The Connected Supply Chain

Enhancing Risk Management in a Changing World

Agustina Calatayud

Institutions for Development Sector

Connectivity, Markets, and Finance Division

DISCUSSION PAPER Nº IDB-DP-508

March 2017

The Connected Supply Chain

Enhancing Risk Management in a Changing World

Agustina Calatayud

March 2017

Inter-American Development Bank

http://www.iadb.org

Contact: Agustina Calatayud, mcalatayud@iadb.org.

Abstract[*]

Not since the end of World War II have supply chains been as highly exposed to risks as they are now. The Fourth Industrial Revolution poses unprecedented challenges for production and distribution systems. It also creates important opportunities, particularly in risk management. Indeed, new digital technologies will foster the emergence of the connected supply chain as a critical element for risk management. Supply chain connectivity is defined as the seamless flow of materials, information, and financial resources along the supply chain, enabled by two factors: information systems connectivity and physical connectivity. This paper analyzes both factors and how new technologies can improve them. It also discusses the barriers that prevent the achievement of a connected supply chain and, with it, improved risk management. Finally, it discusses the role that the public sector can play in overcoming these barriers.

JEL Codes: G20, G21, G28, L25, L16

Keywords: connectivity, finance, risk management, supply chain

[*] Agustina Calatayud is Private Sector Development Specialist at the Connectivity, Markets and Finance Division of the Inter-American Development Bank (IDB).

The author thanks Dr. Juan Antonio Ketterer (Chief of IDB Connectivity, Markets, and Finance Division) and Prof. John Mangan (Newcastle University) for their valuable comments on earlier versions of this paper.

Contents

1. Introduction

As supply chains become more global and interconnected, their exposure to risks increases. Higher demand volatility, unprecedented technological changes, and supply chain speed intensify risk exposure. In this context, academics and practitioners often suggest that not since the end of World War II have supply chains been as exposed to risks as they are now (Christopher and Holweg, 2017). Of the many diverse challenges that supply chain management faces today, the most compelling one is the new technology revolution, with breakthroughs in several fields, such as artificial intelligence, robotics, the Internet of Things (IoT), autonomous vehicles, and 3D printing, among others. Indeed, we are at the beginning of the Fourth Industrial Revolution, a revolution that will significantly change production and consumption as we know them today (Schwab, 2016).

Despite the uncertainties of these unprecedented times, new technologies will critically contribute to improve supply chain risk management. This paper argues that the new technologies will do this by enhancing supply chain end-to-end connectivity. It defines connectivity as the seamless flow of materials, information, and financial resources along the supply chain, enabled by information systems connectivity and physical connectivity. The paper analyzes both factors and how new technologies can improve them. It also discusses the many barriers that stand in the way of achieving a connected supply chain and, with it, improving risk management. Finally, it discusses the role of the public sector in overcoming these barriers.

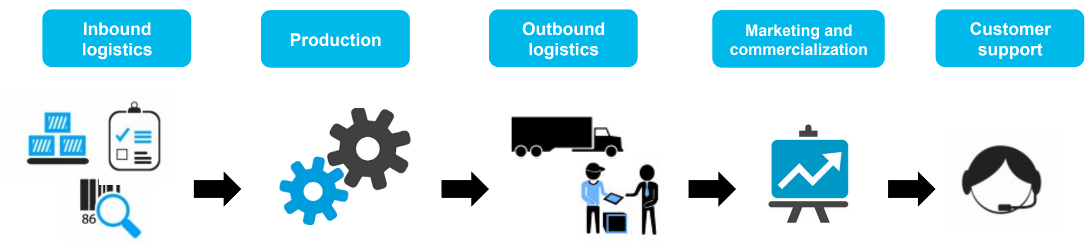
This paper contributes to the efforts of the Inter-American Development Bank (IDB) in the promotion of productivity growth in Latin America and the Caribbean (LAC) through the design of risk management strategies for supply chains in the region. Supply chain risk management strategies encompass the identification of the various threats to which supply chains are exposed, an estimation of the probability of occurrence and severity of such risks, and the design of risk prevention and mitigation actions through the use of a cost-effective combination of financial and nonfinancial instruments (Calatayud and Ketterer, 2016). In the context of growing supply chain complexity and international economic uncertainty, an integrated risk management strategy that includes all the actors and all the links in a supply chain is key for risk management, flexibility, and resilence. The paper makes the case for adoption of technology to improve supply chain risk management, and proposes that moving toward a connected supply chain should be a top priority to transition LAC firms into the Fourth Industrial Revolution and ensure their endurance in increasingly uncertain times.

The paper is organized as follows: Section 2 briefly discusses the importance of managing risks to enhance supply chain performance, as suggested by Calatayud and Ketterer (2016). Section 3 analyzes the need to improve end-to-end connectivity in supply chains as a means to manage risks more efficiently and minimize the undesired consequences of disruptions. Section 4 addresses the role of public policy in improving supply chain connectivity, within the context of designing and implementing strategies to manage supply chain risks. Section 5 concludes.

2. Supply Chain Risks in Complex Times

Productive activities are organized in supply chains. The supply chain includes a combination of activities, ranging from the design of a product or service to its delivery to the consumer. The five main activities are: (i) inbound logistics relating to the appropriate inputs or services in terms of quality, quantity, price, time, and place; (ii) production to transform the inputs into final products; (iii) outbound logistics, which include product storage and distribution to ensure the product is of the right quality, quantity, price, and is at the right place at the right time; (iv) marketing and commercialization, which include the drafting and execution of the goods and/or services sales strategy; and (v) customer support, so that clients can seek information and technical assistance, lodge complaints, and negotiate returns and refunds, among other activities (Figure 1).

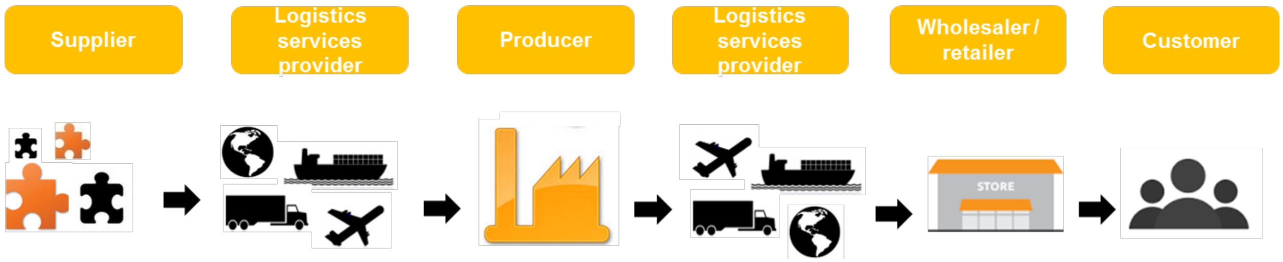
Figure 1. Main Activities in a Supply Chain



Source: Calatayud and Ketterer (2016).

Different actors carry out the activities in a supply chain**.** The main actors in a supply chain are: suppliers of inputs and services; producers; logistics service providers; wholesale and retail distributors; and customers (Figure 2). In addition, other actors not specifically participating in the supply chain can influence the development and performance of the supply chain nodes and linkages. These include, for example, public and private sector institutions and agencies, as well as universities and research centers that, together with the regulatory framework, create the business climate in which supply chains operate. The discipline of supply chain management emerged from the need to coordinate all the actors involved at different stages of the supply chain to achieve operational efficiency. Following Simchi-Levi et al. (2003: 1), supply chain management refers to the "set of approaches utilized to efficiently integrate suppliers, manufacturers, warehouses, and stores, so that merchandise is produced and distributed at the right quantities, to the right locations, and the right time, in order to minimize system-wide costs while satisfying service level requirements."

Figure 2. Main Actors in a Supply Chain



Source: Calatayud and Ketterer (2016).

Supply chain strategies of industrial organizations are becoming more complex. In recent decades, the search for greater efficiency in productive processes has led businesses to employ different supply chain management strategies. Trends such as outsourcing, far sourcing, offshoring, just-in-time production, and consumer-driven production have increased the complexity of supply chains. This complexity is evident at various levels: (i) network complexity, caused by the increase in the number of actors in the chain and the links between them; (ii) process complexity, due to the increased number of processes and faster product development cycles; (iii) product complexity, owing to the higher number of components and shorter product life cycles; (iv) demand complexity, due to increased demand volatility and fragmentation; and (v) organizational complexity, due to the increasing number of levels involved and their tendency to work in silos (Christopher and Holweg, 2017).

Complexity increases uncertainty and raises exposure to risk. This increased risk exposure is a result of the interconnection and interdependence between firms, and the fact that the competitiveness of a business no longer depends solely on its own merits, but also on those of all the other firms in its supply chain (Christopher and Holweg, 2017). Increased risk exposure is also the consequence of increasing demand volatility, unprecedented technological changes, and globalization of production, which has made supply chains more susceptible to changing environmental and political contexts in different countries. With multiple actors, processes, products, linkages, and locations, the presence of risk factors is an inherent element of supply chain operations.

Risk can be defined as the combination of the probability of occurrence of an event and its negative consequences (Holton, 2004). With respect to supply chains, a risk could be any factor that obstructs the flow of information, materials, and products from the supplier to the consumer (Juttner et al., 2003). The literature stresses that risk management, although only of recent interest to business and academia, is becoming both essential and challenging in terms of optimal value chain performance, especially in the context of greater uncertainties in supply and demand and the globalization of production (Goldsby, 2009). Risk management can be defined as foreseeing and evaluating risks, and identifying the actions necessary to avoid them or minimize their impact. Indeed, in the modern economy there is always a risk factor for supply chain operation, with regard to quality or security problems, supply restrictions or disruptions, climate conditions and natural disasters, regulatory or political uncertainty, or inadequate infrastructure, among others.

The literature classifies risk in different ways. Calatayud and Ketterer (2016) divide risk into five categories: (i) systemic, (ii) market, (iii) operational, (iv) credit, and (v) liquidity. These categories can be distinguished according to the level at which the risk arises and where the consequences become evident. While systemic risks can emerge at the global level, independent of a particular industry or chain, and can affect all industries and supply chains, market risks can affect a sector of economic activity. Operational and credit risks are manifested at the local level, in the nodes of a supply chain or the relationship between them. Finally, liquidity risks emerge at the level of a specific node or actor in a supply chain. Table 1 presents each type of risk with its respective sources.

Table 1. Supply Chain Risks

Type of risk	Impact	Sources	Example
Systemic	On the general economy	Political uncertainties	Situations of political instability, changes in government policy, wars, terrorism, coups d'état, piracy.
		Macroeconomic uncertainties	Fluctuations in levels of economic activity, or relative prices.
		Social uncertainties	Changes in peoples' values, attitudes, or beliefs.
		Environmental uncertainties	Floods, droughts, earthquakes, hurricanes.
Market	On a specific sector of the economy	Market uncertainties	Fluctuations in price levels of inputs and products, input availability, technological changes, changes in consumer preferences, availability of alternative products.
		Regulatory or institutional uncertainties	Quality standards and regulations, changes in the specific regulations of the sector.
Operational	On a specific value chain	Supply uncertainties	Delays in deliveries, failures in input quantity or quality.
		Production uncertainties	Mechanical, technical or process failures, forecasting errors, infrastructure failures, failures in product quantity or quality
		Administrative uncertainties	Failures or delays in administrative procedures, such as importation and exportation, compliance with quality standards.
Credit	On a specific value chain or its nodes	Collateral uncertainties	Quality and value of collateral.
		Uncertainty about the sector	Sectors in which there is greater information asymmetry, such as agriculture and the new technologies.
		Uncertainty about the firm segment	Small and medium enterprises, in which there is greater information asymmetry and informality.
Liquidity	On a specific enterprise	Uncertainty about the payment cycle	Non-compliance or extensions in the payment cycles that can cause delays in the firm's short-term commitments. .
		Uncertainty about the firm's financial health	Incomplete or out-of-date financial and accounting records, with low information quality.

Source: Calatayud and Ketterer (2016).

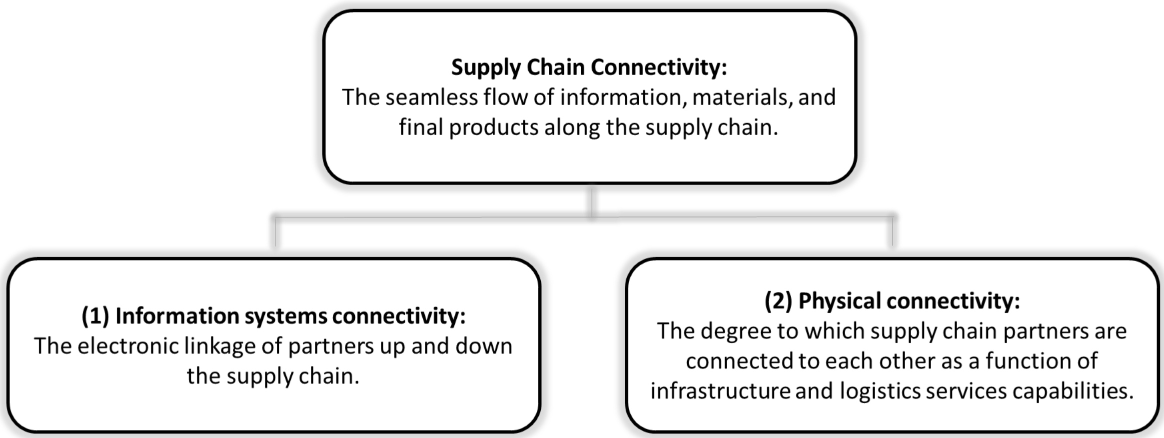
International experiences show the impact of risks on supply chains. The massive earthquake measuring 8.9 on the Richter scale that hit Japan in 2011 had global consequences. Hundreds of companies—among them Boeing, Honda, and General Motors—whose suppliers were located in Japan, were forced to reduce their production levels drastically (e.g., General Motors' production at its U.S. plants fell by half), and they experienced massive disruptions, which were felt through the end of that year, causing losses estimated at US$240,000 million. More recently, the bankruptcy filing of Hanjin shipping line—the world's seventh-largest container line—in August 2016 created confusion in ports and firms around the world. Millions of dollars' worth of merchandise sat on vessels seized on behalf of creditors, denied entry to ports or left unable to dock, while firms tried to make alternative arrangements to meet contractual obligations with their clients and minimize the financial impact of supply chain disruptions. According to empirical evidence, firms experience, on average, a 40 percent decline in their stock price after a disruption, while shareholder value can decrease by 11 percent (Li et al., 2015).

The need to manage risks for better supply chain performance is increasing. The percentage of global companies reporting a loss of income due to supply chain risks increased from 28 percent in 2011 to 42 percent in 2013 (Saenz and Revilla, 2014). Practitioners highlight supply failures, natural disasters, political and regulatory uncertainty, failures in logistical processes, damage to product quality, and delays in customs procedures among the most serious risk factors faced by a supply chain (Hillman and Keltz, 2007; UPS, 2014). Due to the negative impact of these risks on a supply chain, some international surveys show that businesses are now paying more attention to risk management. According to the survey conducted by Deloitte (2015) of 600 large companies in advanced economies, 71 percent considered risk management an important aspect in decision making, and 64 percent acknowledged that they had a specific risk management strategy for their supply chain. According to IBM (2015), risk management is the second most important challenge that supply chain leaders face, after supply chain visibility and before cost containment and changes in demand. However, risk management strategies remain scarce, especially in smaller firms and developing economies. They are usually implemented at the individual business level, even though they encompass other partners. Given the interconnectedness of processes in a supply chain, building collaborative links between all actors in the chain and integrating processes, information systems, and business strategies are as important as—or even more important than—the internal optimization of processes and risk management at the firm level (Christopher and Holweg, 2011). In this context, moving toward a connected supply chain should be a top priority to enhance risk management and ensure survival in increasingly uncertain times.

3. The Need for End-to-End Connectivity

Better supply chain risk management requires end-to-end connectivity. This paper defines supply chain connectivity as the seamless flow of information, materials, and final products along the supply chain.[1] Seamless flows are enabled by two factors: (i) information systems connectivity and (ii) physical connectivity (Figure 3). Since the purpose of any supply chain is to bring a product from its conception to its consumption while minimizing costs and maximizing revenue, both factors are critical to effectively manage supply chain risks and thus avoid supply chain disruptions. The following paragraphs discuss each of these factors and their relevance for supply chain risk management.

Figure 3. Supply Chain Connectivity: Factors and Definitions

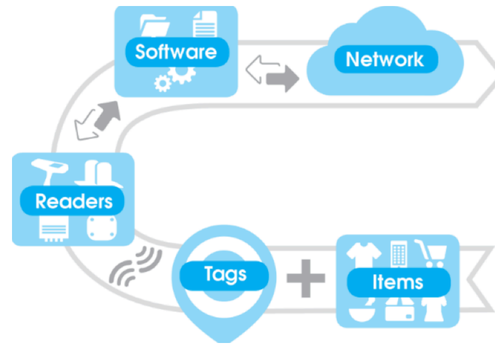


Source: Author's elaboration.

[1] There are different definitions of connectivity in the literature, according to the academic discipline and the research stream to which connectivity is applied (Calatayud et al., 2016). While some definitions focus on the physical aspect of connectivity, that is, the infrastructure needed to connect two nodes, other definitions refer to the ability to exchange information between nodes. In line with current trends in academia and policymaking (ITF, 2012; UNESCAP, 2012), the definition of connectivity suggested in this paper is a broader one that encompasses the entire network of interactions among supply chain nodes.

3.1 Information Systems Connectivity

Figure 4. RFID System



Source: Rain RFID.

Information systems connectivity refers to the electronic linkage of partners up and down the supply chain (Poirier, 1999). The importance of information connectivity has been well documented in the literature (Calatayud et al. 2016). Advances in information technology (IT) have changed modern business models, while geographic location no longer restricts firms to markets and suppliers (Fawcett et al., 2007; Golicic et al., 2002). Technological advances and information sharing allow firms to look for new suppliers, outsource activities, and reach new customers, while reducing costs and increasing efficiency through increased supply chain collaboration. Different technologies can be used to collect and/or exchange information among supply chain partners. Among them are radio frequency identification (RFID), electronic data interchange (EDI), and various data mining (DM) and Big Data technologies. RFID encompasses the technologies that use radio waves to automatically identify and track objects. A wide range of product information can be transmitted using radio waves, including the identification of the product, location details, price, and dates of manufacturing, transportation, and purchase (Xie and Allen, 2013). EDI is a computer-to-computer data transmission system that collects and shares information over the Internet. It is used, for example, to place purchase orders, generate billing and payment orders, transmit sales and inventory data, and give advanced shipping notice. Data mining refers to the process of extracting previously unknown and actionable information from massive amounts of data (Big Data) and using the information for decision making. Applying data mining technology to realize hidden knowledge, relationships, and trends from the Big Data accumulated in the supply chain can help firms to make real-time decision and improve supply chain management.

Information systems connectivity is crucial for supply chain management, since it allows higher visibility and integration of the supply chain. The literature defines visibility as the capability of sharing on-time and accurate data throughout the entire supply chain (Nooraie and Parast, 2015). By making the data on processes, parts, and final products readily available to supply chain partners, information systems connectivity is a key enabler of visibility. Beyond visibility, information connectivity is critical for supply chain integration. Supply chain integration, an important research stream and practice in supply chain management, is defined as the close connection and alignment within a supply chain, both upstream and downstream (Flynn et al., 2010; Schoenherr and Swink, 2012). The logic of supply chain integration is based on the principles of global optimization (Irfan and Irfan, 2014; NAS, 2011). Since in a supply chain the processes for designing, producing, and distributing an end-product are scattered among a variety of firms, working together is essential to optimize collective performance (Simchi-Levi et al., 2003). Following Sanders et al., “the very foundations of the supply chain integration concept rest upon the assumption that collaboration takes place between supply chain partners, which is only made possible through bidirectional flows of voluminous, rich information, including operations and planning data" (Sanders et al., 2011: 179)

Enhanced visibility and integration through information sharing can improve supply chain performance. Fawcett et al. (2007) suggested that there is a strong relationship between the capability of a supply chain to share information and that supply chain's performance. The analysis found that information connectivity, along with the will to exchange information, accounted for over one-third of the variance in operational performance. Similarly, Sanders et al. (2011) found that increased information systems connectivity between a buyer and a supplier was beneficial to both the buyer and the supplier. Sanders et al. (2011) characterized this as a win-win situation, where information connectivity enhanced firms' competitiveness through lower costs, better delivery performance, and greater flexibility. Potential benefits suggested in the literature include: better inventory control; reduced friction, fewer barriers, and less waste of resources on procedures that do not add value; increased functional and procedural synergy between participants; better monitoring of customer behavior and faster response to changing market demands; shorter product realization cycles and lower product development costs; shorter order fulfilment lead times; greater logistics flexibility and improved delivery and logistics asset performance; and lower capital investment in excess capacity (Closs and Swink, 2005; Coronado-Mondragon et al., 2009; Gunasekaran and Ngai, 2004; Swafford et al., 2008). In addition, some evidence suggests that enhanced supply chain integration can enable firms to access various resources and capabilities in the form of knowledge embedded within other supply chain members, subsequently increasing a firm's ability to innovate (Cao and Zhang, 2011).

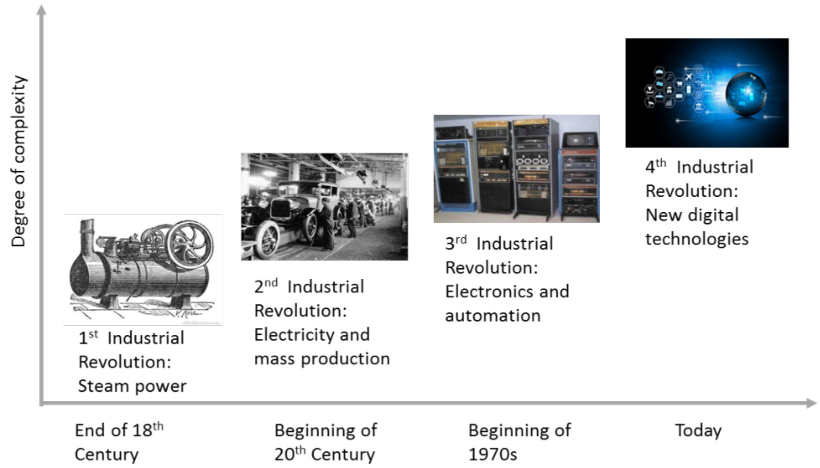
Information systems connectivity is an essential ingredient of supply chain risk management (Christopher and Lee, 2004; Juttner et al., 2003). Specifically, information systems connectivity helps manage risks in three ways. First, it helps identify possible vulnerabilities along the supply chain, thus informing the design of risk management plans. Second, it helps prevent the occurrence of events that could become risks if no action is taken (Yu and Goh, 2014). Third, since it provides real-time information on events in the supply chain, it enables rapid implementation of risk management measures, minimizing the risk of disruptions (Li et al., 2015). Empirical evidence shows that the more information is shared along the supply chain, the better the risk management and the financial performance of the supply chain (Li et al., 2015). It is not surprising that about 80 percent of large companies cite lack of information sharing as their top concern, especially in a context of increased complexity and uncertainty, which requires improved flexibility and responsiveness (Yu and Goh, 2014). For example, a common supply risk that can be reduced by increasing information sharing is the "bullwhip effect," which occurs when information about the final customer's demand becomes increasingly distorted as it moves upstream in the supply chain, distorting in turn decisions on inventory, production, and delivery planning (Danese et al., 2013). Indeed, sharing information with supply chain partners can improve the accuracy of demand information and demand forecasting. Some practices frequently used with this goal are vendor-managed inventory (VMI), continuous replenishment programs (CRPs) and collaborative planning, forecasting, and replenishment (CPFR), which can reduce the operational and financial risks of flawed demand forecasts.

> There will be more than 50 billion devices connected to the Internet by 2020, a trillion sensors connected to and transmitting information to analytical platforms 'in the cloud,' and 44 trillion gigabytes generated.
>
> Cisco (2011) and DHL (2015).

In the context of the Fourth Industrial Revolution, it is expected that information systems connectivity will increase at an exponential rate, improving supply chain risk management and performance. While the First Industrial Revolution used water and steam power to mechanize production, the Second used electric power to create mass production, and the Third used electronics and IT to automate production, the Fourth Industrial Revolution is characterized by an unprecedented advance in digital technology, which is blurring the lines between the physical, digital, and biological spheres (Schwab, 2016) (Figure 5). Among the breakthroughs that characterize the Fourth Industrial Revolution is the ability to collect and analyze massive amounts of data in an automated way, then use this data for decision making and implement decisions in real time.

According to recent data, there will be more than 50 billion devices connected to the Internet by 2020 (Cisco, 2011), a trillion sensors connected to and transmitting information to analytical platforms in the cloud, and 44 trillion gigabytes generated (DHL, 2015). In this context, information that was previously created by people will increasingly be machine-generated, while the entire supply chain will be connected, including parts, products, and other smart objects used to monitor the supply chain (IBM, 2015). Based on these data, supply chains will be able to make decisions more accurately, autonomously, and in real time, to optimize operations, handle incidents that require risk-mitigation actions, avoid disruptions, and satisfy an increasingly volatile demand, thus allowing better risk management. According to recent studies, companies that have invested in these technologies for their supply chain management have cut up to 30 percent out of inventory, increased the average fill rate by up to 7 percent, and raised their revenue by up to 15 percent (DHL, 2015). In addition, wider implementation of such technologies in supply chain operations management by 2025 could generate savings of approximately US$7 trillion globally (McKinsey, 2015).

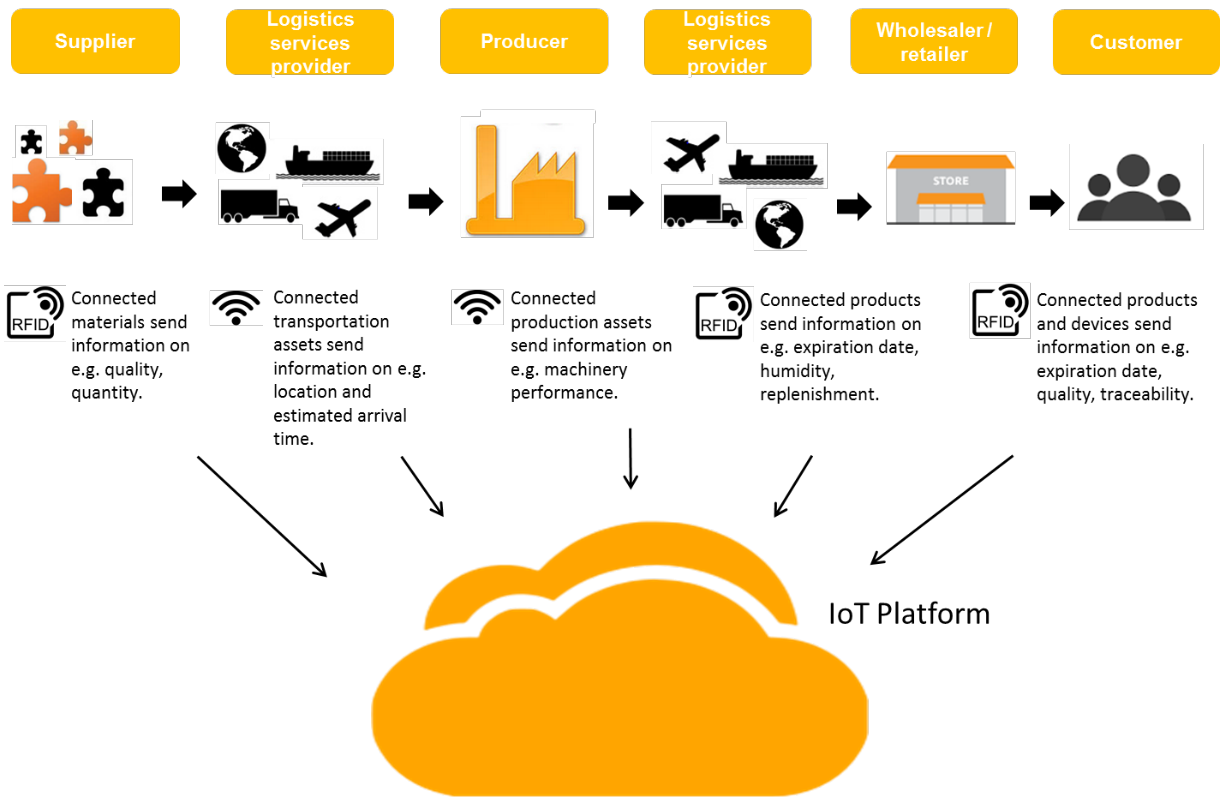
Figure 5. The Industrial Revolutions



Source: Author's elaboration.

The IoT is an important advance in this direction. The term refers to sensors and other types of instruments that can connect objects and machinery to computing systems (McKinsey, 2015). With the advent of IoT, Internet connections now extend to physical objects that are not computers in the classic sense and, in fact, have many other purposes. To light up such "dark assets," IoT encompasses a diverse array of technologies, including wireless local networks (e.g., Bluetooth, RFID, Zigbee, Wi-Fi), mesh networks, and wide area connections (e.g., 3G, LTE), as well as wired connections. For example, with IoT, a connected bottle can send information about temperature, time, and location throughout the bottle's entire journey across the supply chain, in-store, and at the point of consumption. A connected forklift can alert a warehouse manager to an impending mechanical problem or safety risk, or be used to create greater location intelligence of inventory in the warehouse. A connected jet engine can send information about speed, fuel consumption, malfunctioning parts, and others that can be analyzed to identify possible inefficiencies and prevent unnecessary downtime by spotting potential faults earlier. None of these products have traditionally been connected to the Internet. However, when they are, vast amounts of information can emerge, along with potential new insights and business value (DHL, 2015). As an example, a six-hour flight on a Boeing 737 from New York to Los Angeles can generate up to 120 terabytes of data, which is collected and stored on the plane. These data are a valuable asset since they can be analyzed to reveal every aspect of the engine's performance and health (Greengard, 2015). With IoT sensors deployed along the supply chain, extensive connectivity will enable worldwide supply chain partners to plan and make decisions together. Importantly, IoT, advanced analytics, and artificial intelligence will help decision makers evaluate alternatives and even make decisions automatically, thus increasing responsiveness and limiting the need for human intervention (IBM, 2015).

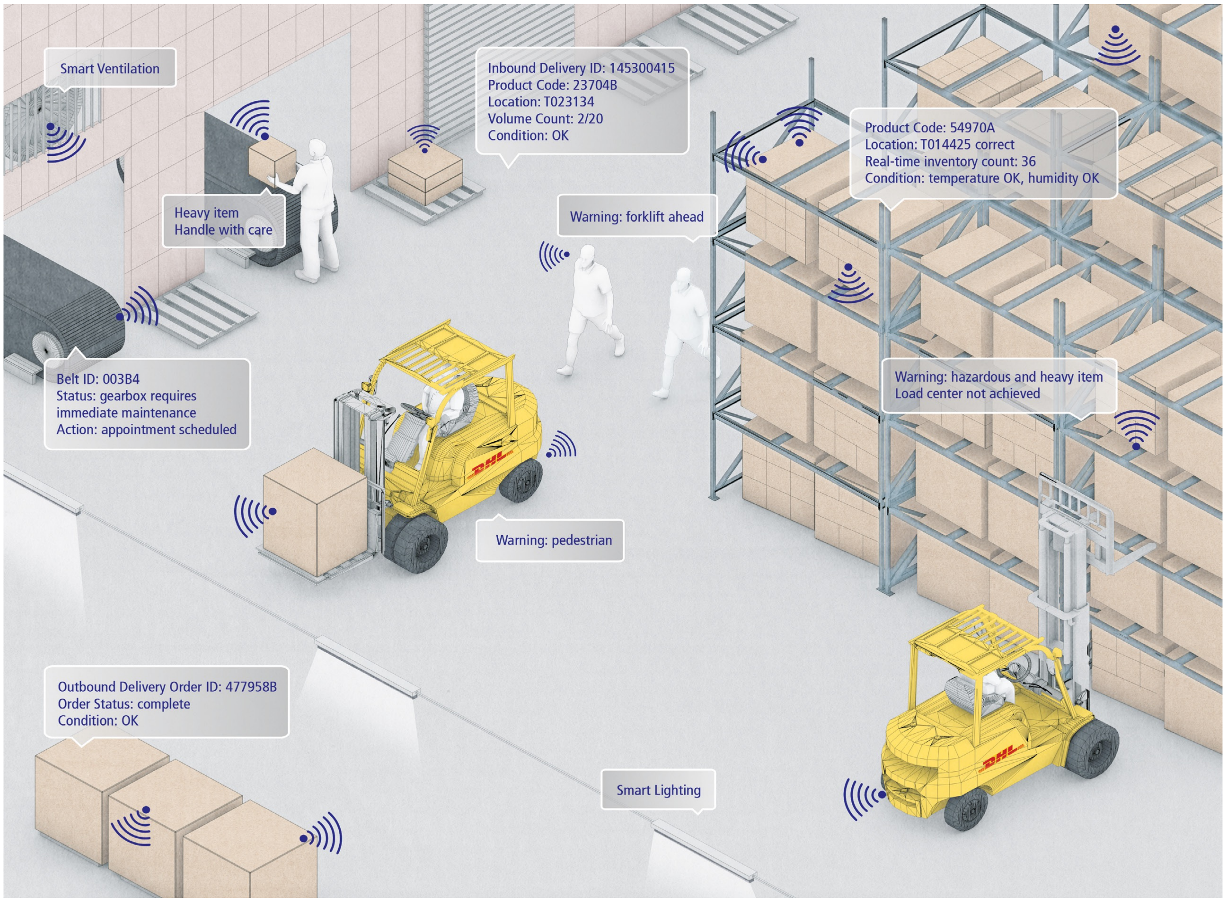
Figure 6. Example of IoT and Supply Chain Management



Source: Author's elaboration.

Recent studies show that supply chain risk management can benefit significantly from IoT technologies. With IoT, objects increase visibility throughout the supply chain by generating information in real time on the different supply chain processes. With thousands or even millions of sensors generating this data, risk management can be greatly improved. For example, placing sensors on supply chain materials can enable a more precise and reliable monitoring of inventories that flow across the actors and processes involved in the supply chain, thus avoiding human errors, input shortages, and the high cost of unnecessary inventory carrying. Moreover, they can enhance product end-to-end traceability, including quality control. Sensors capable of reporting on machinery performance and physical assets can indicate when maintenance is required and when machinery is likely to fail, thus avoiding damage and downtime. The Big Data produced by IoT technologies can be used to predict changes in consumer preferences and avoid the adverse effects of poor predictability, as well as inform probability-based risk assessments, early warning systems, and simulation models. Smart sensors and meters can help improve energy efficiency and reduce water consumption in production processes, using resources in the most efficient way and ensuring the sustainability of the supply chain. In general, IoT technologies enable the performance and the state of equipment, products, and systems to be remotely monitored and managed, thus maximizing physical asset utilization and optimizing operations management. Moreover, in the event of an incident, the supply chain can capitalize on real-time connectivity across the extended supply chain to respond in a rapid, coordinated fashion (IBM, 2015).

Figure 7. IoT and Risk Management in Warehousing

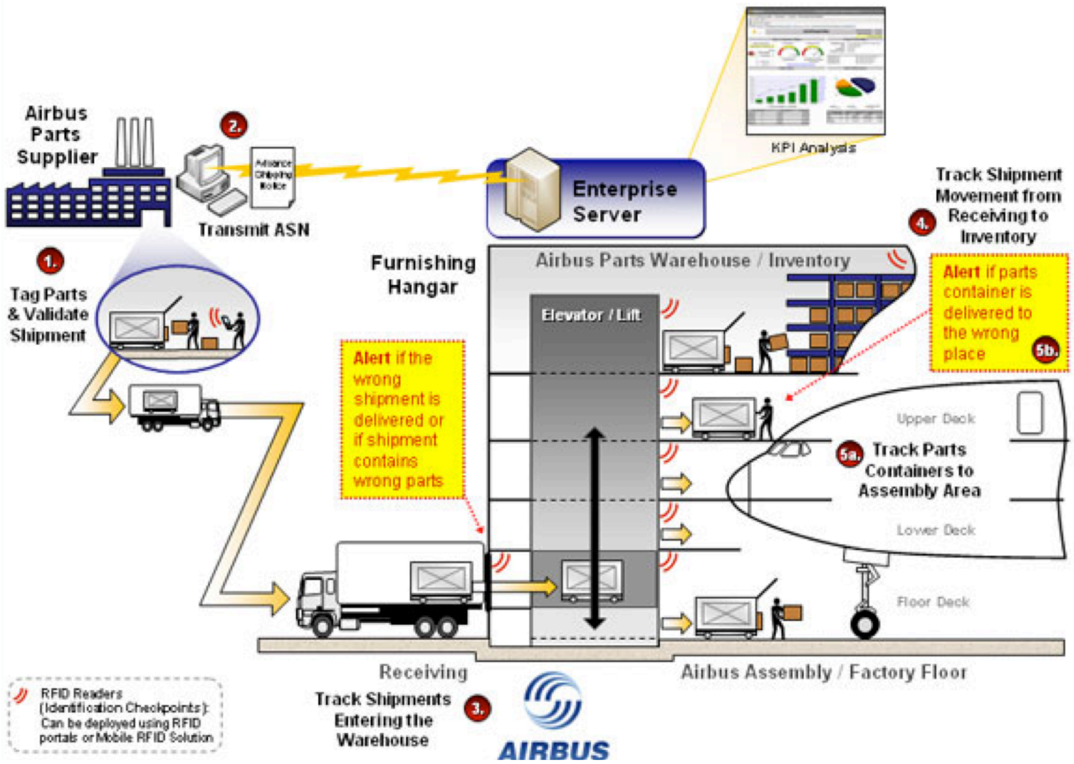


Source: DHL (2015).

Box 1. Examples of IoT Applications

Airbus, Diageo, Rolls Royce, and General Electric are examples of companies that are implementing sensing solutions to enhance risk management and supply chain efficiency. Airbus uses this technology to monitor inbound shipments with RFID-enabled containers that help determine whether they contain the right parts and if they will be delivered at the right location. When anomalies are detected, the system generates an early warning, alerting employees of any problem (Figure 8). With this solution, Airbus has been able to reduce the number of incidents and the number of containers by 8 percent, avoiding significant carrying costs and increasing the efficiency of materials flow (IBM, 2015).

Figure 8. Airbus' Vision for RFID-Enabled Business Processes



Source: Supply Chain Digest (2015).

Diageo has designed a "smart bottle" that uses thin sensors placed on the labels of the bottle. These sensors allow the firm to track bottle movements across the supply chain, in-store, and to the point of consumption. Sensor tags, which remain readable even when the factory seal has been broken, can tell where the bottle is in the supply chain, enhancing monitoring and alerting of any problem. Moreover, they can tell whether the bottle has been opened or not, providing an additional layer of security in protecting the authenticity of the product (Diageo, 2015).

Rolls Royce and General Electric use a range of sensors strategically positioned throughout aircraft turbine engines to record key technical parameters several times during each flight, such as temperature, pressure, speed, and vibration levels, to ensure they are within known tolerances and to highlight when they are not. Among others, these data are used to predict maintenance needs and optimize fuel consumption, thus reducing the risk of failure and operating costs.

Another emerging technology that promises large benefits for supply chain risk management is blockchain. This technology can help create and share information in an immediate, unalterable, and transparent fashion throughout the supply chain, without the need to set up costly centralized information-sharing systems. It also decreases the need for third-party intervention and reduces the number of documents that have to be shared. By using distributed ledger technology, all the information shared in the network is stored in each node, making it easier to access and trace transaction history. Any change to the information stored in the distributed ledger must be approved by consensus by all the nodes in the network. Once the change is approved, the information is immediately stored in each node. This makes the system more resilient to failure or targeted attacks. In addition, since blockchain uses cryptography to guarantee the information stored in the distributed ledger, it makes it virtually impossible to alter the information already stored without having the consensus of the nodes in the network. This is an important feature to avoid forgery and fraud in the information shared. Finally, the decentralized feature of blockchain eliminates the need for third parties to validate the information shared, which in turn reduces transaction costs and increases transparency. One expected benefit of blockchain relates to ensuring materials provenance and end-to-end product traceability (Kim and Laskowsky, 2016). Together with the use of IoT and Big Data, real-time information sensor-generated information can be encrypted, validated, and shared among supply chain partners to ensure, for instance, that the temperature, humidity, and quality conditions of materials and products have been unaltered in their flow thorough the supply chain. This is particularly important for the food industry in LAC, where every year 15 percent of annual production is lost, 74 percent of which is due to inefficiencies in production and logistics processes (FAO, 2012).

Figure 9. Blockchain Technology and Traceability in International Supply Chains

Source: Tabbakh (2016).

Box 2. A Peek into the Future: The "Self-thinking Supply Chain"

Practitioners of supply chain management suggest that, in the not-too-distant future, the supply chain will think by itself. Driven by IoT, robotics, and artificial intelligence, the supply chain will be self-aware and require minimum, if any, human intervention. The self-thinking supply chain will continuously monitor supply chain performance by analyzing a quintillion bytes of data generated by objects; forecast and identify risks; and automatically take actions to prevent risks before they materialize. The supply chain will autonomously learn from these activities and use such knowledge in future decisions. Importantly, large amounts of data and the use of powerful analytical and simulation models will allow the supply chain to predict the future with minimum error and take actions to, for example, address constant shifts in demand. The self-thinking supply chain will thus push supply chain flexibility and agility to limits yet to be discovered.

To maximize the benefits of information systems connectivity and the use of IoT and blockchain technologies, certain challenges have to be faced. Among them are: the lack of, or interruptions to, physical Internet access; component failures within systems; software bugs that generate errors and noise; interoperability of software and platforms; coping with proprietary and competing systems; and dealing with upgrades, patches, and obsolescence (Greengard, 2015). Another challenge is to filter, organize, analyze, and make available the extensive data created by digital technologies in a way that can be useful for supply chain management.

A number of platforms have emerged in recent years to provide analytical capability to supply chain managers based on the information generated by IoT technologies. These platforms are the backbone of IoT technology, since they enable the deployment of IoT applications on devices, connectivity among devices, remote data collection from connected devices, data analysis and storage, data transmission to devices, sensor management, and integration with other platforms or systems. Given the increasing attention that IoT technology is receiving from the private sector, a new business segment has been created: the IoT platform market. Companies offering IoT platforms include, for example, software development leaders (e.g., IBM, Microsoft), e-commerce leaders (Amazon), and industrial leaders (General Electric). In the case of industrial leaders, their participation in this segment takes place within a trend in manufacturing called "servitization." This refers to the strategic decisions of firms—often those operating in the manufacturing sector—to provide services and solutions that supplement their traditional product offerings. By offering an integrated product-service package, firms can differentiate themselves in a growing competitive environment (Baines et al., 2009).

3.2 Physical Connectivity

The connected supply chain also depends on physical connectivity, which is defined as the degree to which nodes in a network are connected to each other as a function of infrastructure and logistics services capabilities. The network of infrastructure and logistics services can speed up or delay the flow of materials, information, and financial resources across a supply chain (Calatayud et al., 2014). This network comprises road, rail, airport, and port infrastructure; logistics platforms, consolidation/deconsolidation centers and warehouses; trucking, rail, air, and maritime transportation services; other logistics services; telecommunications infrastructure and services; and border-crossing facilities (IDB, 2012; Ruiz-Rua and Calatayud, 2012). Indeed, production factors, supply, and demand are distributed across space. Economies of scale, agglomeration economies, product specialization, resource endowment, and geographic differences, among others, determine the location of economic activities. Physical connectivity allows materials and products to move between locations, overcoming the friction of distance and creating spatial convergence of supply and demand (IDB, 2010).

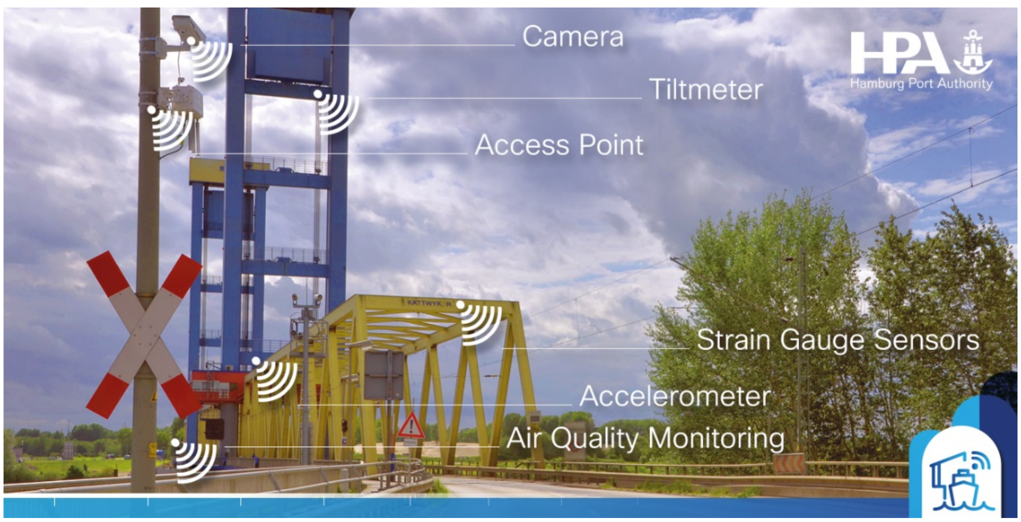
Physical connectivity has a direct impact on supply chain costs and efficiency. Poor transport infrastructure results in higher transportation costs (because of higher fuel consumption and fleet maintenance), large inventories and inventory costs, long and uncertain delivery times, and congestion (Memedovic et al., 2008). Likewise, the lack of adequate infrastructure services results in lower firm productivity and higher production costs (Calderon and Serven, 2002). Gonzalez et al. (2008) showed that poor infrastructure heavily influences inventories and financial costs. According to their study, in Latin America, businesses hold inventories up to an equivalent of 30 percent of GDP, while in Organisation for Economic Co-operation and Development (OECD) countries, inventories are at least half that amount.

Information systems connectivity can help improve physical connectivity. There is evidence that information systems connectivity and supply chain integration have a significant impact on infrastructure performance, since larger amounts of more accurate and real-time data help logistics terminals better accommodate the growing capacity and the other relevant trends in the highly fluctuating, competitive, low-margin logistics industry (Panayides and Song, 2013; Woo et al., 2013). The integration of supply chain information with logistics management and systems is consonant with the emerging interest from public, private, and academic sectors in moving toward integrated transport systems, so that the integrated management of infrastructure, services, policies, and information results in a more efficient and seamless movement of people and goods.

According to the International Transport Forum (ITF, 2012), apart from the infrastructure connection required to minimize transfer time between modes, a modern, integrated, seamless transport system requires the IT connection, which consists of integrating information systems to monitor, manage, and optimize the entire transport system. Hamburg's smartPORT initiative is an example in this direction. The second busiest port in Europe, the Hamburg Port Authority, embarked on an ambitious project of modernizing its IT infrastructure to coordinate all aspect of port operations, including ship, rail, and road traffic. As part of this project, road and waterway sensors were installed to coordinate ship-road traffic and monitor infrastructure performance

(DHL, 2015). The information gathered by sensors is used in a variety of ways, one of them being sending notifications to truck drivers on available parking spaces and bridge closures due to ship activities. This allows drivers to optimize route planning and reduce travel time. Maersk and IBM's initiative to digitize all paperwork currently required to move cargo internationally using blockchain technology is another example in this direction. A pilot recently completed with avocados shipped from Mombasa to Rotterdam showed that replacing paperwork and administrative procedures with blockchain technology could reduce the cost of international shipping between 15 and 20 percent (International Business Times, 2017). At the same time, blockchain technology could significantly increase visibility and reliability in international shipping.

Figure 10. Hamburg's smartPORT Initiative



Source: Cisco (2015).

In the context of the Fourth Industrial Revolution, physical connectivity will benefit from advances in new digital technologies. As illustrated below, unmanned vehicles, artificial intelligence, and IoT are among the main technologies that will revolutionize physical connectivity.

- Companies are already testing unmanned aerial vehicles (UAV)—also known as drones—to expand distribution channels and market access to areas where physical connectivity is difficult due to congestion or lack of (adequate) transport infrastructure. Drones can also be used to ensure delivery in situations where the logistics chain has been disrupted due to, for instance, natural disasters, transport infrastructure failure, strikes, or civil unrest. Pharmaceutics and medicine are supply chains where the use of UAVs is taking a lead. Haidari et al. (2016) cite examples of tests done by Matternet in Bhutan and Papua New-Guinea for medical supply distribution; UNICEF in Malawi for the transport of lab samples; and Delft University of Technology in the Netherlands for delivering defibrillators after cardiac arrest. The authors analyzed the case of vaccine delivery and estimated that the use of UAVs reduced the logistics cost per dose administered by approximately 20 percent. UPS is testing the use of drones to deliver packages in rural areas where physical connectivity is difficult. It has designed a new electric delivery truck with a drone launchpad atop it. After the driver loads a package into the drone's cargo bin and the drone lifts off, the driver can deliver a separate package. Then the drone and truck rendezvous at another location, where the drone is loaded with a fresh package. UPS estimates that this solution could improve operations and save on fuel. If every UPS driver had to cover one fewer mile per day, the company could save up to $50 million per year (CNN, 2017).

Figure 11. UPS Drone Delivery Test

Source: CNN (2017).

- Autonomous, unmanned technologies are being tested on other modes of transportation such as trucking, rail, and shipping. With the implementation of IoT and artificial intelligence, trucks, trains, and ships will be able to communicate with each other, with their passengers, other intelligent devices, supply chain control centers, and traffic controllers to coordinate movements, optimize routes, and transmit real-time data so as to improve reliability and efficiency in logistics processes (DHL, 2016). In road logistics, firms such as Volvo, DAF, Daimler, Scania, and Iveco have been testing truck platooning, a technology that uses adaptive cruise control and vehicle-to-vehicle communication systems to allow two or more trucks to electronically couple (JOC, 2016). This enables the lead truck to transmit information on acceleration and braking information, so that the trucks behind it can replicate these actions. Fuel efficiency and safety are the main benefits of this technology. With fuel accounting for as much as 40 percent of fleet operating costs, the reduction in fuel costs (up to 15 percent according to recent tests) represents significant savings that could be passed on to shippers, suppliers, and ultimately consumers (JOC, 2016). Autonomous technologies are likewise being tested in the maritime shipping industry. Sensors and artificial intelligence are used to allow a ship to monitor its own health, identify and communicate with the environment (e.g., smart ports), and make autonomous decisions on routing, speed, and fuel consumption. Rolls Royce (2016) envisages that a remotely operated local vessel will be in operation by 2020 already, and an autonomous, unmanned ocean ship by 2035.

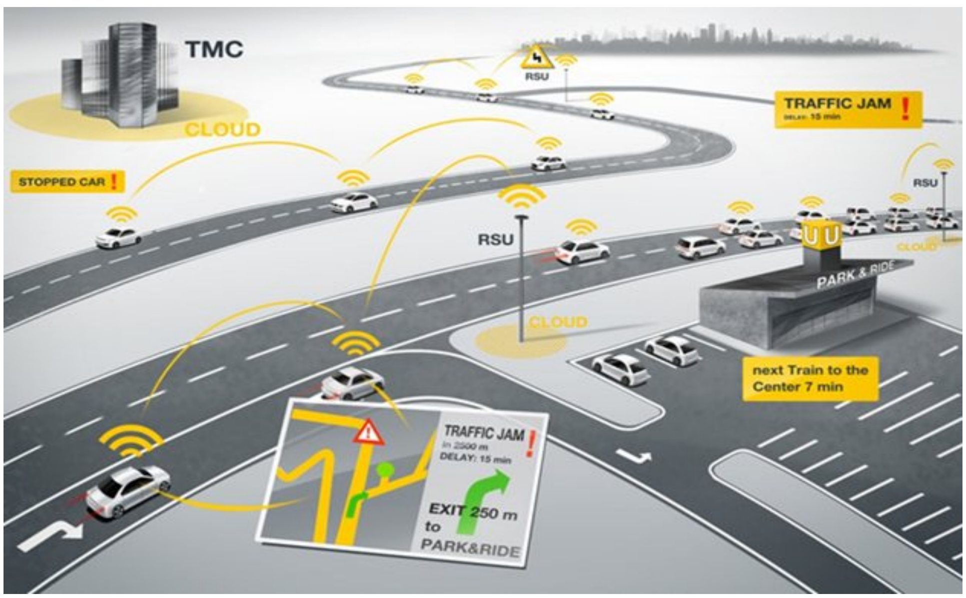
Figure 12. Truck Platooning and Autonomous Unmanned Ocean Ship

Source: Peloton (2016) and Rolls Royce (2016).

- Distribution, wholesale, and retail companies are investigating the potential for anticipatory shipping. Big Data, IoT and artificial intelligence will enhance firms' ability to accurately predict demand and ship products closer to customers before orders have actually been placed (Leveling et al., 2014). Through anticipatory shipping it is expected that companies will be able to optimize logistics asset utilization and reduce delivery time and last-mile costs. Another way to improve asset utilization has recently emerged with the development of Internet platforms that match available capacity on trucks or containers with shippers' needs. Through these platforms, shippers are able to see available space on trucks or containers and book the amount of space they need, even if they do not need all available space. As an example of this, in 2017 the shipping company CMA CGM followed Maersk's lead and signed a memorandum of understanding with the e-commerce platform Alibaba to allow customers to book container space online through Alibaba's OneTouch platform (The Load Star, 2017). OneTouch also offers import and export services, such as customs clearance and logistics, as well as air freight and express booking. Shipping companies are seeing digitization as a means to improve asset utilization and increase value to customers in a highly competitive market. Indeed, available reports suggest that the expected benefits of these platforms are twofold (PwC, 2016). Space utilization is maximized by allowing different shippers to directly book space in the same truck or container, and the fares offered by different carriers are displayed to shippers through the platform, enabling rates to be compared and increasing transparency and competition in the sector.

- IoT sensors placed on infrastructure and logistics assets are making them "smart." Billions of data can now be generated in real time and transmitted from transport, energy, water, and telecommunication infrastructure. Data are analyzed by powerful software and on-the-cloud platforms and transformed into useful information for both human and autonomous decision making on network and resources optimization. For example, sensors placed on traffic lights can measure congestion levels and send this information to truck drivers for alternative routing and to public agencies for traffic management decisions. Sensors placed on parking spots at logistics and port facilities can generate information on available spots, the best route to reach them, and the expected cost. Importantly, the information generated by sensors can dramatically increase real-time performance monitoring, improve the accuracy of simulations, and prevent infrastructure failure before problems even emerge.

Figure 13. Vehicle to Infrastructure (V2I) Communication



Source: Kapsch (2014).

Risk management will benefit from digital technologies applied to improve physical connectivity. The use of IoT technologies can advance risk analysis models by providing information for risk monitoring, prediction, and simulation. They can improve logistics networks and asset utilization, enhance performance monitoring, and alert on any deviation from normal values so as to enact risk mitigation activities before disruptions occur. Importantly, given that the connected supply chain depends on the coordination of a number of infrastructure assets and logistics services for the seamless flow of materials, products, information, and financial resources, the use of new digital technologies can improve information sharing and collaborative decision making—either with or without human intervention—to enhance overall network utilization and avoid delays and disruptions. Moreover, technologies such as UAV can be used to overcome operational risks created by disruptions in, or the lack of (adequate), transport infrastructure, thus improving distribution networks.

4. Barriers to the Connected Supply Chain and the Role of Public Policy

There are a wide range of barriers that prevent the achievement of end-to-end connectivity and, with it, improving risk management in supply chains. Despite the benefits of the connected supply chain in terms of operational efficiency and risk management, the reality is that supply chains and firms, particularly those in developing countries and those of smaller size, are lagging behind in their efforts to achieve connectivity with their partners. According to recent surveys (IBM, 2015; WEF, 2016), the main barriers to the connected supply chain from the private sector's perspective are the following:

- Cost of actions to improve connectivity
- Lack of access to finance
- Outdated or lack of information systems capabilities/resources
- Lack of (adequate) transport, logistics, energy, and telecommunications infrastructure
- Low performance of logistics services
- Managers' short-term perspective
- Poor organizational structures
- Lack of labor skills
- Regulatory uncertainty
- Adverse business climate
- Privacy and security protection
- Cumbersome administrative procedures
- Lack of trust, willingness to collaborate, or common goals

What role can the public sector play in overcoming these barriers? Certainly, private sector action and collaboration are needed to solve connectivity challenges such as lack of trust, unwillingness to collaborate with supply chain partners, lack of common goals, and low organizational compatibility. In other areas, however, public policies can play a critical role in promoting supply chain connectivity. This is because the presence of incomplete markets, externalities, and coordination failures in different areas related to achieving supply chain connectivity make private sector action insufficient to achieve a connected supply chain. Among other things, the public sector can put in place the enabling environment to enhance private sector collaboration or leverage private sector investments (e.g., logistics infrastructure and information systems). In addition, the public sector can directly strengthen connectivity by, for example, increasing access to finance for the productive sector, improving transport, energy, and telecommunications infrastructure, and providing an adequate regulatory framework for firms to operate. The following paragraphs discuss the role of the public sector according to each component of the connected supply chain, namely: (i) information systems connectivity and (ii) physical connectivity. While this section presents the main areas for public policy (Table 2), future IDB publications will further analyze the specific actions that the public sector in LAC countries can take in areas such as UAV legislation and national or sector IoT strategies.

Table 2. Main Areas for Policy Action

<table>
<tr><th colspan="2">General Objective: Improve Supply Chain Connectivity</th></tr>
<tr><th>Specific objective 1: Increase information systems connectivity</th><th>Specific objective 2: Enhance physical connectivity</th></tr>
<tr><td>Area 1.1 - Regulatory framework:
Privacy and safety
Spectrum allocation
Standards and interoperability
Area 1.2 - Policies and programs:
Access to finance
Workforce skills
Broadband infrastructure
Market development
Area 1.3 - IoT strategies</td><td>Area 2.1 - Regulatory framework:
Infrastructure management and maintenance
Private sector investment
Safety
Interoperability
Climate change mitigation
Trade infrastructure
Area 2.2 - Policies and programs:
Infrastructure investment
Climate change resilience
Safety
Trade facilitation</td></tr>
</table>

4.1 Information Systems Connectivity

The public sector can help increase information systems connectivity by: (i) putting in place a regulatory framework that at the same time promotes private sector investment and mitigates risks for the economy and society, and (ii) implementing policies and programs aimed at increasing technology development and adoption by the private sector. The efficiency and productivity gains derived from increasing information systems connectivity across the supply chain are certainly important incentives for the private sector to develop and adopt the technology needed to achieve connectivity. However, while the private sector should be the main driver of the connected supply chain, an array of market failures could limit progress toward increased connectivity. Externalities, public goods, and uncertainties are among the main market failures limiting the private sector's incentives in this area. Externalities are social and economic benefits—or costs—derived from an economic activity that are experienced by a third party not directly involved in that activity. An example of a positive externality in this area is the decrease in water and energy waste in supply chain processes through increased information sharing and improved processes coordination among partners. In this case, the social benefits can be higher than those of firms, discouraging investment. Moreover, the private sector will not be willing or able to provide the public goods needed for obtaining the maximum benefits and the minimum risks of increased information systems connectivity. Among those are ensuring privacy and safety for society and the economy, and having a workforce highly skilled in areas demanded by the new digital economy (e.g., software development, Big Data analytics, web management). Similarly, uncertainties on the benefits or costs from the adoption of new technologies often discourage the private sector from moving toward technology adoption. The following paragraphs will discuss the role that the public sector can play in overcoming these market failures and promoting the connected supply chain.

Regulation is essential for promoting technology adoption by the private sector while mitigating risks for the economy and society. Protecting user and business privacy, safeguarding intellectual property, and strengthening regulation in safety matters are all areas where the public sector has traditionally played a critical role and accumulated significant experience. In the context of the Fourth Industrial Revolution and the rise of new digital technologies, new regulatory challenges will emerge in these areas, namely:

- *Privacy and safety:* The public sector will have to create and protect a favorable environment to facilitate the adoption of technologies like UAV and other unmanned-autonomous vehicles, IoT and artificial intelligence, and at the same time minimize the risks in terms of privacy and safety that these new technologies may generate. The main challenges posed by these technologies are: (i) enabling unauthorized access and misuse of personal or business information; (ii) facilitating attacks on systems; and (iii) creating risks to personal safety (Federal Trade Commission [FTC], 2015). Importantly, there is increasing concern about threats related to cyber espionage and cybercrime (IDB-OAS, 2016). According to a survey conducted by IBM (2016) in 12 countries, there were 1.5 million cyberattacks in 2015 in those countries alone. IBM estimated that businesses were attacked an average of 16,856 times that year. Although an average of only 1.7 attacks per week were successful, the average consolidated total cost of a data breach grew from $3.8 million in 2014 to $4 million in 2015. If not efficiently addressed by both the private and the public sectors, these challenges could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption (FTC, 2015). To face them, governments around the world are working on updating and creating new legislation on consumer protection, privacy, and national security as well as setting legal procedures for regulatory compliance. Other critical steps in this direction are: (i) to enhance intergovernmental collaboration as a means to ensure a consistent and predictable regulatory environment, and (ii) to work closely with the private sector to, for instance, educate consumers, encourage risk-based approaches, and promote security by design (USDOC, 2017).

- *Spectrum allocation:* The deployment of IoT technologies and machine-to-machine (M2M) communications applications will generate billions of connected devices communicating with one another. This influx of new connected devices will create demands for spectrum frequency space that many national spectrum licensing regimes will likely be unable to support (New and Castro, 2015). Therefore, governments will need to make available greater amounts of licensed and unlicensed spectrum. Some countries are already working on estimating the spectrum needs of IoT and M2M, as well as developing roadmaps toward making that space available. For example, Australia is working on amending its regulatory arrangements to remove technical barriers to the operation of narrowband low-powered wireless networks and support a variety applications such as data telemetry, machine data and monitoring, sensor networks, smart metering, security systems, and industrial control. Other proposed changes include the addition of the new frequency bands for radio-determination transmitters used as industrial sensors and in-ground ultra-wide bandwidth transmitters used in automated parking management systems. In 2016, the United Kingdom telecommunications regulator announced that it would reserve a proportion of very high frequency (VHF) wireless spectrum for future use by IoT connected devices. Moreover, a new category of license was created specifically for IoT/M2M communications applications. In 2017, Spain announced that it would cut costs and expedite licensing and administrative procedures for obtaining authorizations regarding the use of radiofrequency by IoT devices.

- *Standards and interoperability:* Although the private sector can and should take the lead in the development and adoption of standards for information systems, coordination with the public sector is important to avoid the undesired effects of incompatible systems and lagging adoption. With this purpose, for example, the U.S. government joined the group formed by firms like AT&T, Cisco Systems, General Electric, IBM, and Intel, which aims at cooperating in establishing engineering standards for IoT equipment. Indeed, the perspective adopted by the United States and other countries is that, with active participation from government experts as needed, the industry is ideally positioned to lead the development of technological standards and solutions to address IoT opportunities and challenges (USDOC, 2017).

Box 3. Regulating UAV

As interest grows in using UAV for commercial purposes, countries around the world are updating their legal frameworks to regulate UAV. Countries are adopting different positions on the commercial use of UAV, from banning operations to allowing flying UAV beyond line-of-sight. Countries such as the United States and the United Kingdom are adopting an incremental approach, meaning that they are putting regulations in place for the current status of the industry, while the authorities gain a better understanding of operational issues such as training requirements, operational specifications, and technology considerations. The current legislation may be changed as more information becomes available and the technology advances to satisfy public safety standards. To help countries in this challenging regulatory area, the International Civil Aviation Organization recently released a toolkit to guide them in the design of regulatory frameworks that consider public and aviation safety first, along with security and privacy protection, while at the same time promoting technological advances (https://www4.icao.int/uastoolkit/home/about).

Public policy and programs can incentivize the adoption of information systems technologies to increase supply chain connectivity. The presence of market failures such as externalities, public goods, and uncertainties can limit private sector investment in the development and adoption of technologies toward increased supply chain connectivity. Without proper action from the public sector, market failures then materialize in the barriers to technology adoption mentioned in the literature, namely: lack of access to finance, lack of (adequate) infrastructure, lack of labor skills, and poor managerial strategies. There are different ways in which the public sector can incentivize technology investments in the supply chain, including the following:

- *Increasing access to finance*: One important barrier to technology adoption that firms often mention is lack of access to finance (WEF, 2016). Improving connectivity requires financial resources to enable investments in software acquisition, IoT equipment, prototyping and testing, physical assets for updating supply chain processes, and others. Given the presence of a number of market failures (positive externalities, coordination failures, uncertainties and risks), access to finance is particularly limited in the case of technology development and adoption. In addition, access to finance is especially low, expensive, and short term in developing countries and for small- and medium-sized enterprises (SMEs) (IDB, 2017). The thorough review of policies and programs worldwide conducted by IDB (2017) shows that the public sector can improve supply chain and firm performance by increasing access to finance for investment, innovation, and market access. Development banks are key actors in designing and coordinating financial strategies to promote investment in economic sectors or market segments with multiple risks and/or barriers between supply and demand for finance (IDB-CMF, 2013). They can combine a wide array of financial (e.g., credit, guarantees, factoring) and non-financial instruments (e.g., technical assistance and training) to enhance technology development and adoption in supply chains. In many LAC countries, such as Brazil, Colombia, and Mexico, development banks are already playing a leading role in providing access to finance for supply chains (Calatayud and Ketterer, 2016). As LAC economies transition into the Fourth Industrial Revolution, development banks will be an important source of financing for advancing technology adoption in supply chains.

- *Improving workforce skills*: The public sector can help diffuse information systems connectivity by promoting training and helping firms address the shortage of human capital in the areas of science and technology, engineering, and supply chain management. According to the OECD (2016), the increasing use of digital technologies at work is raising the demand for new skills along three lines: (i) specialized skills to program, develop applications, and manage networks; (ii) generic skills to use such technologies for professional purposes; and (iii) complementary skills to perform new tasks associated with the use of technologies at work (e.g., information processing, self-direction, problem-solving, and communication). In this context, governments will need to identify the skills on which their workforce will have to be trained; examine how these changes will translate into curriculum reform, teacher training, and professional development; and leverage technologies to improve access to and the quality of education and training (e.g., through online courses, new learning tools at school, and adequate recognition of skills acquired through informal learning) (OECD, 2016). In addition to general workforce training, the public sector can provide firms with resources for technical assistance to improve operations management skills, particularly in SMEs, which often lack trained human capital in these areas.

- *Developing broadband infrastructure*: Meeting the connectivity demand of the digital economy will require deployment and continued modernization of infrastructure networks. Such efforts should have a positive multiplier effect on new digital technology usage and functionality (USDOC, 2017). While many countries agree that the push for infrastructure deployment should be private-sector led, the public sector can play an important role in ensuring that infrastructure continues to expand, that access is inclusive and affordable, and that infrastructure remains innovative, open, secure, interoperable, and stable (USDOC, 2017). Specifically, there are three areas where studies suggest that public policies are needed to enhance broadband deployment: (i) reducing or eliminating special taxes, surcharges, and/or import duties that apply solely to broadband services and terminals; (ii) assessing spectrum requirements and allocating spectrum; and (iii) targeting the use of universal service funds to finance critical broadband infrastructure and elements of adoption, such as subscriptions, content, devices, and training, to close the digital divide in societies (IDB, 2012).

- *Encouraging markets*: The importance of government lies in its role as policymaker and regulator, and as an enabler and adopter of new technologies. Indeed, governments can promote the advancement of information and communications technology usage through increased technology adoption by public institutions. By doing so, government can reduce the perceived risk of technology that limits investment and adoption by the private sector, particularly in cases where those technologies are of recent development (USDOC, 2017). Moreover, these technologies can enable governments to deliver better, cheaper, and more efficient public services. Particularly relevant for the effective performance of supply chains is when public institutions that take part in supply chain processes (e.g., customs, infrastructure and logistics nodes, and sanitary and phytosanitary agencies) adopt these technologies. When information connectivity is achieved throughout firms and public agencies that take part in the same supply chain, all private and public actors gain unprecedented visibility into supply chain operations, enabling new sources of efficiency. Other ways in which governments can encourage market development are by supporting research and development (R&D) and implementing pilot cases to increase awareness of the potential of these technologies for improved supply chain management.

Designing and implementing IoT strategies at the national and/or sector level are important ways to enhance information systems connectivity and promote the benefits of the connected supply chain. In line with the benefits for firms and supply chains discussed in Section 2, countries around the world are recognizing the importance of promoting IoT. China, Germany, Japan, Singapore, and the United States have created specific IoT programs and are moving forward in the design of comprehensive IoT strategies (New and Castro, 2015; USDOC, 2017).

Such strategies should ensure that the technology develops cohesively and rapidly, that firms do not face barriers to adoption, and that both the private and public sectors take full advantage of the coming wave of technological changes. While there is no one-size-fits-all approach to developing IoT programs or strategies, available experiences show that most of these programs or strategies are based on a set of principles that include: (i) enabling infrastructure availability and inclusive access; (ii) encouraging collaboration with private sector and among government agencies; (iii) promoting regulatory frameworks that ensure a stable, secure, and trustworthy IoT environment; and (iv) encouraging market growth and innovation. Regarding specific public sector activities, IoT strategies include at least the following lines of action:

(i) setting a regulatory framework that maximizes IoT benefits and promotes innovation while minimizing the risks for society (e.g., privacy and cybercrime)
(ii) ensuring that the necessary infrastructure for IoT adoption is in place
(iii) allocating funds to increase access to finance for IoT development and adoption by the private sector
(iv) fostering R&D
(v) generating a workforce equipped with the necessary skills to fully capture the benefits of IoT
(vi) increasing IoT adoption by the public sector
(vii) incentivizing private-public partnerships
(viii) enhancing inter-agency coordination

4.2 Physical Connectivity

Public sector participation is important to improve the capacity and quality of transportation, logistics, energy, and telecommunications infrastructure. The private sector mentions lack of adequate infrastructure as one of the main obstacles to achieve a connected supply chain. Because private sector participation in infrastructure investment is often limited by market failures such as public goods and externalities, governments have a critical role in: (i) creating an enabling regulatory environment that incentivizes infrastructure investment; and (ii) directly investing in infrastructure to guarantee inclusive access.

The actions that governments should take in both areas are well documented in the literature. On the regulatory and institutional side, governments should seek to promote, among others: (i) strengthening of regulations for the management and maintenance of infrastructure assets; (ii) the consolidation of regulatory frameworks governing private participation in the sector; (iii) standards for mode inter-operability; (iv) formalization of transportation systems; (v) innovative financing mechanisms (new payment sources, etc.); (vi) plans, regulatory frameworks, or strategies for climate change mitigation and adaptation; and (vii) strengthening of expenditure efficiency measures and data collection on infrastructure (IDB, 2016). The public sector can also play an important role in increasing physical connectivity by directly investing in infrastructure. This could include: (i) expanding the coverage of infrastructure networks; (ii) boosting connectivity for isolated communities and rural areas; (iii) expanding the capacity and improving the quality of road, port, airport, and rail transportation networks and associated transportation services (e.g., to alleviate congestion problems or increase regional development and integration); (iv) supporting the rehabilitation and maintenance of road systems and other degraded infrastructure, with a view to regaining operational capacity; (v) improving the resilience of infrastructure to natural phenomena and the effects of climate change; and (vi) improving the safety of transportation systems (IBD, 2016). Overall, given the wide array of infrastructure needed for good performance of the supply chain (transport, logistics, energy, and telecommunications infrastructure), public sector participation is critical to coordinate infrastructure investments in a way that helps minimize the systemic risks (e.g., natural disasters or adverse weather conditions) and operational risks (e.g., power outages) that supply chains may face in a given country.

Enhancing physical connectivity also requires simplifying administrative and trade facilitation processes. The public sector can facilitate the smooth flow of materials and products throughout infrastructure and logistics gateways (e.g., ports, border crossings) by ensuring that the required logistics infrastructure and services are in place and setting the appropriate administrative and trade procedures (Ruiz-Rua and Calatayud, 2012). There is abundant literature on the actions that governments need to take to streamline such procedures (IDB-WB, 2012), and on the positive impact that of actions on trade flows and infrastructure performance (Calatayud et al., 2016). In the case of international food supply chains, governments can improve connectivity by providing appropriate facilities and regulations for sanitary and phytosanitary analysis and customs compliance, reducing inspection times, and coordinating these processes with firms to improve operations management and the efficient use of logistics infrastructure. This also requires improving information systems connectivity between firms and public agencies (e.g., sanitary and phytosanitary agencies and customs). A step forward in this direction is the adoption of single windows, whose purpose is to provide a platform and processes for an electronic exchange of trade information between participants in the trade process, largely accomplished through a single electronic lodgment (UNESCWA, 2011). With the entry into force in February 2017 of the Trade Facilitation Agreement and its provisions to simplify, modernize, and harmonize export and import processes, it is expected that the burden posed by bureaucratic delays will significantly decrease, which will enhance supply chain connectivity.

Importantly, in the context of the Fourth Industrial Revolution, the public sector should promote the adoption of new digital technologies in infrastructure and administrative procedures, as a way to make the most out of these technologies for supply chain connectivity. As explained in Section 2, a fully connected supply chain needs real-time information sharing with logistics gateways and public agencies that participate in supply chain processes. The adoption of new digital technologies can enable governments to deliver the public services required by supply chains in a better, cheaper, and more efficient way. If they lag in adopting technology, they prevent supply chains from taking full advantage of technological advances. For example, UAV and other unmanned automated vehicles need constant communication with intelligent infrastructure to get information on traffic, road closures, and parking availability. This is not possible without a smart infrastructure, namely, an infrastructure that incorporates sensors and algorithms that use data exchanged between vehicles and infrastructure elements to perform calculations and send alerts to drivers. Likewise, without smart infrastructure it will be difficult to implement dynamic light and traffic control and reduce delays and disruptions in transportation systems. Therefore, public agencies should factor the coming changes into their investment plans, to avoid building the infrastructures of yesterday. In the case of vehicle-to-infrastructure (V2I) communication, this would imply, for instance, including investments on roadside units, signal phase, and timing-enabled traffic signal controllers, data links between V2I components, and a traffic management center or other back office, and any sensors or relays that link to or serve these components (USDOT, 2014).

In addition, governments can promote the advancement of new digital technology usage through increased technology adoption by public institutions. By doing so, they can reduce the perceived risk of the technology that limits investment and adoption by the private sector, particularly in cases where those technologies are of recent development. Hamburg’s smartPORT initiative is an example of this. As part of its project of modernizing its IT infrastructure to coordinate all aspects of port operations in this project, road and waterway sensors were installed to coordinate ship-road traffic and monitor infrastructure performance (DHL, 2015). To realize the full potential benefits of this project, logistics operators are improving their information systems capabilities to receive and use the notifications sent by the port to truck drivers on available parking spaces and bridges closures. This is allowing drivers to optimize route planning and reduce travel time.

5. Conclusions

A connected supply chain can significantly enhance risk management. This paper defined connectivity as the seamless flow of materials, information, and financial resources along the supply chain and suggested two factors that enable connectivity: (i) information systems connectivity and (ii) physical connectivity. Information systems connectivity refers to the electronic linkage of partners up and down the supply chain. Specifically, information systems connectivity helps manage risks in three ways. First, it helps identify possible vulnerabilities across the supply chain, which informs the design of risk management plans. Second, it helps prevent the occurrence of events that could become risks if no action is taken. Third, since it provides real-time information on events in the supply chain, it enables the rapid implementation of risk-management measures. In the context of the Fourth Industrial Revolution, one critical step toward better supply chain risk management is the use of new digital technologies such as IoT, blockchain, and artificial intelligence. Based on the large amount of data generated through these technologies, supply chains will be able to make decisions more accurately, autonomously, and in real time to optimize operations, face incidents that require risk-mitigation actions, avoid disruptions, and satisfy an increasingly volatile demand.

Physical connectivity is the degree to which nodes in a network are connected to each other as a function of infrastructure and logistics services capabilities. Lack of (adequate) infrastructure and logistics services is an important risk for supply chains, since they can delay, or even disrupt, the flow of materials, information, and financial resources. Like information systems connectivity, digital technologies can radically improve physical connectivity, thus reducing supply chain risks. Larger, more accurate, and real-time data can provide information for risk monitoring, prediction, and simulation. Technologies such as UAV can be used to overcome operational risks created by physical disruptions.

The public sector can play a critical role in overcoming the barriers to supply chain connectivity, thus increasing the ability to manage supply chain risks. It can put in place a regulatory framework and business climate that maximize the benefits and minimize the risks of the new technologies, leverage private sector investments in logistics infrastructure and information systems, and enhance public-private sector collaboration, among others. It can also strengthen connectivity by designing programs aimed at, for example, increasing access to finance for technology adoption; promoting training and helping firms address the shortage of human capital in science, technology, engineering, and mathematics (STEM) sectors; promoting R&D; increasing technology adoption by public institutions that take part in supply chain processes; and supporting the construction of logistics, energy, and telecommunication infrastructure in areas where it is needed. While this paper provides an overarching analysis of the connected supply chain and its benefits for risk management in a changing world, future studies should examine the specific role that the public sector can play in the different areas mentioned above.

References

Baines, T. S., H. W. Lightfoot, O. Benedettini, and J. M. Kay. 2009. “The Servitization of Manufacturing: A Review of Literature and Reflection on Future Challenges.” *Journal of Manufacturing Technology Management* 20(5): 547–67.

Calatayud, A. and J. A. Ketterer. 2016. “Integrated Value Chain Risk Management.” Technical Note No. 922, Washington D.C.: Inter-American Development Bank.

Calatayud, A. et al. 2016. “Understanding Connectivity to International Markets: A Systematic Review.” *Transport Reviews* 36(6): 713–36.

Calatayud, A. et al. 2014. “A Novel Concept for Measuring Connectivity to International Markets.” Proceedings of the XVII Pan-American Congress on Traffic, Transport Engineering and Logistics, Santander, Spain.

Calderon, C. and L. Serven. 2002. “The Output Cost of Latin America’s Infrastructure Gap.” Santiago: Central Bank of Chile.

Cao, M. and Q. Zhang. 2011. “Supply Chain Collaboration: Impact on Collaborative Advantage and Firm Performance.” *Journal of Operations Management* 29: 163–80.

Christopher, M. and M. Holweg. 2011. ‘”Supply Chain 2.0: Managing Supply Chains in the Era of Turbulence.” *International Journal of Physical Distribution & Logistics Management* 41(1): 63–82.

-----. 2017. “Supply Chain 2.0 Revisited: A Framework for Managing Volatility-induced Risk in the Supply Chain.” *International Journal of Physical Distribution & Logistics Management* 47(1): 2–17.

Christopher, M. and H. Lee. 2004. “Mitigating Supply Chain Risk Through Improved Confidence.” *International Journal of Physical Distribution & Logistics Management* 34(5): 388–396.

Cisco. 2011. “The Internet of Things: How the Next Evolution of the Internet Is Changing Everything.” *White Paper*, Cisco.

-----. 2015. “Port of Hamburg Paves the Way with Europe’s First smartROAD.” Available from: <https://newsroom.cisco.com/press-release-content?articleId=1646155>. [Accessed 3 March 2017].

Closs, D. and M. Swink. 2005. “The Role of Information Connectivity in Making Flexible Logistics Programs Successful.” *International Journal of Physical Distribution and Logistics Management* 35: 259–77.

CNN. 2017. “UPS Drivers May Tag Team Deliveries with Drones.” Available from: <http://money.cnn.com/2017/02/21/technology/ups-drone-delivery/?mod=djemlogistics>. [Accessed 18 March 2017].

Coronado-Mondragon, A. E., E. S. Coronado, and C. S. Lalwani. 2009. “Wireless Vehicular Networks to Support Road Haulage and Port Operations in a Multimodal Logistics Environment.” *Proceedings of 2009 IEEE International Conference on Service Operation, Logistics and Informatics*: 62–7.

Danese, P., P. Romano, and M. Formentini. 2013. “The Impact of Supply Chain Integration on Responsiveness: The Moderating Effect of Using an International Supplier Network.” *Transportation Research Part E*, 49: 125–40.

Deloitte. 2015. “Supply Chain Talent of the Future.” New York: Deloitte.

DHL. 2015. “Internet of Things in Logistics', Germany: DHL.

-----. 2016. “Logistics Trend Radar.” Germany: DHL.

Diageo. 2015. “Diageo and Thinfilm Unveil the Connected Smart Bottle.” Available from: <http://www.diageo.com/en-row/ourbrands/infocus/Pages/diageo-and-thinfilm-unveil-the-connected-smart-bottle.aspx>.

FAO (Food and Agricultural Organization). 2012. *Pérdidas y desperdicios de alimentos en el mundo*, Rome: FAO.

Fawcett, S. E. et al. 2007. “Information Sharing and Supply Chain Performance: The Role of Connectivity and Willingness.” *Supply Chain Management-an International Journal* 12(5): 358–68.

FTC (Federal Trade Commission) 2015. “Internet of Things: Privacy and Security in a Connected World.” *FTC Staff Report*, Washington D.C.: FTC.

Flynn, B., B. Huo, and X. Zhao. 2010. “The Impact of Supply Chain Integration on Performance: A Contingency and Configuration Approach.” *Journal of Operations Management* 28: 58–71.

Goldsby, J. 2009. “Supply Chain Risks: A Review and Typology.” *The International Journal of Logistics Management* 20(1): 97–123.

Golicic, S., D. Davis, T. McCarthy, and J. Mentzer. 2002. “The Impact of e-Commerce on Supply Chain Relationships.” *International Journal of Physical Distribution & Logistics Management* 32: 851–71.

Gonzalez, J., J. Guasch, and T. Serebrisky 2008. “Improving Logistics Costs for Transportation and Trade Facilitation.” Washington D.C.: The World Bank.

Greengard, S. 2015. *The Internet of Things*, Cambridge, MA: MIT Press.

Gunasekaran, A. and E. W. T. Ngai. 2004. “Information Systems in Supply Chain Integration and Management.” *European Journal of Operational Research* 159(2): 269–95.

Haidari, L., et al. 2016. “The Economic and Operational Value of Using Drones to Transport Vaccines.” *Vaccine* 34: 4062-7.

Hillman, M. and H. Keltz. 2007. “Managing Risk in the Supply Chain: A Quantitative Study.” *AMR Research*.

Holton, G. 2004. “Defining Risk.” *Financial Analysts Journal* 60(6): 19–25.

IBM. 2015. “The Smarter Supply Chain of the Future.” IBM.

-----. 2016. “2016 Ponemon Cost of Data Breach Study: Global Analysis.” IBM.

IDB (Inter-American Development Bank). 2010. *Freight Logistics in Latin American and the Caribbean: An Agenda to Improve Performance.* Washington D.C.: IDB.

-----. 2012. *Bridging Gaps, Building Opportunity: Broadband as a Catalyst of Economic Growth and Social Progress in Latin America and the Caribbean.* Washington D.C.: IDB.

-----. 2013. *Bancos públicos de desarrollo: ¿Hacia un nuevo paradigma?* Washington D.C.: IDB.

-----. 2016. “Transportation Sector Framework Document.” Washington D.C.: IDB.

-----. 2017. "Sector Framework Document on Support to SMEs, Access and Financial Supervision." Washington D.C.: IDB.

IDB-OAS (Inter-American Development Bank and Organization of American States) 2016. *Cybersecurity: Are We Ready in Latin America and the Caribbean?*, Washington D.C.: IDB.

IDB-WB (Inter-American Development Bank and World Bank). 2012. *Transport and Trade Facilitation Assessment*, Washington D.C.: IDB.

International Business Times. 2017. "Maersk and IBM want 10 million shipping containers on the global supply blockchain by year-end." Available from: <http://www.ibtimes.co.uk/maersk-ibm-aim-get-10-million-shipping-containers-onto-global-supply-blockchain-by-year-end-1609778>. [Accessed 18 March 2017].

Irfan, R. and M. Irfan. 2014. "Levels and Barriers to Supply Chain Integration: A Conceptual Model of Supply Chain Performance." *International Journal of Management Science and Business Administration* 1(1): 52–9.

ITF (International Transport Forum). 2012. *Seamless Transport: Making Connections*. Available from <http://www.itf-oecd.org/sites/default/files/docs/motion2012.pdf >. [Accessed 18 March 2017].

Journal of Commerce [JOC] 2016. "Truck Platooning is Closer than you Think." Available from <http://www.joc.com/trucking-logistics/trucking-equipment/truck-platooning-closer-you-think_20160907.html>. [Accessed 18 March 2017].

Juttner, U., H. Peck, and M. Christopher. 2003. "Supply Chain Risk Management: Understanding
the Business Requirements from a Practitioner Perspective." *International Journal of Logistics Management* 16 (1): 120–41.

Kapsch. 2014. "ITS World Congress Detroit." Available from: <http://www.kapsch.net/ktc/events/Events/ITS-World-Congress-Detroit>. [Accessed 3 March 2017].

Kim, H. and M. Laskowski. 2016. "Towards an Ontology-Driven Blockchain: Design for Supply Chain Provenance." Available from: <https://arxiv.org/abs/1610.02922v1>. [Accessed 18 March 2017].

Leveling, J., M. Edelbrock, and B. Otto. 2014. "Big Data Analytics for Supply Chain Management." Proceedings of the International Conference on Industrial Engineering and Engineering Management, Selangor Darul Ehsan, Malaysia.

Li, G., H. Fan, P. Lee, and T. Cheng. 2015. "Joint Supply Chain Risk Management: An Agency and Collaboration Perspective." *International Journal of Production Economics* (16): 483–94.

Mangan, J., C. Lalwani, and B. Fynes. 2008. "Port-centric Logistics." *International Journal of Logistics Management* 19(1): 29–41.

McKinsey. 2015. "The Internet of Things: Mapping the Value Beyond the Hype." June 2015. Available at: <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.
[Accessed 18 March 2017].

Memedovic, O., L. Ojala, J. P. Rodrigue, and T. Naula, T. 2008. "Fueling the Global Value Chains: What Role for Logistics Capabilities?" *International Journal of Technological Learning, Innovation and Development* 1(3): 353–74.

NAS (National Academy of Sciences). 2011. "Surviving Supply Chain Integration: Strategies for Small Manufacturers." Washington D.C.: National Academy Press.

New, J. and D. Castro. 2015. "*Why Countries Need National Strategies for the Internet of Things*." Washington D.C.: Center for Data Innovation.

Nooraie, V. and M. Parast. 2015. "A Multi-objective Approach to Supply Chain Risk Management: Integrating Visibility with Supply and Demand Risk." *International Journal of Production Economics* 161: 192–200.

OECD (Organisation for Economic Co-operation and Development). 2016. "Skills for a Digital World." Background Paper for Ministerial Panel. Paris: OECD.

OECD and WTO (World Trade Organization). 2013. *Aid for Trade at a Glance: Connecting to Value Chains*. Paris: OECD.

Panayides, P. and D. W. Song. 2013. "Maritime Logistics as an Emerging Discipline." *Maritime Policy & Management* 40: 295–308.

Peloton. 2016. "How it Works." Available from: <http://peloton-tech.com/how-it-works/>. [Accessed 18 March 2017].

Poirier, C. 1999. *Advanced Supply Chain Management: How to Build a Sustained Competitive Advantage*. Oakland: Berrett-Koehler Publishers.

PwC (PricewaterhouseCoopers). 2016. "Shifting Patterns: The Future of the Logistics Industry." Available from: <http://www.pwc.com/gx/en/industries/transportation-logistics/publications/the-future-of-the-logistics-industry.html>. [Accessed 18 March 2017].

Rolls Royce. 2016. "Remote and Autonomous Ships," *AAWA Position Paper*. London: Rolls Royce.

Ruiz-Rua, A. and A. Calatayud. 2012. "Best Practices in International Logistics." Integration and Trade Sector Technical Note N. 440, Washington D.C.: Inter-American Development Bank.

Saenz, M. J. and E. Revilla. 2014. "Creating More Resilient Supply Chains." *MIT Sloan Management Review* 55(4): 22–24.

Sanders, N. R., C. W. Autry, and D. M. Gligor. 2011. "The Impact of Buyer Firm Information Connectivity Enablers on Supplier Firm Performance: A Relational View." *International Journal of Logistics Management* 22(2): 179–201.

Schwab, K. 2016. *The Fourth Industrial Revolution*. Geneva: World Economic Forum.

Schoenherr, T. and M. Swink. 2012. "Revisiting the Arcs of Integration: Cross-validations and Extensions." *Journal of Operations Management* 34(1–2): 99–115.

Simchi-Levi, D., P. Kaminsky, E. Simchi-Levi. 2003. *Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies.* Boston: Irwin/McGraw-Hill.

Song, D. and P. Panayides. 2008. "Global Supply Chain and Port/terminal: Integration and Competitiveness." *Maritime Policy & Management* 35: 73–87.

Supply Chain Digest. 2015. "Supply Chain Graphic of the Week – The RFID Vision at Airbus." Available from: <http://www.scdigest.com/assets/newsViews/08-04-24-2.php?cid=1634>. [Accessed on 3 March 2017].

Swafford, P. M., S. Ghosh, and N. Murthy. 2008. "Achieving Supply Chain Agility through IT Integration and Flexibility." *International Journal of Production Economics* 116(2): 288–97.

Tabbakh, A. 2016. "How Supply Chain & Trade Finance becomes the Most Relevant Blockchain Use Case." Available from: <https://www.linkedin.com/pulse/how-supply-chain-trade-finance-becomes-most-relevant-use-tabbakh>. [Accessed on 3 March 2017].

The Load Star. 2017. Available from: <http://theloadstar.co.uk/cma-cgm-alibaba/?mod=djemlogistics>. [Accessed on 17 February 2017].

USDOC (U. S. Department of Commerce). 2017. *Fostering the Advancement of the Internet of Things*. Washington D.C.: USDOC.

USDOT (U. S. Department of Transportation). 2014. *Vehicle to Infrastructure Deployment Guidance and Products*. Washington D.C.: USDOT.

UNESCAP (United Nations Economic and Social Commission for Asia and the Pacific). 2013. *International Supply Chain Connectivity Index*. Available from: <http://artnet.unescap.org/databases.html#fourth>. [Accessed on 18 March 2017].

UNESCWA (United Nations Economic and Social Commission for Western Asia). 2011. *Trade Facilitation and the Single Window*. New York: United Nations.

UPS (United Parcel Service). 2014. "Managing Risk in the Global Supply Chain." Atlanta: UPS.

WEF (World Economic Forum). 2016. "Digital Transformation of Industries: Logistics Industry." *White Paper*. Geneva: WEF.

Woo, S. H., S. J. Pettit, S. J., and A. K. C. Beresford. 2013. "An Assessment of the Integration of Seaports into Supply Chains using a Structural Equation Model." *Supply Chain Management-an International Journal* 18(3): 235–52.

Xie, Y. and C. Allen. 2013. "Information Technologies in Retail Supply Chains: A Comparison of Tesco and Asda." *International Journal of Business Performance and Supply Chain Modelling* 5(1): 46–62.

Yu, M. and M. Goh. 2014. "A Multi-Objective Approach to Supply Chain Visibility and Risk." *European Journal of Operational Research* 233: 125–30.