SocioEconomic Challenges, Volume 5, Issue 4, 2021
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

Cybersecurity, An Axis On Which Management Innovation Must Turn In The 21st Century

https://doi.org/10.21272/sec.5(4).98-113.2021.

Ed. Fernando Alonso Ojeda Castro, ORCID ID: https://orcid.org/0000-0002-3271-0707

Pilot University of Colombia, Faculty of Economic and Administrative Sciences, Business Administration Program, Professor and Researcher. Economist and Specialist in Economics Internacional of Southeast and Central Asia

Abstract

The main objective of this article is to highlight Cybersecurity, as a support for innovation in the 21st century company. It analyzes the two dominant structures under company cases, both from the United States and from PR China.

The work is part of the research project developed by the researcher from the Pilot University of Colombia, called “The sustainable reference of the company in Colombia: support of the innovation of the XXI Century.”

With this, “The Diamond of Innovation” is used, a product of the studies that the author of this document has carried out in the last decade on business models, public policy, culture and education, from Southeast Asia, the RP China and India.

Thanks to this work, nine books have been made from the collection of the "Asian Firms" and about thirty related articles. In the last two years, this study made it possible to create a tool that assesses the situation in which a country, city, or particular company finds itself, in terms of innovation, the "Innovation Diamond", uses eight indicators, which allows ranking and propose immediate, short, medium and long term strategies, one of these eight points is: Cybersecurity.

To achieve the proper context of the subject, initially the historical subject is addressed, of the evolution of the modalities, object and digital expressions of cybercrime, throughout history, based on the Project “Colossus” by John Mauchly and John Eckert in 1943, which takes up the episodes described in Table 1. On the other hand, it offers the possibility of knowing the indicators that, in terms of cybersecurity, have greater credibility and coverage in the world today, and that allow us to know the advances-setbacks in matter, across the five continents.

The document continues, after this context, seeking to explain: What relationship is there between innovation and cybersecurity in the 21st century company? With this purpose, it delves into the subject of Cybersecurity, its continuous relationship with innovation, under its own expression from companies such as Facebook, Netflix, Apple, Samsung, Amazon, etc. The complement is to analyze in this scheme, what is happening in PR China, as the maximum expression of this relationship and a center of criticism and recognition, for its continuous disruption under the slogan "made first in China".

Finally, the conclusions take up what has been achieved in its entirety, to propose scenarios and spaces for action that are present, left as legacies of COVID and in the future, where this key cybersecurity-innovation is indivisible as a determining factor not only in economic-social life, but also in relationships. international, West-East, of the next decades.

Keywords: cybersecurity, innovation diamond, business management, innovation.

JEL Classification: O3.

Cite as: Ed. Fernando Alonso Ojeda Castro (2021). Cybersecurity, An Axis On Which Management Innovation Must Turn In The 21st Century. *SocioEconomic Challenges*, *5*(4), 98-113. https://doi.org/10.21272/sec.5(4).98-113.2021.

ARMG Publishing "Thinking ahead"

SocioEconomic Challenges, Volume 5, Issue 4, 2021
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

Received: 21.06.2021 **Accepted:** 25.10.2021 **Published:** 30.12.2021

Introduction

We are in what is known as the "third wave of Cybersecurity", where the arrival of a virus in any form implies using your cell phone, seizing your USB, reaching the Cloud, getting into your IoT communications, which It implies working in a coordinated way between private and public actors, making use of the information and classification, thrown by a database that is analyzed from an Artificial Intelligence (AI) instrument. The challenge for Entrepreneurs and State actors is to show that the resulting public policy is efficient in light of the results, the associated innovation and the strategic insertion of financial and human resources that guarantee success in this regard. (Banga, 2018).

NATO received its first attacks during the Kosovo conflict, at the end of the nineties of the last century, which caused the fall of its main page on several occasions, as well as its e-mail being closed from the outside, from its headquarters in Brussels (Belgium). One of its 29 member countries, Estonia, in mid-2007 and for three continuous weeks, received massive cyber attacks mainly against institutions that put its national security at risk.

It has gone from the Cold War and the subsequent fall of the Berlin Wall, to the era of "digital espionage", which affects States, their allies, their companies and current world stability. NATO has a "Strategic Concept of the Alliance", and its own "Cyber defense" policy, to such an extent that today it is considered "a possible cause of collective defense" of its members. (REVISTA DE LA OTAN edición digital).

Therefore, we must ask ourselves: Does competitiveness in today's company, have as one of its necessary sources, the relationship between innovation and cybersecurity?

To answer this question, the work addresses several fronts that seek to understand not only this new scenario that the State and the Company must and must face together, but the role of businessmen and politicians in one of the greatest challenges that the world now faces, during the fourth industrial revolution.

Since the eighties, these viruses have been known by their authors, who "signed their digital work", to generate partial damage or publicize their companies, making the leap to specialized malware, with the clear objective focused on damage based on Data from companies, both small and large, from medium impact to large impact, with unknown authors, under the clear scenario of the theft of information, money, and databases, this is how the 21st century begins.

The turning point, compared to what is happening today, is given by the entry of the WannaCry Ransomware virus, showing from 2017 that the cybercriminal is not only a tool to steal industrial information, they are a weapon between States, since their origin was North Korea.

On the other hand, it is important to know references and indicators that must be consulted regarding Cybersecurity. Therefore, in the second part of the document, the different indicators and their sub-indicators are disclosed, which allows an entrepreneur, investors, States, to know, have objective, scientific data, about the structures, laws, logistics, human resources, international cooperation, cases of companies and States, which are examples in this matter, as well as those cases of partial or total failure. In the foreground is "The Global Cibersecuruty Index" by ITU, which shows how the different continents are on this topic associated with innovation, manifesting the clear advantage of Europe, followed by Asia, with special cases from the United States, leaving the vast majority of Central and South American countries at a low and worrying level, in some cases at or below the level of some African countries.

It is followed by “The United Nations –eGovenment Index”, which expressly focuses on observing public policy and Digital Government, its origin, from the United Nations, the Department of Economic and Social

Affairs (DESA) and the Division of Public Institutions and Digital Government. There is also the "National Cyber Security Index", reviewing the treatment against cybercrimes, created by the e-Governance Academy. Finally, “The ICT Development Index” is presented, which observes the management between countries in education, infrastructure and innovation related to logistics, obtained by the United Nations Committee on World Connectivity (ITU).

Having this historical scheme and the indicators, the document seeks to precisely address the cases of companies and their different strategies that are being developed in this regard, emphasizing the precise management that they have been applying in the midst of a context marked by the use of mobile technologies and the defining role of States, as guarantors of operations and providers of logistics conducive to the needs of Industry 4.0 and the cyber-consumer. It is led by the globe-firms such as Facebook, Yahoo, Netflix, Amazon, Spotify, which shine for their Western-style alliances.

This document offers a light, showing that in this field there is much to work on, that the company must understand in its strategic and tactical projections, introduce financial and human resources, as an indivisible management to the company that wishes to create paradigms, typical of this century.

The computer threats, from the university to the company

With this aside, a tour will be made of the emergence of the first computer viruses, which went from simple personal or academic "experiments" to sophisticated software systems, created with the clear intention of stealing, ending, terrorizing users, of Computers, in Companies and States, at a global level, see Table 1. “Evolution of Computer Threats: history and origins”.

Just the first contributions from the ENIAC (Electronic Numerical Integrator And Computer) Project of John Mauchly and John Eckert in 1943 and the Colossus project, which helped solve problems of the US Army, in the middle of World War II, associated with calculation cases Ballistics first and cracking the Nazi code (INFORMÁTICA, 2011), From the mind of a well-known polymath-mathematician, of Hungarian-American origin, who participated in the Manhattan project, what he called "The Viral Computing Theory" emerged in 1949 (McMullin, 2000). It was seen this by John von Neumann its author, as creations "automatons" that could be reproduced in a computer system (Ferreras, 2014).

After the Korean War (1950-1953), the US Army, looking for a means of communication that minimized the interception of electrical signals that gave rise to the use of the Telegraph and the Morse code (Samuel Morse) since 1844, was born almost a century later in 1958, under the auspices of the Ministry of Defense, the Advanced Research Projects Agency or known until today, the ARPANET. This system was made between computers in a direct way, almost a decade and a half later in 1971, there was a whole network of 23 points directly connected, of computers that was also called ARPANET, by then it was working hand in hand with the Academy with MIT, the National Physics Laboratory of the United Kingdom and the famous Rand Corporation (Research and Development), a training center of the United States Armed Forces until today (UPC, s.f.).

This space gives rise to “Creeper”, October 1971, affecting computers that were interconnected by this State-Academy knowledge network, had as its source the then-well-known Firm BBN Technologies (Mayya) The idea, to follow the propagation of a program between directly connected computers, its creator Bob Thomas, in the printed results or on the screen appeared the phrase “I'm creeper: cath me if you can!”. Two years later, "Reaper" is born, which seeks to stop "Creeper", that is, the ant-virus. (INSTITUTO DE ESTRATEGIA, 2017).

The term as we know it "Computer Virus" has two antecedents. First, in a novel "When HARLIE Was One", in 1972, the existence of a program that would be the equivalent of a computer virus is recognized today. Ten years later in the famous comic "X-men" this term is spoken of in the same context as it is used today (Cerra, 2010).

In that same year of 1982, a teenager Richard Skrenta, from Pittsburgh-Pennsylvania, created a program that seeks to "infect the boot floppy" using the Apple II operating system, as a joke towards his friends, sent in January of that year (Silverman, 2017), after booting a floppy that contained it fifty times, it triggered the following message:

SocioEconomic Challenges, Volume 5, Issue 4, 2021
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

“The Cloner: The show with personality. It will get all your discs, it will get into your chips! Yes, it is Cloner! It will stick to you like glue, it will change your RAM too! Pass it on, The Cloner!” (López, 2017).

A year later, this time seeking to demonstrate the existence of a "malware", created with the intention of replicating it on other computers, November 3, 1983. Much more elaborate and knowing a "path" of the malware, from a floppy disk, its creator Fred Cohen, an engineering student at the University of Southern California, inserts a hidden code into a program, which manages to control a computer with a Unix operating system. In 1983 he wrote a "paper" called: "Computer Viruses. Theory and Experiments ", with this he defines what is understood as a virus:" a program that can infect other programs by modifying them to include a possibly evolved copy of itself " (MacNeil, 2019).

A company of Slovak origin called ESET in 2017, declares November 3, as the world day of “malware”, in honor of the work of the then student Cohen (Foltýn, 2019).

The entry of viruses or attacks against operating systems occurred in the mid-eighties, at the university level, when academia and the State worked together as from the ARPANET project and some companies occasionally participate in research on the subject. business security. Likewise, the first Virus, as we know them, was born in the software space and its use in the family business.

By January 1986 the brothers Basit Farooq and Amjad Amjad Farooq Alvi, of Pakistani origin (Information.com, s.f.), They run a company, called *Brain Telecommunications* (RPP Noticias, 2016). Designed a software that sought to avoid that when using their program under an MS-DOS system, they did so from a pirate one. However, unlike that "computer fraud" of today, it affected the "Boot" or boot space of the unforgettable 5.25-inch floppy disks, in their primary version below a 2.0. It also affected data on the floppy disk. as it was almost full and the virus did not transfer to any part of the computer but to another floppy disk.

The curious thing is that when detecting the files and trying to open them, the data of the brothers appeared, such as telephone number, address, etc., in a clear example of what was wanted: detect the use of "unpaid" or pirated programs and contact those who did, to give them formal purchase instructions, we were in January 1988 when the route in the companies of this virus was detected.

In 1988, we entered the period of the sophistication of viruses in Hardware and Software, the creator of a 23-year-old student at Cornell University: Robert Tappan Morris. New forms of "malware" are born, called "worms", due to the fact that it reaches a file and multiplies in different folders (self-replicating), its objective: to paralyze the hardware, since that self-replication saturated the memory of the computers. In this way the "Morris worm" arises, on November 2, through ARPANET, affecting entities such as NASA, the Pentagon, Universities such as MIT, Stanford and Berkley, in about six thousand computers, with UNIX operating systems, computers made by Sun Microsystem, VAX and DEC (Rodríguez, 2013).

For the first time, a conviction was generated by a Federal judge, on January 22, 1990: three years with probation, a fine of USD 10,000 and 400 dedicated to community service, the "Computer Fraud" was born, with the "Computer Fraud and Abuse Act of 1986" (Bortnik, 2013).

More and more sophisticated and of greater geographical scope, under this context “Michelangelo” was born, a virus that attacks DOS systems, this time capable of acting both on “the boot sector of Floppy disks” and on the “Main Boot Record ”Or master boot sector, affected nearly five million computers worldwide, appears for the first time in February 1991 from Australia (industrial, 2016).

This is the era of viruses of unknown origin, of unknown author (s). From the "Playload", it rewrites the hard disk using random data, leaving the information contained, practically lost. If the computer was turned on on March 6, it would act, hence its name, since it is the date of the birth of the painter, architect and sculptor, Michelangelo Buonarroti or Miguel Ángel (Harán, 2018).

The next step has a woman's name, Melissa. It arises on March 26, 1999, ending the century. The author David L. Smith, thirty-four-year-old ex-programmer of the AT&T Firm, gave the name to it on behalf of a "Topless" dancer with whom he had fallen in love in Florida. Its impact reached close to a million computers in the world,

with damage valued at close to one billion dollars, this time affecting Global Firms such as Lucent Technologies, Microsoft and Intel. The author of it, again receives a sentence by a Federal Judge, equivalent to 20 months in prison, a fine of five thousand dollars.

The contagion through an email, with the sender's name, came in a DOC extension text, the message was suggestive and invited to open it out of curiosity: "Here is the document you asked me ... do not show it to anyone" (panda, 2013).

In the same way, “Happy99” or SKA.A appears, on January 20, 1999, a worm that already affected Windows 95-98 or NT. Its damage was in copying, then changing and establishing new files, it restarted under SKA.EXE format. and, SKA.DLL, there were no detainees, nor was the origin clearly located, new trends in computer fraud (INDIANA, 2018).

The era of the millennium virus, in May 2000. It is characterized by its worldwide coverage in a few hours and of great economic impact towards emblematic western companies (HISTORY), a trend until today in the middle of COVID -19, which shows the attacks from Federal Russia and that they have openly promoted contiongency plans against them since the administration of President Biden. (Sanger, 2021).

It begins with the email "I LOVE YOU", it came with a folder recognized as LOVE-LETTER-FOR-YOU.TXT.vbs., It deleted music files, images, CSS, HTA, JS, JSE, JPEG, JPG files, MP2 and MP3. It took him five hours to reach Europe, Asia and America. A damage of EUR 10 billion is valued in Europe, a contagion of about 10% of all connected computers, reached computers of the Federal Reserve, Pentagon and the British Parliament. Its origin is in the Philippines, by Onel Guzman (Garcia, 2018).

Fizzer, a form of "Trojan", year 2003, takes from the keystrokes of the user, personal email passwords, bank accounts, Internet, names, etc. It affects files from emails damaging Windows operating systems type 95, 98, ME, NT, 2000, XP. Save the data in a Windows file called ISERVC.KLG, leave the space for the Hacker to open it and have this information in his possession, that is, his objective to steal money and identities (Liu), there were no detainees.

With the rise of mobile technologies in California, a year later Cabir or Caribe is created, a worm that makes use of bluetooth connections, sending itself to other devices with a message, which gives the entry check from its owner (Charny, 2005). It is spread on cell phones of the best-selling Firm at that time: NOKIA (infobae, 2017).

Its Symbian S60 operating system manages to maintain this connection while minimizing battery life. Created by a member of group 29A of Spanish origin, made up of people dedicated to the study of computer viruses, who wanted to demonstrate the existence of viruses on cell phones, we are now in the era of viruses on smartphones, the favorite device of socialization of the human being of the XXI century (Carlos, 2013).

Starting in the second decade of the millennium, viruses are born that seek to attack infrastructures, a virtual form of attack between States, that is, it is part of the new world geopolitical order, which makes use of 4.0 technology and later points to 5.0. There, Stuxnet arises, a worm that appears in mid-2010, spreads from a USB, operates through Windows, infiltrates the machinery with the software "Siemens Step 7", which is used in systems associated with the industry. In this case, it attacks those used in the Iranian government's nuclear enrichment facilities, where the uranium enrichment centrifuges were being destroyed, 984 of these fell, there were no arrests (Holloway, 2015).

This new modality has in the WannaCry Ransomware a version of a cyber attack, but now with global coverage that affects the infrastructure of a country, as happened since May 2017.

The Internet of Things or IoT, makes use of printers and others devices interconnected to the network, with use of Windows, its objective: to affect government entities, universities, technology providers, hospitals, reached about ¾ parts of the countries of the world, affecting 29,000 institutions of the PR China (countries, s.f.), companies such as Renault, FedEx, the National Health Service of the United Kingdom, etc., use the Windows system in its versions of 2005, 2007, Vista, Windows 8 (Fruhlinger, 2018).

SocioEconomic Challenges, Volume 5, Issue 4, 2021
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

Table 1. Evolution of Computing Threats: history and origins

Computer Virus	Author	Year	Month-Day(s)	City/Country/University/ Company	General Purpose
Theory of the Computing Viral-Theory and Organization of Complicated Automata	John von Neumann	1949	December	United States-University of Illinois	Shows the existence of "automaton creations", which are reproduced in computer systems.
Creeper	Bob Thomas	1971	October	United States, BBN Technologies	It spreads a message on the computers of the ARPANET network "I'm creeper: cath me if you can!". Two years later, it gave birth to the "Reaper" anti-virus.
Cloner	Richard Slrente	1982	30-january	Pittsbourg-Pennsylvania	Program that affects the boot disk, of the Apple II operating system.
In 1983 he wrote "Computer Viruses. Theory and Experiments ", he defines what is understood as a virus:" a program that can infect other programs by modifying them to include a possibly evolved copy of itself ".	Fred Cohen	1983	3-november	United States-University of California	A "malware" is created, to control the Unix operating system
They use the virus to spread and make their company known.	Hermanos Basit Farooq y Amjad Amjad Farooq Alvi	1986	January	Pakistán- Brain Telecomunications	Affects the "Boot" or boot space of 5.25-inch floppy disks, infected other floppy disks, focused on IBM computers.
Worm Morris.	Robert Tappan Morris	1988	November 2	United States-University of Cornell	Nacen nuevas modalidades de malware, conocidos como "gusanos". With ARPANET, it affects NASA, the Pentagon, universities such as MIT, Stanford and Berkley, and about six thousand computers.
Michelangelo	Unknown	1991	February 4	Appears for the first time in Australia.	It affected around five million computers in the world.
Melissa	David L. Smith	1999	March 26th	United States.	It affected approximately one million computers in the world. It reaches Global Firms, such as Lucent Technologies, Microsoft and Intel. The contagion is made through an e-mail.

Table 1. Evolution of Computing Threats: history and origins

Computer Virus	Author	Year	Month-Day(s)	City/Country/University/ Company	General Purpose
I LOVE YOU	Onel Guzman	2000	May 4th	Philippines	Worldwide infections occur in a few hours. It violates national high-impact bodies, the Federal Reserve, the Pentagon and the British Parliament.
Fizzer	Unknown	2003	May 8	Unknown	Used to steal personal keys.
Cabir o Caribe	Created by group named: 29A	2004	June	California	It infects Cell Phones: NOKIA brand.
Stuxnet	Unknown	2010	January	Iran	From a USB, it is a worm that attacks the software associated with Siemens, which are connected to industrial machinery and infrastructure of a country.
Ransomware WannaCry	Unknown	2017	May	North Korea	It affects a large part of the infrastructure of the Government of a country, from universities, technology providers, hospitals, it reached about ¾ parts of the countries of the world.

Source: The author, based on the different bibliographic sources cited in this point.

Cyber security indicators

The Global Cibersecurity Index

As of 2007, the United Nations' World Connectivity Committee (ITU) has structured the Cybersecurity indicator or "Cibersecurity Index" or The Global Cybersecurity Index (GCI). The first time it was released, it was for the 2013-2014 period, with the participation of 105 countries. It is understood that the information associated with Communications Technologies (Information and Communications Technology- ICT) have revolutionized not only the way of communicating, but also of monitoring and being present in front of the databases, resulting from the same, which today for today they handle the companies. The Indicator focuses on the measurement of "progress in Cybersecurity" given a regional context and its position at the global level of each country, thus allowing to observe and analyze the evolution of each one by level and at a relative level, compared to the others.

In order to obtain the precise data, five steps are developed for this purpose: the existence of cyber-threats is identified at the national level; It seeks to identify the measures that are generated at the national level to repel them; the measures taken are selected; Cybersecurity indicators are detected and these are grouped together (Rikk, 2018).

The latest results show how more and more there is awareness of the importance of the issue, and they adopt associated public policies. Data such as these, as they manifest it from before the pandemic, to 2018: about 9 out of ten countries, already have legislation that recognizes the figure of "cyber-crime"; about every 6 countries out of 10, stated to integrate this issue as public policy, increasing by 8%, this data, since 2017 (ENGINEERING AND TECHNOLOGY -E&T, 2019), 58% had a National Cybersecurity Strategy (NCS), complemented by 47% of countries with Cybersecurity indicators, as part of a comprehensive public policy, allowing with these tools to mount more efficient and effective national strategies. to cyber-crime (ITUPublications, 2018).

SocioEconomic Challenges, Volume 5, Issue 4, 2021
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

The five "pillars" or analysis supports of this indicator (through twenty-five indicators), determine not only the base of study of this, but the elements that today every State, City, Company, must take into account to turn Cybersecurity into a source of Management Innovation and a safer client-company relationship, especially in periods like the current ones where more and more are transactions, relationships, marketing, online (UNCTAD, 2021). The organization promotes the creation and continuous management from a National Computer Incident Teams (CIRTs), which also acts in accordance with a "roadmap" in this regard, which focuses on the implementation, monitoring of a national-type strategy (International Telecomonucations Union (ITU)).

The same advances confirm some facts: Europe is the continent of the world that at a supranational level has the best infrastructure, experience of public-private origin and human resources, companies, better adapted to cyber attacks. Second, the figure of "Cybercrime" is recognized by the vast majority of States. Third, response groups or Networking are strongly integrated in Europe and Asia. Fourth, the specialized Human Resource has a continuous and updated educational structure of almost 100% in Europe and Asia. Fifth, the public-private alliances, for the defense of the company-State against Cybercrime, have Europe as a leader, but they see a great lag and void in the countries of America, which can be exploited by these organizations.

Legales Measures

It focuses on the persecution and investigation, laws, regulations, decrees, regulations, official acts, contents, number of institutions, international harmonization, which are in favor of the fight against Cybercrime. Since before the pandemic, great advances have been observed here, which allow "shielding" the commercial performance of BtB, BtC, years 2019-2021. According to the 2018 report, around 91% of the countries of the world created legislation against this type of crime, compared to 79% a year earlier; By continents, in Europe all but one did not have this legal structure, in Asia-Pacific 35 of 38 countries, for America 32 of 35, they created it, in Africa 38 of 44 and in the Arab States, the figure is 18 from 22 countries with this legal support. (ITUPublications, 2018).

Technical Measures

They have “CERTs”, which focus on actions against attacks on the government system, National Cybersecurity Strategies (NCS), response and evaluation groups, child protection mechanisms, standardization processes, use of the cloud as an institutional tool, mechanisms-tools in the fight against spam. These CERTs show that there is work to be done in the years to come. There is a basic coverage in America where only 17 out of 35 States have it, only surpassed by Africa with 13 out of 44 States and the Arab States with 10 out of 22, data that for Europe is 39 out of 45 and in Asia- Pacific, 24 of 38 (ITUPublications, 2018).

Specialized Organizations

It focuses on areas, administrative departments, offices, strategies at the national-international level, indicators, governance, etc., which are aligned from a shared policy, and jointly develop strategies against these actions. Europe is an example in this sense, annually it generates indicators that cover the actions of the company, State and families associated with Cybersecurity, such as: Digital Economy and Society Index, Digital public services. Also supranational reports such as: "Report State of Play of Interoperability in Europe (2016): alignment with the European Interoperability Framework" (electrónica, Resumen del posicionamiento de España en el contexto internacional).

Building Capacity

From Committees, specialized Offices, councils, insurance companies, personnel accreditation offices and specialized agencies, which develop R&D learning-training courses. In the wake of the pandemic, 63% of the countries apply to this specialized training, where America already had a level of coverage equal to that of Africa, for the number of countries involved with 17, which is close to Europe and Asia. to 100% (ITUPublications, 2018).

Cooperation Structure

It is generated, from "Good Practices", Bilateral and Multilateral Agreements, public / private alliances, international agencies, participation in forums, associations. Of this last action, it covered 79% of the countries involved in the indicator, before the pandemic. In public / private alliances, key to internal defense and reaction structures, only 49% of all countries, in America it reaches close to a weak 10%, these are business skills that must be strengthened in this continent (ITUPublications, 2018).

The United Nations e-Government Index

For nearly two decades (2001), it has operated from the United Nations and its Department of Economic and Social Affairs (DESA), with its Division of Public Institutions and Digital Government (DPIDG), plus an international staff of renowned experts (electrónica, Spain is located in the list of "Top Performers" according to the report "UNITED NATIONS E-GOVERNMENT SURVEY 2018", 2018). The members of N.U. are monitored in the matter of e-Government, through a Benchmarking (Naciones Unidas). At a general level, about 70% of the Top 20 belong to Europe, the "Performance" according to the development of electronic administration is observed. Denmark, Finland and South Korea have a perfect score on this sub-indicator since the pandemic. Regarding the sub-indicator related to participation or E-participation, with a perfect level it is headed by South Korea, Denmark and Finland (electrónica, Resumen del posicionamiento de España en el contexto internacional).

National Cyber Security Index

It focuses on the review of about 40 countries, in terms of prevention associated with Cybersecurity, it has 12 indicators. It focuses on five elements: measures and their capacities, identify the main cyber threats, development of associated indicators, identify adopted measures. It monitors annual "incidents" of this nature, associated with related "crimes" and large-scale attacks against the State structure, as well as the established structure, created in the face of these threats.

This is created by the "e-Governance Academy" recognized in English by the acronym (NCSI) and is a global benchmark today (e-Governance Conference, eGA). Beginning periods of pandemic, it was led by France, followed by Germany and Estonia; Of the Top 20, there are 18 countries of European origin, only with the exception of countries of Asian origin: Malaysia (11) and Japan (17) from Southeast Asia. (Rikk, 2018).

The ICT Development Index

Created by the World Connectivity Committee (ITU) in 2009. It has 11 sub-indicators, which seek to review progress in ICT, referencing what happened from countries considered Developed and Developing, plus the steps generated from countries in It is important to observe the matter of competences-skills associated with the management of ICT, infrastructure, access to it and its impact in the country: it is the support and effectiveness of education in the countries, to garn part of the skills of the century. XXI for the company and entrepreneurs (ITU). Observe the progress and innovation related to wireless connectivity and broadband (speed and penetration) associated with the company, the State and the family according to the coverage of households, a determining factor for the relationship between the company and the e-consumer, which is used with such intensity this technology today (ITU, Naciones Unidas, 2019).

Competitiveness, focused on innovation and cybersecurity

Cybersecurity in times of COVID

Now more than ever, this issue is becoming relevant and important to society and business. The arrival of the pandemic has "virtualized" much of the work and activities such as education and public management, triggering the use of digital technologies.

The latest results show how more and more, there is awareness of the importance of the issue, and they adopt associated public policies. Since the first semester of the pandemic, it was observed that those countries that have greater band coverage towards homes, facilitate the high traffic that this situation has awakened, to the

SocioEconomic Challenges, Volume 5, Issue 4, 2021
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

detriment of the use of WIFI, since worldwide it has increased by nearly 80%, "PC loads to the cloud." (ITU, 2020). The OECD countries, in mid-2020, achieved a 5G technology coverage of 34%. This data is 15% for the Asia-Pacific and an insignificant 3.2% for Latin America, which shows other major delays in the area to work (ITU, 2020).

The subject in this matter, then, focuses on closing the "digital gap" between OECD countries, the United States and the rest of the world and taking advantage of the jurisprudence that has been developing on cybersecurity, which today has more than 250 "regulatory responses" in this sense in the world (OMDIA, 2020).

The speed and breadth of the use of the networks, makes clear the need to take care of the databases in the company, the State, consumers and transactions, security controls associated with business operations with the use of the cloud, education, implementation of specialized security teams (Anant, 2020).

The GCI Indicator for 2019 showed, as the leader in the matter was led by the United Kingdom, followed by the United States, France, Lithuania, Estonia, Singapore, Spain, Malaysia, Norway and Canada, in the World Top 10. From the Global Cybersecurity Index, the following data was observed. About 9 out of every ten countries already had legislation that recognized the figure of "cyber-crime"; and 8% integrated this issue as public policy, increasing by 8%, this data, since 2017, important the interest of the issue, led by the State itself. (ENGINEERING AND TECHNOLOGY -E&T, 2019), ad-portals of COVID, 58% had a National Cybersecurity Strategy (National Cibersecurity Strategy- NCS), where 47% had Cybersecurity indicators, as part of a comprehensive public policy, which allows them to be reviewed, projected and adjusted continuously (ITUPublications, 2018).

From that point on, the two predominant models worldwide are analyzed, taking Cybersecurity as the source of the industrialization of the 21st century, and innovation in its continuous management. The business search is observed in the works, investigations that the Company has done during the last two decades in Artificial Intelligence (AI), since it helps to debug, observe, analyze, databases of public and private companies, as well as the same State, which allow preventing and activating Cybersecurity schemes. In this sense, it is headed by IBM, followed by Microsoft, continuing with Siemens AG, Samsung, Google, Intel, Philips, Microsoft Research Asia, General Electric, closing the Top 10 with Siemens; Of these works, the most cited have come in the world of Microsoft, Microsoft Research Asia and Google, which has resulted in a greater number of patents in (AI), for IBM, Microsoft, Samsung Electronics, State Grid Corporation of China and Canon (China Institute for Science and Technology Policy at Tsinghua University, 2018).

Facebook

Its CEO and founder, Mark Zuckerberg, had to appear before the United States Senate in April 2018, in order to explain the existence of invasive practices. They show this version of "virtual neoliberalism", where there is continuous competition, to become databases through social networks. The participation in the market of social networks, between October 2018 to October 2019 in the world, is led by Facebook with 67.73%, that is, for every ten consultations to social networks in the world, about seven are made through of this network, total global penetration. It is followed, almost five times by Facebook, "Pinterest" with 11.08%, Twitter with 10.57%, Instagram with 5.74% and closes the Top 5, YouTube with 3.71%, evidencing the clear leadership of Mr. Zuckerberg's company (statcounter, 2019).

However, this global positioning makes it attractive to consult consumption habits, consultation, preferences, schedules, profiles, for other Firms that seek to segment the market with this information captured on a daily basis.

Global companies such as Yahoo, Netflix, Apple, Samsung, Amazon, Spotify and Huawei, BlackBerry in 2013 and about fifty other firms, receive this database, sold by Facebook to these companies, taking this information without having the approval of its customers, estimated to have totaled about 87 million (Sanchez, 2018). The vast majority of these alliances operate with options for clients that allow them to recognize topics, videos, etc., and let them know with the "like", showing not only their preferences, but also the contacts to whom they send them.

Thanks to this improper exchange, they were able to set up new tools to attract captive customers and multimillion-dollar alliances were formed, of which Facebook is a part of course, thus managing to maintain at least its dominant position in the market and strengthen the existing alliances, which will support it. It also allows to enlarge, improve this database.

(J.X. Gabriel, 2018). Next, some cases are analyzed that allow us to understand this *modus operandi*, which increases the global capture of consumers, under an innovation in the manner of a technological Networking, focused on audio and video interfaces, creating and positioning new sub-brands.

Alliances, a strategy that operates this data obtained and generates global segmentation

Since the beginning of the second decade of the millennium, Yahoo and Facebook, signed agreements that allowed them to develop "cross" or shared patents, or "cross-license", planned and managed Yahoo events, to develop on Facebook, created a portal of daily news from Yahoo to share on Facebook, through the “Social Bar” platform, and integrates with Facebook's “Open Graph” (Facebook, 2012).

With Apple, the interface seeks to allow making contacts that are on Facebook, in addition to sharing the calendar. The approaches with Netflix, mark the 21st century type Alliances, with the help of Artificial Intelligence (AI) and the great coverage of the Internet, under the need to counterbalance its Asian competitors, particularly those of the R.P. China, such as Alibaba, Weibo, WeChat, QQ, etc.

The Alliance forms a global Networking of Information-Communication-Entertainment. By 2017, when Facebook had about 2,000 million users, about 30% of the world population, it was working under the option of “Open Media”, video (streaming, two-way), disclosed by Google, Cisco , Mozilla, with an offer of music and complementary added services, some at very low fees, with the support of Amazon, Microsoft and Netflix.

For firms such as the "Royal Bank of Canada" and streaming champions such as Netflix and Spotify, with the Facebook interface, it was possible to observe the personal emails of customers (Nexton, 2018).

Disruptive innovation arises from the added value of each Firm in alliance with Facebook, which offers new global contributions, but, "searching" the private life of those who make use of Social Networks, which allows them to take "a step forward" than your possible competitors.

In the case of Instagram and WhatsApp, which mark the era of global, graphic and informative communication, as one of their value-added paths to follow, understanding that, through mobile telephony, you get 24 hours a day this value added (Shamkland, 2017).

This disruption in social networks, led by Facebook, seeks in the development of these alliances to create a single interface, where users choose their means of dissemination that integrates, under the chosen modality, the information from WhatsApp (which it acquired in 2014), Facebook Messenger and Instagram (acquired in 2012), process to be consolidated from 2020 (Isaac, 2019).

On Huawei's side, it is similar to Facebook's developed alliances with Lenovo, Oppo, and TCL. It makes use of interfaces with Facebook, which allow us to know what “I like”, leaving the preferences, and further expand the client's profile, given that it gave spaces to comment, make their tastes known on the political, religious, relationships interpersonal, attendance at events, that is, he was able to have a highly personalized profile 20 (Liao, 2018).

The Model of the People´s Republic of China

The Chinese economy has been in the last decades, being filled with "adonorem awards", such as being recognized as the world's factory, the one with the largest consumers, the largest factories, and so on. The digital economy of pandemic periods has catapulted it with new accolades and innovations, labeled "made in China first." The Disruption *made China*, which confirms its robustness in database platforms and its security in handling and storage of this, leading to industrialization 5.0, to its highest in this.

SocioEconomic Challenges, Volume 5, Issue 4, 2021
ISSN (print) – 2520-6621, ISSN (online) – 2520-6214

Here, IIoT, Industrialization by Internet of Things, is being implemented. Cases like that of the Midea Group (1968), in its production of household appliances, resort to "Flexible manufacturing" under this technology, managing to adapt materials, machines, designs, its production is with this technology connected to R&D centers to detect faults, changes, new designs, etc., continuously 7/24; Yaoshibang Pharmaceuticals with its BtB platform (2015) breaks the figures in its sales (Ku, 2021) and maintains this support to review changes continuously in the orders of its customers in health matters, almost in real time (Bu, 2021).

It draws attention to what has been done in other latitudes around the subject, where a Networking is configured, between the Company and the State. This public-private ecosystem, in the case of the R.P. China, at the end of the nineties, in 1997, about a quarter of a century, allows it to recognize the legal figure of "computer crime." This foresight and progress in the matter, which is also an innovation from the State management put into action for more than two decades, led it to build and manage, by 2017, 21 Cybersecurity Institutes (Hathaway, 2015).

This State Cybersecurity Networking helps to strengthen the security not only of their companies, but also of their clients, who know that acquiring a product, service, from a Chinese Firm, has the support of this network and will minimize the assault to your data, or dissemination of these, in favor of other global firms such as the case of the West with Facebook (2017-2018), knowing on the other hand, that this information will remain in the hands of the Chinese State.

The educational support that is being developed in this regard is striking. It was analyzed in a previous point that the (AI) is key in this scheme that associates management with innovation, under a Cybersecurity approach. By 2018, the University of the People's Republic of China, leads in what has been called "AI + X", seeks the integration of the area of knowledge of the (AI) with other opposite and complex areas, ranging from biology, public administration, mathematics, business administration and economics, passing through jurisprudence, physics, psychology and sociology, under a pedagogy focused on continuous training. This educational idea is creating a Human Resource, whose daily "know-how" is involving services, final products, inputs, innovators and related to the (AI), led this process, by the University of Tsinghua, Beijing, the same Chinese Academy of Sciences, Zhejiang and the Shanghai Jiao Tong (China Institute for Science and Technology Policy at Tsinghua University, 2018).

From R + D + i, through specialized global defense companies: the Chinese reality of the 21st century

The Chinese State is clear that Cybersecurity is the center of the industrial development and management of the 21st century. There is a “cybernetic army”, it generates tranquility and stability in the face of future investments that, from the public or the private, you want to do with communications, the IoT, information via the internet as a support, knowing that only for 2014 observed a shortage of "cybersecurity" professionals of one million positions in the world, projected to 3.5 million specialists in the subject by 2021. On the other hand, it integrates "Intelligent Endpoint Protection System" solutions at the national level (IEP), which at this scale, prevents and activates defense mechanisms on computers, "Persistent Threat Analysis System" (PTA), against organized cyber assault groups, which attack institutions or information governance systems and "Advanced Persistent Threat ”(APT), which allows surveillance against groups that attack specific establishments, to block, misinform, steal databases, create computer terrorism in offices of the State of Defense, Telecommunications, Central Government (Morgan, 2019).

The Standard aims to centralize the control and legislation associated with Cybercrime and the Company. In June 2017, a law came out, which regulates the use of email, its data networks, commercial information, for companies, which must remain in Servidores de la R.P. China, any transfer of this data outside the country, will be done with permission (Zhang, 2019). In March 2019, the Chinese State announced the “App Security Certification”, which seeks to ensure that business processes that make use of this tool voluntarily acquire this certificate, for mandatory State companies, which implies that this Firm complies with the standards required at the national level (GB / T35273), recognized as "Information Security Technology- Personal Information Security Specification", to achieve this certificate, it will be delivered by the "China Cybersecurity Review Technology and Certification Center " (Luo Yan, 2019).

The private-public network, has specialized companies throughout the country, with their own research centers, as of 2017 there were 2,681 firms dedicated to this task (Zhang, 2019). Companies with global coverage such as Bluedon (Guangzhou), with products and structures adaptable to company models, Anty Labs (Beijing), has six own research centers, and with latest-generation anti-virus hardware, Beijing Zhizhangyi Co Ltda., works with companies around the world, in the areas of aviation, education, government, military, healthcare, finance, technology, manufacturing, DBAPPSSecurity Ltda., focuses on the heart of the business strategy of the 21st century: Big Data, Mobile Internet, the integrated information system of Smart Cities, Business Apps (Morgan, 2019), Meiya Pico (Fujian, Siming and Xiamen), specialized in this Firm, in digital forensics, etc.

As for the Chinese global firms, they show what will be the trend in this matter worldwide from this second decade of the millennium. Huawei leads the way. It starts from having the domain, control and projection of their own operating systems associated with their Hardware. Since the conflict with the United States government for issues associated with cyber espionage in 2017, it has sought the development of its operating software, hence the Hong Meng system (OS) and develops a corporate Networking, in the Chinese style. The system is being developed and is being sought as an alternative to the Android system and is being worked on as an alternative for Chinese global firms led by Oppo, Xiaomi, Vivo and the Multinational Tencent, with the support of the State. (Doffman, 2019).

Conclusions

Since the first negotiations between the Government of President Donald Trump towards North Korea, since January 2017, denuclearization and the renunciation of the use of the hydrogen bomb on the part of the Korean regime were pointed out. However, since the administration of President Obama, attention had been drawn to these attacks from North Korea to companies such as Sony Pictures in 2014. (THE DENVER POST, 2017).

The famous Cybersecurity company CROWDSTRIKE, with the support of the US Security Agency, based in Sunnyvale, California, since 2014 formally accused hackers of Chinese origin, of carrying out cyber espionage, to United States firms of the pharmaceutical sector, manufacturing and technological, aerospace, this group of was known, under the name of "Putter Panda" (Economista, 2014), from this report, the same US Department of Justice could accuse this "chine team" of carrying out this type of action. Attacks on targets associated with the United States Defense structure are also observed, with the recognized group, such as "Energetic Bear" or "Dragonfly", from the Russian Federation, targeting global firms from the energy sector (Sebenius, 2019).

Part of the piracy, which became famous from the privateering from 17th century England, such as the English interest at the time for the "distribution" of the wealth of the "New Indies", now, in the 21st century, it passes to order of the use of the internet, no longer the sea, by the search for global markets from the net, leaving the "pirate boarding" of the seas, now with hackers, who deal with other people's accounts, databases of client companies and even industrial secrets. This scenario that faced the then all powerful Spanish crown with the English one, now shows the fall of multinationals with parent companies, branches in the United States, in the face of the ruthless attack from computer centers coming from a Hegemon of the cold war that has fallen into disrepair. credibility and global leadership: Russia (Harshaw, 2021).

In its report "Global Threats 2018" CROWDSTRIKE, shows how highly engineered and rapid cybercrime actions come from the R.P. China. Asia does not escape these trends, since from Iran, attacks have been found focused on countries in the Middle East and part of the Maghreb (CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, 2018).

There are trends in cybercrime today. The Multinational Cisco, reports in 2019 that in its customer databases, at least 31% of the Firms have detected a cyber attack associated with their operational management. In this sense, these actions focus on "data breach", "Insecure application user interface" (API, BY ITS ACRONYM IN ENGLISH) ","Cloud Abuse"," Malicious Software attack "(malware Attack), “Database Loss”, “Hacking”, “Simple Passwords”, “insider threats”, the use of the “Internet of Things” (IoT) and the Software-Hardware in the "shadow", not compatible with the IT area of the Firm or Shadow IT System (Magazine, 2019).

There are clearly skills that must be worked on, thinking about the University and its real needs associated with the 21st century and your company in the middle of COVID. From the examples observed, those associated with data analysis, which the company has today as a fundamental basis to sustain itself in the market. From this skill, studies should be proposed in the manner of "AI + X", where not only is Artificial Intelligence used as a complementary source of analysis, but also the development of other competencies associated with group and interdisciplinary work and Resilience, decisive in a globalized world that implies the development of projects with subsidiaries of companies worldwide and / or, developing products, services, supplies, thinking of global consumers.

There is a large space for the workforce, which works worldwide in Cybersecurity, as explained in a few years the demand for this human resource will triple. But a special case is for women in this work, since they only occupy about a quarter of the existing work in the world, at the end of 2019, therefore the universities, the States, must promote this work more in the world within them. and further narrow this labor “gender gap” (BBVA, 2019).

State action spaces against cyber attacks, under modalities such as ransomwere, which seek from the hijacking of databases, massive theft of customer keys, databases, has become transnational spaces of open crime. this space of action implies a couple of reflections (Donnet, 2021): is the Russian federation, the People's Republic of China, North Korea government, an accomplice or actor in this criminal innovation? on the other hand, should the west shield and demand respect for its companies, entrepreneurs and citizens in multilaral spaces? should an international business organization be created to defend and update against these crimes? should moral, economic and political compensation be requested for allowing the servers of the aforementioned countries to give white light to these?

This space of universal history, which now has a before and after covid, has left spaces of reflection that have allowed the arrival of new ideas in the model of life, which has sought in digitization, its natural path of advancement as a society. The european union at the head of the european commission, seeks to regulate and promote innovation in relation to the financial field, "crypto assets", cross-border data crossing via digital, demonstrating that this world of pandemic and looking for the post- pandemic, is aware of the changes insocial paradigms and its space (Pacheco, 2021).

Funding: self-funded.

Author contribution: conceptualization, Ed. Fernando Alonso Ojeda Castro; data curation, Ed. Fernando Alonso Ojeda Castro; formal analysis, Ed. Fernando Alonso Ojeda Castro; funding acquisition, Ed. Fernando Alonso Ojeda Castro; investigation, Ed. Fernando Alonso Ojeda Castro; methodology, Ed. Fernando Alonso Ojeda Castro; project administration, Ed. Fernando Alonso Ojeda Castro; resources, Ed. Fernando Alonso Ojeda Castro; software, Ed. Fernando Alonso Ojeda Castro; supervision, Ed. Fernando Alonso Ojeda Castro; validation, Ed. Fernando Alonso Ojeda Castro; visualization, Ed. Fernando Alonso Ojeda Castro; writing – original draft, Ed. Fernando Alonso Ojeda Castro; writing – review & editing, Ed. Fernando Alonso Ojeda Castro.

References

1. Anant, V. C. (2020). *COVID-19 crisis shifts cybersecurity priorities and budgets.* Mckinsey. [link].
2. Banga, G. (10 de octubre de 2018). How Three Waves Of Cybersecurity Innovation Led Us Her. [Link].
3. BBVA. (2019). *Directivas y expertas en ciberseguridad toman la palabra en BBVA.* [Link].
4. Bortnik, S. (4 de noviembre de 2013). *welivesecurity*. [Link].
5. Bu, L. C. (30 de septiembre de 2021). The Future of Digital Innovation in China: Megatrends Shaping One of the World´s Fastest Evolving Digital Ecosystems. *McKinsey & Company*. [Link].
6. Carlos, U. R. (2013). *EL AUTOR DE "CABIR" ASEGURA QUE JAMÁS DIFUNDIÓ EL VIRUS.* [Link].
7. CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE. (2018). *Iran´s Cyber Ecosustem: Who Are the Threat Actors?* CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE. [Link].
8. Cerra, M. (2010). *200 Respuestas: Seguridad* (1ra ed.). Buenos Aires, Argentina: Fox Andina. [Link].
9. Charny, B. (18 de febrero de 2005). Cabir mobile virus found in U.S. [Link].

10. China Institute for Science and Technology Policy at Tsinghua University. (2018). *China AI Development Report.* [Link].
11. countries, A. s. (s.f.). *Cybersecurity INSIDERS*. [Link].
12. Datosmacro.com. (26 de 08 de 2019). *Expansión/Datosmacro.com.* [Link].
13. Datosmacro.com. (26 de 08 de 2019). *Expansión/Datosmacro.com.* [Link].
14. Doffman, Z. (12 de junio de 2019). Tencent, Xiaomi And Oppo Testing Huawei´s ´60% Faster´ Android OS, Report Claims. [Link].
15. Donnet, P. (22 de julio de 2021). Cybercriminalité: les États-Unis et leurs alliés occidentaux accusent la Chine. *Asialyst*. [Link].
16. Economista, E. (10 de 06 de 2014). Detectan una segunda unidad del ejército chino dedicada a lanzar ciberataques contra EEUU. *El Economista*. [Link].
17. e-Governance Conference, eGA. (s.f.). [Link].
18. electrónica, P. p. (2018). *Spain is located in the list of "Top Performers" according to the report "UNITED NATIONS E-GOVERNMENT SURVEY 2018".* [Link].
19. Electrónica, P. p. (s.f.). *Resumen del posicionamiento de España en el contexto internacional.* [Link].
20. ENGINEERING AND TECHNOLOGY -E&T. (2019). *UK tops ITU´s global cyber security index.* E&T. [Link].
21. Facebook. (6 de julio de 2012). *Yahoo¡ and Facebook Launch Strategic Alliance and Resolve Patent*.
22. Ferreras, A. (10 de abril de 2014). *Blogthinkbig.com*. [Link].
23. Foltýn, T. (3 de noviembre de 2019). *Welivesecuruty*. [Link].
24. Fruhlinger, J. (30 de agosto de 2018). What is WannaCry ransomware, how does it infect, and who was responsible? *CSO*. [Link].
25. Garcia, B. (10 de mayo de 2018). I LOVE YOU: ÑA HISTORIA DEL VIRUS QUE PARALIZÓ AL MUNDO HACE 18 AÑOS. [Link].
26. Harán, J. M. (12 de noviembre de 2018). *welivesecurity*. [Link].
27. Harshaw, T. (17 de July de 2021). What Can Biden Do About Russian Hackers? Not Much. *Blomberg*. [Link].
28. Hathaway, M. (2015). *CYBER READINESS INDEX 2.0, A PLAN FOR CYBER READINESS: A BASE LINE AND AN INDEX*. Potomac Institute for Policy Studies. [Link].
29. HISTORY. (s.f.). *HOY EN LA HISTORIA.* [Link].
30. Holloway, M. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities.* [Link].
31. INDIANA, U. D. (2018). *ARCHIVED: What is the Happy99 virus, and how do I remove it?* [Link].
32. industrial, E. d. (2016). *ANÁLISIS VIRUS MICHELANGELO.* [Link].
33. infobae. (18 de enero de 2017). Cuáles son los 20 celulares más vendidos de la historia. [Link].
34. INFORMÁTICA, B. H. (5 de diciembre de 2011). *Proyecto ENIAC*. [Link].
35. Information.com, H. O. (s.f.). *historyofinformation.com*. [Link].
36. INSTITUTO DE ESTRATEGIA. (25 de agosto de 2017). *Creeper, el primer virus de la hsitoria que infectó nuestros ordenadores*. [Link].
37. International Telecomonucations Union (ITU). (s.f.). *Global Cybersecurity Index.* [Link].
38. Isaac, M. (28 de enero de 2019). WhatsApp, Instagram y Facebook Messenger Juntos: el plan de Mark Zuckerberg. [Link].
39. ITU. (2020). *ECONOMIC IMPACT OF COVID-19 ON DIGITAL INFRAESTRUCTURE*. Ginebra, Suiza. [Link].
40. ITU. (s.f.). *The ICT Development Index (IDI): conceptual framework and methodology.* [Link].
41. ITU, Naciones Unidas. (2019). *ICT Development Index- background document.* [Link].
42. ITUPublications. (2018). *Globalo Cybersecurity Index (GCI) 2018.* [Link].
43. J.X. Gabriel, L. M. (19 de Diciembre de 2018). Todo lo que Facebook compartió con empresas pese a prometer más privacidad. *The New York Times*. [Link].
44. Judson, J. (16 de julio de 2019). A necessary rise: Lithuania bolsters its cybersecurity, catching the attention of other nations. [Link].

45. Ku, L. (16 de junio de 2021). La plataforma farmaceútica china Yaoshibang recauda 270 millones de dólares. [Link].
46. Liao, S. (0 de junio de 2018). Why Facebook´s secret data-sharing deal with Huawei has the US concerned. [Link].
47. Liu, Y. (s.f.). *W32.HLLW.Fizzer@mm.* Symantec. [Link].
48. López, A. (11 de abril de 2017). Elk Cloner: 35 años del primer virus informático. *TECNOXPLORA*. [Link].
49. Luo Yan, Y. Z. (2019). *China Introduce Mobile Application Security Certification Scheme.* [Link].
50. MacNeil, J. (10 de noviembre de 2019). *The computer virus is born, November 10, 1983*. [Link].
51. Magazine, U. S. (2019). Top 10 Cybersecurity Risks For 2019. *United States CYBERSECURITY Magazine*. [Link].
52. Mataf.net. (26 de 08 de 2019). *Mataf.net.* [Link].
53. Mayya, R. (s.f.). *BLITZ The IT Quiz Book* (cuarta ed.). Bangalore, India: Universidad de Nueva Delhi.
54. McMullin, B. (2000). *John von Neuman and the Evolutionary Growth of Complexity: Looking Backwards, Looking Forwards.*. MIT Press. [Link].
55. Morgan, S. (22 de julio de 2019). China Cybersecurity Companies. *CYBERCRIME MAGAZINE*. [Link].
56. Naciones Unidas. (s.f.). *UN E-Government Knowledgebase.* [Link].
57. Nexton, C. (18 de diciembre de 2018). Facebook gave Spotify and Netflix acces to user´s private messages. [Link].
58. OMDIA. (2020). *Telecoms regulation COVID-19 Tracker.* [Link].
59. Pacheco, L. &. (14 de enero de 2021). Estrategia europea de finanzas difitales: claves para el éxito. *BBVA*. [Link].
60. panda. (18 de octubre de 2013). *Los virus más famosos de la historia: Melissa*. [Link].
61. REVISTA DE LA OTAN edición digital. (s.f.). Nuevas amenazas: el ciberespacio. [Link].
62. Rikk, R. (2018). *National Cyber Securuty Index 2018.* e-Governance Academy, Ministry of Foreign Affairs within Estonian Development Cooperation. [Link].
63. Rodríguez, J. (25 de marzo de 2013). *TICSUDI0206.* [Link].
64. RPP Noticias. (19 de enero de 2016). BRAIN, el primer virus de PC, cumple 30 años. [Link].
65. Sanchez, L. (4 de julio de 2018). Cambridge Analytica says more than 87 millon could have had information breached. *THE HILL*. [Link].
66. Sanger, D. B. (9 de September de 2021). Preparing for Retaliation Against Russia, U.U. Confronts Hacking by China. *New York Times*. [Link].
67. Sebenius, A. (19 de febrero de 2019). China Has Abandoned a Cibersecurity Truce With the U.S., Report Says. *Bloomerg*. [Link].
68. Shamkland, S. (14 de noviembre de 2017). Facebook joins to improve online video. [Link].
69. Silverman. (2017). *On the Day In CALIFORNIA HISTORY.* Estados Unidos: The History Press Charleston. [Link].
70. statcounter, G. (2019). *Social Media Stats Worldwide - October 2019.* [Link].
71. THE DENVER POST. (19 de diciembre de 2017). Trump administration blames North Korea for WannaCry ransomware atteck. [Link].
72. UNCTAD. (2021). *How COVID- 19 triggered the digital and e-commerce turning point.* UNCTAD. [Link].
73. UPC, F. (s.f.). *RETRO INFORMÁTICA, EL PASADO DE FUTURO*. [Link].
74. Zhang, J. (18 de enero de 2019). China steps up push to nurture cybersecurity companies to support digitisation of economy. [Link].