Original: **Spanish**

www.cepal.org/transporte

number 7 / 2019 / ISSN: 1564-4227

FAL

BULLETIN 375

FACILITATION OF TRANSPORT AND TRADE IN LATIN AMERICA AND THE CARIBBEAN

Industry 4.0 and the emergence of Logistics 4.0

Background

The fourth industrial revolution is bringing about a series of disruptive changes in both business models and the production chains that support them. Logistics, which is a fundamental element of these processes, is inevitably affected by these significant changes. This fourth industrial revolution is characterized by its speed, magnitude and depth. The changes are so dramatic that they will alter the way we live, work and relate to one other (Schwab, 2016), affecting countries, companies, industries and society as a whole. Therefore, the logistics system of the future must aim for interconnected information and optimized time and resources, with significant investment in innovation and development to maintain competitiveness (Pérez and Sánchez, 2019).

This *FAL Bulletin* presents the opportunities and challenges facing the region in the light of the emergence of Logistics 4.0, deriving from the incorporation of a series of disruptive technologies into the production sector that gave rise to Industry 4.0.

The authors are Eliana P. Barleta, consultant, and Gabriel Pérez and Ricardo J. Sánchez, both Economic Affairs Officers in the Infrastructure Services Unit of ECLAC. Patricia Izarra also contributed to a preliminary version of the document.

UNITED NATIONS
ECLAC

70 ECLAC FOR SUSTAINABLE DEVELOPMENT WITH EQUALITY

In the next few years, the digitalization of a number of processes and the widespread growth of technologies such as the blockchain, the Internet of Things (IoT), augmented reality and artificial intelligence (AI) are expected to bring about paradigmatic changes in the logistics sector and international transport, creating new opportunities for those who are able to leverage these technologies and generating widening gaps with sectors that fail to adapt to the new context in a timely fashion.

With regard to logistics in Latin America and the Caribbean, the challenge is even bigger given the region's heterogeneity. As in other moments of the region's history in transport, some production sectors and infrastructure associated with international trade, for example large ports and airports serving as cargo hubs, will be able to access cutting-edge technology and will demand logistics services capable of adapting to this hyperconnected environment. However, at the same time, a large share of the more traditional production sectors, especially small and medium-sized enterprises (SMEs), will continue to operate under the traditional logistics system. This difference implies a technological and regulatory challenge for the State, which will have to provide services and facilitate processes for those operating in a Logistics 4.0 environment as well as those continuing to operate under the traditional system. The speed with which the two converge will be crucial to fully leverage the potential harboured in these changes and to prevent technology from becoming a barrier to entry into some markets or worsening the current concentration in international logistics.

This *FAL Bulletin* provides a preliminary assessment (which will be developed further in a later publication) of the technologies that are able to bring about disruptive changes in logistics, their potential impacts on industry and the challenges they pose for appropriate regulation and competition in global markets. The first and second sections of this document provide some background on the emergence of Logistics 4.0, and describe some of the technologies with the most disruptive effects on trade logistics. Part three analyses the particular situation of the region, with special emphasis on the detection of possible barriers to entry that could arise from the introduction of these technologies in some markets and the regulatory changes needed to avoid them. Part four provides details of some standards and the systematization of international best practices related to the adoption of technology and logistics. Lastly, part five presents a set of recommendations to ensure suitable convergence of traditional logistics and Logistics 4.0, including the interoperability of systems associated with production and trade.

I. The emergence of Logistics 4.0

The digitalization of business processes began in the 1960s with the first efforts to foster electronic data interchange (EDI).[1] These processes grew more complex over time, with new applications and the integration of technologies that improved the flow, speed, reliability and security of the information exchanged. The management and exchange of data among participants in the logistics chain is proving a key source of innovation and insight into customers' needs, contributing to the design of value-added services (Pérez and Sánchez, 2019).

Applications must therefore be seen as a technological filament that connects and feeds an increasingly complex and extensive logistics chain, increasing participants' competitiveness and maximizing the productivity of available infrastructure and services (Pérez, 2012). These technological applications combine and coordinate different information control, transmission and processing technologies to improve the efficiency, security and sustainability of infrastructure services, generating opportunities for distinctive value-added services and reducing negative social and environmental externalities (Pérez and Sánchez, 2019).

Now, in the midst of the fourth industrial revolution, the foreign trade business model is changing once again, placing emphasis on the quality of services, with continuous information management and increasingly indistinct borders between both actors and countries, which enables real-time supply chain management.

A disruptive technology is an innovation that creates a new market or considerably transforms an existing market, displacing or eliminating products or services that had been used by society on a daily basis previously. This type of disruptive innovation tends to be produced by outsiders and entrepreneurs arriving on the market, rather than existing market-leading companies (Voege, 2019).

A series of technologies, such as the blockchain, the IoT and big data, are driving the fourth industrial revolution by interweaving and producing disruptive changes in the corporate sector with a view to increasing operating efficiency, providing the flexibility needed to adapt production rapidly to changes in demand and reducing associated costs and negative externalities. Logistics 4.0, which provides services for the fourth industrial revolution, is characterized by the optimization of time and resources, chain traceability, security and integrity of data and suitable interoperability between different human and digital actors. This digital ecosystem also favours innovation and the creation of new knowledge-based services and business models that foster more socially and environmentally sustainable trade.

Cooperation between the agents of the supply chain and better visibility and traceability of the entire logistics chain facilitates real-time management of cargo flows and better use of infrastructure and of available human and technological resources. The availability of large volumes of information in real time benefits evidence-based decision-making, thereby increasing operating efficiency, improvements in associated costs and services, and economic productivity, as shown in diagram 1.

The technological changes that pave the way for new types of knowledge-based logistics services are mainly supported by the integration of services and systems to manage and optimize changes in demand or available infrastructure in real time, which cuts costs and transit times and improves the customer delivery experience. According to Drewry (2019), disruptive technologies in port logistics include robotics, AI, the IoT, automation, and of course, the blockchain. These elements coexist and are connected with each other or with other existing technological tools such as cloud computing, geographic information systems (GIS), 5G and

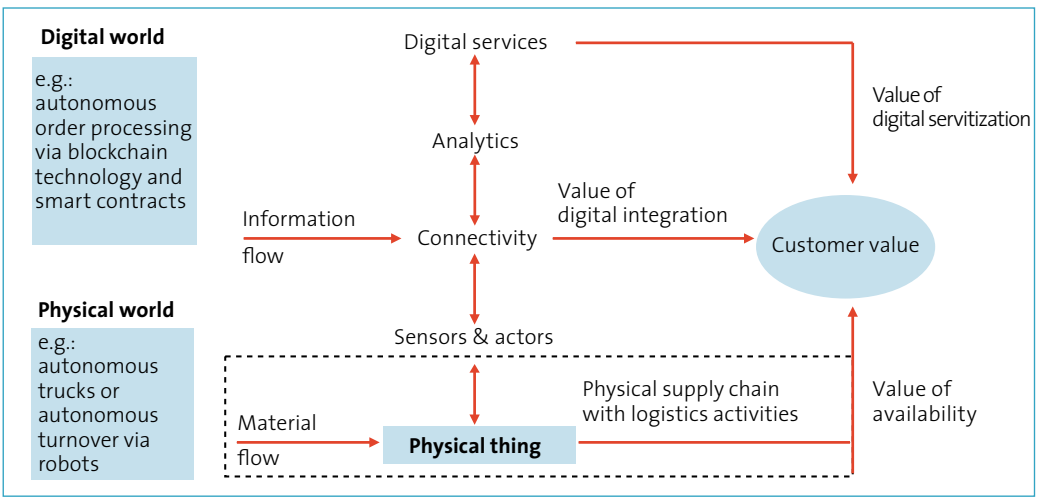
[1] Electronic data interchange is a system of communication between businesses that allows the effective exchange of information, involving either commercial or financial documents, through language that is standardized, known and shared by participants (Pérez-Salas, 2001).

Port Community Systems (PCS), among other information technology (IT) developments.

With a view to providing a broader perspective, diagram 2 extends this analysis to the entire logistics chain, integrating both international and hinterland logistics, and emphasizing their links with the different geographic and productive areas of application.

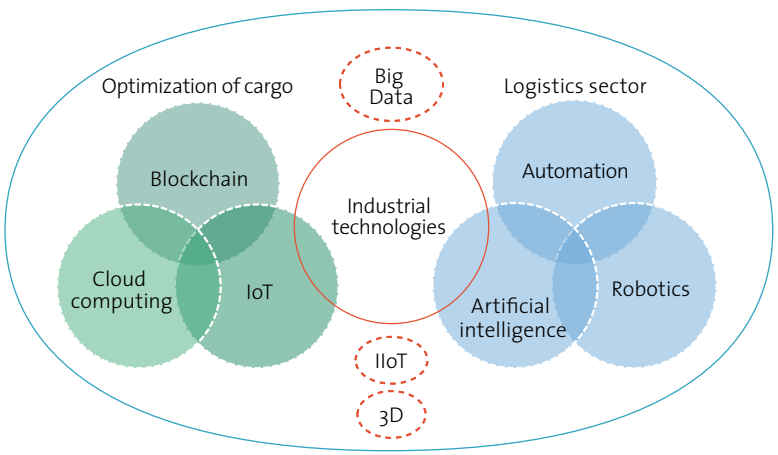
Flexibility in the configuration of production processes and the ability to adapt automatically to demand are the essence of the fourth industrial revolution (Lage, 2019). Capturing, securely transmitting and analysing disparate data is fundamental to make guided decisions that trigger new optimization processes dynamically and continuously.

Diagram 1
Digitalized business model



Source: Prepared by the authors on the basis of E. Hofmann and M. Rüsch, "Industry 4.0 and the current status as well as future prospects on logistics", *Elsevier*, 2017.

Diagram 2
The technological ecosystem linked to logistics



Source: Economic Commission for Latin America and the Caribbean (ECLAC).

II. The technological bases of Logistics 4.0

A number of the technologies available on the market today harbour considerable potential to disrupt the logistics industry, owing mainly to the fact that they represent the possibility of integrating information and facilitating interoperation with other production and distribution systems, and even with intelligent transportation systems (ITS),[2] thereby favouring communication among production actors, devices and logistics infrastructure. Some of the desired effects of this interoperability are the reduction of times, costs, and negative social and environmental externalities, and the provision of technological support to strengthen the facilitation of processes or co-modality. This is facilitated by the provision of real-time information to ensure that the modal change in a logistics operation is much simpler and safer, and of information to optimize routes or encourage collaborative logistics, thanks to which companies can partly or fully share their distribution chain for all products for which the distribution service is not a differentiating element of competition, under a coopetition scheme.

Technologies with disruptive capacities will affect almost all aspects of logistics and economic processes related to both domestic and international transport, where the convergence of economic and technical change forms part of the technological change of the future (Sánchez and Mouftier, 2016). Change will therefore be a constant, so the biggest challenges will be linked to knowledge management, continuous training and innovation as a differentiating source of competition. The following are examples of technologies with the biggest disruptive impacts on trade logistics.

Automation and robotics are two technologies that go hand in hand as they allow repetitive actions or procedures to be carried out automatically. Growth in available information and IT techniques for real-time analysis facilitates much more efficient operations management, a reduction in operational failures and a sharp decline in total costs once social investment has been amortized. In logistics, automation and robotization are present especially in ports where output has increased sharply thanks to high efficiency and productivity. In the medium term, they are expected to be incorporated autonomously into the rest of the logistics chain, in intermodal terminals as well as in the operation of boats, trucks and other modes of transport, which will improve output, security and responsiveness to

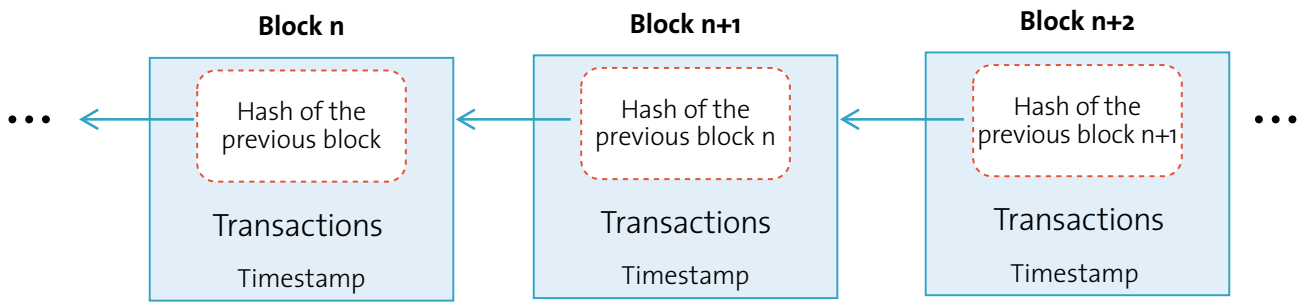
[2] Intelligent transportation systems (ITS) use, process and manage information gathered by different applications to implement and manage strategies that improve security, raise the level of service and capacity, reduce transit times and increase the productivity of transportation systems (Pérez-Salas, 2001).

specific changes. Automation requires careful technical and operational planning, and a gradual adjustment of the workforce (Sánchez y Mouftier, 2016), including retraining in other areas of the sector.

Blockchain technology offers a security mechanism for the exchange of information between the different elements of the production and logistics chain, through data encryption and distributed storage that ensures there is no single point of failure or fraudulent data tampering. This technology was initially employed in cryptocurrency, although its use was later extended to other sectors such as foreign trade, transport, telecommunications and energy, and new applications are emerging every day in areas requiring procedures and relationships between actors connected digitally in a reliable and secure manner.

The concept implicit in the blockchain is that each database record comprises a series of blocks, in which the same transaction is recorded and shared in multiple network nodes, whereby each node maintains a copy and all copies are updated and validated simultaneously. To ensure that transactions cannot be erased or altered, a timestamp is used to encrypt the date, time of creation and change in a transaction, as well as the information that links these elements to the previous block. Each block contains a hash, which is a unique identifier that allows direct access to the previous block, and which is created when transaction data are processed by an encryption tool to ensure that they remain confidential, as shown in diagram 3.

Diagram 3
How a generic blockchain works



Source: Prepared by the authors.

Blockchain technology generates both public and private keys that differ in terms of the type of information they allow access to and utilize in the shared chain. It guarantees the integrity of the information available and the security, transparency and auditability of the entire flow of processes and information contained in the logistics chain, which in turn improves the efficiency and traceability of production, distribution and reverse logistics processes, ensuring the level of security needed for the automation of some logistics processes.

Smart contracts are one example of blockchain use, and allow the autonomous execution of specific IT procedures or algorithms and data processing, ensuring that only the user ever has access to these data (Zyskind, Nathan and Pentland, 2015). Unlike traditional paper contracts, in this case the clauses are laid out in scripts (lines of code in a specific programming language), wherein the contract terms are commands and lines that are executed automatically by software once all the stipulated conditions have been met. It is hoped that in the short term, these algorithms can directly access participants' information systems, be executed autonomously and carry out the actions stipulated in the contracts completely transparently and automatically without human interference, thus reducing processing times and the risks associated with the questioning of the stipulated clauses.

Smart contracts therefore not only define the rules and penalties for an agreement in the same way as traditional contracts signed between parties, but they are also self-executing and thus automatically fulfil these obligations, with no intermediaries and without being subject to legal judgements or territorial jurisdictions. Given that this type of contract can be created and executed by natural and/or legal persons, as well as by machines or other programmes that function autonomously, the encryption and security provided by blockchain technology is fundamental to its functioning and widespread use.

Three other applications in addition to the traditional uses of blockchain in cryptocurrencies and the previously mentioned smart contracts are: (i) traceability of monetary, physical and documentary flows; (ii) interoperability between different systems, ensuring data sovereignty; and (iii) the reliability and security needed for the successful implementation of the industrial IoT (Lage, 2019).

The **Internet of Things (IoT)** allows the interconnection, through Internet, of smart devices that share specific information and data with each other and with other remote digital platforms for real-time decision-making by the user or by other smart devices through machine-to-machine (M2M) communication. The global installed base of IoT devices is expected to rise from 27 billion in 2017 (IHS Markit, 2018) to 64 billion in 2025 (Business Insider, 2019).

Another element expected to favour the widespread use of this technology is the implementation of 5G telecommunications, which will provide Internet access speeds 10 to 100 times faster than the existing technology and with low latency of less than one second which improves cloud-based services and is fundamental, for example, to autonomous vehicles and other services such as the industrial IoT (see below).

For the logistics sector, the IoT represents a huge opportunity to make services more efficient and economically profitable through real-time data capture that facilitates the flexible management of assets and the increase in value added for the client, either through the follow-up of shipments, the optimization of routes, or the improvement of last mile delivery. It also facilitates the gathering of data for the optimization of warehouse capacity, planned maintenance of fixed assets and adaptation of logistics configuration in keeping with dynamic market variations.

The **industrial Internet of Things (IIoT)**, as the name suggests, is a specific application of the IoT in the industrial environment, with a view to maximizing and automating data capture to improve the traceability of processes and real-time decision-making relating to production. In both cases, data reliability and security are fundamental.

Big data involves the processing of large volumes of different types of data from various sources at high speed, facilitating the detection of historical patterns and trends that help to improve decision-making or the automation of processes through the establishment of suitable parameters. Big data may also be seen as complementary to the IoT —which generates large volumes of varied data— as it analyses these data through data mining and big data techniques and facilitates the management and conversion of these data into useful information for strategic planning and decision-making. A suitable characterization of big data includes four elements:

- Volume: amount of information stored (gigabytes, terabytes, petabytes, exabytes).
- Velocity: speed with which data flows are created and captured.
- Variety: diversity of data, representation and semantics.
- Veracity: precision and accuracy of data.

Cloud computing allows users to access technological infrastructure (hardware) through external providers that supply shared and unlimited access to data servers, storage, applications and services via the Internet, based on a pay-as-you-go model. This model presents undeniable advantages in terms of costs and scaleability of infrastructure, although it requires high-speed uninterrupted Internet access and strict security controls to protect critical applications and data (McKinsey, 2018).

3D printing creates objects by superposing (printing) successive layers of material based on a 3D model or drawing. While the quality and speed of 3D printing are still being debated, private investment in this technology is concentrated in the United States, which accounts for 39% of the global market, followed by Asia and the Pacific (29%), and Europe (28%) (ING, 2017). However, it is important to distinguish between applications used in households and in industrial settings. In the first case, rather than reducing demand for logistics services owing to the printing of objects in situ, demand is likely to remain stable or increase slightly because of the need to provide each household with the basic supplies to print products. Meanwhile, 3D printing in an industrial setting is different as it involves the printing of polymer parts locally, which could bring about significant changes in some value chains. For example, in automobile manufacturing, it could change the operating model by shortening the value chain and allowing the production of objects directly in factories or nearby, saving time and transport costs, and also providing greater flexibility in production in response to changes in demand or clients' tastes.

Artificial intelligence (AI), is a machine learning system which enables the replication of human skills, and is generally used for tasks that require repetitive movements, replacing human labour with that of machines operating independently. It also facilitates the identification of patterns and triggers specific actions based on a large volume of data from different sources.

In logistics, AI is used mainly to predict demand, which allows the flexible and rapid adjustment of inventories and the optimization of product distribution with a view to reducing costs and delivery times.

Augmented reality (AR) is an application that uses viewing devices to combine reality in a logistics environment with 3D information and vital computer data that are overlaid onto a display with a view to improving decision-making.

In logistics, it is mostly being used in warehouse management to improve selection, quality control and product packaging processes, which are routine tasks that account for a considerable amount of time and cost. The use of AR could drastically cut costs and errors (e.g. packaging errors that delay deliveries or result in product returns), improving delivery times and customer service quality.

III. Impact of the emergence of Logistics 4.0 in Latin America and the Caribbean

The emergence of disruptive technologies in logistics, examined in the previous section, should be considered by national authorities and professionals in the logistics sector in Latin America and the Caribbean, given that these innovations will bring about profound changes in the perception of logistics. The question is not whether these changes will affect the sector, but rather how soon. The fourth industrial revolution is already under way, and as in the past, with globalization and the digital economy, the speed at which governments and the private sector adapt to these changes determines, in large part, the ability to succeed in the new scenario. Thus, the most urgent steps to be taken are to address unresolved issues such as digital literacy, the cost and speed of Internet access, and cybersecurity and cyber safety.[3]

The blockchain, as seen in the previous section, creates an interesting scenario and opportunities to improve the traceability and security of the logistics chain. In the region in particular, it also represents some uncertainties. The main one has to do with the operating cost of this technology, either as part of global initiatives such as TradeLens by

[3] Cybersecurity involves the prevention of cyberattacks and is concerned with the protection of information technology (IT) —which focuses on the processing of data into information—, of operational technology (OT) —which concentrates on the use of data to control or monitor physical processes—, and of data from unauthorized access, manipulation and disruption. Meanwhile, cybersafety covers the risks from the loss of availability or integrity of safety-critical data and operational technology (BIMCO and others, 2018).

Maersk and IBM, or through an entity's development of its own system. In both cases, in addition to the costs to implement, maintain and update the platform, consideration must be given to transaction costs, interoperability with other systems, and security. It is also important to bear in mind the possible impact of these decisions on the concentration process under way in the industry. In the fourth industrial revolution, data are the most valuable commodity, and if the necessary precautions are not taken, this could result in a scenario in which the concentration of the global logistics market extends to the digital sphere, favouring complete vertical and horizontal integration.

According to Machina Research, in Latin America the IoT is expected to grow at an annual rate of 27% between 2014 and 2024, from 14.6 million connected devices to around 160 million at the end of the period. This widespread growth may represent an opportunity for the region to take a huge step forward in terms of the quality of logistics, by allowing active follow-up and traceability of the entire supply chain, at a lower cost than the methods currently in use. The IoT also provides a large quantity of information that not only makes it possible to improve decision-making, but —if well managed and integrated with other platforms— would also favour better integration and management of co-modality, encouraging modal exchange and the development of more balanced modal distribution, which is fundamental to the reduction of costs, times and negative social and environmental externalities.

However, Logistics 4.0 represents an enormous regulatory challenge for the governments of the region owing to the disruptive effects it can have on the competitiveness and productivity of the economy. These information platforms, most of which are located in the cloud (cloud computing), may also fall outside the jurisdiction of many of the regulations or taxes currently in effect in the foreign trade environment. This was the case with other sharing economy platforms such as Uber and Airbnb, which disrupted their respective economic sectors in which national regulations were unable to adapt with sufficient speed and flexibility to ensure that these systems operated competitively with the other traditional economic players and generated social benefits at the local level.

The regulation of telecommunications services has a considerable impact on the widespread growth and utility of IoT. In particular, radio spectrum management, the granting of licences, standardization of equipment and definition of national and ideally regional standards will be fundamental to ensure market competition and international competitiveness. Attention must also be paid to regulations on data protection, privacy and security.

There is also a need for a modern institutional framework that adapts easily to this new context, favouring the adoption of these new technologies and fostering their interoperability with other national IT systems, both public and private, through a national technological architecture. This ensures the interoperability of the different technologies and providers while avoiding barriers to competition or proprietary schemes that function as monopolies in the provision of hardware or associated services. The framework would also try to ensure the protection of personal data and the privacy and security of shared commercial information. This architecture must also evolve in line with technological progress to guarantee suitable standardization of data semantics, connectivity, transmission, interoperability and any other aspect needed to ensure a suitable technological ecosystem.

Given the existence of value chains and the importance of fostering interregional trade, it is advisable to develop or coordinate standardization and technological architecture at the regional level to ensure the interoperability of the different trade and regional integration agreements, as well as leverage economies of scale and encourage interregional trade and greater regional integration in line with the proposals and goals of the 2030 Agenda for Sustainable Development.

The ubiquity of these systems also makes these platforms vulnerable to cyberattacks. Cyberattacks, unlike the viruses of the past (which were based mainly on tactics to

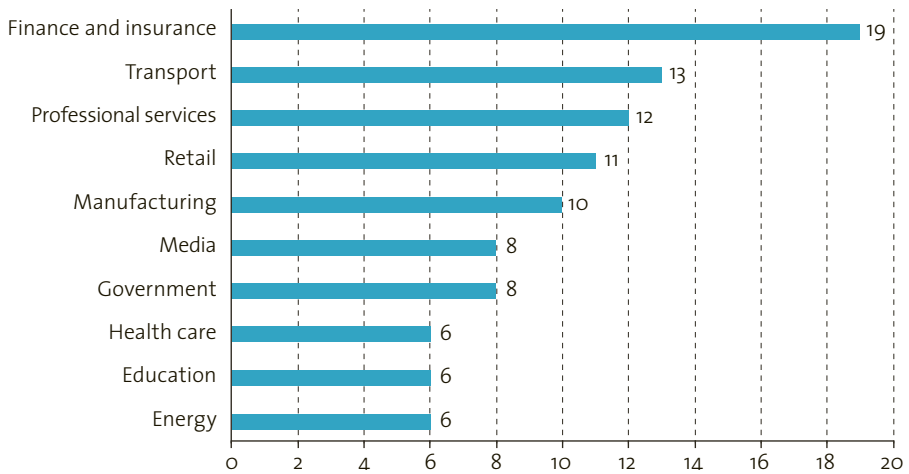
exploit or to expose the generic vulnerabilities of IT systems) are now being carried out by specialized groups targeting specific critical systems in order to steal commercial information or industrial property and to exploit vulnerabilities to hijack systems and demand a ransom, and by other specialized groups seeking to disrupt the proper functioning of supply chains and therefore to affect the economy or the Western development model itself (cyberterrorism).

Amid this backdrop, it is fundamental that governments provide security for critical telecommunications and energy infrastructure, and that they foster initiatives for the private sector to take the necessary measures to ensure that logistics operations are resilient to these attacks, containing and limiting the repercussions on the rest of the supply chain.

The logistics sector, including transport, is part of all countries' economic infrastructure, and is therefore an attractive target for malicious threat actors. As the transport industry's supply chain continues to integrate and automate, the risk associated with cyberattacks will increase exponentially. Transport and logistics services are currently the second most targeted sector, experiencing 13% of total cyberattacks and incidents in 2018 (IBM, 2019), surpassed only by attacks on the finance and insurance sector, as shown in figure 1.

For example, according to UK P&I Club and others (2018), in 2011 the Port of Antwerp in Belgium fell victim to an advanced persistent threat (APT) attack commissioned by a drug cartel. "The attack targeted terminal systems which were subsequently compromised by hackers and used to release containers without port authorities becoming aware. Illicit drugs and contraband worth approximately US$ 365 million, firearms and approximately US$ 1.5 million were seized when authorities finally became aware." Another case that helps to place the seriousness of the problem in perspective is that of A.P. Moller Maersk in June 2017, when an attack known as ExPetr led to computer system outages which affected both oil and gas production and port operations. "Following the incident, Maersk claimed to have changed its IT systems to prevent similar incidents from occurring in the future. The incident resulted in an estimated US$ 300 million of losses." (UK P&I Club and others, 2018).

Figure 1
Sectors targeted most frequently by cyberattacks



Source: IBM, "X-Force Threat Intelligence Index 2019", 2019 [online] https://www.ibm.com/security/data-breach/threat-intelligence.

Lastly, it is important to point out that the coordination of initiatives and investments in technology by the public and private sectors, and the required regional coordination, for example in smart transport systems, single-window facilities for foreign trade, electronic data exchange and transmission, cargo tracking, among many available options, would

also be conducive to a more efficient regional transport system, better process security, and greater competitiveness for all participants (Pérez-Salas, 2013).

IV. International standards and best practices in the introduction of technological rules

Suitably managing technological standards, encouraging cooperation and introducing international best practices are fundamental to the introduction of technological rules and the provision of guidelines for adequate security in line with the speed of changes in these areas.

Hence, for example, the technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have developed international standards for the Internet of Things (ISO/IEC JTC 1, 2014) and an Internet of Things Reference Architecture (ISO/IEC 30141), published in 2016. The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) has also formed a working group with the aim of developing a standard for an architectural framework for the Internet of Things, IEEE P2413 (IEEE-SA, 2016).

Since 2017, ISO has sought to standardize the blockchain and distributed ledger technologies (ISO/TC 307 - Blockchain) based on the following structure: reference architecture, taxonomy and ontology, use cases, security and privacy, identity, smart contracts, governance of blockchain and distributed ledger technologies, interoperability of blockchain and distributed ledger technologies, terminology. The International Telecommunication Union (ITU) has also expressed interest in standardizing blockchain technology. The ITU Telecommunication Standardization Sector (ITU-T) has also set up a focus group on application of distributed ledger technology (FG DLT), which will develop a workplan for the standardization of interoperable services based on distributed ledger technology (ITU-T, 2017). IEEE-SA is also developing a standard for the framework of blockchain use in the IoT (IEEE-SA, 2017), and the Linux Foundation along with other companies has worked to create an open source platform called the Hyperledger Project based on blockchain technology for a distributed ledger that can be used in multiple industries, and is optimized for myriad use cases (Linux Foundation, 2016).

There are also cyberrisk management standards, such as ISO/IEC 27001 established by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), which establishes the requirements for an information security management system. It advocates for the combination of three pillars: people, processes and technology. As regards people, organizations must provide cybersecurity training for employees to prevent and reduce cyberthreats. In terms of processes, information technology must be used to define and audit organizations' activities, functions and documents used to mitigate cybersecurity risks. Lastly, with regard to technology, after identifying the cyberthreats facing organizations, plans must be implemented to address these threats and reduce the impact of a possible attack.

BIMCO has created guidelines to incorporate cyberprotection into ships' safety management systems, including risk assessments of operational technology, navigation systems and engine controls, and also provides a guide on addressing cyberrisks for ships deriving from other elements of the supply chain. These guidelines are based on the following principles: (i) awareness of the security and commercial risks arising from the lack of cybersecurity measures, (ii) protection of IT infrastructure on-board ships and of connected equipment, (iii) a user authentication and authorization system to guarantee appropriate access to the necessary information, (iv) protection of data used on-board the ship, guaranteeing suitable protection based on the sensitivity of information, (v) management of IT users, to ensure that only authorized persons have access and rights to information, (vi) management of communication between the ship and coastal areas, and (vii) development and implementation of a response plan to cyberincidents based on risk assessment.

Another guideline is MSC-FAL.1/Circ.3 of the International Maritime Organization (IMO) which provides high-level recommendations on the management of maritime cyberrisks in order to protect maritime transport from current and emerging cyberthreats and vulnerabilities that can lead to operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised or their use to commit illicit or terrorist acts.

V. Concluding remarks

The ongoing technological changes associated with the fourth industrial revolution have the capacity to transform the world, affecting all areas of daily life, including the production system and forms of work. As logistics is part of this paradigm shift, new tools and knowledge are needed to facilitate adaptation to the new technological environment. Technology is not an end in itself, but a means to improve the competitiveness and sustainability of the logistics operations needed to satisfy current demands for development with intergenerational equity.

A number of the technologies analysed in this document seek to reduce costs and improve decision-making, and to foster the traceability and security of shipments and information, thereby increasing trust among actors, reducing bureaucracy and encouraging administrative transparency in order to create value added and profitable services in the region. Therefore, policymakers and specialized regulatory agencies must be aware of these changes in order to leverage political opportunities and moments to create the appropriate framework for developing these instruments so that they benefit competitiveness, the transformation of production and the creation of good quality jobs. The information technologies presented in this paper generate volumes of data that allow evidence-based decision-making, improving not only public-private cooperation but also fostering transparency, digital governance and legitimate decisions.

It is also important to acknowledge the challenges raised by the new approach. There is a need for data privacy protection policies which are compatible with the development of technological solutions that incorporate information by leveraging the potential of artificial intelligence, big data and other technologies to develop and market new data that enable business models and opportunities (Voege, 2019), encouraging open solutions in addition to proprietary architecture.

There is a wide digital divide between the region and countries that have accumulated technological and institutional capacities. In Latin America and the Caribbean, there is resistance to digitalization, driven by a fear of job losses and the lack of opportunities for digital learning. Hence, along with digital literacy in the logistics sector, it is important to implement initiatives that train and refocus human resources that may be affected or displaced by automation and digitalization of processes towards other economic sectors where they can generate greater value and access better paid jobs.

With the increase in technology, cyberattacks are also becoming more sophisticated as cybercriminals use different tactics and technologies to exploit vulnerabilities, so logistics must learn to address this issue and incorporate it into the risk model, as with other threats seen in the past, such as drug trafficking and terrorism.

Technological advancement demands a revision of the current business model. The space-time paradigm is very different from what was seen a few years ago, and will change much more in the near future. The magnitude of these changes calls for a profound cultural shift in logistics governance, especially in relation to public-private cooperation, cybersecurity and the incorporation of resilience objectives in all logistics chain processes.

Amid this backdrop, there are important spaces to bring about regional improvements and combine competition with cooperation (coopetition) in favour of greater regional competitiveness. Given the limited cultural and linguistic barriers between the three

major subregions of Latin America and the Caribbean, creating technological structures with the aim of transparently sharing data and information, and common strategies for maintenance and technological development, is a way to advance actively in the transformation of production, taking full advantage of the potential of disruptive technologies in trade logistics. The scope of the changes that have already occurred and those expected in future also implies the need for greater cooperation and knowledge partnerships between the public and private sectors and regional academic institutions.

VI. Bibliography

BIMCO and others (2018), *The Guidelines on Cyber Security Onboard Ships. Version 3* [online] https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/cyber-security-guidelines-2018.ashx.

Business Insider (2019), "IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers", [online] https://www.businessinsider.com/internet-of-things-report

Corvera, R. (2005), "Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información", ISO/IEC 17799, Estándar Internacional.

Delawari, A. A. (2013), *Shared Situational Awareness Between Inland Actors at Port of Rotterdam*, MSc Thesis TU Delft.

Drewry (2019), *Ports & Terminals Market Briefing*, 1 October.

Evans, D. (2011), "The Internet of Things: How the Next Evolution of the Internet is Changing Everything", Cisco Internet Business Solutions Group (IBSG) [online] https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.

Hofmann, E. and M. Rüsch (2017), "Industry 4.0 and the current status as well as future prospects on logistics", *Elsevier*.

IBM (2019), "X-Force Threat Intelligence Index 2019" [online] https://www.ibm.com/security/data-breach/threat-intelligence.

IDC (2017), "En 2018, una de cada nueve empresas en LA estará emprendiendo una estrategia de Transformación Digital (DX): IDC", *IDC Releases* [online] http://cl.idclatin.com/releases/news.aspx?id=2262.

IEC/MSB/SAP/Fraunhofer AISEC (International Electrotechnical Commission/Market Strategy Board) (2016), "IoT 2020: Smart and secure IoT platform", *IECWP IoT Platform:2016-10(EN)* [online] http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf.

IEEE-SA (Instituto de Asociación de Estándares de Ingenieros Eléctricos y Electrónicos) (2017), "2418 - Standard for the Framework of Blockchain Use in Internet of Things (IoT)" [online] https://standards.ieee.org/develop/project/2418.html.

(2016), "IEEE P2413 – Standard for an Architectural Framework for the Internet of Things (IoT)" [online] http://grouper.ieee.org/groups/2413/.

IHS Markit (2018), *8 in 2018: The Top Transformative Technologies to Watch this Year*, London.

IMO (International Maritime Organization) (2019), "MARPOL. Annex VI and NTC 2008 with guidelines for implementation", February [online] http://www.imo.org/en/Publications/Documents/Supplements%20and%20CDs/Spanish/QC664S_022019.pdf.

ING (2017), *3D Printing: A Threat to Global Trade*, Economic and Financial Analysis Global Economics, Technology, September [online] https://www.ingwb.com/media/2088633/3d-printing-report-031017.pdf.

ISO/IEC JTC 1 (2015), "Information technology. Big Data", *Preliminary Report 2014* [online] https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/big_data_report-jtc1.pdf.

(2014), "Internet of Things (IoT)", *Preliminary Report 2014* [online] https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/internet_of_things_report-jtc1.pdf.

ITU (International Telecommunication Union) (2017), "Global Cybersecurity Index (GCI)" [online] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf.

ITU-T (ITU Telecommunication Standardization Sector) (2017), "Security reference

architecture for lifecycle management of e-commerce business data", *Series X: Data Networks, Open System Communications and Security* (X.1040) [online] https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1040-201710-I!!PDF-E&type=items.

Lage, O. (2019), *Blockchain: From Industry 4.0 to the Machine Economy* [online] https://www.intechopen.com/online-first/blockchain-from-industry-4-0-to-the-machine-economy.

Linux Foundation (2016), *The Year of the Open Blockchain* [online] https://www.linuxfoundation.org/blog/2016/02/the-year-of-the-open-blockchain/.

Machina Research [online] https://machinaresearch.com/what-we-do/advisory-service/iot-forecasts/.

McKinsey (2018), *Creating Value with the Cloud*, Digital McKinsey Insights, December [online] https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Creating%20value%20with%20the%20cloud%20compendium/Creating-value-with-the-cloud.ashx .

(2017), *The Future of Connectivity: Enabling the Internet of Things* [online] https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things.

Pérez, G. (2013), "The need to facilitate and secure logistics processes in Latin America and the Caribbean", *FAL Bulletin*, No. 321, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

____ (2012), "Sistemas inteligentes de transporte: oportunidades para una logística sostenible y competitiva", *Las tecnologías de la información y de las comunicaciones (TIC) y el desarrollo sostenible en América Latina y el Caribe: experiencias e iniciativas de política, Seminars and Conferences Series*, No. 74 (LC/L.3679), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

___ (2001), "Telemática: un nuevo escenario para el transporte automotor", *Natural Resources and Infrastructure series*, No. 30 (LC/L.1593-P), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

Pérez, G. and R. Sánchez (2019), "Logistics for production, distribution and trade", *FAL Bulletin*, No. 369, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

Sánchez, R. and L. Mouftier (2016), "Reflections on the future of ports: from current strains to the changes and innovation of the future", *FAL Bulletin*, No. 352, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC).

Schwab, K. (2016), *The Fourth Industrial Revolution*, World Economic Forum (WEF).

Tavasszy, L (2018), "Innovation and technology in multimodal supply chains", *International Transport Forum Discussion Papers*, Paris, OECD Publishing.

UK P&I Club and others (2018), *Risk Focus: Cyber – Considering threats in the maritime supply chain*, 10 June [online] https://www.ttclub.com/fileadmin/uploads/tt-club/Publications___Resources/Document_store/UK_NYA_TT_Risk_Focus_-_Cyber_WEB.pdf.

Voege, T. (2019), "The future of transport services" *Discussion Paper*, No. IDB-DP-680, Washington, D.C, Transport Division, Interamerican Development Bank (IDB), June.

Zyskind, G., O. Nathan and A. Pentland (2015), "Enigma: Decentralized Computation Platform with Guaranteed Privacy", 10 June [online] https://arxiv.org/abs/1506.03471.

VII. Publications of interest

FAL Bulletin 305

Intelligent transport systems in Latin American sea port logistics

Georgina Febré
Gabriel Pérez Salas

This issue of the FAL bulletin analyses the role of intelligent transport systems (ITS) in sea port logistics in Latin America.

This work forms part of Unit activities within the "Sustainable Transport in Ibero-America project", financed by Puertos del Estado, España.

Available in: Spanish English

Sistemas inteligentes de transporte: oportunidades para una logística sostenible y competitiva

Gabriel Pérez Salas

Published in:
Las tecnologías de la información y de las comunicaciones (TIC) y el desarrollo sostenible en América Latina y el Caribe: experiencias e iniciativas de política. Memoria del seminario realizado en la CEPAL Santiago, 22 y 23 de octubre de 2012. Santiago: CEPAL, 2013. LC/L.3679. p. 40-44

To achieve sustainable economic growth and higher levels of equality, the countries of Latin America and the Caribbean must tackle the challenge of consolidating structural reform policies, progressing towards more diversified production with strong uptake of technical progress and smaller productivity gaps, together with greater energy and environmental efficiency.

Available in: Spanish