International Journal Multidisciplinary Business Management (IJMBM)

EISSN: 2286-8445 **www.ijmbm.org**

The identity and development of female teachers in technical education among young women and needlework teachers

[1]Ana António, [2]António Teodoro

[1]Professor of Sociology of Education and Comparative Education in Lusophone University, at Lisbon,
[2]Director of the Interdisciplinary Research Centre for Education and Development (CeiED)

Abstract: Our paper addresses part of the approach to a topic integrated in the research project entitled The Construction of a Teaching Career in Secondary Education (1947 – 1974). Training, Development, Identities, funded bythe Portuguese national funding agency for science, research and technology, FCT.

The study we developed starts from the exploration of the ideas and an understanding of the feelings expressed by needlework teachers from technical education. We studied the testimonials of technical courses' former pupils regarding their own needlework teachers, their instruction and their careers, and it was beneficial for us that therecollections and views of these pupils, who later became needlework teachers themselves and arenow elderly ladies, could be gathered. Thus, it seemed clear that this study should give the floor to these women, and, as a result, we defined their life stories as the main research instrument.

By establishing a link between the professional and personal lives of these women, we aim to appreciate their professional growth as well as identify decisive stages in their professional performance and their educational beliefs. The framework of these goals is the purposes given to female training courses within the technical education in which these teachers worked.

Our research, therefore, does not have an extensive character; but being of an individual nature, it becomes significant. There are never two identical ways of living human situations. Since the goal of this investigation is to open the possibility of a better understanding of reality, we intend to attribute greater importance to the professional paths that unfold through the testimonials of needlework teachers than to the accounts themselves.
Considering the purpose of the Female Training Course, we decided to work along two parameters to effectively define the boundaries of this research: *Girls were trained in a public situation to successfully playtheir roles in the domestic domain* and *Girls were trained to be able to enter a public domain.*

We found differences between male courses and female courses. For instance, only female courses and female classes integrated the subjects of home economics, childcare and ageneral notion of nursing, in accordance withArticle 73 of Decree 37,029/1948, of 25 August. This piece of legislation defines the curriculum of the women'straining course. We should add that, besides the above-mentioned subjects, girls also took classes in Portuguese, French, Mathematics, Drawing and Physical Education.

We believe it is important for our research to be included in this journal, as the Women's Training Course allowed girls access, through aesthetics, to a public space. We must not forgetthat at this time Portugal constituted a closed environment where women were assignedthe sentimental dimension and the responsibility of being the caregivers. The discussion we proposeis also an opportunity to question the long way that we still have to go with regard to women's rights, so that female discrimination is definitely a thing of the past.

KEYWORDS: life stories; Teachers; Technical education; Women

INTRODUCTION

We are in whatisknown as the "Third wave of Cybersecurity", where the arrival of a virus in anyformimpliesusingyourcellphone, seizingyour USB, reaching the Cloud, gettingintoyour IoT communications, whichimplieswork in a coordinatedwaybetweenprivate and publicactors, making use of the information and classification, thrownby a databasethatisanalyzedfroman Artificial Intelligence (AI) instrument. The challengeforEntrepreneurs and State actorsis to showthat the resultingpublicpolicyisefficient in light of the results, the associatedinnovation and the strategicinsertion of financial and human resourcesthatguaranteesuccess in thisregard(Banga, 2018).

The North Atlantic TreatyOrganization (NATO), receiveditsfirstcyberattacksduring the *Kosovo conflict* at the end of the nineties of the lastcentury, whichcaused the fall of itsmain page onseveraloccasions, and the closure of its e-mail fromoutside, corresponding to its office in Brussels (Belgium). One of its 29 membercountries, Estonia, in mid-2007 and forthreecontinuousweeks, receivedmassivecyberattacksmainlyagainstinstitutionsthatputitsnationalsecurity at risk. It has gonefrom the ColdWar and the subsequentfall of the Berlin Wall, to the era of "digital espionage", whichaffects States, theirallies, theircompanies and currentworldstability. NATO has a "Strategic Concept of the Alliance", and itsown "Cyber Defense" policy, to suchanextentthattodayitisconsidered as "a possible cause of collective defense" of itsmembers(REVISTA DE LA OTAN edición digital).
Therefore, wemustaskourselves: WHAT IS THE RELATIONSHIP BETWEEN INNOVATION AND CYBERSECURITY IN THE 21ST CENTURY COMPANY?

To answerthisquestion, the workaddressesseveralfrontsthatseek to understandnotonlythis new scenariothat the State and the Company must and must face together, butalso the role of businessmen and politicians in one of the greatestchallengesthat the worldnow faces during the FourthIndustrial Revolution.

The document, in the firstpartshows the evolutionthatviruseshavehad in the field of cybersecurity. In summary, with Table 1. "Evolution of ComputerThreats: history and origins", itisobservedhowitwentfromexperiments, product of analysis of possiblevulnerabilityraisedfrom the studies made by John von Neumann in histext of "The theoryfrom Viral Computing ”from 1949 with“ automaton ”creations, to real creationsthatstartedfrom a geniuslike Bob Thomas, creator of“ Creeper, ”capable of infectingcollectiveconnectionsystemslike ARPANET.
Since the eighties, theseviruseshavebeenknownbytheirauthors, who "signedtheir digital work", to generatepartialdamageorpublicizetheircompanies, making the leap to specialized malware, with the clearobjectivefocusedondamage to databases of companies, bothsmall and large, frommediumimpact to highimpact, withunknownauthors, under the clearobjective of the theft of information, money, and databases, thusshowing the era of the cyberattack of the XXI century. The turningpoint, compared to whatis happening today, isgivenby the entry of the *WannaCry Ransomware* virus, showing as of 2017 thatcybercrimeisnotonly a tool to steal industrial information, butalso a weaponbetween States, giventhatitsoriginwas North Korea withclearintentions to affectsecurity and institutionalstability of the affected States.

Itisimportant, on the otherhand, to knowreferences and indicatorsthat in the matter of Cybersecurity must be consultedfor States, Companies and with the coverage of COVID and "work at home", for social and familynuclei. Therefore, in the secondpart of the document, the differentindicators and theirsub-indicators are disclosed, whichallowsanentrepreneur, investors, States, to know, haveobjective, scientific data, about the structures, laws, logistics, human resources, internationalcooperation, cases of companies and States, which are anexample in thismatter, as well as those cases of partialor total failure. In the foregroundis “The Global Cibersecuruty Index” by ITU, whichshowshow the differentcontinents are onthistopicassociatedwithinnovation, manifesting the clearadvantage of Europe, followedby Asia, withspecial cases from the United States, leaving the vastmajority of Central and South American countries at a low and worryinglevel, in some cases at the levelorbelowthat of someAfricancountries.

Anotherindicatorisfollowedby “The United Nations –eGovenment Index”, whichexpresslyfocusesonobservingpublicpolicy and Digital Government. Born from the United Nations, the Department of Economic and Social Affairs (DESA) and the Division of PublicInstitutions and Digital Government. Thereisalso the "National Cyber Security Index", itreviews the management of cybercrimes, itiscreatedby the *e-Governance Academy*. Finally, “The ICT Development Index” ispresented, which observes the management betweencountries in education, infrastructure and innovationrelated to logistics, obtainedby the United Nations Committeeon World Connectivity (ITU).

Giventhishistoricalcontext and the indicators, the documentseeks to preciselyaddress the cases of companies and theirdifferentstrategiesthat in thissensehavebeendeveloped, emphasizing the precise management thattheyhavebeenapplying in the midst of anenvironment, markedby the use of mobiletechnologies and the defining role of the States, as guarantors of the operations and providers of the logisticsconducive to the needs of Industry 4.0, COVID 19, and the cyber-consumer. Thissectionanalyzes cases that are led by the globe-Firmssuch as Facebook, Yahoo, Netflix, Amazon, Spotify, whichshinefortheir Western-stylealliances.

On the otherhand, thereis the case of the Chinesemodel, which has one of the beststructures in the form of Networking, wherecredibility and vigilanceis made fromstructures and mega-serversadministeredby the State, at the nationallevel. At the end of 2019, this country alreadyhadone of the highestspeed and connectivityinfrastructures in the world, with 150,000 5G-type stations (compared to 10,000 in the United States), working in fiftycitiesthroughout the country, supportedby human resourcesqualified, byan "army" of 1,700,000 engineers, who in numberhavemultipliedbyfoursince the beginning of the millennium, whentherewereabout 360,000(Rios, 2020). Thismodeliscomplemented, as a central and verytypicalelement of Southeast Asia, byaneducationalstructure, in the form "AI + X", wherehigherstudyisbeingpromoted, with multi and interdisciplinaryteamwork, around Artificial Intelligence (AI), seeking to have a “digital army” thatsufficiently and effectivelycovers the needs in thisfield, whichincludescontinuousresearch in thisfield. Finally, the creation and work of companiesspecialized in thismatterisobserved, whichfrom the R.P. China offersitsservices, both to States and to companiesaround the world.

Thisdocumentoffers a light, showingthat in thisfieldthereismuch to workon, that the companymustunderstand in itsstrategic and tacticalprojections, introduce financial and human resources, as an indivisible management to the companythatwishes to createparadigms, typical of thiscentury.

COMPUTERTHREATS, FROM THE UNIVERSITY TO THE COMPANY

Withthisaside, therewill be a tour of the emergence of the firstcomputerviruses, whichwentfrom simple personal oracademic "experiments" to sophisticated software systems, createdwith the clearintention of stealing, ending, terrorizingusers, Computers, in Companies and States, globally, see Table 1. "Evolution of ComputerThreats: history and origins".

Only the firstcontributionsfrom the ENIAC (Electronic NumericalIntegrator And Computer) Project of John Mauchly and John Eckert in 1943 and the *Colossus Project*, whichhelpedsolveproblems of the US Army, in the middle of World War II, associatedwithcalculation cases ballisticsfirst and cracking the Nazi Code(INFORMÁTICA, 2011), From the mind of a well-knownpolymath-mathematician, of Hungarian-American origin, whoparticipated in the Manhattan project, whatwasknown as "The Viral Computing Theory" emerged in 1949(McMullin, 2000). Thistheorywasseenbyitsauthor John von Neumann, as "automaton" creationsthatcould be reproduced in a computersystem(Ferreras, 2014).

After the KoreanWar (1950-1953), the US Army, lookingfor a means of communicationthatminimized the interception of electricalsignalsthatgaverise to the use of the Telegraph and the Morse code (Samuel Morse) since 1844, wasbornalmost a centurylater in 1958, under the auspices of the Ministry of Defense, the Advanced Research Projects Agency orknownuntiltoday, the ARPANET. Thissystemwasdevelopedbetweencomputers in a directway, almost a decade and a halflater, in 1971, therewas a wholenetwork of 23 pointsconnecteddirectly, of computersthatwascalled ARPANET, bythenitwasworkinghand in handwith the Academy with MIT, the *National PhysicsLaboratory* of the United Kingdom and the famous*Rand Corporation* (Research and Development), a training center of the United States ArmedForcesuntiltoday(UPC, s.f.).

Thisspacegivesrise to “Creeper”, October 1971, whichaffectscomputersthatwereinterconnectedbythisknowledgenetwork made up of the State-Academy, itssourcewas the then-knownFirm BBN Technologies (Mayya). The idea was to follow the spread of the virus of a programbetweendirectlyconnectedcomputers, itscreatorwas Bob Thomas, he achievesthat in the printedresultsoron the screen the phraseappears: “I'm creeper: cath me ifyou can! ”. Twoyearslater, "Reaper" isborn, seeking to stop "Creeper," thatis, the ant-virus isborn. (INSTITUTO DE ESTRATEGIA, 2017).

The term as weknowit "Computer Virus" has twoantecedents. First, in a novel "When HARLIE WasOne", in 1972, the existence of a programthatwould be the equivalent of a computer virus isrecognizedtoday. Ten yearslater, in the famous comic "X-men," thistermisspoken of in the samecontext as itisusedtoday.(Cerra, 2010)
In thatsameyear of 1982 in January, a teenager Richard Skrenta, from Pittsburgh-Pennsylvania, creates a programthatseeks to "infect the boot disk" using the Apple II operatingsystem, as a joketowardshisfriends, (Silverman, 2017). After booting a floppy disk, whichcontaineditfifty times, ittriggered the followingmessage:
“The Cloner: The programwithpersonality. Itwillgetallyour discs, itwillgetintoyour chips! ¡Yes, itis Cloner!Itwillstick to youlikeglue, itwillchangeyour RAM too! Pass iton, The Cloner! (López, 2017).

A yearlater in 1983, seekingthis time to demonstrate the existence of a "malware", with the intention of replicatingitonothercomputers, much more elaborate and knowing a "route" of the malware, from a floppy disk, *Fred Cohen,*student of Engineering of the University of Southern California, creates a program, inserts a hiddencodeintoit, whichmanages to control a computerwith a Unix operatingsystem. Thatyear, he wrote a "paper" called: "Computer Viruses. Theory and Experiments", withthis he defines whatisunderstood as a virus: "a program that can infectotherprogramsbymodifyingthem to include a possiblyevolved copy of itself(MacNeil, 2019). A company of Slovakorigin, called ESET in 2017, declares November 3, as the worldday of "malware", in honor of the work of the thenstudent*Cohen*(Foltýn, 2019).

The entry of virusesorattacksagainstoperatingsystemsoccurred in the mid-eighties at the universitylevel, when academia and the State workedtogether as from the ARPANET project, somecompaniesoccasionallyparticipate in researchon the subjectbusinesssecurity. Likewise, the first Virus, as weknowthem, wasborn in the software space and its use in the familybusiness.

ByJanuary 1986 the brothersBasitFarooq and AmjadAmjadFarooq Alvi, of Pakistaniorigin(Information.com, s.f.), They run a companycalled*Brain Telecommunications*(RPP Noticias, 2016).
Theydesigned a software thatsought to preventthatwhenusingtheirprogramunderan-MS-DOSsystem, theydid so from a pirateone, affecting the "Boot" orbootspace of the unforgettable 5.25-inch floppy disks, in theirprimaryversionbelow a 2.0. Itaffected data on the floppy disk as itwasalmost full and didnot transfer the virus to anypart of the computerbut to anotherfloppy disk.

The curiousthingisthatwhendetecting the files and trying to open them, the data of the brothersappeared, such as telephonenumber, address, etc., in a clearexample of whatwaswanted: detect the use of "unpaid" orpiratedprograms and contactingthosewhodidit, to givetheminstructionsfor the legal purchase of the program, was in January 1988 when the route of this virus wasdetected in the companies.

In this 1988, the period of sophistication of viruses in Hardware and Software isreached, the creator, a 23-year-old studentfrom Cornell University: Robert Tappan Morris. New forms of "malware" are born, called "worms", becausetheyreach a file and multiply in different folders (self-replicating), theirobjective: to paralyze the hardware, sincethisself-replicationsaturated the memory of the computers. In thisway the "Morris worm" arises, onNovember 2, through ARPANET, affectingentities of importancefornationalsecurity and academia, such as NASA, the Pentagon, universitiessuch as MIT, Stanford and Berkley, in aboutsixthousandcomputers, with UNIX operatingsystems, computers made by Sun Microsystem, VAX and DEC (Rodríguez, 2013). For the first time, a convictionwasgeneratedby a Federal judge, onJanuary 22, 1990: threeyearswithprobation, a fine of USD 10,000 and 400 hoursdedicated to communityservice, thus the figure of *ComputerFraud*wasborn., recognizedwith the "ComputerFraud and Abuse Act" of 1986(Bortnik, 2013).

Increasingly more sophisticated and far-reaching, underthiscontext emerges "Michelangelo", a virus thatattacks DOS systems, this time capable of actingbothon "the boot sector of Floppy disks" and on the "MainBootRecord" or*master boot sector*, affectedaboutfivemillioncomputersworldwide, appearsfor the first time in February 1991 from Australia(industrial, 2016). Thisis the era of viruses of unknownorigin, of unknownauthor (s). From the "Playload", itrewrites the hard disk usingrandom data, leaving the containedinformation, practicallylost. If the computerwasturnedon March 6, itwouldact, henceitsname, sinceitis the date of the birth of the painter, architect and sculptor, *Michelangelo Buonarroti*or*Miguel Ángel*(Harán, 2018).

The next step has a woman'sname, "Melissa." Itariseson March 26, 1999, ending the century. The author*David L. Smith*, thirty-four-year-oldex-programmer of the AT&T Firm, gave the name to itonbehalf of a "Topless" dancerwithwhom he had fallen in love in Florida. Itsimpactreachednearlyonemillioncomputers in the world, withdamagevalued at close to onebilliondollars, this time affecting Global Firmssuch, as Lucent Technologies, Microsoft and Intel. Itsauthor, againreceives a sentencefrom a Federal Judge, equivalent to 20 months in prison, a fine of fivethousanddollars.

Itscontagionthroughan-email, with the sender'sname, came in a textwith a DOC extension, the messagewas: "Here is the documentyouaskedfor ... do notshowit to anyone" (panda, 2013). In the sameway, "Happy99" or SKA.A appears, onJanuary 20, 1999, a worm, whichalreadyaffected Windows 95-98 or NT. Itsdamagewas in copying, thenitchanged and established new files under SKA.EXE format. and, SKA.DLL, therewere no detainees, norwas the originclearlylocated, itwasclearthatitsauthor (s)wanted to cause damage to thosewhohad Windows installed and not be discovered(INDIANA, 2018).

The era of the *millennium virus*isobserved in May 2000. Itischaracterizedbyitsworldwidecoverage in a fewhours and of greateconomicimpact(HISTORY). Itbeginswith the email "I LOVE YOU", itcamewith a folder recognized as LOVE-LETTER-FOR-YOU.TXT.vbs., Iteliminated files associatedwithrecreational and relaxationactivities, thosethatcontained music, images, of typeextension CSS, HTA, JS, JSE, JPEG, JPG, MP2 and MP3. Ittookfivehours to reach Europe, Asia and America. Itisvalued in Europe, a damage of EUR 10,000 million, a contagion of about 10% of allconnectedcomputers, reachingcomputers of the Federal Reserve, the Pentagon and the British Parliament. Itsoriginis in the Philippines, itscreator, *Onel Guzman*(Garcia, 2018).

*Fizzer*appears, a form of "Trojan", year 2003, takesfrom the keystrokes of the user, personal email passwords, bankaccounts, Internet, names, etc. Itaffects files from emails damaging Windows operatingsystemstype 95, 98, ME, NT, 2000, XP. Save the data in a Windows file called ISERVC.KLG, leave the spacefor the Hacker to open it and havethisinformation in hispossession, thatis, hisobjective to stealmoney and identities(Liu). Therewere no arrests.

With the rise of mobiletechnologies in California, a yearlater*Cabir*or*Caribe*wascreated, a wormthatmakes use of bluetooth connections, sendingitself to otherdeviceswith a message, whichgives the approval of entrybyitsowner(Charny, 2005). Itis spread oncellphones of the best-sellingFirm in the world at that time, NOKIA (infobae, 2017)and its Symbian S60 operatingsystem, manages to maintainthisconnectionwhileminimizingbatterylife. Created by a member of *Group 29A* of Spanishorigin, made up of peoplededicated to the study of computerviruses, whowanted to demonstrate the existence of virusesoncellphones(Carlos, 2013).

Starting in the seconddecade of the millennium, viruses are bornthatseek to attackinfrastructures, a virtual form of attackbetween States. That'swhere Stuxnet arises, a wormthatappears in mid-2010, spreads from a USB, operatesthrough Windows, infiltrates the machinerywith the software "Siemens Step 7", whichisused in systemsassociatedwith the industry. In this case, itattacks the structuresused in the Iraniangovernment's nuclear enrichmentfacilities, where the uraniumenrichmentcentrifugeswerebeingdestroyed, 984 of thesefell, therewere no arrests(Holloway, 2015).

This new modality has in the WannaCry Ransomware, a version of cyberattack, butnowwith global coveragethatthreatens the infrastructure of a country, since May 2017. Itmakes use of printers and otherdevicesinterconnected to the network, with the use of Windows, itsobjective to affectgovernmententities, universities, technologyproviders, hospitalsthatreachedabout ¾ parts of the countries of the world, affecting 29,000 institutions of the PR China (countries, s.f.), companiessuch as Renault, FedEx, the UK National HealthService, etc., that use the Windows system, in itsversions of 2005, 2007, Vista and Windows 8(Fruhlinger, 2018).

Table 1. Evolution of ComputerThreats: history and origins

COMPUTER VIRUS	Author	Year	Month-Day(s)	City/Country/University/Company	General Purpose
Viral- Theory and Organization of ComplicatedAutomata	John von Neumann	1949	Diciembre	United States- Illinois University	Itshows the existence of "automatoncreations", which are reproduced in computersystems.
Creeper	Bob Thomas	1971	October	United States, BBN Technologies	Itpropagates a messageon the computers of the ARPANET network "I'm creeper: cath me ifyou can!" Twoyearslater, itgavebirth to the anti-virus: "Reaper".
Cloner	Richard Slrente	1982	January 30	Pittsbourg-Pennsylvania	Programthataffects the boot disk, of the Apple II operatingsystem.
In 1983 he wrote "Computer Viruses. Theory and Experiments", defines what is	Fred Cohen	1983	3-November	United States-California University	Itcreates a "malware" thatcontrols the Unix operatingsystem.

understood as a virus:“a program that can infect other programs by modifying them to include a possibly evolved copy of itself ”.				
They use the virus to spread and maketheircompanyknown.	Hermanos BasitFarooq y AmjadAmjadFarooq Alvi 1986	January	Pakistán- Brain Telecomunications	Itaffects the “Boot” orbootspace of 5.25-inch floppy disks, itinfectedotherfloppy disks, focusedon IBM computers.
Worm Morris.	Robert Tappan Morris 1988	November 2	United States- Cornell University	New forms of malware are born, known as "worms". With ARPANET, it affects NASA, the Pentagon, Universities such as MIT, Stanford and Berkley, and about six thousand computers.
Michelangelo.	Unknow 1991	February 4th	Appearsfor the first time in Australia.	It affected around five million computers in the world.
Melissa.	David L. Smith 1999	March 26	United States.	It affected approximately one million computers in the world. It reaches Global Firms, such as Lucent Technologies, Microsoftand Intel. The contagion is made through an e-mail.
I LOVE YOU	Onel Guzman 2000	May 4	Philippines	Worldwide infections occur in a few hours. It violates high-impact National bodies, the Federal Reserve, the Pentagon and the British Parliament.
Fizzer	Desconocido 2003	May 8	Unknow.	Used to steal personal keys.
Cabir o Caribe	Creado por grupo llamado 29A, en el 2004	June	California	It infects Cellphones, NOKIA brand.
Stuxnet	Desconocido 2010	January	Iran	From a USB, it is a worm that attacks the software associated with Siemens, which is connected to industrial machinery and infrastructure of a State.
Ransomware WannaCry	Desconocido 2017	May	North Korea	It affects a large part of the Government's infrastructure, from universities, technology providers, hospitals, it reached about 75% of the countries of the world.

	Source: the author, based on data obtained from the documents, issued and related in this document.

CYBERSECURITY INDICATORS.

The Global Cibersecurity Index

As of 2007, the United Nations' World ConnectivityCommittee (ITU) has structured the Cybersecurity indicatoror “Cibersecurity Index” or The Global Cybersecurity Index (GCI). The first time itwasreleased, itwasfor the 2013-2014 period, with the participation of 105 countries. Itisunderstoodthat the informationassociatedwith Communications Technologies (Information and Communications Technology- ICT) haverevolutionizednotonly the way of communicating, butalso of monitoring and beingpresent in front of databases, resultingfrom the same, whichtodayfortodaytheyhandle the companies.

The Indicatorfocuseson the measurement of "progress in Cybersecurity" given a regional context and its position at the global level of each country, thusallowing to observe and analyze the evolution of eachonebylevel and relative to the others.

In order to obtain the precise data, fivesteps are developed: the existence of cyberthreatsisidentified at the nationallevel; Itseeks to identify the measuresthat are generated at the nationallevel to repelthem; the measurestaken are selected; Cybersecurity indicators are detected and they are groupedtogether(Rikk, 2018).

The latestresultsshowhow more and more thereisawareness of the importance of the issue, and theyadoptassociatedpublicpolicies. Data likethese show it as of 2018: about 9 out of every ten countriesalreadyhavelegislationthatrecognizes the figure of “cyber-crime”; aboutevery 6 countriesout of 10, state to integratethisissue as publicpolicy, increasingby 8%, this data, since 2017(ENGINEERING AND TECHNOLOGY -E&T, 2019), 58% alreadyhave a National Cybersecurity Strategy (NCS), complementedby 47% thathave Cybersecurity indicators, as part of a comprehensivepublicpolicy(ITUPublications, 2018).

The five "pillars" oranalysissupports of thisindicator determine notonly the basis forstudyingit, butalso the elementsthattodayevery State, City, Company, musttakeintoaccount to make Cybersecurity a source of Innovation of Management.

Theyconfirmsomefacts: Europe is the continent of the worldthat at a supranationallevel has the bestinfrastructure, experience of public-privateorigin and human resources, companies, betteradapted to cyberattacks. Second, the figure of "Cybercrime" isrecognizedby the vastmajority of States. Third, response groupsor Networking are stronglyintegrated in Europe and Asia. Fourth, the specialized Human Resource has a continuous and updatededucationalstructure of almost 100% in Europe and Asia. Fifth, the public-privatealliances, for the defense of the company-State againstCybercrime, have Europe as a leader, butsee in the countries of America a greatlag and voidthat can be exploitedbytheseorganizations.

Legal measures

Itfocuseson the persecution and investigation, laws, regulations, decrees, regulations, officialacts, contents, number of institutions, internationalharmonization, that are in favor of the fight, againstCybercrime. According to the 2018 report, around 91% of the countries in the worldalreadyhavelegislationagainstthistype of crime, compared to 79% a yearearlier, bycontinents in Europe, allexceptone do nothavethis legal structure, in Asia-Pacific 35 out of 38, forAmerica 32 out of 35 haveit, in Africa 38 out of 44 and in the Arab States, the figure is 18 out of 22(ITUPublications, 2018).

Technicalmeasures

Theyhave "CERT", whichfocusonactionsagainstattackson the governmentsystem, National Cybersecurity Strategies (NCS), response and evaluationgroups, childprotectionmechanisms, standardizationprocesses, use of the cloud as aninstitutionaltool, mechanisms-tools in the fightagainst spam. TheseCERTs show a basiccoverage in America, whereonly 17 out of 35 States haveit, onlysurpassedbyAfricawith 13 out of 44 States and the Arab States with 10 out of 22, data thatfor Europe is 39 out of 45 and in the Asia-Pacific, 24 of 38(ITUPublications, 2018).

Specializedorganizations

Itfocusesonareas, administrativedepartments, offices, strategies at the national-internationallevel, indicators, governance, etc., that are alignedfrom a sharedpolicy, and jointlydevelopstrategiesagainsttheseactions. Europe isanexample in thissense, annuallyitgeneratesindicatorsthatcover the actions of the company, the State and familiesassociatedwith Cybersecurity, such as: Digital Economy and Society Index, Digital publicservices. Alsosupranationalreportssuch as: "Report State of Play of Interoperability in Europe (2016): alignmentwith the

EuropeanInteroperability Framework"(electrónica, Resumen del posicionamiento de España en el contexto internacional).

Buildingcapacity

FromCommittees, specializedOffices, councils, insurancecompanies, personnelaccreditationoffices and specialized agencies, whichdevelop R&D learning-training courses. By 2018, 63% of the countriesapply to thisspecialized training, whereAmerica has a coveragelevelequal to that of Africabynumber of countriesinvolvedwith 17, whichisclose to 100% for Europe and Asia(ITUPublications, 2018).

CooperationStructures

Basedon "Good Practices", Bilateral and Multilateral Agreements, public / privatealliances, international agencies, participation in forums, associations. Of thislastaction, itcovered 79% of the countriesinvolved in the indicator, by 2018. Forpublic / privatealliances, keyforinternal defense and reactionstructures, only 49% of allcountries, in Americareachesclose to a weak 10%,(ITUPublications, 2018).

The United Nations e-Government Index

Fornearlytwodecades (2001), it has operatedfrom the United Nations and itsDepartment of Economic and Social Affairs (DESA), withitsDivision of PublicInstitutions and Digital Government (DPIDG) , plus aninternational staff of renownedexperts(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, 14 countries in the Top 20 are from Europe. Observe the "Performance" according to the development of electronicadministration. Denmark, Finland and South Korea allhaveperfect scores onthissub-indicator. Compared to the sub-indicatorrelated to participationor E-Participation, South Korea, Denmark and Finland, lead with a perfect score(electrónica, Resumen del posicionamiento de España en el contexto internacional).

National Cyber Security Index

Focuseson the review of about 40 countries, in preventionassociatedwith Cybersecurity, has 12 indicators. Itfocusesonfiveelements: measures and theircapacities, identifying the maincyberthreats, developingassociatedindicators, identifyingadoptedmeasures. Itmonitorsannual "incidents" of thisnature, associatedwithrelated "crimes" and large-scaleattacksagainst the State structure, as well as the establishedstructure, created in the face of thesethreats.

Thisiscreatedby the "e-Governance Academy" recognized in English by the acronym (NCSI) and is a global referencetoday(e-Governance Conference, eGA). As of 2018, itis led by France, followedbyGermany and Estonia, from the Top 20, they are 18 countries of Europeanorigin, onlywith the exception of countries of Asianorigin: Malaysia (11) and Japan (17), fromSoutheast Asia(Rikk, 2018).

The ICT Development Index

Createdby the *World ConnectivityCommittee* (ITU-United Nations) in 2009. It has 11 sub-indicators, whichseek to reviewprogress in ICT, referencingwhathappenedfromcountriesconsidered as Developed and Developing, plus the stepsgeneratedfrom the countries in terms of competencies-skills, associatedwith the management of ICT, infrastructure, access to it and itsimpacton the country(ITU). Progress and innovationrelated to wirelessconnectivity and broadband (speed and penetration) associatedwith the company, State and family, according to the coverage of households(ITU, Naciones Unidas, 2019).

Competitionfocusedon Innovation and Cybersecurity, the reality of today

Fromthatpointon, the twopredominantmodels at the worldlevel of Business and State are analyzed, taking Cybersecurity as the source of 21st centuryindustrialization and innovation in its management. A support of thisbusinesssearchisobserved in the works, investigationsthat the Company has done during the lasttwodecades in Artificial Intelligence (AI), sinceithelps to debug, observe, analyzedatabases of public and privatecompanies, as well as those of the same State, whichallowspreventing and activating Cybersecurity schemes. In thissense, itis led by IBM, followedby Microsoft, continuingwith Siemens AG, Samsung, Google, Intel, Philips, Microsoft Research Asia, General Electric, closing the Top 10 with Siemens; Of theseworks, the mostcitedhave come from Microsoft, Microsoft Research Asia and Google, which has resulted in a greaternumber 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 appearbefore the United States Senate in April 2018, in order to explain the existence of invasivepractices. Theyshowthisversion of "virtual neoliberalism", wherepeople compete incessantly, to gainaccess to databasesthrough social networks. The participation in the social networksmarket, betweenOctober 2018 to October 2019 in the world, was led by Facebook with 67.73%, thatis, forevery ten inquiries to social networks in the world, aboutsevenwere made through of thisnetwork, total global penetration. Itwasfollowedalmostfive 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 clearleadership of Mr. Zuckerberg'scompany(statcounter, 2019).

However, this global positioningmakes the Company'sdatabasesappealing to consultconsumptionhabits, queries, preferences, schedules, profiles, forotherFirmsthatseek to segment the marketwiththisinformationcaptureddaily.
Global companiessuch as Yahoo, Netflix, Apple, Samsung, Amazon, Spotify and Huawei, BlackBerry in 2013 and aboutfiftyotherfirms, receivethisdatabase, soldby Facebook to thesecompanies, takingthisinformationwithouthaving the approval of itscustomers, estimated to havetotaledabout 87 million(Sanchez, 2018). The vastmajority of thesealliancesoperatedwithoptionsforclientsthatallowthem to recognizetopics, videos, etc., and letthemknowwith the “like”, showingnotonlytheirpreferences, butalso the contacts to whomtheysendthem.

Thanks to thisimproperexchange, theywereable to set up new tools to attract captive customers and multimillion-dollarallianceswereformed, of which Facebook is of course a part, thusmanaging to maintain at leastitsdominant position in the market and strengthen the existingalliancesthatItalsoallows to enlarge and improvethisdatabase(J.X. Gabriel, 2018). Next, let'sanalyzesome cases thatallowus to understandthis*modus operandi*, whichincreases the global capture of consumers, underaninnovation in the manner of a technological Networking, focusedon audio and video interfaces, creating and positioning new sub-brands.

Alliances, a strategythatoperatesthis data obtained and generates global segmentation

Since the beginning of the seconddecade of the millennium, Yahoo and Facebook, signedagreementsthatallowedthem to develop "cross" orsharedpatents, or "cross-license", planned and managed Yahoo events, to developon Facebook, created a portal fordaily news from Yahoo to share on Facebook, through the “Social Bar” platform, and integrateswithFacebook's “Open Graph”(Facebook, 2012).
With Apple, the interfaceseeks to makecontactswho are on Facebook, in addition to sharing the calendar.

The approacheswith Netflix, marks the 21st centurytypeAlliances, with the help of Artificial Intelligence and the greatcoverage of the Internet, under the need to counterbalancetheirAsiancompetitors, particularlythose 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 hadabout 2,000 millionusers, about 30% of the worldpopulation, itworkedunder the option of "Open Media", video (streaming, two-way), disclosedby Google, Cisco , Mozilla, withanoffer of music and complementaryaggregateservices, some at verylowfees, with the support of Amazon, Microsoft and Netflix. Forfirmssuch as the "Royal Bank of Canada" and streaming championssuch as Netflix and Spotify, with the Facebook interface, itwaspossible to observe the personal emails of customers(Nexton, 2018).

Disruptiveinnovationarisesfrom the addedvalue of eachFirm in alliancewith Facebook, whichoffers new global contributions, but, "searching" the privatelives of thosewhomake use of Social Networks, whichallowsthem to take "a step forward" aboveyourpossiblecompetitors.

In the case of Instagram and WhatsApp, whichmark the era of global, graphic and informativecommunication, as one of theirvalue-addedpaths to follow, understandingthatthroughmobiletelephony, thisvalueisobtained 24 hours a dayaggregate(Shamkland, 2017). Thisdisruption in social networks led by Facebook, seeks in the development of thesealliances to create a single interface, whereuserschoosetheirmeans of disseminationthatintegrates, under the chosenmodality, the informationfrom WhatsApp (whichitacquired in 2014), Facebook Messenger and Instagram (acquired in 2012), process to be consolidated in 2020(Isaac, 2019).
In the case of the Chinesecompany Huawei, itis similar in terms of the alliancesdevelopedby Facebook with Lenovo, Oppo and TCL. Itmakes use of interfaces with Facebook, whichallowus to knowwhat “I like”, leaving the preferences, and furtherexpand the client'sprofile, giventhatitgavespaces to comment, maketheir tastes known in the political, religious, relationships interpersonal, attendance at events, thatis, I wasable to have a highlypersonalizedprofile(Liao, 2018).

The ChineseModel

On the otherhand, what has been done in other latitudes around the subjectisstriking, where a Networking isconfiguredbetween the Company and the State. Thispublic-privateecosystem, in the case of the R.P. China, at the end of the nineties, in 1997, allowedhim to recognize the legal figure of "computercrime". Thisforesight and progress in the matter, whichisaninnovationfrom the State management, putintoactionfor more thantwodecades, led it to build and manage, by 2017, 21 Cybersecurity Institutes(Hathaway, 2015). This State Cybersecurity Networking helps to strengthen the securitynotonly of theircompanies, butalso of theirclients, whoknowforsurethatacquiring a product, service, from a ChineseFirm, has the support of thisnetwork and willminimize , the assaultonyour data, ordissemination of these, in favor of other global firmssuch as the case of the West with Facebook, knowingon the otherhand, thatthisinformationwillremain in the power of the Chinese State.

The educationalsupportthatisbeingdeveloped in thisregardisstriking. Itwasanalyzed in a previouspointthat Artificial Intelligence (AI) iskey in thisschemethatassociates management withinnovation, under a Cybersecurity approach. As of 2018, the Chinese University leads what has beencalled "AI + X", whichseeks to integrate the area of knowledge of the (AI) withotheropposite and complexareas, rangingfrombiology, publicadministration, mathematics, businessadministration and economics, passingthroughjurisprudence, physics, psychology and sociology, under a pedagogyfocusedoncontinuous training. Thiseducational idea iscreating a Human Resource, whosedaily "know-how" isinvolvingservices, final products, inputs, innovators and related to the (AI), headedby the University of Tsinghua, the same Academy of the ChineseSciences, Zhejiang and the ShanghaiJiaoTong(China Institute for Science and Technology Policy at Tsinghua University, 2018).

From R + D + i, throughspecialized global defense companies: the Chinesereality of the 21st century

The State isclearthat Cybersecurity is the center of the development and industrial management of the XXI century. Thereis a "cyberneticarmy", whichgeneratestranquility and stability in the face of futureinvestmentsthat the publicorprivatewants to make. The focusisoncommunications, the IoT, informationvia the Internet, more, knowingthatonlyfor 2014 therewas a shortage of professionals in "cybersecurity" of onemillionjobs in the world, projected to 3.5 millionspecialistsfor 2021. On the otherhand, the country integrates at the nationallevel “IntelligentEndpointProtection System” (IEP) solutions, which at thisscale, prevents and activatesdefense mechanismsoncomputers, “PersistentThreatAnalysis System” (PTA), againstorganizedcyberassaultgroups, whichattackinstitutionsorinformationgovernmentsystems and “Advanced PersistentThreat” (APT), whichallows to be onguardagainstgroupsthatattackspecific establishments, to block, misinform, stealdatabases data, createcomputerterrorism in offices of the State of Defense, Telecommunications, Central Government(Morgan, 2019).

The Standard aims to centralize the control and legislationassociatedwithCybercrime and the Company. In June 2017, a lawcameout, whichregulates the use of email, its data networks, commercialinformation, forcompanies, whichmustremain in Servidores de la R.P. China, any transfer of this data outside the country, will be done withpermission(Zhang, 2019). In March 2019, the State released the "App Security Certification", withwhichitissoughtthat the businessprocessesthatmake use of thistool, voluntarilyacquirethiscertificate, for State companiesitismandatory, whichimpliesthatthisFirmcomplieswith the standardsrequired at the nationallevel (GB / T35273), recognized as "Information Security Technology- Personal Information Security Specification", to achievethiscertificate, itwill be deliveredby the "China Cybersecurity Review Technology and Certification Center "(Luo Yan, 2019).

The private-publicnetwork, has specializedcompaniesthroughout the country, withtheirownresearch centers, as of 2017 therewere 2,681 firmsdedicated to thistask(Zhang, 2019). Companieswithworldwidecoveragesuch as *Bluedon* (Guangzhou), withproducts and structures adaptable to companymodels, *AntyLabs* (Beijín), has sixownresearch centers, and withlatestgeneration antivirus hardware; *Beijing Zhizhangyi Co Ltda.*,workingwithcompaniesaround the world, from the area of aviation, education, government, military, healthcare, finance, technology, manufacturing, *DBAPPSSecurity Ltda.*,Focuseson the heart of the businessstrategy of the century XXI: Big Data, mobile Internet, the integratedinformationsystem of Smart Cities, business Apps(Morgan, 2019), *Meiya Pico* (Fujian, Simingand Xiamen), specialized in thisFirm, in digital forensics, etc.

As for the Chinese global firms, theyshowwhat the trendwill be during COVID-19 and in the future, thatis, to havetheirownoperatingsystems, quality and securitystandardsfrom the R.P. China, whichalsoallowsyou to generateyourown Networkings. Huawei leads the way. Itstartsfromhaving the domain, control and projection of theirownoperatingsystemsassociatedwiththeir Hardware. Since the conflictwith the United States governmentforissuesassociatedwithcyberespionage in 2017, it has sought the development of itsoperating software, hence the *Hong Meng System* (OS) and showswhatcorporate Networking is, in the styleChinese. The systemisbeingdeveloped and isbeingsought as analternative to the *Android System* and isbeingworkedon as analternativeforChinese global firms led by Oppo, Xiaomi, Vivo and the Multinational Tencent, with the support of the State.(Doffman, 2019).

EL COVID- 19

The businessfocus, since the beginning of 2020, has focusedonthreeoperationalactions: continuingwith the company (possiblynow in a segmentassociatedwith the valuechains of products-servicesrelated to the pandemic), achievingremotework and adapt the strategic plan to this new reality, fueledby Big Data, now of greatmagnitude. In otherwords, a largepart of corporateexistencegoesthroughtechnologyproviders.

In the organization chart of the company, having a Big Data architect, the data engineers, havebecomean indivisible and fundamental partfor the existence of the Firmor Company. The Chief Data Officer or CDO or the onewhoperforms the functions of this in the company, today more thaneverisnotonlyresponsiblefor the data derivedfrom the company, to whichtoday the dailyoperation of the worksisintensivelyadded ,butitis the guarantorwithitsworkteam, of the strategicdailyactions and of the staff in general, leavingaside the routine, established, plannedbefore the COVID.

Thisimpliesthatfinancial and human resourcesmust FOCUS on Cybersecurity, and greater training in thisregardforworkers in general, as well as fortechnology and logisticsprovidersassociatedwith a businessplatform, whateveritmay be. According to a McKinsey study, once the pandemic has begun, the crimesmostused in thisregard are centeredon the side of the clients in "spear phishing", on the side of the workers "isolated at home", the trendpoints to the emails and the corporate page wherecyberattacks are located. The cybersecuritytrendbybusinesssectors, thosethat are investing the most in thismatter to prevent, control, is led byhealth, banking and financialservices, technology and telecommunications, public sector services, wherelargecompanies are the onesthatthey lead this expense(Anant, 2020).

CONCLUSIONS

Since the firstnegotiationsbetween the Government of President Donald Trump towards North Korea, in January 2017, denuclearization and the renunciation of the use of the hydrogenbombby the North Koreanregimewerepointedout. However, since the administration of President Obama, attentionhadbeendrawn to theseattacksfrom North Korea to companiessuch as Sony Pictures in 2014, wherecybersecuritywastested in a worryingway(THE DENVER POST, 2017).

The famous Cybersecurity company CROWDSTRIKE, with the support of the US Security Agency, based in Sunnyvale, California, since 2014 formallyaccused hackers of Chineseorigin, of carryingoutcyberespionage, to United States firmsfrom the pharmaceutical sector, manufacturing and technology, aerospace, thisattackgroupwasknown, under the name of "Putter Panda"(Economista, 2014), Fromthisreport, the same US Department of Justicecouldaccusethis “chine team” of carryingoutthistype of action. Attacks are alsoobservedtowards targets associatedwith the United States Defense structure, with the recognizedgroup, such as “Energetic Bear” or “Dragonfly”, from the RussianFederation, targeting global firmsfrom the energy sector, (Sebenius, 2019)showingthat the "new era of cybercrime "points toGloobalFirms, the infrastructure of the State and National Security, of the countries.

In itsreport "Global Threats 2018" CROWDSTRIKE, showshowthesehighlyengineered and fastactions come fromthispart of the world, determiningthatabout a quarter of operations of thisnature in 2018 come from the P.R. China. The continent of Asia doesnot escape thesetrends, sinceattackshavebeenfoundfromIranfocusedoncountries in the Middle East and part of the Maghreb(CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, 2018).

La Multinacional Cisco, reporta en el 2019, que, en sus bases de datos de sus clientes, por lo menos un 31% de las Firmas han detectado un ataque cibernético, asociado a su gestión operativa. En tal sentido estas acciones se centran en “violación de datos”, “Interfaz de usuario de aplicación insegura” (API, POR SU ACRÓNIMO EN INGLES)”, “Abuso de la Nube”, “ataque con Software Malicioso” (malware Attack), “Pérdida de Base de datos”, “Hacking”, “Contraseñas simples”, “amenazas internas”, “Internet de las cosas” (IoT, por su acrónimo en inglés) y Software-Hardware a la “sombra”, no compatible con el área IT de la Firma o *Shadow IT System* (Magazine, 2019).

El Cibercrimen, se ha convertido en una base de la agenda mundial y de su equilibrio, no se trata por tanto solo de reconocer a esta figura legal, como fuente de la legislación local o regional, sino como aporte claro y evidente, frente a las grandes potencias mundiales, como las no-convencionales provenientes de Norcorea, como estandarizar las normas y estructuras nacionales, para generar un sistema de defensa oportuno y efectivo, tanto con la empresa público-privada, como desde los propios Estados a nivel nacional y supranacional.

Existen claramente habilidades que se deben trabajar, pensando en la Universidad y sus reales necesidades asociadas al siglo XXI y su empresa. Desde los ejemplos observados, las asociadas al análisis de datos, con la que la empresa cuenta hoy como base fundamental para sostenerse en el mercado.

Desde esta habilidad, se debe proponer estudios a la manera de "AI+X", donde no solo se hace uso de la Inteligencia Artificial, como fuente complementaria del análisis, sino el desarrollo de otras competencias asociadas al trabajo en grupo e interdisciplinar y la resiliencia, determinante en un mundo globalizado que implica el desarrollo de proyectos con filiales de empresas a nivel mundial y/o, desarrollar productos, servicios, insumos, pensando en consumidores globales.

Existe un gran espacio para fuerza laboral, que trabaje a nivel mundial en Ciberseguridad, como se explicó en pocos años la demanda por este recurso humano se triplicará. Pero caso especial es para las mujeres ene sta labor, pues solo ocupan cerca de una cuarta parte de la existente en el mundo, a finales del 2019, por ello las universidades, los Estados, deben promover más este trabajo en el mundo dentro de Ellas y estrechar más esta "brecha de género" laboral (BBVA, 2019).

La (AI), es determinante como fuente infinita y como directriz de cualquier estrategia o táctica empresarial a seguir. La misma se logra aprovechar en el momento que al contar con varios datos de un cliente o, una empresa, logra generar un perfil de una u otra por "variables proxy" o correlaciones. Por ello, cuidar, revelar, proyectar una base de datos, implica construir previamente los pasos a seguir de la Firma o Empresa, pero igual, contar con un soporte de Ciberseguridad, que garantice la custodia de este "secreto" empresarial, hoy base y verdadera riqueza intangible de la misma.

En una empresa, sea esta FAMIPYME, PYME, MULTINACIONAL, de capital privado, público, mixto, de alcance local, regional, global, implica que una estrategia-táctica empresarial, que se enfoque en la innovación de un proceso, bien final, servicio, insumo, debe incluir una logística propia, un recurso humano especializado y actualizado, que vea en la Ciberseguridad su enfoque de largo plazo.
El concepto *visional* y *misional* de una empresa, para el siglo XXI, ha de tener en cuenta que la relación con su cliente, cada vez más se hará a través de tecnologías fijas y móviles de la información, en cada proceso, acercamiento, información, venta, entrega, seguimiento.

Ello implica proyectar la empresa desde el corto al largo plazo, bajo un enfoque claro en el tema de la relación segura y eficiente entre empresa y cliente, con un esquema claro y preciso en el tema la innovación.
Para un empresario, empresaria, para un estudiante de posgrado, un gestionador de política pública, asociado a la estructura industrial de un país, es necesario entender, que ha de tener en sus acuerdos regionales comerciales, bilaterales, multilaterales, a la Ciberseguridad, como un tema de primer orden que le dé confianza a futuro a las empresas e inversionistas, que vean en el país un espacio de soluciones para sus futuros intereses.

Cuantificar el efecto de los virus, debe ser tarea de todos los empresarios del mundo, las cifras así lo muestran: hasta comienzos del 2020 su costo era de USD 55 mil millones al año(PODCAST, EL COSTO DE LAS PANDEMIAS INFORMÁTICAS, 2020), equivalente la deuda pública de todo un país como Ecuador a septiembre del 2019 (RTU, 2019), el monto mínimo de la renegociación de la deuda argentina proyectada para la próxima década (Lewkowicz, 2020), cerca al equivalente del paquete de ayuda por parte del gobierno canadiense destinado a empresas y trabajadores afectados por el COVID- 19 (Ellsworth, 2020).
En ese espectro, los acuerdos, deben contar con alianzas en lo privado y lo público, tanto con empresas de capital público como privado especializadas en el tema, que superen el campo de la consejería, al de la implementación y ejecución de planes y programas, de orden tanto nacional como supranacional, para conformar un Networking de prevención y defensa frente a un ataque Cibernético.

REFERENCIAS

1. Anant, V. C. (2020). *COVIDS- 19 crisis shifts cybersecurity priorities and budgets.* Retrieved from https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets?cid=other-eml-alt-mip-

mck&hlkid=7886123efcdf4486812c3dfa49531ce5&hctky=10112779&hdpid=26909de0-4489-4f7f-9567-dbd54ae3a06b

2. Banga, G. (2018, octubre 10). How Three Waves Of Cybersecurity Innovation Led Us Her. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/10/10/how-three-waves-of-cyber-security-innovation-led-us-here/#1332d1ba43d7
3. BBVA. (2019). *Directivas y expertas en ciberseguridad toman la palabra en BBVA*. Retrieved from https://www.bbva.com/es/directivas-y-expertas-en-ciberseguridad-toman-la-palabra-en-bbva/
4. Bortnik, S. (2013, noviembre 4). *welivesecurity*. Retrieved from https://www.welivesecurity.com/la-es/2013/11/04/5-curiosidades-gusano-morris-25-aniversario/
5. Carlos, U. R. (2013). *EL AUTOR DE "CABIR" ASEGURA QUE JAMÁS DIFUNDIÓ EL VIRUS*. Retrieved from https://www.redaccionaula-urjc.es/leganes/el-autor-de-cabir-asegura-que-jam%C3%A1s-difundi%C3%B3-el-virus
6. CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE. (2018). *Iran´s Cyber Ecosustem: Who Are the Threat Actors?* CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE. Retrieved from https://carnegieendowment.org/2018/01/04/iran-s-cyber-ecosystem-who-are-threat-actors-pub-75140
7. Cerra, M. (2010). *200 Respuestas: Seguridad* (1ra ed.). Buenos Aires, Argentina: Fox Andina.
8. Charny, B. (2005, febrero 18). Cabir mobile virus found in U.S. Retrieved from https://www.cnet.com/news/cabir-mobile-virus-found-in-u-s/
9. China Institute for Science and Technology Policy at Tsinghua University. (2018). *China AI Development Report*. Retrieved from http://www.sppm.tsinghua.edu.cn/eWebEditor/UploadFile/China_AI_development_report_2018.pdf
10. countries, A. s. (n.d.). *Cybersecurity INSIDERS*. Retrieved from https://www.cybersecurity-insiders.com/a-synopsis-of-wannacry-ransomware-attack-on-150-countries/
11. Datosmacro.com. (2019, 08 26). *Expansión/Datosmacro.com*. Retrieved from https://datosmacro.expansion.com/paises/francia
12. Datosmacro.com. (2019, 08 26). *Expansión/Datosmacro.com*. Retrieved from https://datosmacro.expansion.com/paises/alemania
13. Doffman, Z. (2019, junio 12). Tencent, Xiaomi And Oppo Testing Huawei´s ´60% Faster´ Android OS, Report Claims. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/06/12/tencent-xiaomi-and-oppo-all-testing-huaweis-faster-android-os-report-claims/#3d288a0d388e
14. Economista, E. (2014, 06 10). Detectan una segunda unidad del ejército chino dedicada a lanzar ciberataques contra EEUU. *El Economista*. Retrieved from https://www.eleconomista.es/tecnologia/noticias/5849384/06/14/Detectan-una-segunda-unidad-del-ejercito-chino-dedicada-a-lanzar-ciberataques-contra-EEUU.html
15. e-Governance Conference, eGA. (n.d.). Retrieved from https://ega.ee/news/the-national-cyber-security-index-gives-governments-a-tool-for-developing-cyber-security/
16. electrónica, P. p. (2018). *Spain is located in the list of "Top Performers" according to the report "UNITED NATIONS E-GOVERNMENT SURVEY 2018"*. Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2018/Julio/Noticia-2018-07-27-Espana-en-lista-Top-Performers-seg-n-informe-E-GOVERNMENT-SURVEY-2018.html?idioma=en#.XddL0dUzZqw
17. electrónica, P. p. (n.d.). *Resumen del posicionamiento de España en el contexto internacional*. Retrieved from https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/Posicionamiento-Internacional/Resumen-posicionamiento-Espana.html#.XddObtUzZqw
18. Ellsworth, B. (2020, MARZO 19). Canadeá anuncia nuevo paquete de ayuda de USD 56 mil millones por coronavirus. *AA*. Retrieved from https://www.aa.com.tr/es/mundo/canad%C3%A1-anuncia-nuevo-paquete-de-ayuda-de-usd-56-mil-millones-por-coronavirus/1771191
19. ENGINEERING AND TECHNOLOGY -E&T. (2019). *UK tops ITU´s global cyber security index*. E&T. Retrieved from https://eandt.theiet.org/content/articles/2019/04/uk-tops-itu-global-cyber-security-index/
20. Facebook. (2012, julio 6). *Yahoo¡ and Facebook Launch Strategic Alliance and Resolve Patent*.
21. Ferreras, A. (2014, abril 10). *Blogthinkbig.com*. Retrieved from https://blogthinkbig.com/john-von-neumann
22. Foltýn, T. (2019, noviembre 3). *Welivesecuruty*. Retrieved from https://www.welivesecurity.com/2019/11/03/antimalware-day-2019-building-culture-cybersecurity-awareness/
23. Fruhlinger, J. (2018, agosto 30). What is WannaCry ransomware, how does it infect, and who was responsible? *CSO*. Retrieved from https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

24. Garcia, B. (2018, mayo 10). I LOVE YOU: ÑA HISTORIA DEL VIRUS QUE PARALIZÓ AL MUNDO HACE 18 AÑOS. Retrieved from https://tecno.americaeconomia.com/articulos/i-love-you-la-historia-del-virus-que-paralizo-al-mundo-hace-18-anos
25. Harán, J. M. (2018, noviembre 12). *welivesecurity*. Retrieved from https://www.welivesecurity.com/la-es/2018/11/12/malware-anos-90-virus-michelangelo-melissa/
26. Hathaway, M. (2015). *CYBER READINESS INDEX 2.0, A PLAN FOR CYBER READINESS: A BASE LINE AND AN INDEX.* Potomac Institute for Policy Studies. Retrieved from https://www.belfercenter.org/sites/default/files/legacy/files/cyber-readiness-index-2.0-web-2016.pdf
27. HISTORY. (n.d.). *HOY EN LA HISTORIA*. Retrieved from https://latam.historyplay.tv/hoy-en-la-historia/se-expandio-en-el-mundo-virus-informatico-i-love-you
28. Holloway, M. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities.* Retrieved from http://large.stanford.edu/courses/2015/ph241/holloway1/
29. INDIANA, U. D. (2018). *ARCHIVED: What is the Happy99 virus, and how do I remove it?* Retrieved from https://kb.iu.edu/d/agyo
30. industrial, E. d. (2016). *ANÁLISIS VIRUS MICHELANGELO.* Retrieved from https://www.eoi.es/blogs/ciberseguridad/2016/04/14/analisis-virus-michelangelo/
31. infobae. (2017, enero 18). Cuáles son los 20 celulares más vendidos de la historia. Retrieved from https://www.infobae.com/tecno/2017/01/18/cuales-son-los-20-celulares-mas-vendidos-de-la-historia/
32. INFORMÁTICA, B. H. (2011, diciembre 5). *Proyecto ENIAC.* Retrieved from https://histinf.blogs.upv.es/2011/12/05/proyecto-eniac/
33. Information.com, H. O. (n.d.). *historyofinformation.com*. Retrieved from http://www.historyofinformation.com/detail.php?id=1676
34. INSTITUTO DE ESTRATEGIA. (2017, agosto 25). *Creeper, el primer virus de la hsitoria que infectó nuestros ordenadores*. Retrieved from http://www.institutodeestrategia.com/articulo/politica/creeper-primer-virus-historia/20170825164222005323.html
35. International Telecomonucations Union (ITU). (n.d.). *Global Cybersecurity Index.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
36. Isaac, M. (2019, enero 28). WhatsApp, Instagram y Facebook Messenger Juntos: el plan de Mark Zuckerberg. Retrieved from https://www.nytimes.com/es/2019/01/28/whatsapp-instagram-facebook/
37. ITU. (n.d.). *The ICT Development Index (IDI): conceptual framework and methodology*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2017/methodology.aspx
38. ITU, Naciones Unidas. (2019). *ICT Development Index- background document.* Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/IDI2019consultation/IDI_BackgroundDocument_E.pdf
39. ITUPublications. (2018). *Globalo Cybersecurity Index (GCI) 2018.* Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
40. J.X. Gabriel, L. M. (2018, Diciembre 19). Todo lo que Facebook compartió con empresas pese a prometer más privacidad. *The New York Times*. Retrieved from https://www.nytimes.com/es/2018/12/19/facebook-privacidad/
41. Judson, J. (2019, julio 16). A necessary rise: Lithuania bolsters its cybersecurity, catching the attention of other nations. Retrieved from https://www.fifthdomain.com/smr/a-modern-nato/2019/07/15/a-necessary-rise-lithuania-bolsters-its-cybersecurity-catching-the-attention-of-other-nations/
42. Lewkowicz, J. (2020, marzo 20). El FMI pide alivio de entre 55 y 85 mil millones en los próximos diez años. p. 12. Retrieved from https://www.pagina12.com.ar/254236-el-fmi-pide-alivio-de-entre-55-y-85-mil-millones-en-los-prox
43. Liao, S. (2018, junio 0). Why Facebook´s secret data-sharing deal with Huawei has the US concerned. Retrieved from https://www.theverge.com/2018/6/8/17435764/facebook-data-sharing-huawei-cybersecurity
44. Liu, Y. (n.d.). *W32.HLLW.Fizzer@mm.* Symantec. Retrieved from https://www.symantec.com/es/es/security-center/writeup/2003-050821-0316-99
45. López, A. (2017, abril 11). Elk Cloner: 35 años del primer virus informático. *TECNOXPLORA*. Retrieved from https://www.lasexta.com/tecnologia-tecnoxplora/ciencia/divulgacion/elk-cloner-anos-primer-virus-informatico_2017040758ec8a110cf2f2c8756479de.html
46. Luo Yan, Y. Z. (2019). *China Introduce Mobile Application Security Certification Scheme.* Retrieved from https://www.insideprivacy.com/international/china/china-introduces-mobile-application-security-certification-scheme/
47. MacNeil, J. (2019, noviembre 10). *The computer virus is born, November 10, 1983*. Retrieved from https://www.edn.com/electronics-blogs/edn-moments/4437117/The-computer-virus-is-born--November-10--1983
48. Magazine, U. S. (2019). Top 10 Cybersecurity Risks For 2019. *United States CYBERSECURITY Magazine*. Retrieved from https://www.uscybersecurity.net/risks-2019/
49. Mataf.net. (2019, 08 26). *Mataf.net.* Retrieved from https://www.mataf.net/es/cambio/divisas-USD-EUR

50. Mayya, R. (n.d.). *BLITZ The IT Quiz Book* (cuarta ed.). Bangalore, India: Universidad de Nueva Delhi.
51. McMullin, B. (2000). *John von Neuman and the Evolutionary Growth of Complexity: Looking Backwards, Looking Forwards.*. MIT Press. Retrieved from https://pdfs.semanticscholar.org/d26e/60138ccc3756f50676096adc38579d253073.pdf
52. Morgan, S. (2019, julio 22). China Cybersecurity Companies. *CYBERCRIME MAGAZINE*. Retrieved from https://cybersecurityventures.com/china-cybersecurity-companies/
53. Naciones Unidas. (n.d.). *UN E-Government Knowledgebase*. Retrieved from https://publicadministration.un.org/egovkb/en-us/About
54. Nexton, C. (2018, diciembre 18). Facebook gave Spotify and Netflix acces to user´s private messages. Retrieved from https://www.theverge.com/2018/12/18/18147616/facebook-user-data-giveaway-nyt-apple-amazon-spotify-netflix
55. panda. (2013, octubre 18). *Los virus más famosos de la historia: Melissa*. Retrieved from https://www.pandasecurity.com/spain/mediacenter/malware/virus-melissa/
56. PODCAST, EL COSTO DE LAS PANDEMIAS INFORMÁTICAS. (2020). *Digital TOO*. Retrieved from http://www.digitaltoo.com/2020/06/15/podcast-el-costo-de-las-pandemias-informaticas/
57. REVISTA DE LA OTAN edición digital. (n.d.). Nuevas amenazas: el ciberespacio. Retrieved from https://www.nato.int/docu/review/2011/11-september/Cyber-Threads/ES/index.htm
58. Rikk, R. (2018). *National Cyber Securuty Index 2018.* e-Governance Academy, Ministry of Foreign Affairs within Estonian Development Cooperation. Retrieved from https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf
59. Rios, X. (2020, julio 20). Huawei y el mantra de la seguridad. *Observatorio de la Política China*. Retrieved from https://politica-china.org/areas/sociedad/huawei-y-el-mantra-de-la-seguridad?utm_source=mailpoet&utm_medium=email&utm_campaign=boletin-semanal-del-opch-nonewsletter-number2019_79
60. Rodríguez, J. (2013, marzo 25). *TICSUDI0206*. Retrieved from https://ticsudi0206.wordpress.com/2013/03/25/primer-virus-informatico-gusano-morris/
61. RPP Noticias. (2016, enero 19). BRAIN, el primer virus de PC, cumple 30 años. Retrieved from https://rpp.pe/tecnologia/pc/brain-el-primer-virus-de-pc-cumple-30-anos-noticia-930895
62. RTU, C. (2019). *Deuda pública es de 55 mil millones de dólares.* Retrieved from https://www.youtube.com/watch?v=hczo_D9K6tw
63. Sanchez, L. (2018, julio 4). Cambridge Analytica says more than 87 millon could have had information breached. *THE HILL*. Retrieved from https://thehill.com/policy/technology/382116-cambridge-analytica-says-users-impacted-in-scandal-could-be-over-87-million
64. Sebenius, A. (2019, febrero 19). China Has Abandoned a Cibersecurity Truce With the U.S., Report Says. *Bloomerg*. Retrieved from https://www.bloomberg.com/news/articles/2019-02-19/china-abandons-cybersecurity-truce-with-u-s-report-says
65. Shamkland, S. (2017, noviembre 14). Facebook joins to improve online video. Retrieved from https://www.cnet.com/news/facebook-joins-effort-to-improve-online-video/
66. Silverman. (2017). *On the Day In CALIFORNIA HISTORY.* Estados Unidos: The History Press Charleston.
67. statcounter, G. (2019). *Social Media Stats Worldwide - October 2019.* Retrieved from https://gs.statcounter.com/social-media-stats
68. THE DENVER POST. (2017, diciembre 19). Trump administration blames North Korea for WannaCry ransomware atteck. Retrieved from https://www.denverpost.com/2017/12/19/north-korea-blamed-for-ransomware-attack/
69. UPC, F. (n.d.). *RETRO INFORMÁTICA, EL PASADO DE FUTURO*. Retrieved from https://www.fib.upc.edu/retro-informatica/historia/internet.html
70. Zhang, J. (2019, enero 18). China steps up push to nurture cybersecurity companies to support digitisation of economy. Retrieved from https://www.scmp.com/tech/article/2182547/beijings-cybersecurity-park-signs-10-new-firms-city-aims-us148-billion-market