliciously an information infrastructure or destroy the integrity of the data or steal controlled information"; *see* National Institute of Standards and Technology (NIST), *Glossary of Key Information Security Terms* (2013), *https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf*.

[62] In 4th and 5th place respectively, only preceded by 3 climate-related risks; *see* World Economic Forum, *Global Risks Report 2019, http://www3.weforum.org/docs/WEF_GRR18_Report.pdf*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

cyber-attacks has surpassed terrorist attacks as the number one risk of greatest concern in doing business.[63]

As a consequence, governments in many countries have begun to develop strategies or laws and national cybersecurity policies to protect themselves against cyber threats, with a risk management vision that allows them to identify their vulnerabilities while trying to promote the benefits of a hyperconnected and cyber-enabled world. The development of national cybersecurity strategies has become a national policy priority in several countries.[64] The NATO Cooperative Cyber Defense Center of Excellence has identified more than 50 countries that have published a cybersecurity strategy or national cybersecurity strategy where they define “what security means for their future national and economic security initiatives”.[65]

Cybersecurity strategies or national cybersecurity strategies (NCSS) involve action plans to facilitate the attainment of a national competitive advantage regarding cybersecurity. They constitute action plans designed to improve the security and resilience of national infrastructures and services. These documents articulate an approach to cybersecurity adapted to a specific national or legal context. In this sense, the implementation of the strategies must be accompanied by planning technological development, as well as generating skills and human capital to work for it.

Just as there is no single definition for cyberspace and cybersecurity, there is no single strategy that can be followed given the characteristics of each country. However, we can identify common themes, which in the end does not make us so different. These include cooperation (international and national), the protection of users’ human rights and risk management.

IV. Cybersecurity in Free Trade Agreements

Concerns about national security and trade policies are not new. However, given the electronic nature of international and national commercial transactions, the theme has acquired a new and urgent prominence, especially in more developed countries due to an increasingly growing link and dependence on ICT, its services and its infrastructure. Turning now to the specific context and considering the fact that most developed and developing economies have laws and regulations that restrict foreign direct investment (FDI) based on concerns related to national security or the loss of countries’

[63] World Economic Forum, *Global Risks Report 2018*, *http://www3.weforum.org/docs/WEF_GRR18_Report.pdf*.

[64] Organización para la Cooperación y Desarrollo Económicos (OCDE), Cybersecurity Policy Making at a Turning Point. Analyzing a New Generation of National Cybersecurity Strategies for the Internet Economy 9 (OCDE) (2012).

[65] *See* NATO Cooperative Cyber Defense Centre of Excellence, *https://www.ccdcoe.org/cyber-security-strategy-documents.html*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

natural resources, what would be the equivalent for protection in cyberspace? Economic security deals with trade, production and finance.[66] Although developed and developing countries[67] have different points of view regarding economic security threats associated with cybersecurity, as mentioned above, there are common and global problems.

As technologies are being rapidly adopted by governments, individuals and organizations, ICTs are gaining importance in the national security equation. Allegations related to cybersecurity have given rise to various barriers to international trade and investment. Obstacles related to cybersecurity cover at least the following categories of concerns: political[68] and economic[69] espionage and information security of countries[70] and citizens.[71]

In relation to e-commerce, a cybersecurity strategy should ensure that it does not become an obstacle or barrier to these electronic transactions. That is, just as there are trade barriers, which constitute restrictions imposed on the free flow of trade and investment, a cybersecurity-related barrier for international trade and investment is defined as "any problem related to real and perceived security risks in the cybernetic environment that directly or indirectly hinders the growth of international trade and investment".[72]

1. *Association of Southeast Asian Nations (ASEAN)*

In the case of the Association of Southeast Asian Nations,[73] Chapter 1 of its Charter[74] establishes that one of its purposes is to "enhance peace, secu-

[66] Mathias Albert, & Barry Buzan, *Securitization, sectors and functional differentiation.* 42 SECURITY DIALOGUE 413, 425 (2011), *http://journals.sagepub.com/doi/abs/10.1177/0967010611418710*.

[67] For Kshetri, the United States is concerned about the theft of IP and other problems associated with economic espionage. The BRICS states (Brazil, Russia, India, China and South Africa), on the other hand, have argued that developing countries' dependence on Western technologies is a threat to economic security; *see* NIR KSHETRI, THE QUEST TO CYBER SUPERIORITY. CYBERSECURITY REGULATIONS, FRAMEWORKS AND STRATEGIES OF MAJOR ECONOMIES 13 (Springer) (2016).

[68] While espionage practices between states are not new, ICT has made it easier, mass surveillance, between states, as well as between states and non-state actors towards citizens. Recall Edward Snowden's declarations on the practices of massive, illegal surveillance carried out by the U.S. government, a situation that even led to the UN Recommendation on "Privacy in the Digital Age".

[69] One example is the theft of industrial secrets.

[70] This focuses more on critical infrastructure and strategic information, national or public security, among others.

[71] These include freedom of expression, access to information, privacy and protection of personal data, in addition to the exercise of other human rights on the Internet.

[72] NIR KSHERI, *supra* note 5.

[73] The ASEAN nations are Indonesia, Philippines, Malaysia, Singapore, Thailand, Vietnam, Brunei Darussalam, Cambodia, Laos and Myanmar. Papua New Guinea is an observer.

[74] The Charter entered into force on December 15, 2008. The document codifies ASEAN

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

rity and stability and further strengthen peace-oriented values of the region", through mutual cooperation. In 2013, ASEAN and Japan signed the "Joint Ministerial Declaration of the ASEAN and Japan Ministerial Policy Meeting on cooperation in cybersecurity",[75] where in addition to recognizing the importance of a secure cyberspace as one of the "major drivers" of innovation, it is also essential in "promoting social and economic activities and strengthening ASEAN connectivity".[76]

2. *From TPP to CPTPP*

The *Trans-Pacific Economic Cooperation Agreement*, better known by its acronym TPP (Trans-Pacific Partnership),[77] covered different aspects aimed at making trade more agile and simple, reducing costs and times for doing business, always under the protection of clear and precise rules for everyone. For Sigmond, the TPP incorporated commitments that did not exist in the previous Free Trade Agreements. For example, the author says, "the parties committed to have protection for consumers and stop unsolicited commercial messages. They also promoted the commitment to help small and medium-sized businesses".[78]

In January 2017, the U.S. Government decided to withdraw permanently as a signatory from the TPP negotiations in search of better conditions for its country. In response to this and in an effort to give effect to the treaty, on November 11, 2017, the trade representatives of the 11 remaining countries[79] agreed on the *Comprehensive and Progressive Agreement for Trans-Pacific Partnership* (CPTPP). On January 23, 2018, the 11 countries participating in the CPTPP reached an agreement in Tokyo, Japan. This agreement incorporates some provisions contained in the TPP, while others were suspended.[80]

standards, laws and values, as well as creates a legal framework for the organization's institutions.

[75] On that occasion, reference was made to the fact that the concept of "cybersecurity" would be understood according to the provisions of Recommendation ITU-T X.1205, which has been cited in this paper.

[76] ASEAN-Japan, *Joint Ministerial Statement of the Asean-Japan Ministerial Policy Meeting on Cybersecurity Cooperation* (2013), *http://www.asean.org/storage/images/Statement/final_joint_statement%20asean-japan%20ministerial%20policy%20meeting.pdf*.

[77] The TPP was signed by 12 countries on February 4, 2016.

[78] Karen Sigmond, *El comercio electrónico en los tratados de libre comercio de México*, IUS REVISTA DEL INSTITUTO DE CIENCIAS JURÍDICAS DE PUEBLA, Jan-June 2018, 372.

[79] These countries are Australia, Brunei Darussalam, Canada, Chile, Japan, Mexico, New Zealand, Malaysia, Peru, Singapore and Vietnam.

[80] Gobierno de México, *Tratado Integral y Progresista de Asociación Transpacífico*, (2018), *https://www.gob.mx/tratado-de-asociacion-transpacifico#que_es*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

The TPP contains a section on electronic commerce (Chapter 14), where, in addition to recognizing it as a driver for economic growth and opportunities, it recognizes the importance of frameworks that promote consumer confidence, as well as the need to avoid obstacles for its use and development (Article 14.2.1).[81] This section was incorporated into the CPTPP.

Within its definitions, the Agreement identifies computer programs, texts, "image, sound recording or other product that is digitally encoded, produced for commercial sale or distribution and that can be transmitted electronically" as digital products.[82] This definition, in accordance with the text of the Agreement, should not be understood to "reflect a Party's view on whether trade in digital products through electronic transmission should be categorized as trade in services or trade in goods".[83]

The Parties to the Agreement recognize the economic and social benefits derived from the protection of personal information[84] of e-commerce users, which also improves consumer confidence (Article 14.8.1). To guarantee this protection, each Party undertakes to adopt or maintain a legal framework that encourages the protection of users' personal information, based on the principles and guidelines of the relevant organizations (Article 14.8.2). The purpose is to promote a secure framework that allows the cross-border transfer of information (including personal information) by electronic means when the business is carried out by a "covered person" (Article 14.11.2). It also refers to protection against unsolicited commercial electronic messages.

In addition the treaty establishes the duty of the Parties to maintain a legal framework that governs electronic transactions consistent with the principles of the Model Law of Electronic Commerce of UNCITRAL or with the *United Nations Convention for the use of Electronic Communications in International Contracts* (Article 14.5.1.).

Regarding the barriers to electronic commerce, the parties agreed to strive to: "a) avoid any unnecessary regulatory burden on electronic transactions; b) facilitate input by interested persons in the development of its legal framework for electronic transactions" (Article 14.5.2). The foregoing implies, on the one hand, not applying unnecessary barriers, and on the other, coopera-

[81] The treaty refers to consumer safety and establishes the parties' obligation to adopt or, where appropriate, maintain laws that prohibit fraudulent and deceptive commercial practices that cause harm or potential harm to consumers who participate in the activities carried out online (Article 14.7.2).

[82] Government of New Zealand, *Comprehensive and Progressive Agreement for Trans-Pacific Partnership. Chapter 14* (2018), *https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf*.

[83] *Id.*

[84] For purposes of the CPTPP, personal information constitutes "any information, including, about an identified or identifiable natural person" (Article 14.1).

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

tion among the multiple stakeholders in shaping the legal framework, which is in line with the multistakeholder model of Internet Governance.

Chapter 14 of the aforementioned CPTPP highlights a section on Cybersecurity, which is aimed at promoting cooperation between the contracting parties. In addition, the instrument refers to committing to the development of capacities of the national entities responsible for responding to computer security incidents, as well as to employ collaborative mechanisms for the identification and mitigation of malicious intrusions or the dissemination of malicious codes that affect the electronic networks of the Parties (Article 14.16).

Although it does not make a single reference to the concept of cybersecurity, the framework around the countries that make up this treaty is as follows.

Table 1. Applicable Legislation on Cybersecurity by CPTPP Member Countries

	CPTPP countries with strategies or cybersecurity documents		*GCI Ranking*[85] *(global ranking/ score)*
Country	*Instruments*	*Cybersecurity Concept*	
Australia	- National security and defense strategy. *Strong and Secure: A Strategy for Australia's National Security* (2013)[86] - 2016 *Defense White Paper.*	Measures relating to the confidentiality, availability and integrity of information that is processed stored and communicated by electronic or similar means.[87]	10/0.890
Brunei Darussalam	Computer Misuse Act (2007)[88]	**89	64/0.624

[85] The Global Cybersecurity Index (GCI) prepared by the International Telecommunication Union (ITU) within the framework of the Global Cybersecurity Agenda (GCA) measures the degree of each country's commitment to cybersecurity by using a series of individual indicators on legal, technical and organizational aspects, measures, capacity building and international cooperation efforts. The indicators are prepared on the basis of a survey that reviews laws, regulations, computer security incident response teams (CSIRT), national policies and strategies, standards, certifications, vocational training, awareness and alliances; *see* International Telecommunication Union (UIT), *Global Cybersecurity Index 2018*, *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf.*

[86] Government of Australia, *Strong and Secure: A Strategy for Australia's National Security*, 2013, *https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf.*

[87] *See* Government of Australia, *Cyber Security, https://www.staysmartonline.gov.au/glossary*.

[88] *Computer Misuse Act, 2007*, *http://www.agc.gov.bn/AGC%20Images/LOB/PDF/Computer%20Misuse.pdf.*

[89] It is still developing a framework for cybersecurity.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

Canada	- Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada (2010)[90] - Action Plan 2010-2015 for Canada's Cyber Security Strategy (2013) - Action Plan for Critical Infrastructure 2014-2017 (2014)	Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global common where more than 1.7 billion people are linked together to exchange ideas, services and friendship[91]	9/0.892
Chile	Política Nacional de Ciberseguridad (2017)[92]	Cybersecurity is a condition characterized by a minimum amount of risks to cyberspace, understood as the set of physical, logical infrastructures and human interactions that occur there.[93]	88/0.438
Japan	National security and defense strategies: - Defense White Paper Japan (2015) - Cybersecurity Strategy-Towards a World-Leading, Resilient and Vigorous Cyberspace (2013) - International Strategy on Cybersecurity-j-Initiative for Cybersecurity (2013) - Cyber Security Strategy (2015)[94]	Japan aims to construct a "world-leading", "resilient" and "vigorous" cyberspace, and incorporate this cyberspace as a social system to realize a "cybersecurity nation" as a society that is strong against cyber-attacks, full of innovations and of which its people will be proud.[95]	14/0.880

[90] Government of Canada, *Canada's Cyber Security Strategy. For a Stronger and More Prosperous Canada*, *2010, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf*.

[91] In its strategy, reference is made to cyberspace.

[92] *See* Government of Chile, *Política Nacional de Ciberseguridad* (2017), *http://ciberseguridad.interior.gob.cl/media/2017/05/PNCS-CHILE-FEA.pdf.*

[93] "La ciberseguridad es una condición caracterizada por un mínimo de riesgos para el ciberespacio, entendido como el conjunto de infraestructuras físicas, lógicas y las interacciones humanas que allí ocurren". The concept states that, in accordance with international standards, the key attributes to be protected are "the confidentiality, integrity and availability of information", which in our opinion coincides with the definition of ITU on cybersecurity, *Id*.

[94] Government of Japan, *Cyber Security Strategy 2015, http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku.pdf.*

[95] *See Compilation of Existing Cybersecurity and Information Security Related Definitions*, Open Technology Institute New America–2013, *https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

Malaysia	The National Cyber-Security Policy (NCSP, 2006)[96]	Vision: Malaysia's Critical National Information Infrastructures will be secure, resilient and self-reliant. Infused with a culture of security, it will promote stability, social wellbeing and wealth creation.	8/0.893
Mexico	Estrategia Nacional de Ciberseguridad (2017)	Set of policies, controls, procedures, risk management methods and standards associated with the protection of society, government, economy and national security in cyberspace and public telecommunication networks.[97]	63/0.629[98]
New Zealand	National security and defense strategies: - NewZealand's National Security System (2011) - Defense White Paper (2010) - New Zealand's Cyber Security Strategy[99] (2015) - New Zealands Cyber Security Strategy Action Plan (2015) - National Plan to Address Cybercrime (2015)	The practice of making the networks that constitute cyber space as secure as possible against intrusions, maintaining confidentiality, availability and integrity of information, detecting intrusions and incidents that do occur, and responding to and recovering from them.[100]	36/0.789[101]

[96] The National Cyber-Security Policy (NCSP), Malaysia, (2006), *http://cnii.cybersecurity.my/main/ncsp/NCSP-Policy2.pdf*.

[97] "Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicación"; *see* Government of Mexico, *Estrategia Nacional de Ciberseguridad* 2017, *https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguri dad.pdf*.

[98] In 2017, it ranked 38th (0.660).

[99] *New Zealand's Cyber Security Strategy 2015*, *https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy- december-2015.pdf*.

[100] *See* New Zealand's Cyber Security Strategy, 2011, *https://www.dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2011*.

[101] In 2018, New Zealand did not respond the Index questionnaire. However, in 2017 it was ranked 19th with a score of 0.718.

Peru	-Política de Seguridad y Defensa Nacional (2017)[102] -Decreto Supremo N° 066-2011-PCM. -Agenda Digital Peruana 2.0 -Decreto Legislativo 1141, Decreto de Fortalecimiento y modernización del Sistema-de Inteligencia Nacional –SINA y de la Dirección Nacional de Inteligencia –DINI	Digital Security at the national sphere is the level of confidence in the digital environment resulting from managing and implementing a set of proactive and reactive measures against risks that affect the security of individuals, economic and social prosperity, national security and national objectives in that environment. It is based on collaboration with actors from the public sector, the private sector and others who support the implementation of controls, actions and measures.[103]	95/0.401
Singapore	- National Cyber Security Masterplan 2018 (2013) - Factsheet on National Cyber Security Masterplan 2018 • Cyber security strategy (2016)[104] • Cybersecurity Act (2017)	…the security of a computer or computer system against unauthorized access or attack, to preserve the availability and integrity of the computer or computer system, or the confidentiality of information stored or processed therein.[105]	6/0.898[106]

[102] This document has a section called 4.2.14 Infrastructure to face attacks on information systems: Cybersecurity, where the commitment to the development of military and police skills stands out, with the purpose of "guaranteeing international peace and internal order"; through the integration of security-related systems to dissuade, confront, effectively combat and eliminate terrorist and drug trafficking organizations; *see* Presidencia de Perú, *Decreto Supremo Nº 012-2017-DE. Decreto Supremo que aprueba la Política de Seguridad y Defensa Nacional*, 2017, *https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-aprueba-la-politica-de-seguridad-y-defen-decreto-supremo-n-012-2017-de-1600032-1/*.

[103] "La Seguridad Digital en el ámbito nacional es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas"; *see* Presidencia de Perú, *Decreto Supremo Nº 050-2018-PCM por que se Aprueba la definición de Seguridad Digital en el Ámbito Nacional* (2018), *https://busquedas.elperuano.pe/download/url/aprueban-la-definicion-de-seguridad-digital-en-el-ambito-nac-decreto-supremo-n-050-2018-pcm-1647865-1*.

[104] *Cyber security strategy*, Singapore, (2016), *https://www.ccdcoe.org/sites/default/files/documents/SingaporeCybersecurityStrategy.pdf*.

[105] *See* Cybersecurity Bill 2017, Singapore, *https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx? la=en*.

[106] In 2017, the IGC placed Singapore at number 1 with 0.925.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

Socialist Republic of Vietnam	Law on Network Information Security (2016)[107]	Network information security means the protection of network information and information systems against any illegal access, use, disclosure, interruption, amendment or sabotage in order to ensure the integrity, confidentiality and availability of information.[108]	50/0.693

Source: Developed by the author.

3. *The North American Free Trade Agreement (NAFTA)*

For the purpose of establishing the basis for strong economic growth and greater prosperity for the countries that integrate it, in 1994 the North American Free Trade Agreement (NAFTA) entered into force between Canada, the United States[109] and Mexico. In this way, one of the largest free trade zones in the world was created. On August 13, 2017, the rounds of NAFTA renegotiations began. Beyond the statements of the U.S. Government regarding the treaty, the 3 countries agreed that the treaty needed to be modernized.

The original NAFTA did not contain provisions on electronic commerce or cybersecurity. So, we are witnessing a new chapter in the commercial flow among the three nations, as well as new agreements about security, but this time, to safeguard cyberspace, which is common as well as global.

The USMCA has incorporated (among other provisions) Chapter 19 on Digital Trade, where several issues are addressed, including the principles on access and use of the Internet for digital commerce (Article 19.10), as well as the protection of personal data and the cross-border flow of information by electronic means (Article 19.11).

Regarding cybersecurity, which is addressed in the same chapter, the agreement focuses on international cooperation and capacity development among the 3 countries.

[107] National Assembly of the Socialist Republic of Vietnam, *Law on Network Information Security* (2016), *http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf*.

[108] *Id.*

[109] In 2018, the CGI placed the United States (0.926) in 2nd place, below the United Kingdom (0.931). At the regional level, the index positions the United States as the 1st with Canada in 2nd place, followed by Uruguay (0.681) and Mexico in 4th; *see* International Telecommunication Union (UIT), *Global Cybersecurity Index 2018*, *https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf*.

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

Table 2. Comparison on Cybersecurity:
CPTPP vs. NAFTA

Cybersecurity in Free Trade Agreements	
CPTPP	*US-Mexico-Canada Agreement*
• It highlights a section on Cybersecurity aimed at promoting cooperation between the contracting parties. • In addition to committing to the development of capacities of the national entities responsible for responding to computer security incidents, as well as to employ collaborative mechanisms for the Identification and mitigation of malicious intrusions or the dissemination of malicious code that affect the electronic networks of the Parties (Article 14.16).	• Cybersecurity (Article 19.15). The Parties shall endeavor to: a) build the capacities of their 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.

Source: Developed by the author

V. Final Considerations

Although some countries, like Mexico, have not adhered to or ratified international conventions on specific cybersecurity or cybercrime issues, like the Budapest Convention, it is through free trade agreements that cooperation, collaboration and international protection for the flow of information, products and services that circulate daily in cyberspace is being generated.

The threats and risks in cyberspace arise in a global common space. Networks are so interconnected[110] that it can be difficult to limit the effects of an attack on a single part of the system without damaging others or interrupting it altogether. Our information assets flow together in cyberspace. Nowadays, sharing and safeguarding are critical to protecting public and private interests in the area of security, growth, human rights protection and economy.

In the physical world, there is no system that is 100% secure, and this also applies in cyberspace. We must consider that individuals, organizations, companies, governments and societies depend more on ICT every day. And although creating and implementing strategies or policies regarding cyberse-

[110] This situation that has been a matter of concern in the UN General Assembly, which has recognized "that this growing technological interdependence is based on a complete network of essential information infrastructure components"; *see* Preamble Resolution A/RES/58/199 dated January 30, 2004, *https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.*

DOI: http://dx.doi.org/10.22201/iij.24485306e.2020.1.14808

curity has an economic cost, the cost of inaction may be higher. In this sense, it pays to be prepared and resilient.

Regardless of its definition, cybersecurity must be implemented holistically, covering economic, social, educational, legal, police, technical, diplomatic, military and intelligence aspects. It must be based on risk management that respects human rights and is managed through a *multistakeholder* approach.

Concerns related to cybersecurity should strive not to give rise to barriers to electronic commerce and foreign investment. Although e-commerce requires a regulatory framework that guarantees legal certainty while protecting security of people who choose to use electronic means instead of conventional ones. These frameworks cannot impose barriers that prevent the development and economic growth that this kind of trade brings. For the OECD, national cybersecurity strategies must have two objectives: to promote economic and social prosperity, and to protect societies that depend on cyberspace against cyber threats. This must be done while preserving the openness of the Internet as a platform for innovation and new sources of growth.

The way in which cybersecurity is linked to national economic security has new forms and contexts. With the development of technologies that enable digital economy and encourage electronic commerce, the economic security associated with high technology is being recognized as a substantial source of national security.

Countries are increasingly dependent on the Internet to maintain their services, infrastructure and economies in cyberspace. Therefore, they should be the most concerned in keeping it safe. Thus, those responsible for drafting public policies face an immense task to follow the rapid pace of technological change in the midst of great uncertainty about what the future holes.[111] In addition to considering issues like education and building digital skills, the labor market, science and innovation, competition, the development of technology, and commercial and industrial policy systems, countries should be responsible for the protection of their infrastructure (critic and strategic), which largely depends on national policies and priorities. But it must also be carried out with the cooperation of the various stakeholders, considering that most of the service providers are private companies. These issues are also of public interest since threats to cyberspace can affect countries and entire societies.

[111] United Nations Conference on Trade and Development (UNCTAD), *Informe sobre la economía de la información, 2017. Digitalización, comercio y desarrollo. Panorama general* 6 (United Nations, New York/) (2017).

Received: May 19th, 2019
Accepted: August 7th, 2019