Information and security in cyberspace: The influence of globalization on the intensification of risks and threats in the last decade

Informação e Segurança no Ciberespaço: A influência da globalização na intensificação de riscos e ameaças na última década *(PT: 193-212)*

Bruno Garcia*

NOVA IMS Information Management School (NOVA IMS),
Universidade Nova de Lisboa, Portugal

DOI: 10.33167/2184-0644.CPP2021.VVIIN1/pp.213-231

ABSTRACT

This article provides a brief history of information security, with emphasis on cybersecurity threats and how these are influenced by globalization. A comparative analysis of three different sources is conducted to capture some patterns about this relationship: 1) ENISA reports on cyberthreats, 2) The Global Risks Report, on global threats and the 3) DHL-Global Connectedness report for globalization indicators. To avoid dispersion, the analysis is circumscribed roughly to the last decade. This report points to an intensification of cyber threats in the last few years, while the globalization indicators suggest a slowdown in global interconnections. A number of hypotheses to explain these patterns are recommended for further research.

Keywords: Cybersecurity, Globalization, Information Security, Global Threats

RESUMO

Este artigo fornece uma breve história da segurança de informação, com ênfase nas ameaças à segurança cibernética e como estas são influenciadas pela globalização. É realizada uma análise comparativa de três fontes diferentes para captar alguns padrões sobre esta relação: 1) relatórios da ENISA sobre ameaças cibernéticas, 2) relatório global de riscos, sobre ameaças globais e 3) relatório DHL – Global Connectedness para indicadores de globalização.

Article received on 18/04/2020 and approved for publication by the Editorial Council on 24/09/2020.

* E-mail: garcia.bruno.c@gmail.com ORCID: http://orcid.org/0000-0003-1502-7567

Para evitar dispersão, a análise é circunscrita aproximadamente à última década. Este relatório aponta para uma intensificação das ameaças cibernéticas nos últimos anos, enquanto os indicadores de globalização sugerem um abrandamento nas interligações globais. São recomendadas para investigação adicional algumas hipóteses para explicar estes padrões.

Palavras-chave: Cibersegurança, globalização, segurança de informação, ameaças globais

1. Introduction

Information is a means of eliminating uncertainty (Gleick, 2011). At least since Man began organizing collectively, information is of central importance in his survival. Since prehistory, knowing where to hunt, knowing where to collect food, knowing what to cultivate and at what time, provided an overwhelming competitive advantage to some tribes and made the difference between surviving and perishing. Keeping information secure, in the sense of protecting it from undue disclosure or modification, has therefore been a latent concern of humanity since time immemorial. All the great civilizations throughout history have set up information security networks - from the ancient Roman Empire, with the Frumentarii (Gibbon, 1985), and the Chinese Empire with the Jinyiwei (Miller, 2009) to the European Renaissance courts.

This historical and perennial legacy can lead to the temptation of claiming that information security is not an original reality — it has always existed. However, globalization in general and the fast pace of technological development in particular, confer information security with a different nature from the one we have traditionally become accustomed to. Scale differences matter, often altering the intrinsic nature of phenomena, and the interdependent, interconnected and globalized world in which we live have profoundly changed the domain of security (Nunes, 2016).

It was the industrial revolution that started to integrate different world regions into a global economy. Globalization is not a modern development, but the technological advances in transportation and communications, and particularly in information systems, have significantly deepened the connections between countries, the complexity of international relations and their scope (Trade & Globalization, 2006). Here, too, differences in scale count and globalization is today a phenomenon of a different nature from its traditional meaning.

It should be noted that reflections on globalization almost always go hand in hand with technological development. It is therefore fundamental to understand in what way the existing threats in this technological arena influence or are influenced by globalization. A well-informed perspective on the way in which the patterns of interrelationship between cybersecurity and globalization indicators

are modified over time is essential for decision-making regarding public policies in this domain. For example, policy makers influence foreign investment flows through fiscal policies. They can also encourage, in a more or less ostensive way, the training of professionals technically prepared to deal with cyber threats. At the macro level, policy makers set the standards for international cooperation to combat cybercrime. The purpose of this article is precisely to outline some patterns on the way in which globalization and cyber security threats are interrelated.

It should be stressed that this work does not intend to establish a cause-and-effect relationship between the increase in cybersecurity threats and globalization, or to understand to what extent globalization has boosted the growth of the electronic network, or to what extent the network has potentiated globalization. The causal relationship is likely to be bidirectional. The existence of intermediary factors mediating this relationship surround it in a complexity that is not intended to be explored here.

To achieve the defined purpose, the next section will be devoted to sketching a recent history of information security up to the present day and the section following that one is dedicated to a specific case study — the impact of NotPetya malware on Maersk and on global supply chains. These two sections will enable the demarcation of current globalization and the domain of information security in particular as essentially new phenomena, emphasizing the global character of information networks and of the threats that underlie them.

In the subsequent section, a comparative analysis will be carried out between cybersecurity reports issued by the European Union Agency for Cybersecurity (ENISA), the reports designated by The Global Risks Report of the World Economic Forum and finally, as a barometer of globalization, the DHL – Global Connectedness report. In order to not overload the article, the analysis will be limited to the last ten years. Finally, an attempt will be made to establish some general patterns in the relationship between globalization and cybersecurity threats.

2. Information security: a historical outline

The most recent historical background that led to the modern meaning of information security is outlined in very general terms below.

In World War II, the success of the first computers used to decode German communications made evident the potential of these machines for the storage of information and resolution of complex problems. Soon after the war, some governments invested in the development of computer technology — the first mainframes appeared: large computers dedicated to critical processes or to storing large sets of data. At that stage, the security of these assets was of a physical nature: the concern was to keep protected those places where these large computers were

housed. It was also advantageous to transport information between mainframes, however doing so was costly and inefficient. At the same time, the cold war climate stressed the need for redundancy between critical systems. These difficulties would only be overcome if somehow these mainframes communicated with each other automatically. In the second half of the 1950s, the American Department of Defense created the Advanced Research Project Agency (ARPA) specifically to address this problem. By the late sixties it had become obvious that this group, concertedly with other groups originating from academic, scientific and corporate circles had reached a solution — ARPANET was born: two computers in different Californian universities had established communication with each other. Over the next few years, these connections increased, with nodes being added to the network. At this point, reports emerged about the vulnerabilities of this network; it started to become evident that the security of these assets transcended physical defense —the first security protocols and incipient mechanisms of logical security appeared (Yost, 2007). In the early 1970s, an experimental program also appeared, designed to be transported between operating systems, that was then improved to create a copy of itself. This program, named CREEPER by its creator, was recognized as the first computer virus. Note that this program had no malicious effect, triggering only one message to the user — but the disruptive potential of this type of program was obvious (DeNardis, L., 2007).

In the late seventies, companies such as Microsoft (in software conception), IBM, (mainly in the production of hardware) and Apple (in the development of software and hardware), created the conditions that made it possible to bring a computer to every person's home at a reasonable price — the personal computer is born. The decentralization of electronic information takes place: large mainframes continue to be the critical assets, but part of the information is also directly available on each local device, giving rise to the architecture that became known as client-server.

The basic principle of these computer communication networks was that messages can be fragmented, sent via a network in a series of transmissions and then reassembled at the destination quickly and efficiently. To make this possible, a protocol, or set of rules, was applied that allow computers to work together. Different networks had different protocols, which made communication between them impossible. This challenge was also overcome by ARPA (now renamed DARPA, Defense Advanced Research Project Agency) whose scientists developed the TCP/IP protocol that made communication possible between virtually any computer network, regardless of the hardware, software or language used. With the implementation of this protocol in 1983, the Internet, or network of interconnected networks, was consolidated. For some time, the project of creating TCP/IP in-

volved the implementation of encryption mechanisms, or the practice of encoding messages so that only the intended recipient can decode them, using a mathematical key. But this process was costly, requiring more computational power and specific hardware. At this time, it was also unclear how to distribute encryption keys securely, a problem that still complicates encryption systems today. Faced with these insurmountable barriers, the focus of the scientists involved continued to be the technical challenge of moving information quickly and reliably. The outlook with regard to security was that the central risks of the Internet had to do with military threats, or intruders external to the network, but few foresaw that the network's own users could use it to attack other users, even though there were some warnings. Soon afterwards, the first cyberattacks in the contemporary sense of the term appeared, typically referred to as hacking — attacks triggered remotely that use the computer network to intrusively obtain information or otherwise corrupt a system today (DeNardis, L., 2007). One of the most famous cases in the 80s was the First National Bank of Chicago attack that allegedly led to the theft of seventy million dollars.

In its conception, the Internet proves to be essentially fast, effective, frictionless, but also permeable and vulnerable. These elements are essential to take in the framework in which information security and its challenges are developed.

In the late 80s, another major change occurs: the Internet opens up to the general public with the creation of the World Wide Web. There is a cleaving in the terms of interaction between parties that may go unnoticed: with this change the relationship of trust is altered — a type of communication takes place where the parties do not necessarily know the entity that is on the other side. Personal data becomes available on the Internet. Organized crime networks are attentive and are start looking for ways to exploit this information. Meanwhile, during the nineties, online commerce emerges, which quickly assumes impressive proportions, generating companies and business models entirely oriented towards electronic transactions. The network explodes, continuously expanding until the present day (DeNardis, L., 2007).

As the perimeter of network security widens, traditional computer threats take a leap in sophistication and at the same time a whole range of new concepts emerge. We are faced with a new jargon: malware — malicious software to corrupt a system, adware — software installed to trigger targeted but not necessarily solicited online advertising, spyware — specific software to monitor our online behavior, ransomware — software that can block access to information (through some encryption mechanism that is also an increasingly evolving discipline) and that can be unblocked in exchange for a ransom, typically paid in cryptocurrency; Phishing, a social engineering technique, which in practice is a disguised mecha-

nism to get victims to behave online in a way they normally would not — either by providing personal data, or providing access credentials to systems with sensitive information (Kim , D., & Solomon, M. G., 2016). These are just a few examples of the terms currently in vogue.

The dissemination of this networked communication technology is based on the propagation of the physical infrastructure that supports it. We tend to think of the internet as an organism suspended in the ether, but it is surprising to note that this organism actually has a body: hundreds of thousands of kilometers of cables, running along roads and railway lines, communications towers, satellites and large buildings, called network exchanges, which are in practice major points of contact within the network (Blum, 2012). The transnational character of these physical structures is also one of the factors that characterize the internet as a component of the globalized world.

In response to the combined increase in the security perimeter, the complexity of the systems and their reach, structured regulations for data protection emerge — the most prominent and current example of this being the General Data Protection Regulation. The discipline of Information Security becomes a domain structured by multiple layers: people protection layer, hardware protection layer, software protection layer, data protection layer, process protection layer and network protection layer. The distinctions are sometimes vague, but it is common to separate cybersecurity from information security more broadly, by the layers of security over their sphere of action — cybersecurity essentially covers the security of software, data and network layers, and partially of hardware (Kim, D., & Solomon, M. G., 2016).

In order to give shape to the threats and concepts of information security listed here and highlight their relationship with the globalized world, let us briefly analyze the ransomware incident (the aforementioned fraudulent ransomware of computer systems) that hit Maersk in 2017.

3. The globalization of threats in cyberspace: the Maersk case

Maersk is a colossal company with eight business units, which include the management of approximately eighty ports, logistics, shipbuilding and oil exploration. With 574 offices operating in about 130 countries, Maersk is a symbol, par excellence, of the global corporation. In June of 2017, a group of employees of this company in the Copenhagen offices detected an unusual behavior on their computers - messages appeared on their screens that announced: "C file system: under repair", with a warning not to turn off the computer. In others it read: "Ooops, your important files have been encrypted" (Greenberg, 2019).

The context of this attack is imminently geopolitical. More precisely, its origin goes back to the conflict between Russia and Ukraine in the five years prior to the attack. This conflict, initiated by Russia's aggression against Ukraine, specifically the takeover of the Crimean Peninsula, is said to have triggered the biggest security crisis in Europe since the Cold War. Several states intervened to sanction Russia, but little was achieved in the way of restoring territorial integrity in Ukraine (Stanovaya, 2019). In geopolitics, as in history, there are no single causes. This conflict is complex and scrutinizing its nature will not fit in this article. Only a close cause will be emphasized: Ukraine was a central element of power in the former Soviet Union, having been the second most populous and powerful of the fifteen Soviet republics, and was also a territory seen as the "granary" of the Union because of its weight in agricultural production; it also held much industry in the areas of defense and military, including the Black Sea fleet and some nuclear arsenal. After the fall of the Soviet Union, Ukraine sought to become closer with the West, namely the European Union and NATO; which is contrary to the growing pretensions of hegemony in the region by the Russian leadership. By taking Crimea, Russia consolidates its control of the Black Sea. With a military presence in this area, Russia will be able to project influence to the Mediterranean region, the Middle East and North Africa. At the same time, energy and military alliances are strengthened with Turkey, the other major power of the Black Sea (Stanovaya, 2019; Ramírez & Telman, 2016).

In parallel, a group of hackers linked to the Kremlin, known as Sandworm, had launched a number of successful attacks on other countries, including the USA. This group had become one of the most prominent facets of Russia's cyber-attack potential. With the prolonging of the conflict between Ukraine and Russia, Ukraine had become in practice a test laboratory for Russian capabilities in the cyber arena (Greenberg, 2019).

In the spring of 2017 this group had managed to penetrate a system hosted on Linkos Group servers. This small Ukrainian company hosted the update servers — with bug fixes, security remedies and new features — for an accounting software called M.E.Doc. This was the most commonly used software for submitting tax information, and was present in most companies in Ukraine. We do not intend here to anatomize this attack with technical details, we wish only to stress that in practice the attackers had managed to find a gateway to all the computers that had installed M.E.Doc. Taking advantage of this gateway, in June they unleashed the ransomware campaign through a piece of malicious code called NotPetya. The attack was overwhelming, hitting several entities and companies in Ukraine, namely some of the largest banks, two airports, hospitals, energy companies and various payment systems. It is pertinent to point out that numerous entities paid

the ransom — to no effect. By this time, the IT team at Maersk's office in the Ukrainian city of Odessa had installed M.E. Doc on a single computer — it was enough to inexorably compromise much of the company's interconnected IT infrastructure.

The impact was devastating. The software for Maersk's ships was unaffected, but the software at the port terminals — designed to automatically update data on goods transported and expected at the ports — stopped working, making the complex management of the loading and unloading of containers impossible. In seventeen of the nearly eighty ports managed by Maersk, there were queues of trucks waiting for instructions. Let's look at just a few examples of the extent of this impact: Merck, a major pharmaceutical company, was temporarily unable to produce new drugs, TNT Express was unable to ship or receive orders, the construction company Saint-Gobain ran out of raw materials. All of these companies incurred financial losses amounting to millions of euros. Numerous companies that depended on immediate and timely delivery of products were affected.

The recovery from this disaster was heavy and time-consuming, involving at the technical level the recovery of security copies (backups) of all the electronic information contained in Maersk's servers prior to the attack. One technical aspect in particular illustrates the scale of the problem: there is a critical layer in the organizational IT infrastructure corresponding to a type of server called a domain controller. These servers provide a detailed map of an organization's computer network and incorporate the elementary rules that determine which systems users can access. Maersk had about 150 domain controllers programmed to synchronize information, precisely in a logic of redundancy. But this configuration did not foresee a scenario in which all these servers were corrupted at the same time. Without these servers, it would be difficult to recover other components of the network. The computer technicians were able to detect an uncorrupted domain controller — due to a fortuitous power outage — at Maersk's site in Ghana and perform the laborious task of copying the information on this server to other data centers. It took the company two weeks to stabilize its network enough to reconnect workstations — on "clean" computers — and months to stabilize its operations. The disaster exposed flaws in the company's security policies, highlighting the use of outdated software, failure to fix vulnerabilities in various systems; the failure to update operating systems and failure to use multiple authentication access mechanisms in critical systems. The costs incurred by Maersk, which include payment of compensation to clients, are difficult to measure.

The intent of the attack is not entirely clear. Greenberg (2019) speculates that this operation allowed for the sweeping of traces of espionage or future sabotage plans from the network while simultaneously leaving a warning: any company

maintaining operations in Ukrainian territory may incur heavy costs. It is also possible that its global impact was not anticipated by the attackers themselves — it has even spread to some Russian companies, of note the state-owned energy company, Rosneft.

Regardless of its intent, this case unveils an unavoidable reality: it is now possible for a nation or group to mobilize a weapon in an arena where there are no borders, where distance truly does not matter. An attack on a small company in Ukraine hit Maersk and thereby much of the commercial world. Underlying this attack is a very specific causal logic of the cyberspace domain.

In the next section, some cybersecurity reports, global threat reports and globalization indicators will be compared in order to establish some patterns between globalization and cybersecurity threats in the final section.

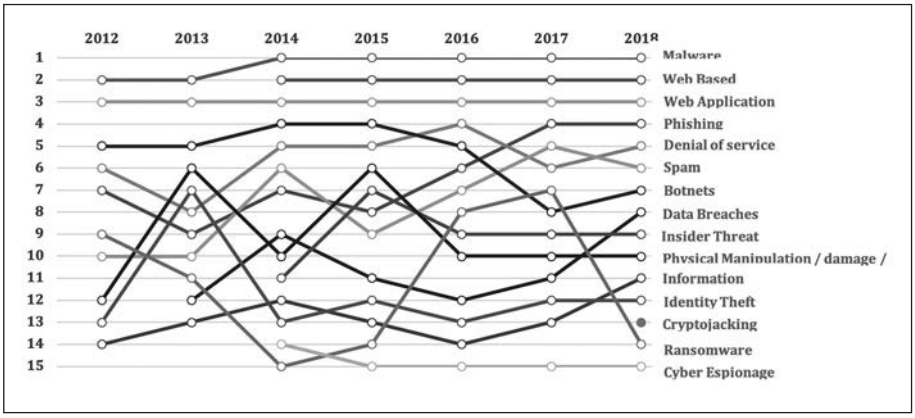
4. Analysis of cybersecurity reports, global threat reports and globalization indicators

In this section, three sources of information will be compared in order to identify some patterns in the relationship between cybersecurity threats and globalization.

The first source of information are the ENISA Threat Landscape reports regarding cybersecurity threats in the European space (ENISA, 2019)[1]. This source is selected primarily because it is one of the bases for developing public policies in the area of cybersecurity among European Union member states. The information gathered for these reports comes from three sources: a) the MISP, an open platform for the sharing of malware information funded by the European Union, b) the CERT-EU, Computer Emergency Response Team for the European Union institutions and c) the portal of the company Cyjax, a company specializing in digital threats intelligence services.

The seven published editions of this report show an ordered list of the top 15 cybersecurity threats for the period under review. Graph 1 shows the relative positions of the cybersecurity threats from 2012 to 2018, with reference to the previous year's ranking.

1. The reference included in the bibliography corresponds to the most recent report, so as not to overload this section. In practice, the same address made it possible to consult all editions of the report.



GRAPH 1. Top 15 cybersecurity threats from 2012 to 2018, with reference to the 2018 ranking, from each year's *ENISA Threat Landscape* reports

The following briefly describes each threat, in the order presented in the 2018 ranking. Due to its widespread nature in the jargon of the information security field, we have decided to keep the original Anglophone designation. (1) Malware is the designation given to malicious software — note that this designation is explicitly included only in 2014; in previous editions, this category was more specific, with the designation of Viruses (which spread by parasitizing other files) and Worms (similar to viruses, but potentially more destructive because they do not need to parasitize other files); (2) Web based attacks are attacks that use electronic network systems and services as the primary means or arena to compromise the target; (3) Web application attacks are the direct or indirect attempts to exploit a vulnerability in web services or applications; (4) Phishing, already mentioned in a previous section, is an electronic social engineering mechanism; (5) Denial of service (DoS) is a threat of great impact, in which attackers essentially seek to deny access or to interrupt a certain system or application; (6) Spam, corresponds to the abusive use of email or messaging technologies to flood users with unsolicited information; (7) Botnets, corresponds to a network of robots or interconnected devices on the web that can be used together for denial of service (Distributed Denial of Service – DDoS), Spam or information theft; (8) Data breaches or data compromise corresponds to a successful malicious attack attempt, which led to the compromise or loss of information; (9) Insider threat, or internal threat, which can mean internal regarding an entity, organization and company and corresponds to the threat represented by the possibility of individuals intentionally or unintentionally abusing access to digital assets; (10) Physical manipulation/damage/theft/

loss, while not exactly a cybersecurity threat, even so allows for the compromise of digital assets and may lead to information losses; (11) Information Leakage or Data Leakage can encompass personal data collected by companies operating on the Web, or corporate data stored in IT infrastructures exposed in an undesired way; (12) Identity theft or appropriation of identity corresponds to fraud resulting from the theft of personal information and enabled by the massive digitalization of personal data; (13) Cryptojacking, also known as cryptomining, refers to programs that misuse the processing capacity of a given target, for verification and validation processes of cryptocurrency transactions — very computationally demanding processes; (14) Ransomware, or illegal ransom of digital systems, was detailed in the previous section — the attacker takes control over files or devices and blocks access from its legitimate guardian; to release control, a cryptocurrency ransom is typically requested and finally (15) Cyberespionage, whether corporate or leveraged by nation-states, a category that has gained prominence, and which corresponds to a generic class of techniques applied in order to exercise geopolitical influence, or to steal commercial and state information or to steal intellectual property, particularly in strategic domains.

Note that some of the categories listed are interconnected or are very dependent of each other. ENISA itself has made adjustments to the categories over time. As an example, the category of ransomware appeared only in 2014, wherein previously there was a category with the designation of rogueware or scareware. To guarantee comparative continuity, in the graph we have chosen to consider these categories equivalent, hence the ransomware line extends back to 2012. The malware category also appears in 2014, whereas previously it included the more specific designations of Virus and Worm — here too we have chosen to consider these categories equivalent, which explains the line right from 2012. On the other hand, the category of Web based attacks replaced at least one category of a slightly different specificity — drive-by exploits (corresponding to the occurrence of infection of a system resulting from visiting a malicious internet site) — in this case we opted for a break in the series, assuming that the threat only appears in 2014 among the top 15 threats.

These caveats aside, it is possible to draw some general patterns. The categories in the top three positions are fundamentally the same over the last decade: malware, Web-based attacks and Web application attacks, which is revealing of the broad character of these categories — they are a sort of a macro category in relation to others. The ransomware category shows the most variable behavior in these rankings, which is likely related to the disruptive nature of this threat in the years when successful attacks occur (Wannacry and Not-Petya in 2017). The categories related to Data Breaches and Identity Theft show some alignment with each

other, in different positions of the ranking, which highlights the interdependence between these categories — the loss of personal information will allow for the appropriation of identity. It is also worth noting the appearance of new categories in 2014, such as insider threat, as a specific category, and also cyberespionage, coinciding with the moment in which the first major attacks promoted by nations gained media visibility — neither category shows signs of being removed from the list of most prominent threats. Also visible in the graph and pointed out in the conclusions of the last report, email and Phishing have consolidated themselves as the main mechanism or initial vector of infection (in the fourth position in the last year). Finally, the need to nimbly convert assets into cash introduced a new threat in the last year analyzed, Cryptojacking, which in practice allows for the leveraging of computer resources to generate cryptocurrency, often used to cover up payments in illicit activities such as ransomware.

One of the sources for probing wider-reaching threats are the Global Risk reports, promoted by the World Economic Forum (World Economic Forum, 2019[2]), which include risk categories more directly related to globalization dynamics. These reports are prepared annually based on surveys of hundreds of experts in different fields and threats are ranked according to impact and probability of occurrence — with risk usually measured as the product between impact and probability. Based on the last ten editions of this report, as a next step we propose to analyze the position of technological threats related to information security hold among global threats. It must be noted that, since 2012, these reports include three categories associated with information security — a) cybersecurity, b) fraud and data theft and c) collapse of critical information infrastructure — there is another category in the field of technology, designated as risks arising from technological advances — too generic to be included in the group of information security risks within the meaning of the present article. The Global Risks Report includes another 26 risk categories, in domains such as Economy, Geopolitics and the Environment.

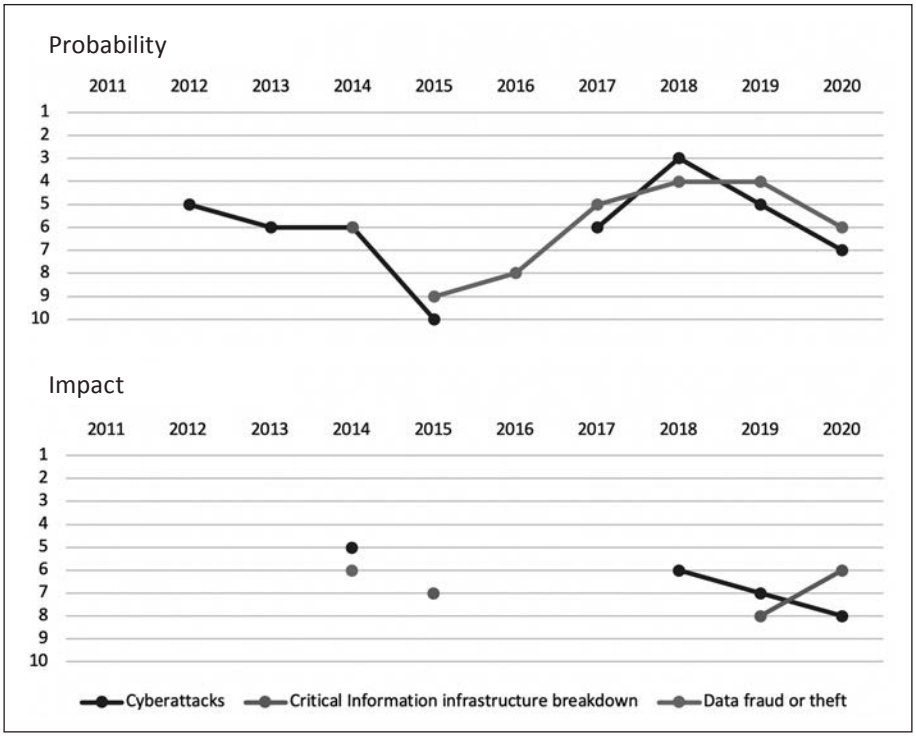
Precisely, Graph 2 shows the positioning of the categories directly related to information security risks in the ordered list of the top ten risks, in terms of impact and probability, over the last decade.

The first fact to point out from observing the graph is that in 2011 there were no information security threats registered within the top ten global threats. In this edition, the report did not include the categories of cybersecurity and data fraud, but it already included the category of collapse of critical information infrastruc-

2. In this context, not all reports are available on the same website, so two separate references are included in the bibliography. In practice, all reports since 2011 have been consulted.

tures and a category that has since been discontinued — Information security and online data. It is curious to note that in this 2011 edition specific cybersecurity risks were highlighted in a separate section, as risks to be monitored — essentially due to a lack of consensus among experts regarding confidence levels or great disparity in assessing impact and probability for these risk categories. The specific categories of cybersecurity and data fraud emerge only as of 2012.

Looking specifically at the axis of probability of occurrence over the last decade, the risk of cybersecurity stands out in terms of probability of occurrence as of 2012 — only in 2015 and 2016 does it not appear in the top 10 list. On the other hand, the risk of data fraud or data theft appears in the list of the top ten risks in terms of probability of occurrence from 2015 and remains on the list of top risks until the most recent edition. Note that as of 2017, there are two risks associated with information security in the top ten positions in terms of probability.



GRAPH2. Positioning of categories directly related to information security risks in the ranking of the top ten risks in dimensions of impact and probability

Source: World Economic Forum.

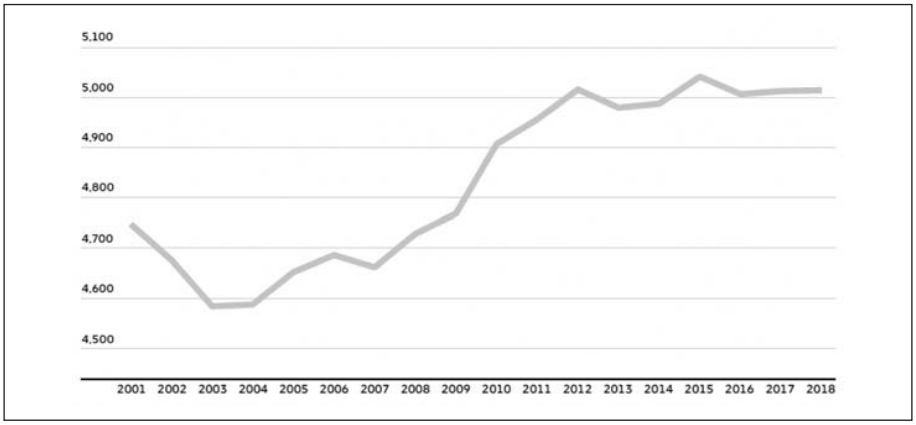
In terms of impact, information security risks appear only occasionally, in different categories, in 2014 and 2015, but as of 2018 the cybersecurity risk emerges among the top 10 and the following year the risk of collapse of critical information infrastructure also appears.

Finally, we highlight a report that seeks to measure the degree of global interconnections, the DHL Global Connectedness Report (hereinafter designated simply as DHL-GCR) by Pankaj Ghemawat, Steven Altman and Phillip Bastian (DHL, 2019). In practice, these authors produce a globalization index based on four major dimensions: capital flows, trade flows, information flows, and migratory flows. Below is a sample of some of the indicators used in these dimensions, obtained from official entities: foreign direct investment flows between countries, number of tourists between countries, internet traffic between countries, number of foreign university students, number of foreign residents. In this report there is a concern with weighting each indicator with explicit criteria and a use of relative, rather than absolute, metrics. The report's methodological approach is detailed in section VI of the report. Regardless of the methodological rigor underlying the preparation of the report, it is important to emphasize that measuring a reality as complex as globalization is not without its challenges that are difficult to overcome. The authors recognize, for example, the difficulty in measuring information flows. In a broader sense, the reduction of the concept of globalization to a set of general indicators will lead to the loss of relevant information to capture fundamental elements of this phenomenon. Nevertheless, bearing in mind that these indicators only partially capture the dynamics of globalization, it is possible to identify some patterns of interest for the purpose of this article.

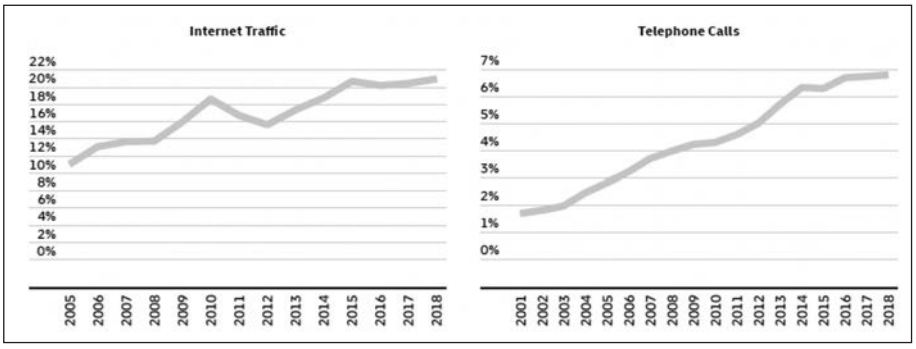
As a way of measuring trade dynamics, the DHL-GCR report presents a graph with the average distance traveled by goods at a global level since 2001. After a fall following 2001 and until 2003, this indicator has shown a progressive increase — but it is also noticeable that from 2012 it will have reached a plateau without, however, showing signs of a subsequent drop.

Another interesting indicator, shown in Graph 4, is concerned with information flows — namely the proportion of international internet traffic and the proportion of international calls (including VoIP). In the case of the internet, a pattern of growth is visible, broken between 2010 and 2012, then accentuating up to 2015, whereby from this stage on, the indicator stabilizes at around 20%. With regard to telephone calls, this indicator shows a continued increase up until 2014, at which time it decelerates and begins to stabilize near 7% in 2018.

The DHL-GCR includes the results of a survey of 6035 company managers in three advanced economies (Germany, the United Kingdom and the United States) and three emerging economies (Brazil, China and India) that allows us to glimpse



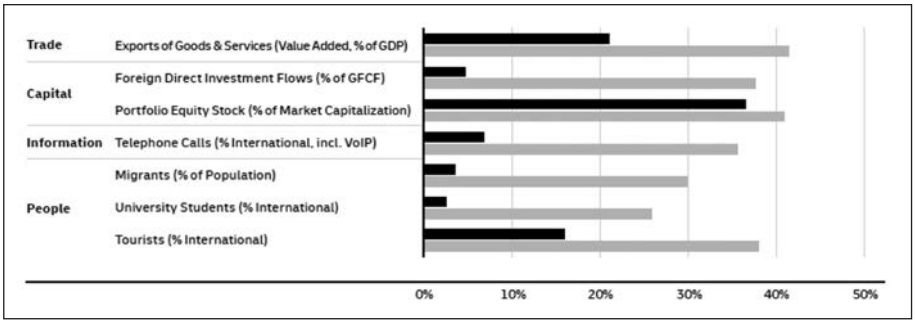
GRAPH 3. Average distance traveled by goods (in km), 2001-2018
Sources: IMF Direction of Trade Statistics (DOTS); UN Comtrade and CEPII GeoDist database.



GRAPH 4. Information trends: Percentage of international internet traffic (2005-2018) and Percentage of telephone calls traffic (2001-2018)

a third trend that is interesting to emphasize. This trend is represented in Graph 5, which compares the actual values of some of the globalization indicators with the respondents' perceptions with regard to these same indicators. Looking at the graph, it becomes immediately obvious that these managers significantly overestimate all measures of global interconnection. This result indicates that people do not properly estimate the limits of globalization and tend to consider that the world is more interconnected than it actually is. Take, for example, the indicator analyzed above which focuses on telephone call traffic — on average, the managers surveyed assume that 35% of traffic is international, but the actual estimated value for this metric is around 7%.

Based on the analysis of these results, in the next section some patterns of influence between globalization and cyber security threats will be proposed.



GRAPH 5. Measures of globalization VS Perceptions of managers (black line: Estimated actual result; gray line: value perceived by managers from 6 countries)

5. Analysis of the patterns of influence between globalization and cybersecurity threats

By analyzing the reports shown in the previous section, we are able to highlight three major patterns, one in each report: (1) In the specific context of security threats, there is to note the emancipation of the category of cyberespionage in the top ten threats, closely associated with major attacks promoted by nation-states, and also cryptojacking, which indicates an growing need to monetize assets illicitly; (2) Information security threats have gained prominence in recent years in the global threats analysis framework — with two categories of information security threats appearing in the top 10 in recent years, both in terms of impact and probability; and (3) Some of the global interconnectedness indicators, while not showing signs of decrease, show a slowing trend in recent years and are perceived to be more intense (at least among administrative boards) than they really are.

Never before have cybersecurity issues dominated the media as much as they do today. Cases such as the Cambridge Analytica consultancy scandal, in which millions of personal records from Facebook were used without consent to influence voting intentions, exacerbate fears of manipulation and loss of privacy (Cadwalladr & Graham-Harrison, 2018). Senior government officials frequently mention cyberspace as an arena of opportunities and threats. Major world powers have developed sophisticated devices for gathering and analyzing information on a global scale, shielding themselves in the need to ensure their national security and defense (Nunes, 2016).

Cyberspace threats are not easy to define and often appear as part of the menu of hybrid threats, that is to say, threats by adversaries who use both conventional and unconventional means to pursue their goals adaptively. The list of technologies explored in cyberspace continues to grow: in addition to servers, personal computers, and laptops, we must also consider smartphones, smart metering devices (e.g., electricity consumption meters); wireless pacemakers; electronic industrial control systems, etc. Managing this complexity has generated calls for internet governance, which refers to the involvement of the private sector and civil society, in their respective roles, in the application of shared principles, standards and rules, as well as decision-making procedures and programs that shape the evolution and use of the internet. However, it is important to note that there is no single state, organization, or institution with the capacity to autonomously govern the internet. Internet governance is embedded in the myriad infrastructures, devices, data flows, and technical architectures that — discretely, sometimes invisibly — underlie and build the increasingly articulated network of networks (Bachman, 2012). Also, from this perspective, globalization provides the background for the evolution of the Internet. It is also from this perspective that the influences between threats in cyberspace and indicators of globalization deserve attention.

On the other hand, the fears inherent to globalization are also known — to its critics, globalization has no philosophical basis and is merely a modern form of economic and cultural colonialism that uses intellectual property laws to impose itself in fundamental areas such as food production or health (Stiglitz, 2002). However, the predictions that globalization would collapse under the weight of economic nationalisms have proven to be as misguided as the proclamations of a flat world — based on the notion of an increasingly balanced competitive sphere between countries — that dominated political discourse a decade ago (Ghemawat & Altman, 2019).

Billions of people use information and communication technologies to conduct their businesses, to interact with each other and with governments. A high proportion of these people have only recently stepped into this digital realm. If policy makers assume an inexorable relationship between cybersecurity threats and the intensity of globalization, policy solutions will be different from those that assume the possibility of building a more secure and trusted cyberspace. These solutions may involve developing, at the international level, rules of behavior in cyberspace that are able to reduce threats, increase trust, and support improved security in the cyber ecosystem. An accurate interpretation of cyber threats and of their relationship to other global threats will enable the design of more resilient disaster recovery plans.

6. Concluding remarks

A counterintuitive element emerges from the analysis made in this article: the intensification of cybersecurity threats appears to come at a time when the dynamics of global interconnectedness seem to be slowing down — a trend that will eventually become more pronounced in the aftermath of the current Covid-19 pandemic context. While fears of globalization and cybersecurity threats seem to go hand in hand in the public debate, their practical reality seems out of sync.

Will cybersecurity threats decrease the dynamics of global interconnectedness? Or is it that globalization is stagnating except in the specific field of technological innovation? It is likely, but the data in this report do not provide sufficient data to answer these hypotheses. However, it is clear that cyberattacks are now a disruptive factor in themselves and are no longer triggered solely as a support mechanism for conventional attacks. The relationship between globalization patterns and cybersecurity threats and the consequent impact on public policies deserve further investigation.

References

Bachmann, S. D. (2012). Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats – mapping the new frontier of global risk and security management. *Amicus Curiae, 88*.

Blum, A. (2012). *Tubes: A Journey to the Center of the Internet.* New York: Ecco.

Cadwalladr, C., & Graham-Harrison, E. (2018). The Cambridge Analytica files. *The Guardian*, *21*, 6-7.

DeNardis, L. (2007) A History of internet security In de Leeuw, K. M. M., & Bergstra, J. (Eds.). *The history of information security: a comprehensive handbook*. (pp. 595-621). Elsevier Science.

DHL (2019). *DHL Global Connectedness Index*. Retrieved from <https://www.dhl.com/content/dam/dhl/global/core/documents/pdf/go-en-gci-2019-update-complete-study.pdf>.

ENISA (2019). *ENISA Threat Landscape Report*. Retrieved from <https://www.weforum.org/reports/the-global-risks-report-2020>.

Ghemawat, P., & Altman, S. A. (2019). The State of Globalization in 2019, and What It Means for Strategists. *Harvard Business Review.*

Gibbon, E. (1985). *The decline and fall of the Roman Empire: an abridged version*. Penguin Books.

Gleick, J. (2011). *The information: A history, a theory, a flood*. New York, NY, US: Pantheon Books.

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York, NY, US: Doubleday.

Joseph. E. Stiglitz. (2002). *Globalization and its discontents*. Penguin Books.

Kim, D., & Solomon, M. G. (2016). *Fundamentals of information systems security*. Burllington, MA, US: Jones & Bartlett Learning.

Miller, H. (2009). The Wanli Emperor, 1596–1606. In *State versus Gentry in Late Ming Dynasty China, 1572–1644* (pp. 75-94). New York: Palgrave Macmillan.

Nunes, P.F..(2016). Ciberameaças e quadro legal dos conflitos no ciberespaço In Borges, J. V., & Rodrigues, T. F. (Eds). *Ameaças e Riscos transnacionais no novo Mundo Global*. (pp. 199-216). Porto: Fronteira do Caos.

Ramírez, S. Telman, P. (2016). The conflict in Ukraine: The first serious confrontation between Russia and the West in the post-cold war age. *Foro internacional*, *56*(2), pp. 470-502. Retrieved from <http://www.scielo.org.mx/scielo.php?script =sci_arttext&pid=S0185-013X2016000200470&lng=es&tlng=en>.

Stanovaya, T. (2019, December 6). *What the West gets Wrong about Russias intentions in Ukraine.* Retrieved from <https://foreignpolicy.com/2019/12/06/what-the-west-gets-wrong-about-russias-intentions-in-ukraine/>.

Trade & Globalization (2006) *Chambers Dictionary of World History*. Chambers.

World Economic Forum (2015). *The global Risks Report 2016* Retrieved from <http://www3.weforum.org/docs/GRR/WEF_GRR16.pdf>.

World Economic Forum (2019). *The global Risks Report*. Retrieved from <https://www.weforum.org/reports/the-global-risks-report-2020>.

Yost, R. (2007) A History of computer security standards In de Leeuw, K. M. M., & Bergstra, J. (Eds.). *The history of information security: a comprehensive handbook*. (pp. 595-621) Elsevier Science.