Drivers and Barriers identification

Final Version of 20/09/2019

Deliverable Number D.5.1.1.

DISCLAIMER

This document reflects the author's views; the Programme authorities are not liable for any use that may be made of the information contained therein

Copyright message

Document Control Sheet

Project number:	10043002
Project acronym	TRANSPOGOOD
Project Title	Transport of Goods Platform
Start of the project	January 2018
Duration	21 months

Related activity:	WP5 5.1. – TRANSPOGOOD Roadmap and Forum discussion
Deliverable name:	D5.1.1 Drivers and barriers identification
Type of deliverable	Report
Language	English
Work Package Title	Guidelines and requirements for migrating to the TRANSPOGOOD platform
Work Package number	5
Work Package Leader	Agenzia di Sviluppo

Status	Final
Author (s)	Agenzia di Sviluppo
Version	3
Due date of deliverable	September 2019
Delivery date	20th September, 2019

Summary

European Regional Development Fund

Glossary of terms and abbreviations used

Abbreviation / Term	Description
AdSP	Port Authorities according to the new definition of the Italian Government
AIDA	Integrated Automation Custom excise duties
AIS	Automatic Identification System
BAM	Business Activity Monitoring
DDoD	Distributed Denial of Services
GUI	Graphical User Interface
HOIC	High Orbit Icon Cannon
IMO	International Maritime Organization
IOT	Internet of things
ISD	Instructional Systems Design
M2M	Machine 2 machine
MUPCS	Modello unico di Port Community System
NLP	National Logistic Platform
PCS	Port Community Systems
PMIS	Port Management Information System
PSNPL	National Strategic Plan for ports and logistics
RAD	Rapid Application Development
RCD	Rapid Content Development
RSDSAS	Resolution service and the distribuited security access policy server
SISTRI	Waste Tracking System (IT)
SOA	Service Oriented Architecture
UIRNET	Public body in charge for the development of the national logistic platform (it)

Executive summary

The present delivarable, produced within the framework of the TRASNPOGOOD project, provides a broader view of the identification of the drivers and identified barriers that must be considered to speed up the process and allow more fluid interactions between the various actors involved in the entire logistics chain.
40% of the world's population, or around 2.9 billion people, use the Internet today. By 2020, as expected, over 40 billion devices will be developed "intelligently".
Currently, the Internet of Things has grown and entered every market and industry and consequently fully in the entire land and sea logistics chain. Growth is expected to be exponential, as observed by experts. This transformation involves difficulties that some have called "Industry 4.0". In any case, this important change will be related to how the digitization process is transforming the current affiliation and balance of powers, as well as the responsibilities between the various actors along the value chain such as substitutes, buyers, suppliers and competitors.
The economic growth of regional livelihood logistics platforms requires the coordinated development of infrastructures, proactive education of specialists, logistics and information communication technology.
To achieve this, regional logistics platforms are essential as it is essential to implement a common strategy that focuses on interoperability between different management systems, both public and private, and which takes into account not only the "core" areas but also those peripherals whose "digital evolution" can allow the development of the territory, local supply chains, but above all act as a support hub where you can transfer the goods or specialize in the market allowing a homogeneous distribution of traffic and raising the quality level.
In doing so, it will be possible to start new lines of services that can be realized in a short time, putting in place "retro-fitting" plans and modernization of logistic sites; all this is facilitated by digital transformation and new technological paradigms that allow you to seize these opportunities with significantly lower costs than in the past.
The deliverable analyzed the state of the art of the adoption of the ICT platform and their evolution according to the European Directives, with a focus on the advancement at the Italian level, the impacts of the technologies and the relevant aspects of IT security that could jeopardize the whole chain including the impacts and trends of new technology, such as blockchain and the importance of human capital as well as the need to constantly train people and future generations to manage these changes.
The result also provides an introduction / suggestion on the role of the hybrid port that can be considered as a hypothesis and a starting point to satisfy the new paradigms relating to the full digitalization of the markets.

Introduction

This delivarable, produced in the framework of the TRASNPOGOOD Project, wish to provide a wider overview of the drivers and barriers identification identified that need to be considered to speed up the process and allow a more fluid interactions between the several actors involved in the whole logistic chain. The deliverable analysed the state of art of the adoption of the ICT platform and their evolution according the Eu Directives, the impacts of technologies and relevant aspects of cybersecurity that could jeopardize the entire chain including the impacts and trends of the new tech such blockchain and the importance of the human capital and the needs to training constantly the people and the future generations to manage these changes. The deliverable provide also an introduction/suggestion on the role of the Hybrid port that, being an hypothesis need to be considered as a starting point to meet the new paradigms related to the fully digitalization of the markets.

Maritime transport and ports are very important in trade in the world and form a vital part of strategic and economic interests. This gives a great reason why ships and ports which in turn creates a lot of effects on the trade flows between countries and is damaging to companies. Maritime cyber-space security threats target all stakeholders in the maritime sector and should treat the threat as being concrete and strong enough. In this regard, cyber-space can be explained as the domain of a system which helps in the prevention of threats or responding to threats and shows the prevention of malicious actions conducted to compromise a system in either a direct or indirect way (Caponi & Belmont, 2015).

Cyber-security helps in protecting against APTs (advanced persistent threats) through the use of various measures of defence like defence computer system, information assurance, applications hardening, access control, malware protection, and network security. The protective methods are implemented because the latest developments in technology have led to hackers improving their methods of attack on computer systems. Various ports are increasingly growing in terms of sophistication and dependency on the digitization of various processes related to Platform and IT solutions which impact the whole supply chain. Very few countries at the moment have been able to formulate as well as sustain programs and strategies for maritime security.

For example, the United States in the year 2004, launched the program of port security grant which enables companies to offer assessments for cyber vulnerability. This was followed by the UK when it developed an approach whereby the Transport, Maritime transport department provided guidance on ship security to help operators of ships in development of assessment of cyber-security and also planning and devising the best measures of mitigation to make sure that there are correct mechanisms of operation with responsibilities and roles. The International Maritime Organization (IMO) has also created plans for review to create guidelines and recommendations for managing risks in the maritime sector, safeguarding ships from emerging and current vulnerabilities and threats (Shah, 2004).

Market globalization as well as increased competition impulse vendors, producers, and distributors to integrate their processes, therefore increasing extensive networks for materials management, capital, information, and products (Gajšek, Kovač & Hazen, 2018).

To assist companies in these efforts, it is good to incorporate logistics and transport and to comprehend the connected, changing governance relationship (Gajšek, Kovač & Hazen, 2018). Several years of research, experiments in research together with interdisciplinary thinking have indicated that there is a need for restructuring of an organization and other modes of governance. Novel structures offer a chance for innovation, improved efficiency, new technologies, higher resources utilization, and interoperability among modes of transport, supply chain coordination, sustainable environmental performance, and administrative barriers' removal. Nevertheless, coordinated tactics towards making of policies which will induce those improvements are yet to be defined fully. We propose as well as examine in this paper one of the technique by defining the regional logistics platform concept, its fundamental concepts, business or geographic areas of operation and effects of implementation.

Globalization, as well as employment of information and communication equipment, has reduced businesses' dependency on the locations geographically in these days (DiRenzo, Goward & Roberts, 2015). With the fast development of e-commerce, the aim of the business world is changing to a circular economy to quantity production (Wilshusen, 2015). Also, the movement of long-distance cargo's cost of transport is decreasing gradually Gajšek, Kovač & Hazen, 2018). This reduction is because of several reasons like new optimal routing usage as well as refuelling of policies and structural integration advent (DiRenzo, Goward & Roberts, 2015). For the world trade to rise physical exchange efficiency between enterprises that are geographically dispersed, it is merely insufficient to modernize information and communication technologies in regards to more regularly needed physical rerouting of trade movements to other new geographical areas. Various companies have employed maturing and new SC strategies and contemporary tools as well as techniques in transport and logistics over time (Wilshusen, 2015). In addition, these technologies have led to embracing new SC tactics which have increased SC integration and management roles within various organizations (Gajšek, Kovač & Hazen, 2018). SCs research is in the frontline of the efforts of scientists, influencing the impacts of SCs at the regional level is highly disregarded.

40% of the globe's population, that is, around 2.9 billion people use the internet today. By 2020 as it has been predicted, more than 40 billion gadgets will be developed "smart" via intelligence and embedded processors. Currently, the internet of things has grown beyond medical applications and industrial niche and has gone into every market as well as industry. The growth is expected to be exponential as seen by the observers. The transformative expects difficulties which some have branded it as 'Industry 4.0'. In any case, the transformation will be effected from how digitalization is transforming current affiliation and power balance as well as responsibilities among various actors along the chain of value like substitutes, buyers, suppliers, and competitors.

The economic growth of regional sustenance logistics bases needs infrastructure's coordinated development, logistics specialists' proactive education, as well as information communication technology. To attain that, RLPs, Regional Logistics Platforms are essential. The secrets regarding the successful development of logistics areas lie in its capability to come up with a technique for coordinating and managing a certain operation and development of the logistics system and which is the area that researched further.

The findings of this research offer clear and valuable understandings into various aspects that can be important for business owners as well as regional authorities who are eager to stimulate the growth of the regional economy (Wilshusen, 2015).

1. Integrated Logistics Platform

Currently, there is a lot of competition in different industries around the world and the business sector is always changing to suit the demands and changes in the environment. As a result, the port sectors in respective countries is faced with so many opportunities and challenges. The challenges can be seen with the continuing environment that has been restructured by logistics, and the need to ensure that the ports remain more efficient through connecting all supply chains. Consequently, the opportunities come from research that has been extensively conducted on value-adding chains supply chain management. This changing need reinvigorated the concept of an integrated platform of logistics (Almotairi, 2012).

A lot of research has been conducted and it has been identified that roles played by ports are evolving and changing over time within supply chains. Thus, ports are not just pints of transhipment, but also play other key roles. The integrated form of the framework of supply chain management has played a key part in pointing out the main mechanisms and elements which support the systematic integration of the logistic platform (Almotairi, 2012). The electronic exchange of data at the port focuses on barriers as well as failures and success connected to paperless process administration. The standardization of processes has materialized thus facilitating information flow to be faster when novel technologies are used in the port. The information communication technology innovations are cost-effective because they reduce the cost of operation within the port as well as between the stakeholders and the port (Kooistra, 2008).

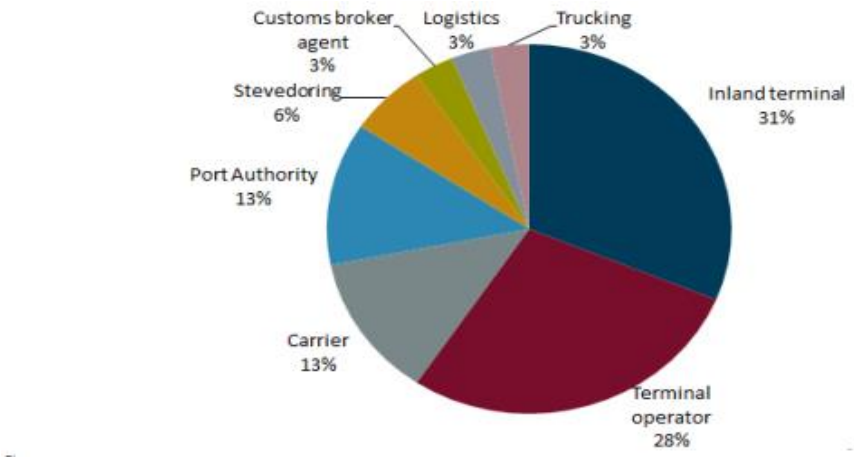

Fig 1: actors in the logistics industry (Carlan, et al., 2017).

There are various actors who are involved in the port industry. The figure above shows the percentage of various actors in the industry. Inland terminal is the leading with 31 percent followed by terminal operators with 28 percent. Carries is the third one with 13 percent followed by the port authority and stevedoring with 13 percent each.

European Regional Development Fund

Customs broker agents, logistics and trucking are last with each have a portion of 3 %. All the actors need to be integrated and connected for easy exchange of information.

Strangely, providing value-added and distributed logistics operations within the position of gateway of main seaports has turned out to be a major source of a competitive advantage and a vital business model. An integrated platform of logistics and concept is one of the important strategies that are aimed at integrating the land and sea interfaces with the in-land logistics. The ability of integrating various types of interfaces is reliant on the organization of the port to adopt vital business processes interaction through identification of linkages to activities of logistics and also enable optimization of systems which enables the supply chain to be visible in the whole system (Almotairi, 2012).

The figure below describes the 3 main categories that operate in the whole chain of the integrated logistic platform, showing the public, Internmodal rail transport operators and the private operators.

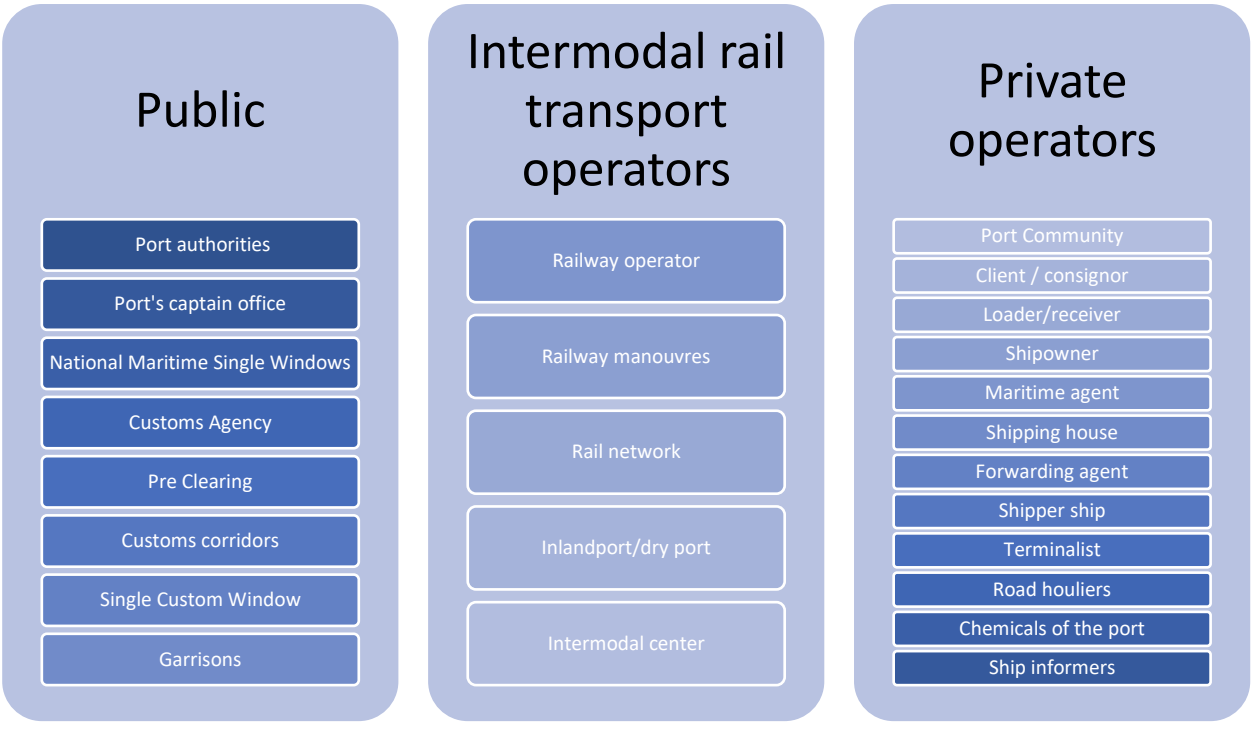

Figure 2: Actors involved in the logistics platform.

1.1 Transitional Best Practices concerning ICT tools to improve Multimodal Transport in Ports

The use of new technologies for inland traffic and vehicles management will be vital to lowering the emissions from transport in the EU and also around the world. The race to have

sustainable mobility can be considered to be global because it is taking place around the world. However, timid introduction of new technologies and delayed action could negatively affect the transport industry in the EU to experience a decline that will be hard to recover from. The transport sector of the EU faces an increasing completion in the world markets that are developing at a high rate. As a result, the elements of a single transport system in the EU and the greening of freight transport are two important targets that the EU policies are aimed at for transport and mobility.

The two elements currently depend a lot on the diffusion and adoption of innovative solutions all aimed at optimizing and rationalizing the flows and vehicles as well as goods for moth the multimodal and single mode solutions. Adopting solutions of technology in supporting automation and dematerialization processes can also reduce the gaps existing in terms of being competitive in the railway, maritime as well as combined solutions in the transport sector while comparing them to the road transport.

Integrating hinterland and maritime goods transport needs smooth flows of information between chain actors and ports through electronic forms. In this regard, integrating the technologies among the hinterland nodes and ports, between business players/institutions and ports, can be of great benefit to the cloud and development solutions, big data, augmented reality, cyber security, robotics to develop and establish functional and technological as well as international scale that supports the development if one European transport system. Figure 3 below presents the number of best practices practiced in the EU per service provided.

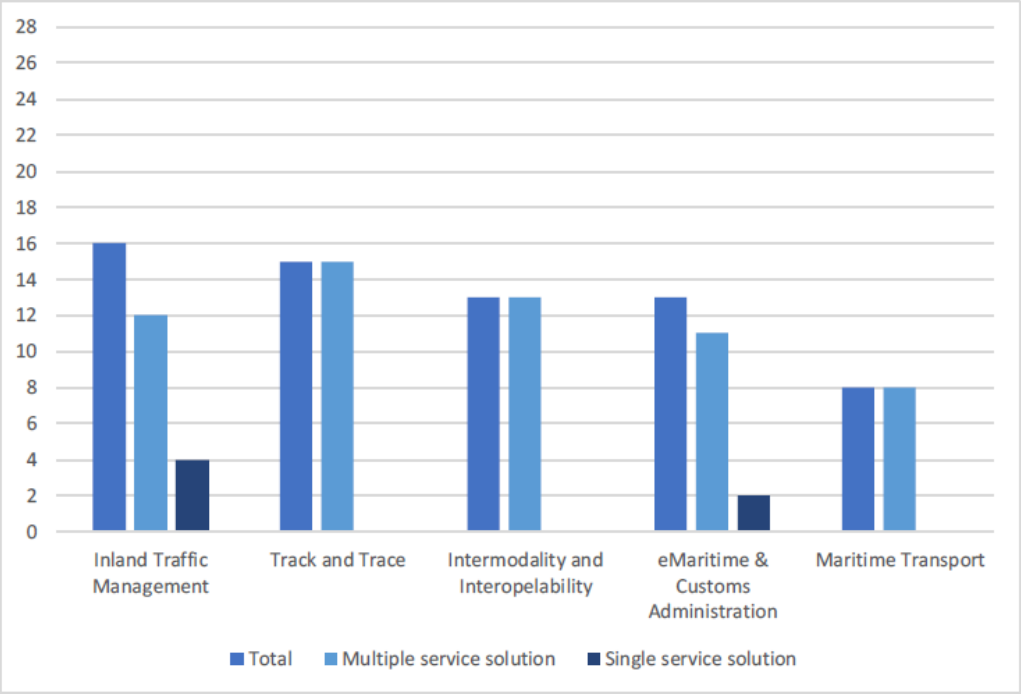

Figure 3: Number of best practices per provided service. (Interreg Adrion, 2018).

1.2 Projecting the future state of Transportation and logistics industry

The world never stops moving, so does age and changes keep on coming up each and every day. In many of the economies within the developed bracket, an increase in the number of workers are making considerations on the right time to retire from their respective jobs. This is a great problem in sectors such as road freight, which are likely to hit by shortages in labour because the requirements that are already starting to change. However in the developing economies, logistics and transportation as a sector is growing at a very high rate, but the development of workforce is not going at the same rate. It remains to be seen how the logistics and transportation companies will be able to cope and manage to live under such circumstances (Cooper, 2015).

By the year 2030, there will be more than 8 billion living on planet earth. That will be a billion more than the population recorded in the year 2010. A total of 95% of the new population will be born in the developing economies. For over 50 years now, the population growth in the developing countries has been more than seen in Europe. To be precise, by the year 2030, only 23% of the earth's population will be living in Australia, North America and Europe. The world economy is changing and this translates to change in wealth distribution. With the growth in world trade, the challenges faced in the logistics and transport industry will also increase. The world trade in services and goods is likely to increase by over three times to $27 trillion by the year 2030. That puts a lot of pressure on various industries to have goods flowing, hence increasing the rates at which transport and logistical operations are conducted. Back in the year 2010, derivers of logistical vehicles accounted for the top 10 jobs which employees are finding hard to fill in 36 nations around the world. In many nations, economic growth already is increasing the development of talents, which has led to a crisis and shortage of skills. Transport and logistics organizations in the developing economies will have to improve. This will translate to provision of in-house skills and training and programs of developing the employees to become better (Cooper, 2015).

Expectations from customers are changing and increasing a lot. Both businesses and individuals anticipate to receive goods faster, with more flexibility and also for the case where they are consumers, at a low cost of delivery. Manufacturing is changing and turning out to be more customized, which is a good sign for the consumers and tougher for the logistics industry. The only hope that businesses have is making good use of technology, from automation to data analytics. This creates a good anticipation for reduced costs, enhanced efficiency as well as the chance to genuinely breakthrough in the manner that the industry operates. However, having 'digital fitness' is a great challenge for the sector that is at the moment, struggling to satisfy many of its customers in this regard. Ensuring that the organisations are able to attract and retain the right skills is one problem, but the

development of the best strategy is even more vital. This is one of the greatest challenges likely to be faced in the near future in the logistics and transport industry (PWC, n.d).

There is a high rate of competition as the environment gets more players coming in and different types and levels of products being sold. Some of the own customers in the sector are creating logistics operations on their own and the new players coming into the industry who are developing new ways to develop elements that are more lucrative in the value chain through exploitation of the digital technology (PWC, n.d).

2. Information communication technology innovation barriers and drivers in the logistic sector

Drivers are the motivating factors that facilitate an efficient and effective way of developing information communication technologies in a business or organization. It is crucial for the port authorities and other actors to understand that, drivers as well as barriers so as to come up with solutions by developing and implementing information communication technology (Carlan, et al., 2017).

Drivers that are relative to information include: sharing of information on the logistics flows for interoperability, collaboration, traceability amongst various actors within supply chain; the need to address problems of curtailed limited and visibility on the exchange of information between port terminals and all the shareholders in the container validation process; identifying causes of the loss of cargo severity; for testing and clearing examples on how contemporary computations, as well as technologies, can be used in the real-life (Cristea, et al., 2017).

There are various barriers which relate to information communication technology innovation at the port. Nonetheless, it is important to identify industry-specific and generic drivers and barriers in various sectors in the industry. Such identification provides a stride ahead in developing information systems planning by linking the right personnel and resources as well as, managing shareholders' expectations so as to maximize the rate of success of developing and implementing information communication technologies at Maritime (Hidalgo & López, 2009). There is lack of cooperation by various actors in logistics, legislation uncertainty, and integration across the supply chain of maritime, shifts of primary needs for information communication technology developments and headquarters' strategic decisions due to globalization. The stakeholder is not willing to pay for the information communication technology equipment and services (Grawe, 2009).

The logistics sector has changed its business from the transportation business concept to serving the whole logistical requirements by the customers. The independent logistics companies and manufacturing companies need to be alert to the products' service aspects they provide to their customers. It is important for the transport companies to manage and control its information effectively and integrate multiple activities such as fleet management, distribution, warehousing, and outbound transportation so as to make more efficient physical products movements of their clients.

Therefore information communication technology is crucial to logistics because it ensures that the required information is available at the right place and at the right time. Information communication technology systems are important for logistics operation management.

In previous years, the maritime supply chain and forward-thinking firms invested in information systems that were stand-alone to facilitate their operations as well as maintain

their competitive advantage. Combinations of variables within the port can be identified which leads specific groups towards success. Cooperation within the maritime is crucial for successful innovation adoption. This comprises of managing various activities to attain cooperation from the stakeholders with respect to information communication technology applications in the ports (De Martino, et al., 2013). Co-innovation is a crucial challenge for the industry for the future. The co-innovation is whereby the shareholders acquire novel expertise and develop opportunities for the novel partnerships in the supply chain. The existing solutions of information communication technology are considered to be standard and thus bringing lock-in effect and creating barriers for developments of novel applications (Christopher, 2016).

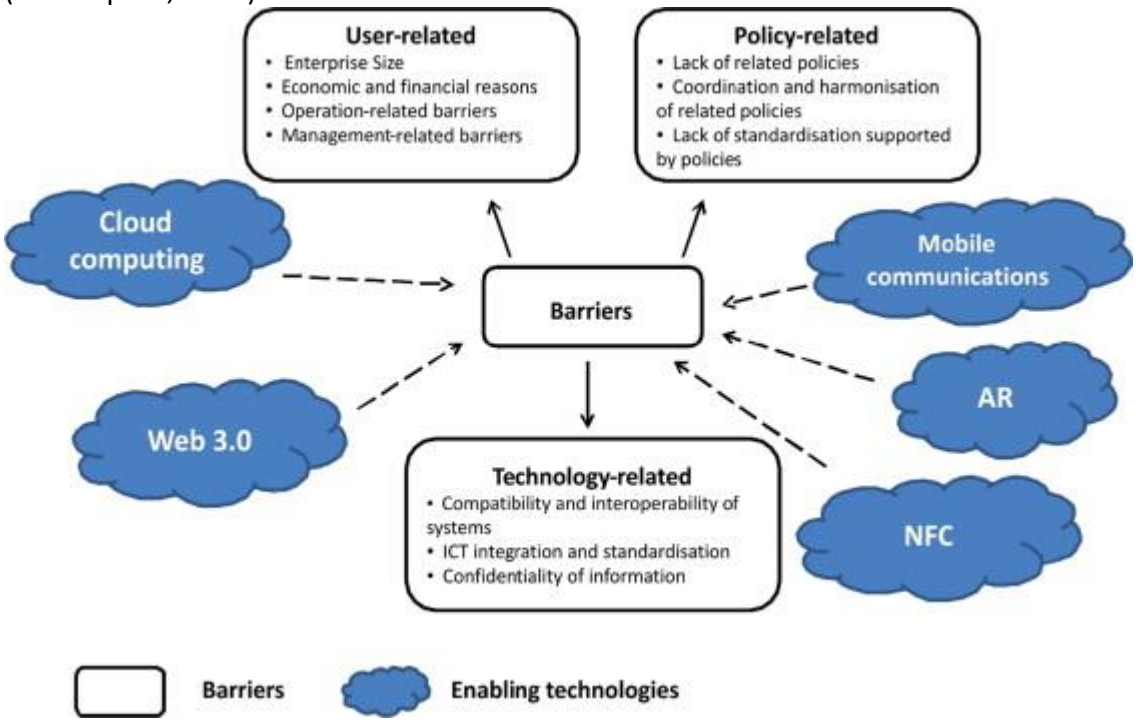

Fig 4: Barriers to Information Communication Technology implementation in Logistics. (Harris, Wang & Wang, 2015).

Many shareholders have realized the importance of implementing information systems in businesses in improving communication, visibility, and performance between various modes of transport operators. There are various barriers that exist to information communication technology adoption in various sectors. The adoption of information systems is grouped into three groups which are policy-related, technology-related and user-related (Harris, Wang & Wang, 2015).

Port management can be perceived as being a driver and a barrier in logistics for an information technology system in the port. Technology innovation is the key to effective communications and exchange of information within the port as well as to external factors. Ports that have adopted information systems and they are using them, their operations tend

to be faster and more efficient as compared traditional business models. Well-Organized management has embraced information technology systems in their operations and this assists them in getting information at the right place and at the right time as requested.

The lack of financing gap and knowledge capabilities is among the main reasons for losing and failure of innovation potentials at the port as well as stakeholders. Capability, in this case, is the expertise and knowledge with respect to the providers of innovations, and the innovation itself. Capabilities can be financial interests and contributions from the actors. The ports that do not have enough support in terms of capital which it would use to develop information systems in the logistics, implementation of information communication technology will be a challenge (Black & Van Geenhuizen, 2006). Lock-in effect, as well as technology mismatch, can contribute towards failing of adopting a certain innovation.

2.1.1. Digital innovation cases of the port

Technology has been advancing for the past years and information communication technology developments have been well established in the modern processes of the business for better and quality service delivery to its customers. Information communication technology systems have numerous advantages when it comes to service provision.

Development of novel information communication technology innovations in the port facilitates communications platforms to manage and exchange information. Developments of information technology assist at the flow of cargo and help in monitoring of cargo or equipment through advancements of information technology (De Martino, et al., 2013). Improved information exchange between the shareholders and the port concerning cargo, the arrival of vehicle or vessel preannouncement at the terminals and ports, and secure official document transfer electronically have facilitated information communication technology innovation in the port sector.

The maritime and port sector supply chain services show an amplified information communication technology platforms usage thus replacing outdated business models. Information communication technology innovations at the seaport improve communications between various actors who are involved within the supply chain (Peansupap & Walker, 2006). Before information communication technology implementation at the ports, there was excess capacity which was unutilized while the modern ports which have integrated information communication technology equipment in their operations reach their capacity level. The aim of the information communication technology platforms at the port is to optimize the amount of capacity used in the port.

2.2.2. Importance of digital innovation

Shareholders in the sector have realized that communication is crucial and embracing information communication technology in the port offers a competitive advantage. Information communication technology innovations have encouraged the supply chain of

maritime stakeholders to adopt information communication technology in their operational activities at the port. The supply chain of maritime, gate-appointment systems at the terminal integrates trucking companies' schedule with the infrastructure planning of the terminal (Grawe, 2009). Opening of opportunities concerning collaboration for the shareholders who are involved in the competition in seaport information communication technology systems deployment's next challenge.

The trucking transport companies are able to share information easily using the information communication technology platform concerning transport activities. The diffusion, as well as adoption of novel technologies in logistics, can be spurred by several various drivers. Information communication technology diffusion in various business areas is the main enabler of technological innovation and change which results in economic development. In the industry of logistics, service innovation can facilitate manufactures to improve services to their customers (Wagner & Sutter, 2012). The various port actors should be well-informed regarding the importance of adopting information technology application on how they should adopt information communication technology in their businesses.

The actors can choose to integrate their systems or they the can choose to use their own systems.

3. The Normative Framework (Ethical regulations in the Maritime sector)

One of the most important aspects of transportation operations more so maritime, road and air transport is having transparency and adherence to rules and regulations.

This helps to prevent organizational silos within the parts that exist in the supply chain and help in the leadership of supply chains, like the C-level executives to comprehend various ways that the supply chain efficiency works and how it can be more productive. Blockchain technology can be used to align the firm into the right path and ensure that all rules and regulations are followed and adhered to (Skovgaard, 2014). The table 1 below provides a list of the most important actions in Maritime safety and their respective activities and also responsible body mandated to implement them.

Table 1: a list of the most important actions in Maritime safety and their respective activities.

No	Priority actions	Activities	Expected Results	Input requirements	Dead-line	Applicable countries	Responsible party for implementation.	Comments
1	Improve the information exchange between countries about vessel traffic movement to attain full compliance with instruments of IMO related to AIS, LRIT, and Vessel traffic monitoring and information system adoption of corresponding measures providing for ships safety in the water areas and navigation channels.	A. Create one national window for shipping safety data and electronic exchange information mechanism on vessel traffic in the black and Caspian seas. B. Introduce real-time electronic mapping, data storage, and exchange. C. Establish an MOU on AIS data. D. Develop regional AIS server. E. Further, support the activities of the BSC. F. Carry out staff training and TNA. G. Plan and Carry out regional workshops regarding AIS and LRIT. H. Carry out relevant research in the black and Caspian Seas and prepare corresponding recommendations ensuring maritime safety in the ports and areas and navigation channels.	> National and regional vessel traffic databases established. > Maritime safety in the region improved. > Full compliance with IMO instruments achieved. > NA completed and staff trained. > Workshops conducted > Improvement of conditions forms Maritime safety.	> Technical Support. > IT hardware and software. > Funding for training and workshops. > Operational and maintenance costs > Technical assistance.	2015-2018	All participating states.	All concerned ministries and departments	> One state to become host country and responsible for the operation of the regional server. > Cost-sharing modality to be determined.
2	Promote the adoption and implementation of ILO-OSH 2001 by participating states.	Development and implementation of national legislation and or guidelines from hazards to eliminate work-related injuries, ill health, diseases, incidents, and deaths.	Guidelines for occupational safety and health established; Safety and health conditions improved.	TA support	2014	All participating states		
3	Promote the ratification of ILO MLC 2006 by participating states.	Development and adoption of national legislation on decent, fair and safe working conditions for seafarers. Subsequent submission of ratification to the ILO.	ILO MLC 2006 ratified by the partner states; Working conditions and rights of seafarers improved.	TA support.	2014	Littoral states of the Black Sea and the Caspian Sea, which have not ratified ILO MLC 2006 yet.		

As such, there is a framework created by the EU to regulate the deployment and use of Intelligent Transport Systems in the sector of road transport and other modes of transport

like Marine transport. The EU commission for maritime transport and is mandated with developing the specifications required to make sure that there is enough compatibility, continuity, and interoperability for the operational use and deployment of intelligent transport systems for the actions given top priority. The main aim of the commission is adopting the specifications for one priority actions or more (Gajšek, Kovač & Hazen, 2018).

The following laws are applicable in Maritime use of Intelligent Transport Systems and logistics: Creation of encouragement at the nodes of logistics are consistent and harmonized with National Logistics platform UIRnet, for data, documents, and information exchange amongst the operators to quicken, abridge and increase all managerial as well as operational processes in the modes of transport which are of multifaceted sequence. That is, by the Verdict for the growth of intelligent transport systems of 1st Feb 2013, issued by MIUR, MIT, and MINT that are offered at article 6.

Table 2: Laws applicable to Maritime use of Intelligent Transport Systems and logistics

Law	Date of issue	Created by	Function
EuDir 2010/40/EU	2010	European Union.	Describes the importance of ITS freight transport services and traffic management continuity.
Dir 2010/65	2010	European Union Parliament.	Reports procedures of the departing and arriving of the ships from the ports of the European Union.
D.L. n.179/n.221	2016	European Union Parliament.	Indicates that the transport systems innovation and then predicts the abstracts regarding the projects. Intelligent transport systems' overall outline for diffusion in the road transport field as well as in interfaces with other modes of transport as long as the necessity for the timely acquiescence enforced by the order, according to the current article.

The following are the main objectives of sectors of intervention for both use and diffusion in a coherent and coordinated way of intelligent transport systems:

a) Connection of telematics between the transport infrastructure and vehicles.
b) The prime use of mobility data, traffic, and road.
c) Applications of the intellectual transport system for transport safety.
d) Freight services and Intelligent transport systems traffic management continuity.

In the sectors of intervention referred to the fourth paragraph, ITSs guarantee on the national land the following:

i. The coordinated preparation of service electronic emergency call.
ii. Information services provision for secure parking zones for motor vehicles, as well as heavy goods and commercial vehicles.
iii. Provision of Information services on the mobility of various modes of transport.
iv. To the users, procedures and data are provided for free communication of minimum universal traffic information connected to road safety.
v. Provision of real-time movement of the information services.

To reduce weaknesses of the managerial procedures which are applied to transport of sea with information forwarding in rationalization of information and declaration made by sea vessels at the ports, engaging international traffic around European Union as well as going to ports or coming into the ports of the European Union, the managerial procedures linked to departure and arrival occur by using the following systems in table 3:

Table 3: EU parliament laws on maritime security and their applicability.

Law details	Date of issue	Created by	What it entails
Port Management Information System, administrative management's information system of the activities of the port according to the legislative decree 19 August 2005, article 14-bis, n. 196 and more changes.	2005	European Union.	The interoperability's proper stages and procedures simplification among different public systems that operate in the logistic area must be ensured according to paragraph 13 provisions. The Single interface implementation consists of the Port management Information System ensures interoperability of keyed-in data into the system with a secure customs information system and Sea Net. According to customs jurisdiction aspects and information accessibility to competent specialists, there must be an assurance of interoperability with respect to the creation of port authorities' platform for the functions best performance of coordination as well as addressing the logistics nodes which they should be accountable.
Paragraph 1 of article 2, letter t-bis, of the legislative verdict of 19th August 200, n.196, and subsequent changes by SafeSeaNet.	2010	European Union Parliament.	Exchange of the sea data by the European Union system referred to

3.1 Law and regulations referred to PLN/PCS

The August 4, 2005, Circular Statement: Ministerial Decree's application modalities of 20th June 2005 December 30[1], 2004 paragraph 456 n.311 of the law implementation.

The official loans are 10 million euros for the year 2005, 2006, 2007 each are expected for the payment of the contribution which is directed to system construction for national logistics network managing permitting modal interchange nodes interconnection so that to raise freight transport safety.

24th January 2012 decree article 61/Bis: Platform for national logistics network management indicates that:

a) The UIRNet Company implements a body just for management as well as construction platform and national logistics network management as indicated in the June 20, 2005, ministerial decree n.18t that stretched to logistics hubs, freight centers, and ports.
b) The funds are settled to be 1 million euros every year for 3 years since 2012 to 2014, with a particular destination so as to improve road transport's operating conditions and the parts are included in the platform experimentation for national logistics network management in the UIRNet project context of the infrastructure and transport ministry.
c) The Economy and finance minister is allowed by decree to make essential changes to the budget of a nation.
d) The charges from paragraph 1 are implemented with respect to reduction in the special fund allocation for the present share entered for the three year budget purposes of 2012 to 2014, under the program is known as Special and reserve Funds of the capitals to be distributed and the estimates mission for the year 2012 of the Ministry of finance and Economy purpose was using provisions connecting to labor and Social policies Ministry.

[1] June 20, 2005 Number 18T Ministerial Decree; Subject: Grants and contributions: Organizational structures of reference: Overall Direction for intermodality and road transport.

4. The Italian case: The National Strategic Plan for Seaport and Logistics (PSNPL)

For the communication and management operations, the logistics system, as well as port systems, are reinforced amongst several players in the logistic chain by a variety of the information system (Grabara, Kolcun & Kot, 2014), like Single Customs Desk, PMIS, PCS, GDP, PIC as well as PLN UIRNet s.p.a and Ferrovie group RVMS which:

a. The Port Community System to be precise is available in few ports and if there are in any, there is a big non-homogeneous maturity level at the national land. Therefore, various companies have applied the procedures in regards to certain requirements of a solo community without any centralized logic.
b. Follows self-dependent growth without a road map which is shared.
c. They have a point of interoperability for the managerial obligations with the involvement of supervisions which is limited because of many procedures or processes.
d. They have a limited level of use because of local bureaucracies and passivity.

The model of governance indicates that among many things, the AdSP's functions and roles as a single users' speaker of the port, being the holder of the responsibilities of administrative as well as essential managerial and professional skills possession. According to telematics specific subjects for transport and logistics, the first objective of PSNPL, the point 1.1 of the Ministerial decree gives one-stop-shop completion for the directives actualized by the agency of customs for reduction of the progressive and pre-established deadlines in accordance to the reforms of governance that acts in harmonization with the AdSp (Allen et al., 2019).

Concentration, competences and procedures simplification in point 5.2.1 of the ministerial decree show that competitiveness or efficiency recovery of the port systems of Italian comprises of simplifying administrative obligations which are linked to port activities performance. Competences concentration cannot be assumed that causes the process of decision making to be lower and costs worsening. To the same point provides that:

- In the new AdSP, Single Administrative center creation according to letter (a) have management and connection power (particularly on the administrative plan, taking charge of costs, provision of the sufficient funds towards all the administrations of the public that have competence on activities to be implemented in the port.
- Single Desk creation for administration which is responsible for the duties linked to entrance and exit of goods from the national land like phytosanitary controls which are identified in the Customs Agency. The novel responsibilities fulfillment, important specialized personnel that belongs to various organizations will be effected via this subject).
- The following roles and activities are the methods to motivate technological innovation, development, and research in the ports of the Italians according to action 6:

The supply chain digitalization via:

I. System integration support which increases successive systems versions which meet the Italian or European Karen architecture requirements which are established by infrastructure and transport ministry.
II. Investing and promoting initiatives which enable and support transport and logistics administrative procedures.
III. The coordination table at MIT and measures definition describe governance as well increase interoperability, integration and coordination significantly among various information systems of the organizations that are not integrated completely like PMIS, AIDA, PCS, NLP, PIC, PIL, Sistri, PAT, RVMS but already operating, in addition to improve technological offers effectively and improve its penetration which are devoted to the Community Business in order to support the whole chain of transport and logistics.
IV. Systems employment which will monitor hazardous goods, access to the passengers and special waste with points of access to regulate counting systems as well as access.
V. Architecture of modular cooperative which permits information and services integration linked to modes of transport, air transport, control and waste management, node of transport, sea routes transport, transport of rail freight with the purpose of coordinating measures of intervention by evaluating as well as monitoring the impacts on safety, environment and transport and logistics system efficiency.

Considering gratuity for the first two years provided and PNL Manager who guarantee management costs, technological efficiency and maintenance of the platform, the ministry will look for financial resources alternatives for that period to ensure the financial plan and economic sustainability by recognizing the manager of PNL. The manager is identified by the tender. For similar tactic encouragement in the sector of logistics informatization, the procedures of legislative will be effected to unite the platform of National Logistics which will be provided for 2 years and all the authorities of the port systems must use it because it follows employs Port Communities.

The logistic and port system for interviews and operations management amongst various players involved in the chain of logistics by information systems diversity PMIS, One Stop Shop customs, PLN of UIRNet spa, as well as, PCS, PIC, PIL and RVMS of the Ferrovie group, which follow a self-dependent growth without a road map which is shared.

Some port realities have Port Community System and at any point they are present they have a certain level of non-homogeneous maturity as every organization has applied procedures and services in regards to each community's specific needs that the ministry guarantee devoid of an appropriate centralization logic via the platform of the National Logistics (Evangelista et al., 2012).

The minister of infrastructure and transport gave a directive on 20/3/2018, that is, course of action for normalizing and establishing the Port Community Systems which was to be executed vial National Logistic Platform.

i. The Port Community Systems of the AdSP in the second Article as implemented in accordance with the current article that comprised of National Logistic Platform perimeter. Obligations Port Community Systems is described as a neutral and open information technology system what enables aimed and safe information exchange amongst public bodies and economic operators so as to raise the community competitiveness for the directive purpose. This systems manages, optimizes and automates processes of the port that include administrative, logical process, authorization. This automation is done via single data entry and information exchange with the supply chain and transport.
ii. The operation cost according is the concessionaire's responsibility. In case AdSP is not provided with the Port Community Systems, it takes on with the same 30th Sep 2018 deadline, Port Community Systems National Logistic Platform which is the MUPCS first step as discussed in the premises.
iii. Article 3, on the use of National Logistics Platform in agreement with re-use principle denoted in the Digitally Administration Code according to 7th march 2005 legislative verdict n.183, the Port Community Systems that comes from MUPCS profits from the PLN services and forms. AdSP can request Concessionaire to create Port Community Systems modes and customize according to MUPCS which do not attain its overall requirements. The AdSP has to continue in this case using its own resources.
iv. The UIRNet comprises of the port operator organizations and a single AdSP for embracing Port Community Systems that comes from MUPCS until PCS PLN Article 5 is implemented. The UIRNet in particular with concessionaire defines time schedule for the MUPCS implementation and a plan of action in connecting to the single AdSP with the heard and same agreement with the organizations of the port operator. The action plan defines sources of funding, roles, responsibilities, tasks, and costs. The concession can be terminated if the early close proposition of the concession in case of any reason, the compliance, and obligations recognized by the law, concessionaire current decree and concession itself return to UIRNet. The agreement of UIRNet with general affairs and personnel, navigation and the transport department will take steps to actualize necessary actions for the ongoing activities pursuit. Around European as well as national resources will identify any essential resources' substitute. The rewarding measures and incentives for the authorities of the port system in article 6 indicates that the AdSP which act in accordance with the decree obligations that are established in article 2, first and second paragraph, will contain special title to access economic nature measures which are founded on the national resources for implementation, construction and management of the intelligence technology systems.

The PLN services are used on the AdSP as foretold by PSNPL act 6.4 and considering art. 61-bis of 24 January 2012 of the decree-law provisions, n.1, changed with Art. 4 March 24, 2012, n. 27 by the law amendments. Single actuator obligations for the PLN "UIRNet S.p.a" management and construction takes steps to stimulate proper actions so as to attain PSNPL established objectives of standardization, homogeneity as well as proper PCS centralization.

v. The PCS NLP services charges will be described by concessioner after coming into terms with the port communities' operator and AdSP which are certified by the UIRTNet after consultation with infrastructures and transport ministry.
vi. By September 30, 2018, as the paragraph 1 provisions results, move their Port Community System into the National logistics platform's cloud at the ministry so as to give permission the same managed by the pursuant concessionaire to December 27, 2013 article 1, n. 147, and paragraph 90. The individual Port Community System transformation is stared for the PCS PLN adoption with funds which the concessionaire will pay.

5. Effects of cybersecurity on logistics and maritime transports

The overall trend in having data of high risk require as well as improvements in technology requires security which is better to avoid distortion or theft of software. In previous decades, there was no connection between computers and some researchers were connected to the internet. In this generation, the internet is used all over thus connecting computers. Through this connection, computer viruses can be transferred amongst the connected computers in various ways. The major role of cybersecurity is to assure data availability, confidentiality, and integrity (Evangelista et al., 2012).

Considering many facts, digitalization lags behind even if maritime transport can be seen as the backbone of the global business. This project confirms the application of the state-of-the-art currently to eight domains of digital which are: big data, internet of things, additive engineering and 3D printing, autonomous vehicles and robotics, edge and cloud computing, mixed and augmented reality, virtual reality and digital security. There are domains that no proper study has tackled and therefore there are critical parts that need to be further researched attentively. There is an increasing concern on the matter which arises from the need of raising the industry just like other industries to the same digitalization levels.

Cyber and physical security enhancements are important at the ports in ensuring proper freight flows, operation as well as serving travellers. The ports are well-thought-out to be susceptible infrastructure because of the ports' numerous operations that take place the sea proximity and issues that are encountered while monitoring any threats that come via it, the number of individuals that works at the porta and their diverse nature. The relevant port security legislation internationally is the International Ship and Port Facility Security Code abbreviated by ISPS which is implemented by EU / 65/2005 also EU / 725/2004 at the European Level that needs authority's identification, goals, and skills of acts so as to create and maintain security. In this context, Port Security Plan definition which the Port Security Officer draws up justifies the port facility and the ships' risks analysis. It also identifies the Port Facility Security Officer's tasks and responsibilities in the Port Facility. Several ports of Europeans connect to all city's parts thus the greater complexity is presented by impacts of dividing the areas that are under security checks.

Table 4: EU Maritime regulations vs USA regulations on maritime cybersecurity.

Regulations of the European Union	United States Regulations
European Union Cyber Security Strategy National Intelligence Service Directive (2016)	US WH EO 13636
CPPP Initiative (2015)	(PPD-21) Presidential Policy Directive
Security agenda of the European (2015)	Information Sharing and Analysis Organization of Maritime and Port's security
EIDAS Regulations in 2014	Port security grant program
The European Union's cyber-security strategy	NIST 800-30
CIIP Directive in the year 2012	USA H.R. 3878(2015)
Cyber act 2019	

According to the report of ENISA concerning challenges of cybersecurity in the sector of Maritime, it indicates clearly that the cyber risks are an increasing danger which spreads to all sectors of the industry which depends on the system of information communication technology.

Such cases can be barred by rules and regulations that neutralize different failure of markets that acts as a hindrance in cybersecurity for private investment optimization from both private and public institutions where there is effective coordination and cooperation of experiences in the real world show the economic requirements for a cyber-defense which is coordinated to reduce the security expenses for all partners who are involved.

As from 2008 in the NIS Directive framework covers an important infrastructure from the legislation perspective. The breach cost may not entirely drop on the immediate casualty. Several systems of computers store confidential and critical information regarding entities other than the owner of the system. Cyber-attack issues are consolidated already regarding maritime transports. Accessing computers of the port or sending signal that are fake of the GPS so as to change ship route, automatic change of the ship signal for proof of identity in order to report a incorrect position, software and electronic chart and information systems infiltration to change maps as well as pirates identifying possible victims by listening into AIS transmissions. Disruption of the automation system such as Stuxnet indicates that infrastructures can be affected by cyber-attacks. Such ICT systems disturbances may have impacts on the member states governments of the European Union and their social wellbeing as well. Arising of a challenge ensures that the robustness in the ICT contrary to the cyber-attacks at the national and pan-European level.

Findings of some of the reports emphasized that at the present there is a curtailed cybersecurity of maritime awareness as well as a holistic approach based on risks and maritime cyber risks valuation that are associated with authorities of maritime and indicating crucial assets around this sector is important. Cybersecurity and physical of the network is to

assure the users' Privacy Integration Protocols. An answer is represented by holistic security. Various initiatives have come in due to the current attacks, which containers abstraction from the port legal manner. MSC, for instance, introduced a Container Release System that was new and it enabled securely containers collection from the port. The users have to log into the system which is secure where their verification takes place so as to get access to the data of container releasing.

APCS has made an effort to ensure that this technology is used in the port. The Las Angeles port implemented Cyber-security Operations Centre's state-of-the-art thus curtailing risks of cyber-attacks. This Cyber-Security Operations Centre comprised of software and hardware that were advanced that is employed to control or monitor the environments of the computers so as to detect a breach and then respond to it quickly in case it occurs. Cyber-security Operations Centre collects data on cybersecurity which analysed and the shared among other agencies (Srour et al., 2008).

The United States adopted a crucial instrument known as the Port Security Grant Program. This instrument supports National Preparedness System implementation by giving support to sustainment, building, and main capabilities deliverance that is important to achieving the goal of the national preparedness of a resilient and secure country by improving capabilities of the cybersecurity. Although there is nothing that has been done at the European Union level, this delay is an excellent opportunity of defining the strategy of the European related to the resilience of the port cyber program that identifies financial instruments such as incentives or specific plan of an institution which is to be cooperated in connecting the facility fund of Europe as well as crucial information infrastructure hadronization such as Domain name system, internet exchange points, optic fibre of submarine.

6. Maritime cyber risk

Maritime cyber risk can be explained as a measure of the level to which an asset of technology could face a threat from a potential event or circumstance, which may lead to security failures that are related to shipping operations as a result of the system being compromised, lost or corrupted. There are a lot of cyber risks involved in maritime operations. Connected devices, as well as ports, have a very high likelihood of being attacked through overstepping the device security in many ways. Safety is very important in transportation as it is connected to the integrity of the transportation agents. Cases like the latest increase incidents of illegal immigrants coming into Europe through the coastal regions of Mediterranean Sea and also smuggling of illegal products needs to have increased protection of the vital infrastructure like port operations. The innovative mechanism for cybersecurity
should be formed to manage to respond or preventing all the possible threats that are faced by critical infrastructure. The port authorities in various countries play a vital role in the economy and international trade operations. Infrastructures of transportation face a lot of threats which include sabotage, physical disasters, sabotage, terrorists and insider threats among many others.

There are many upcoming risks that are facing the Maritime Transportation System because of vulnerabilities that are related to insecurities in the cyber systems. Facility and vessel operators are increasingly depending on computers and systems to navigate, communicate, engineer, and enhance safety, handling of cargo and several other applications in operations. Together, the technologies have helped in enabling the marine transportation system to operate with a good reliability record and at capacities that help in driving their respective economies and also the national security. Nevertheless, the misuse, exploitation or failure of the cyber systems in various incidents in the systems could harm the operations, disrupt the operations or even lead to deaths and injuries.
To ensure better security IMO has provided the following set of changes and instruments to be followed:

European Regional Development Fund

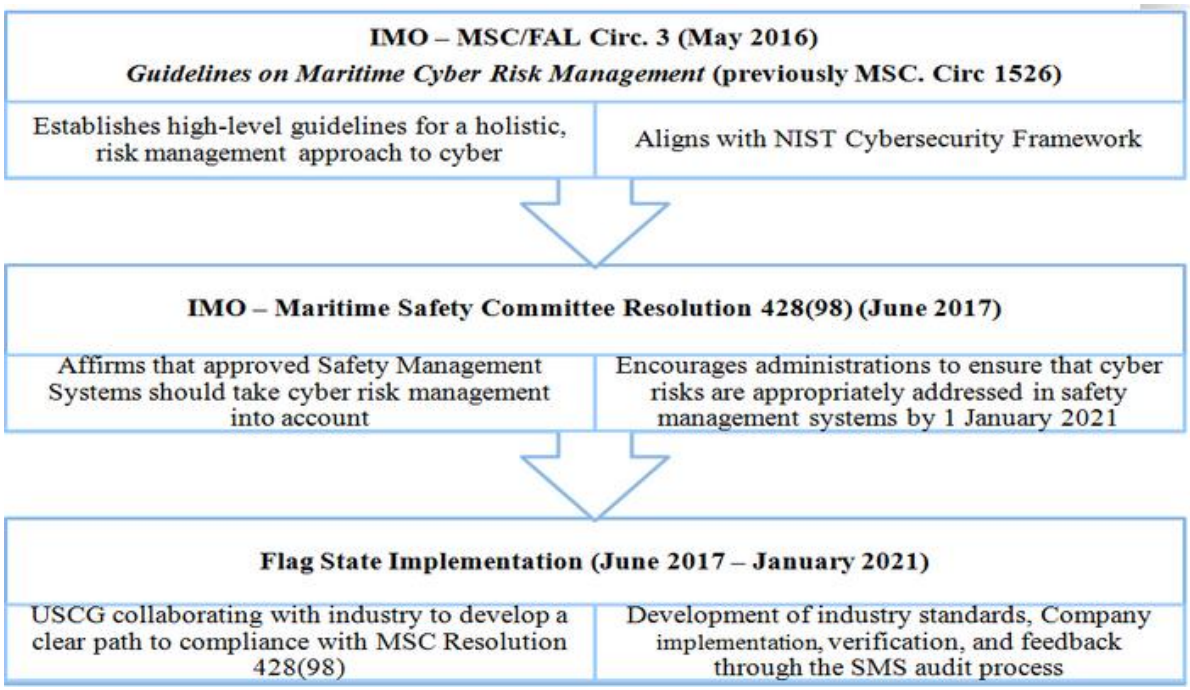

Figure 5: Instrumental changes provided by IMO for better security in ports.

There are different reasons and motivations behind maritime cyber-attacks. Table 5 below indicates the different motivators behind their attacks, the individuals or actors involved in the attacks and the various targets that they aim to affect with their attacks.

Table 5: Motivators, actors, and targets of cyber-attacks in ports.

	Motivators	Actors	Targets
Hacktivism	Egoism and political change.	Hacktivist and activist individuals.	Individuals, governments and maritime organizations.
Cyber-criminality	Informational, financial or economic advantage, smuggling, and trafficking.	Criminals	Different types of maritime assets, individuals and maritime organizations.
Cyberespionage	Stealing crucial information.	Organizations and nations.	Maritime Individuals, governments and maritime organizations.
Cyberterrorism	Ideological goals, fear, political change, religious or ideological motives.	Nations and terrorists.	Individuals, infrastructure, organizations or public targets.

Cyberwar	Social change or political change.	Terrorist groups, individual hackers or nations.	Military maritime forces, critical maritime infrastructure or other critical maritime targets.

From the table, some of the motivators (reasons) the various types of maritime cyber-attacks include espionage, criminality, espionage, warfare or terrorism. The different cyber-attackers might be intending to gain social or political control or create some political changes, steal vital maritime information or even gain an economic and political edge or even some doing it to just satisfy their ego. However, Maritime security is a serious aspect and such attacks should never be allowed to materialize.

6.1 Maritime Cyber Attacks

Whereas there is increasing use of artificial intelligence and automation which has opened new shipping routes, system vulnerability has become a common norm. In the middle of the year 2017, the maritime industry was highly shaken by a major and historic cyber-attack that was propagated on Maersk, which is the largest container shipping organization in the world. This attack led to the sector adopting a new way to look at the cybersecurity matters. The year 2018 was used to validate the trend as incidents of cyber-attacks progressed, impacting ports, operators, as well as the builders of various types of ships.
Some of the major maritime cyber-attacks include the following incidents represented in Table 6 below.

Table 6: Major Maritime global attacks

Incident and affected port/Organization	Date/Year	Attack details	Impact
Cosco Operations attack on the US Port of Long Beach.	24th July 2018.	The network of the company was attacked and it broke down. Some electronic communications were cut off completely and unavailable to all users. However, it only affected operations in the USA only as those outside the country proceeded normally.	All of the company's daily operations were halted.
Port of Barcelona cyber-attack.	20th September 2018.	The security breach caught little attention as it only impacted the internal IT systems at the port.	No ship movements were disrupted.
US Port of San Diego cyber disruption.	25th September 2018.	This was a serious cyber disruption which forced the employees to operate with 'limited functionality'.	Impacted normal operations by employees.
Austal (an Australian defense shipbuilder)	30th October 2018.	The company's data management systems were hit by a cyber-attack, and the hackers demanded money from the organization to return the data they stole.	A minor impact on the company's operations as they were later taken back to normal.

Despite all those latest individual incidents, there are many others around the world. For instance, there is a famous criminal Nigerian gang that targets the world maritime industry and has been running several business email compromise scams, earning many thousands of dollars.

The group is commonly regarded as 'Gold Galleon' and has been operating by sending messages to enable them to infiltrate payments within the companies of shipment. Some of the major victims include a Japanese shipping company and a South-Korean shipping company (Yadav, 2014).

7. The concept of hybrid port

Because of technological innovations and advancements, operations of ports and ships are currently operated through connected and automated systems for accountability and more effectiveness. However, the challenges that are facing ports and other maritime institutions call for urgent help and response. Ships and ports now need to have strong surveillance systems and intelligence at multi-level, which all point towards creating a HYBRID PORT Security system (Chiappetta 2017). The HYBRID PORT offers accurate physical awareness, real-time security awareness and also cyber situational awareness alongside providing timely warnings to stakeholders operating in ports. This will, in turn, inform better decision-making when it comes to dealing with maritime cyber impact and threat assessment and help also in suggesting the possible actions to mitigate the threats (Wang et al., 2014). The concept of HYBRID PORT works through a fusion of contributions from various types of physical (front end) systems of sensing as well as systems of cyber detection (new innovative and legacy systems) from various sectors of security. Some of the most common events of maritime cybersecurity threats are mainly pointed out through the "bottom-up" integration of various forms of sensors that are real-time and also sub-systems used in collecting data in a number of forms, which include cyber and physical and the way they correlate to one another to create:

a) alarms that are prioritized with various threats;
b) sequences for making decisions for the security operators

In this regard, the 'fusion' is created based on the available scenarios of maritime security threats as defined by P-SOC (Port Security Operation Centre) as a top-down technique. The idea of having a HYBRID PORT is intended to make sure that the solution created by technology is made of loosely coupled elements and various aspects that are connected by a functional cohesion. At the same time, with proper standards application, the HYBRID PORT will help in facilitating improved maritime security in the industry and will also offer further reference model for activities of research within the paradigm of IoT and issues that are related to cybersecurity (Wang et al., 2014).

The technique of having a HYBRID PORT will offer a means to interoperate in services among the companies involved in cargo carriage and also various ports around the world. In Europe, there have been two failed attempts to create appropriate EU Port services directive to create policies, a vital theme of the policy of EU has been establishing free access to markets to offer port services in ports operating within the EU. Notwithstanding the important regulatory changes, the HYBRID PORT will help in facilitating open service access through the provision of the important infrastructure and roadmap for electronic services that are port-based in the container supply chain as well as passengers, more so when dealing with the sea motorways.

7.1 Architectural Principles of the HYBRID PORT

The HYBRID PORT has a number of principles underlying its operations and applicability. Some of the principles include the Internet of Things (IoT), Complex event processing, Service-Oriented Architecture (SOA) and cloud computing.

Internet of Things: The use of the Internet of Things model is vital in ensuring that the communication architecture works well as expected as well as ensuring that there is enough interoperability. The important component provides services which are mainly required to implement the architecture of IoT called RSDSAS (Resolution Service and the Distributed Security and Access Policy Server). At the same time, all the devices operating under IoT (inclusive of the cloud-based port service framework) might be offered an IoT-A communication interface based on services, thus enhancing real-time M2M secure, communication-based exchange of data and service support that is remote embedded (Wang et al., 2014).

Complex Event Processing: the communication of M2M that is based on events might be applied in the HYBRID PORT, which in turn enables direct relation between various gadgets and individuals connected through IoT. Nevertheless, many of the issues can be dealt with by looking into the IoT Communications Service Layer, which is a critical cloud computing node. Through this, the cloud infrastructure might get a considerable number of activities which have options of discard, resend or process in real-time.

Service-Oriented Architecture (SOA): This is a vital aspect in a HYBRID PORT, which is introduced which to help in attaining loose coupling among vital components. The layer, in this case, might expose services of SOA offered by the architectural components. Every service is determined by a contract of service that entails features like an interface that is well-defined, constraints of security, SLAs as well as service quality. At the same time, the SOA layer offers standard services to connected gadgets and individuals.

Cloud Computing: instead of applying the solution in a conventional data center, a HYBRID PORT in this regard might apply cloud computing. At the time of the project, the advancements could be regarded as the model for cloud computing, which is the best considering factors like security, costs as well as service quality. At the same time, it could explore the probability of mixing various types of cloud computing (Wang et al., 2014).

BAM (Business Activity Monitoring): above Business Intelligence, HYBRID PORT could give the platform for presenting and analyzing concurrently the port's activities through the integration of a BAM solution. At the same time, BAM enhances the establishment of SLAs concurrent measurements and emphasizes on the improvement of the effectiveness and speed of port operations.

8. Logistic cyber risk

Cyber-attacks are common in all industries at this current digital age, no matter how updated or forward-thinking the organization becomes. Logistics is no exception. With its increased reliance on automation, cloud services, and IoT, the supply chain is always changing and becoming better (Byson, 2014). At the same time, the tendency of relying on the cutting edge technology creates a chance for businesses like that to a wide range of security threats. Thus, the impacts can vary from minor loopholes in the services to large risks that are potentially fatal to the business. Sadly, cyber-attacks are now unavoidable, they the main aspect towards the mitigation of instances is understanding the threats that are most commonly experienced.

The following are some of the most common logistics threats:

a) Social Engineering losses

This is a common method that is used by attackers to take advantage of some companies into giving them vital information, get access to important information, or even loss of funds. Even if the attackers do not get the chance to enter into the computer network of the firm, they can create what looks like a legitimate email message from one of the company's authorized officers with directives to the department of accounts payable to send funds into the account of the criminal.

In this regard, the criminal may also monitor the activities of the authorized officer and notice when he or she is not at the office and unable to stop or verify the fraudulent directives. Research by FBI shows that there are several thieves that have managed to steal a lot of money using this method (Boyson, 2014).

b) Distributed Denial of Services (DDoS)

DDoS can be explained as the use of several computers to create an unnecessary and excessive flow of traffic towards an asset that uses the internet. In this case, the DDoS is directed towards logistics systems and maritime service systems.

Table 7: DDOS attack detail

Intended Effect	Examples of attacks	Targets	Procedures and techniques
The major intended impact of a DDoS attack is to make a device or many devices useless because of an excessive flow of traffic that targets the devices or exhausting resources. The types of attacks can totally kill the external-facing network of an organization which could be applied for distribution, e-commerce, banking, an acting organization website and much more. There are many sizes of attacks, starting from 1 Gbps to more than 400 Gbps.	The greatest DDoS in history was carried on the BBC website. The attack's total size was more than 600 Gbps.	Mostly entail external-facing network devices which can cause a considerable amount of losses.	➢ The hijacking of several machines to form a botnet to perform attacks. ➢ Single Machine DDoS attack. ➢ Traffic obfuscation through the use of VPN (Virtual Private Network) or Tor in hiding the attack's origin. ➢ Booter Service and other services for DDoS that are paid for. The use of such services grants anonymity to the attackers as they are not actually doing the attack, but the booter service is doing it. ➢ Multiple machines DDoS attack.

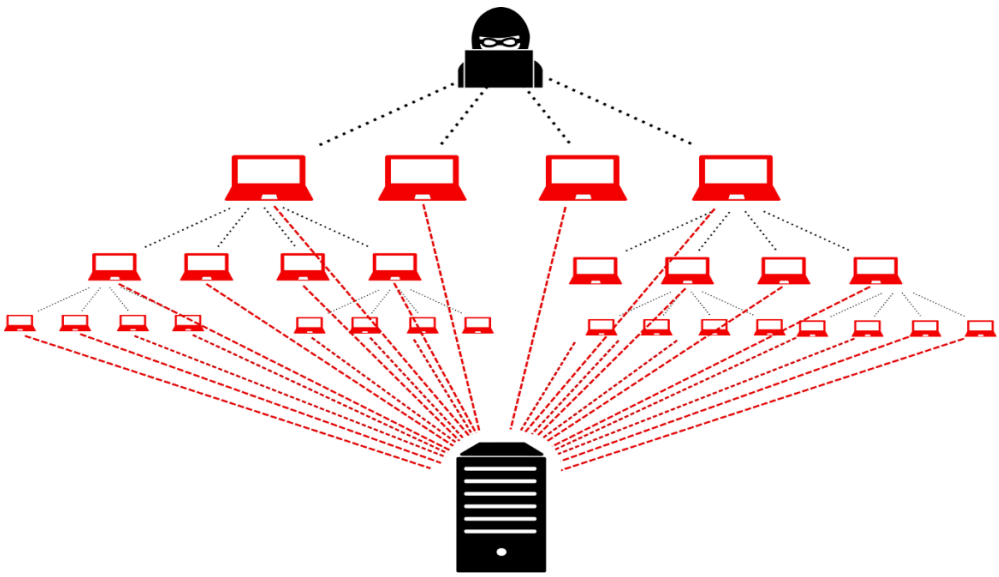

Figure 6. Basic DDoS attack.

Tools used for the attack

i) High Orbit Ion Cannon (HOIC)

This is an open-source application of DDoS which needs minimum training and is one of the tools mainly used to perform DDoS attacks. HOIC utilizes high-speed HHTP flooding that is multi-threaded against the target.

Mitigation of HOIC: ensure firewall filtering policies are implemented and also traffic limiters and uses anti-DDoS services.

ii) Slowloris

Does DDoS attacks against different forms of apache and other different web servers through exhaustion of the existing connections. The tool works through sending HTTP traffic that is partial to the server for a long time, making the service unavailable for any new requests since all the processes and threads are taken by the incomplete HHTP traffic.

Mitigation of Slowloris: Utilize load balancers and also change the timeout directive.

c) Web Defacement

This technique entails making any unauthorized verbal or visual changes to a certain targeted website. This way, many maritime and logistic websites have been targeted and affected greatly.

Table 8: Web Defacement details

Intended Effect	Examples of attacks	Targets	Procedures and techniques
The main effect is vandalizing of the website targeted and post the verbal or visual propaganda of the hacktivist which can lead to damage to reputation.	In the year 2004, the NZ Government (National Party) website was defaced by BlackMask, a hacktivist group.	They normally entail government, corporate and religious sites connected to the campaign being protested.	➢ Use of security tools to do reconnaissance to determine the path that has is least protected to the webserver targeted. ➢ Social engineering while attempting to collect credential information for the website being targeted. ➢ The exploitation of backdoor entry. ➢ The exploitation of misconfigurations or vulnerabilities of the website being targeted.

Tools used

i) Havji
ii) Nikto
iii) Cross-site Scripting (XSS)
iv) Acunteix
v) Metasploit

9. Enhancing cybersecurity of port community systems

The main disturbance of large ports will most likely lead to great negative impacts on the supply chain of maritime sector and even the entire economy. On top of the physical threats, ports are also susceptible to cyber-attacks because of how much they depend on Information Communication Technology (ICT). PCSs (Port Community Systems) are hubs for information that ports use to integrate information from different sources for international supply chains, connecting systems of carriers, terminal operators, authorities and freight forwarders (Meyer-Larsen & Müller, 2018). Through this, PCSs should be considered to be critical infrastructures, since any successful cyber-attack can create great problems in the port operations, and in worst-case scenarios, total disruption of operations (Srour et al., 2008).Cyber-attacks can also act as bottlenecks in the supply chain and logistics networks. The latest incident of Maersk being attacked by NotPetya, which led to the central systems being disabled for many days around the world, is approximated to have made the company lose about USD 200-300 million (Meyer-Larsen & Müller, 2018).

9.1 Disaster Recovery and Business Continuity in Port Community systems (PCSs)

PCSs are all-inclusive information hubs that are geographically bound in international supply chains which basically serve the purpose of a diverse collection of organizations that are related to ports.

Importantly, they are naturally complex because of the diverse base of the stakeholders involved and operate in a similar environment (the port community). Normally, the economic activity which is executed is geographically spanned over a certain area that is enclosed (at times sites that are disclosed and adjacent which serve certain purposes) (Robert, 2016).

The implementation of PCSs is a complex process that entails all stakeholders in the community and the central governing authorities. Thus, the best way to manage information security at the PCSs is by creating an ICT system. Here, there is need to have a clearly stated security policy, analysis of risks, the applicability statement as well as treatment of risks, and after that, an audit test to ensure that the controls are efficient enough. This will ensure that the organization is well prepared when it comes to managing and recovering from disasters. Creating procedures for disaster recovery and formulation of a robust framework within the company to enable sustainability of disasters is a great challenge for any company since its efficacy can be traced back through the use of simulations. Many of large organizations only spend about between 2-4 % of their budget of IT on planning for disaster recovery, with the motive of avoiding larger casualties and losses just in case the business is unable to function after losing data and IT infrastructure (Tijan, Kos & Ogrizović, 2009). The figure below shows a list of the main causes of disasters in logistic, supply chain, and port organizations.

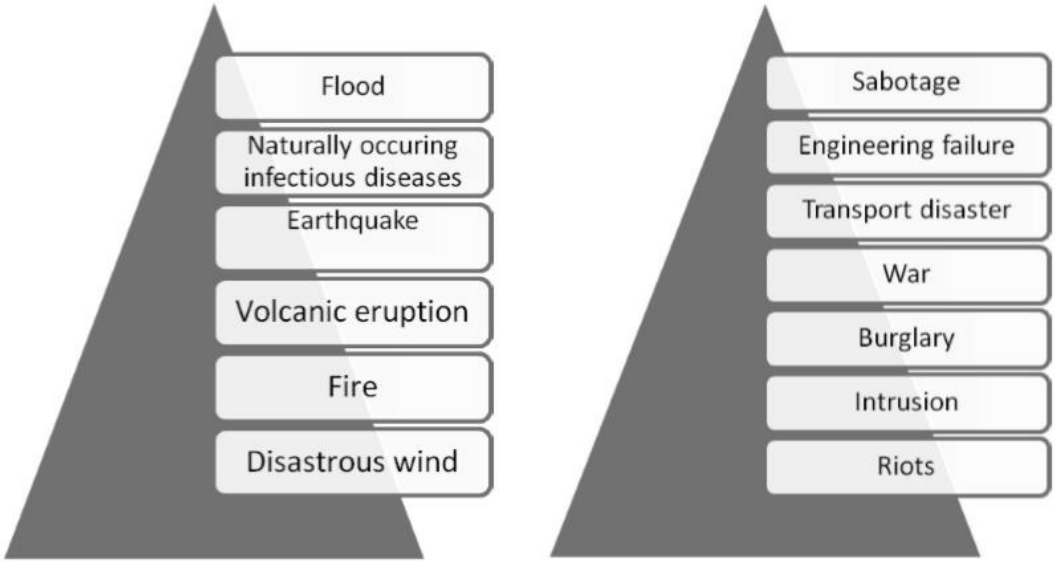

Figure 7. Main causes of disasters (Tijan, Kos & Ogrizović, 2009).

9.2 Port Community Systems' Integral Security

In environments that are complex such as in the PCS ICT systems, it is important that business functions are treated separately and attempt to make sure that they continue and generally have security without general coordination.

There is need to formulate am integrated model of the community security which will help in the integration of the best practices in general security and ICT, align the port communities with legal requirements, offer a solid basis to certify and review continuously, enable seamless integration of many new stakeholders, offer optimization of cost and in the end, promote internal goals for innovation. It will be almost impossible to implement all the aforementioned functions, which partially exist within the participant systems in a PCS scene if they do not allow a part of their governing sovereignty to the authority of maintaining PCS.

Thus, it will be recommendable to form a separate function in the PCS (an integrated security function) which is found at the top of PCS managing entity, entrusted with the formulation, management and influence of the integral security, considering the particular interests of the PCS stakeholders involved and the given goals of the PCS.

For the PCS CSO, it is vital to take into consideration the complete picture and prevent focusing in the area with the previous experience of a candidate whereby the executives normally feel very comfortable. At times, while executing the integral security or the port access security, the individuals with the ICT background and technical knowledge focus on security of applications, networks as well as logical security controls, whereas the CSOs with

criminal or military investigation knowledge try to react instead of being proactive and have thorough reactions only when a specific threat has already come up.

In the end, the decision is left with the stakeholders to make a decision on the model of ISF execution they will choose and decide if to look for candidates at the open labour market or do internal

recruitment from the existing employees. The two methods have their cons and pros, but it is vital that in every case, the candidates of CSO need to promote the overall integral security of the PCS, therefore increasing the external and internal perceived satisfaction levels through the use of new model of integration.

The most common and successful Port Community system is the Polish Port Community system, that was created through the use of SWIBZ. The important information from the SWIBZ system is applicable and used widely by the international and national administration institutions to attain the anticipated standards and levels of monitoring on shipping as well as control. The analysis SWIBZ system has to point out different ways to introduce the Port Community System in Poland. Robert (2016) outlines the need to have a full empirical analysis and determine the probabilities of the application of SWIBZ informatics system used by the Polish Marine Authority to form Polish Port Community System. The SWIBZ system is the major database of the Polish Marine Administration and retrieves information and data from the databases such as: Small ports, VTS, position of the vessel in the seaports, AIS, Dysport, PHICS 2008, iMARE SSN, iMare DMIS, SSN, EMSA Vessels, data base of vessels, Navtex messenger, LRIT and VHF.

Another application of the Port Community System is in the seaports of Croatia. The seaport handles so many transactions and operations. Because of the slow rates at which items are checked and cleared at the seaport, the Croatian Marine Authority has implemented an IT solution that is meant to improve the way operations are sorted out and goods cleared in good time. The Croatian seaports have realized the need to implement PCS on their business. Coordinating among the PCMs in the seaport of Croatia is still happening through the traditional communication methods. The implementation of PCS in the Croatian seaports is a great investment that requires a lot of funding.

After being fully implemented, it will lead to great savings in terms of cost, reducing paper documentation and also enhance effective and speedy processing of transactions.

The utilization of the SWIBZ system has to identify the form of incidents and explain the procedure of acting with some forms of incidents. The system's user may formulate some incidents automatically or manually based on the recorded data from the appliances, the database or other communication systems. When some data about incidents is input into the SWIBZ system, the system will serve the incident as per the exact procedure for those form of incidents (Tijan, Agatić & Hlača, 2012).

10. New technologies adoption in logistics – the case of blockchain

Blockchain is a concept of technology that emanates from Bitcoin and Cryptocurrency and disrupts the areas of the economy that are always enlarging. The Blockchain concept is in the development stages, while Bitcoin's future seems to remain quite unclear. It is clear that the Blockchain has great potential for improvements in the large scale (Allen et al., 2019). Nevertheless, considering that it is a technology that might reduce the significance the importance of several of today's great global organizations, power structures and institutions, in preserving hierarchies, the potential Blockchain has might well remain not exploited (Tijan et al., 2019). Blockchain presents a great promise of overwhelming trust issues, creating room for secure, untrustworthy and authenticated supply chain and logistics information exchange in networks of supply. The latest implementations within the supply chain are changing from Blockchain to a wider perspective of using distributed ledger techniques (Mansouribakvand, 2019). The supply network of a specific supply chain member (a manufacturer in this case) entails the network's supply-side (the network of the supplier) and the side of demand (distributive network). The supply-side entails all the supply chain's entities which offer inputs, either indirectly or directly to the focal organization (Dujak & Sajter, 2019). The demand side entails all the members of the supply chain through which the product passes on its way to reaching the consumer.

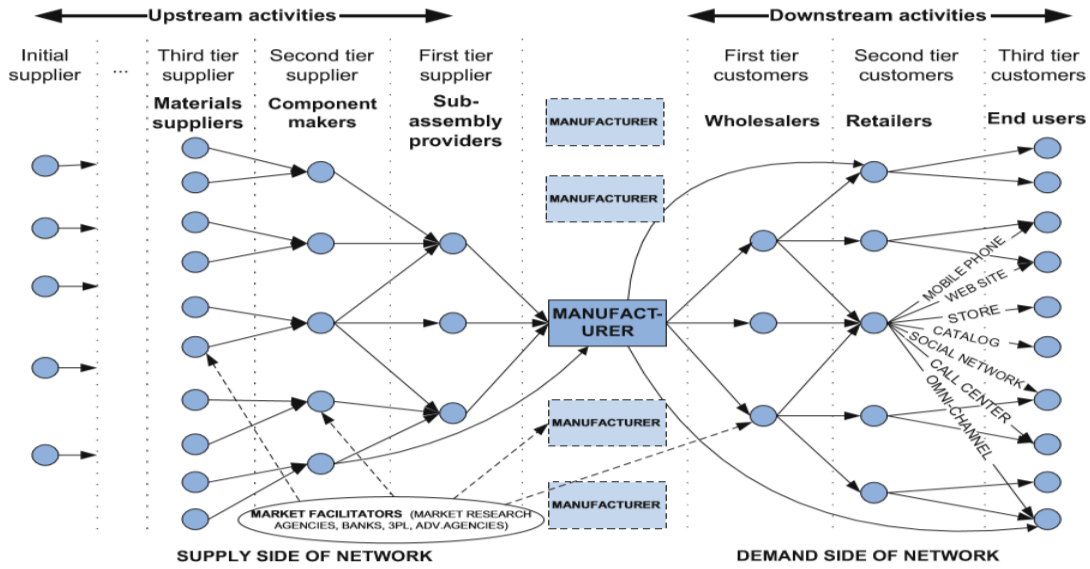

Figure 8. The supply chain surrounding a manufacturer (Dujak & Sajter, 2019).

The figure above shows the wide range of choices of channels of distribution that a retailer can apply in reaching the end-use. At the same time, several contemporary retailers concurrently utilize multi-channel technique, and some use the single-channel retailing approach. The single-channel retailing is integrated and unified experience that is centered towards customer service which enables the customers to do shopping through all the probable channels of distribution at any time of the day (Dujak & Sajter, 2019).

Blockchain offers a state that is shared and distributed, which all the participants willingly use an algorithm of consensus. Their features of being tamper-proof provide the best chance to introduce a world view of supply chains that are multi-tier. To use business logic in Blockchain, there has been an introduction to smart contracts. The smart contracts are computer programs which apply rules without the need for a third party. In the Blockchain of bitcoin, a primary version of smart contracts is applied through the use of a scripting system which enables use cases such as multi-user accounts as well as escrow services (Christodoulou, Christodoulou & Andreou, 2018).

10.1 Applications of Blockchain Technology in supply chain and logistics

Blockchain has emerged as a saviour of many companies as they try to get accountability and streamline their operations accordingly. According to Niels & Moritz (2017), Blockchain use can be a threat or a trick towards enhancing proper operations. As a result, Blockchain has several uses in the logistics and supply chain sector. Blockchain works through enabling immutable and decentralized storage of data that has been verified (Christodoulou, Christodoulou & Andreou, 2018). The Blockchain is a digital ledger of transactions that are tamper-proof because it uses cryptographic methods (Niels & Moritz, 2017).

The figure below indicates the use case examples that highlight the need to have and use Blockchain the supply chain and logistics sector.

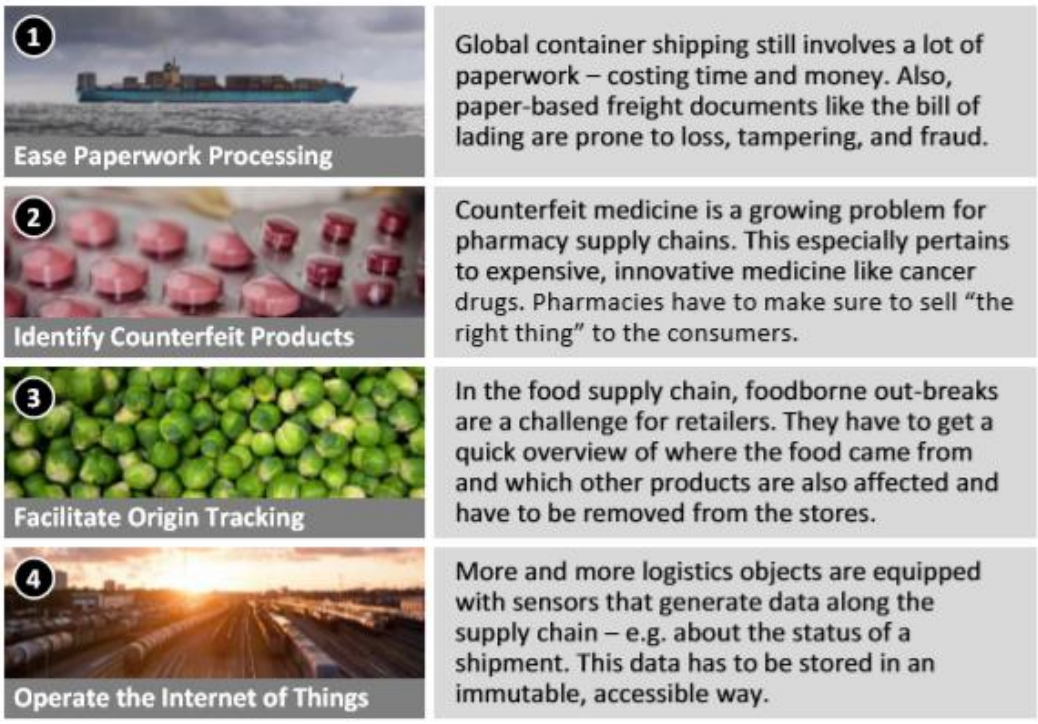

Figure 9. An overview of use cases where Blockchain is applicable (Niels & Moritz, 2017).

From the figure above, there is an emphasis on the need to digitize port operations as it will help manage many aspects at once and also improve the effectiveness of the systems.

10.2 Supply Chain Information on a Blockchain

Blockchain is a new technology of governance used by institutions used to maintain and create distributed informational ledgers. Governments can use and accommodate supply chains that are based on Blockchain in several ways. Some of the governments that have embraced the use of Blockchain in their respective ports include Japan, Australia, the United States, and Singapore. The leading position that these governments have taken in imposing fiscal and regulatory policies relating to Blockchain could help in contributing towards policy compatibility semblance across many countries. Research indicates that the latest assessment of the countries indicate that they have always kept a nature that accommodates Blockchain and cryptocurrency, with part of their motivation being getting the innovations that come with Blockchain as an opportunity to grow their domestic economy (Allen et al., 2019).

There are many other issues with regulations that will create discomfort and should be dealt with under crypto-friendliness. One of such legal issues is legally recognizing information that is based on Blockchain. Various governments have various requirements on how compliance with domestic regulations should be done. Some of the legal requirements

include the nature of provision of information. This creates many wrangles around the way governments recognize information that is based on Blockchain on provenance as being enough to comply with the domestic regulations (Allen et al., 2019).

10.3 Future trends of blockchain adoptions

The future of Blockchain adoption is in the hands of many people who are now learning how technology can be used. However, there are several issues such as systems security and data protection that are likely to affect the adoption of the technology. The modern-day world has seen the levels of cybercrime increase greatly (Perboli, Musso, & Rosano, 2018).

With a likely increased demand for projects related to cybersecurity, the use and adoption of Blockchain technology are likely to be high. The start-ups which provide real means of protecting cryptocurrencies from the criminal acts will also become very popular in future (Dujak & Sajter, 2019).

Blockchain will be applied in ensuring better service delivery for those in the gambling industry to resolve problems associated with projects of ICO/STO as well as computer security will offer new chances for the gambling industry to develop. For instance, the team that created Faireum has even created a Blockchain that is completely independent based on the strengths of Hyperpledger, Ethereum, and Bitcoin.

Not long ago, Blockchain has been connected with basically projects of experiments. Just a small number of them have been moved to the full-fledged production level. It is possible that this will be different in the near future. Nevertheless, in the future, Blockchain will be of great help with effective making of decisions, considering certain projects' profitability (Tijan et al., 2019).

10.4 Blockchain and IoT-based Disruption in logistics

The new technology of Blockchain, together with Cloud Computing and IoT (Internet of Things) is anticipated to disrupt the current business processes at levels that are unprecedented.

The creation of smart contracts is a new technique that has been created to replace the traditional paperwork and unnecessary meetings between companies. The smart contracts are mainly consolidated by the architecture of Blockchain. A smart contract, in this case, is a program that executes automatically which will be automatically triggered on the events created by sensors of IoT, IoT tags or IoT actuators. Smart contracts and Blockchain that optimally suit in arrangements between many parties are expected to create a great paradigm shift in the sectors of logistics and supply chain (Pervez & Haq, 2019)

There are many efforts being made to use Blockchain to enhance Supply Chain Management. The main pioneer for this technique is IBM as the company has made efforts

to streamline the application of Blockchain in logistics and supply chain. The use of performance measures (KPI) as well as performance metrics plays a key role in the operations of logistics in any competitive market. Some of the metrics and KPIs may not be useful to explain the ever-changing logistics activities on the basis of disruptive technologies like Blockchain and logistics. To measure non-financial performance and intangible measures creates a great challenge in the knowledge economy (Pervez & Haq, 2019)

11. The lack of human capital competences

Numerous factors associated with maritime industry comes from the human capital domain. Some of the factors associated to human capital are: estimated long-run qualified engineers officers, and masters shortage, reduction of number of merchant ships' crew members; maintaining low operational cost is a challenge for the efficient global trade; shipping industry is unable to attract young and capable human resources; challenge in redirecting crews to more interesting as well as demanding work so as to draw attention and maintain professional human resources (Burmeister, et al., 2014).

The development of human resources for regional strategic sectors and industries has become a common emphasis on the development of industries with enough potential to grow. In the modern competitive world of business, information technology and knowledge are vital factors in the development of regions. It is always important to rely on human capital instead of material capital. Many developed nations like Ireland, Finland as well as Singapore and other developing nations such as Poland, Kenya, and St. Lucia are currently making use of the National Human Resource Development in adapting to the society that is changing at a very high rate.

Lack of competent human capital is a great concern because it affects the operations of ports and their logistical processes as a whole. According to Ahn & McLean, (2008), organizations are mainly concerned about human competence at their disposal and how the human capital is developing.

The logistics, distribution, and transportation Competency Model are created in a tiered graphic. The way tiers have been arranged is in a shape of a pyramid and it is meant to be in terms of a hierarchy to show that the competencies at the top are at a higher level of skills. The shape of the model is a representation of the increasing specialization and more so in skill application as an employee goes up the tiers. However, moving up the tiers, the numbers of specialized individuals reduce because there are very few people who have taken the initiative to get the right skills for logistics and port operations Ahn & McLean, (2008),

Many countries port operations have developed rapidly, but the lack of skilled workers is holding
back their ability to operate and perform to expected standards. At the same time, the search for skilled employees has become a bigger problem for many countries, with developing countries like Vietnam finding it hard to succeed. The main issue with the providers of logistic services in Vietnam is that they do not have the logistical expertise and in-depth knowledge in the field, hence inefficient delivery of services (Le, 2015).

Developing the ability for a company to recruit and the train does not entirely solve this issue of shortage completely, but developing competency from within the company works well in ensuring that all employees are competent. The basic functions of HRM include the recruitment, training, evaluating performance, motivation, safety and communication at the workplace and much more. Thus, to ensure that logistic performance improves, human capital development should be enhanced in all countries, with a mixture of developing

existing employees and recruiting a new crop of employees a preferred way of ensuring top quality and highly skilled employees are selected.

Port problems and operations are becoming complex by day. One of the main problems is developing human resources that can match the organizational requirements, which affects the human resources in different ways. Human Resource Development, in quantity and quality aspect has grown to become the vision, stated in the master plan of many national ports. One of the most vital aspects is improving the human resources, with the focus being on the people who handle equipment since the technical employees in ports play a critical role in the determination of the overall productivity of the organization.

Many of the container workers are trained from maritime and shipment schools. However, companies fail because 80% of their training is based on job training and not imparting the direct skills that are required on the field.

The modern day world has seen ports transformed from being purely sip-shore interfaces into complex logistical platforms whereby activities related to logistics take place and are also vital clusters of economic activities.

Thus, the role played by seaports and their respective human capital is important because the nodes of transport are vital and indispensable for the efficient and effective management of product flows as well as informational flow in the supply chain. With such changed roles and ways of operations, it is important that the personnel at ports have the required competencies to hep contribute to the efficiency of their respective ports and make the port an effective partner of supply chain.

Estimated long-run qualified engineers, officers, and masters shortage, reduction of the number of merchant ships' crew members has hindered implementation the information technologies at maritime. The number of skilled labor diminishes as time goes by and the sector is not able to replace the skilled labor with millennial workers to the port. The crew members of the merchants' ships have reduced at the maritime. Implementation of information communication technology becomes a challenge as there are few actors in the sectors. The cost of operation is insufficient for the global trade and this slows down embracement of the information technology at the maritime sector (Burmeister, et al., 2014). Adopting information communication technology will curtail the cost of operation and the sector will be able to conduct its activities in an effective manner. One of the advantages of using information systems is to reduce cost of operations in an organization or a business. The high number of aged workers at the maritime have hindered development and implementation of digital innovation.

The young generation has embraced digital lifestyle and it would be possible for the sector to adopt information system if they hire young and skilled individuals at the port. They can be able to handle tasks faster as compared to the aged people at the port. Maintaining professional labor is key to implementation of digital innovation at the ports as they can give views regarding crucial matters that need to be tackled effectively by using digital innovations. Unskilled labor at the port may not see the need for information systems

because they are used to traditional systems and moving to information systems use will be a challenge to them (Porathe, 2016).

11.1 The role of training in the logistic sector and Maritime cyber safety

The worldwide maritime sector relies more on automation, operations integration and digitalization that works stringtly with the logistic platforms. The widespread and fastness of internet communication and information technologies implementation for ships at the maritime in all parts of the globe brings an urgent and novel requirement of operational safety maintenance of critical systems at the sea (Fitton, et al., 2015). Cybersecurity is a common issue in the international sea sector as in the logistics becoming a priority. Both national authorities and international organizations have created cybersecurity laws specifically for the sea sector and national orr international plat to digitalize the logistic sector.

Development and implementation of these regulations for the land and sea sector have been a concern for a long period of time (Cimpean, et al., 2011). The guidelines put an obligation on the stakeholders, operators, and ship-owners to the embrace rich management technique with the prime objectives.

The aim of adopting guidelines is to curtail dangers posed to the crew, financial consequences of partial and full loss of confidentiality, integrity, and availability of critical data, and to the safety and security of the environment.

Information security is critical in the sector because it ensures that information and data are not accessible by the wrong person who might alter with it. The data integrity, availability, and confidentiality must be maintained for proper operation of businesses in the port sector. Integrity is ensuring that information or data is free from unauthorized information access. Data confidentiality ensures that data is accessed by only people who it was intended for, and data availability is ensuring that data can be accessed by the authorized people at any time and there is easy access of information (Cimpean, et al., 2011).

The international administrations aim at a close connection between security and safety of the port and in the logistic platform. The aim of cybersecurity at the port and in the logistic platform is to protect information and data of information technologies from unauthorized access, data tampering, and manipulation. Safety on the risk of operational technologies and data, integrity or availability is crucial for an individual and vessel safety and other facilities at the maritime. There are various cyber-attacks on information and data and this can be minimized by implementing cybersecurity to guard the entire systems of the maritime (Fitton, et al., 2015).

12. Training course methodology

This deliverable explained the different needs that interest the whole logistic operators (SEA/LAND/RAIL) showing clearly the importance to share the competences to the work force in order to provide the new technological skills to increase the quality and in particular the security (cyber) of the different platforms that every day are used to move cargos and persons globally.

The proposed training method is based on E-learning course, being an advanced form of learning across computer networks where electronic devices are used by the final users to enable them to interact with the colleagues and the lecturer or expert on the other. Horton defined it as the use of web technology and the Internet to bring about learning. Ghirardini defined it as "the use of computer and Internet technologies to deliver a broad array of solutions to enable learning and improve performance". It can also be defined as an educational system that provide educational and/or training programs for learners at anytime and anywhere using interactive information and communication such as the Internet. A number of studies confirmed the importance of e-learning, as studies have revealed a significant impact of e-learning in developing students' research skills. Another study showed there were statistical differences between an experimental group of students who studied through the e-learning environment.

The development process of educational systems can be defined as "a description of the teaching process that takes place in a special learning unit (e.g., courses, lessons or any other event in which a learning design occurs)". Elearning development methods can be divided into traditional and agile methods.

Instructional Systems Design (ISD) is the traditional approaches to developing educational and training systems. It is used to increase practice and skill in developing instructional courses that make knowledge and experience more efficient, effective and attractive. The development process in this approach is to identify the current environment and learners' needs, then determine the goal of education, and then make some adjustments to assist in the transition process. The Dick and Carey system is another instructional approach model that addresses instruction as an entire system and focusing on the interrelationship between context, content, learning and instruction.

The Rapid Application Development (RAD) is one of agile methods that describes a software development which emphasizes on prototyping and iterative processes, is an approach to software product development based on small planning. Rapid Content Development (RCD) is a model that has iterative design, reusable components and e-learning tools for rapid and cost effective execution.

12.1 Course elaboration methodology

In order to realize a qualified course, that cover the gaps of the work force involved in the sector there are principles described in this sub chapter, it is important adopt the procees and methodology described below.

The most important aspect is the analysis phase, the system requirements are defined and information from the real world is collected. The gap between the actual behavior and the desired goals are also determined. Information about the particpants, the environment, the technology used, and the scientific content is obtained in an effort to bridge this gap.

Table 9: Course elaboration methodology

Research or questionnaire	This is the instrument useful to get the needs to be satisfied.
Direct and indirect observation	Ask to the different stakeholders what they want to improve
Interviews	Plan several interview with the entire chain from Origin to destination (land/sea/rail operators)
Information gathering	This stage includes information gathering about the e-learning system and requirements analysis. It consists a number of steps, such as: preparation of the information document, identification
Analysis of educational objectives	The objectives or outcomes are defined or clarified, after understanding the nature of the work or learning objective, the results are obtained for all the skills needed to achieve the desired goal.
Define sub-tasks and behaviors	This is a crucial stage towards developing behavioral learning objectives that become the basis of educational content. At this stage, sub-tasks and special behaviors are defined to achieve educational goals.
Identify the target group	The target group (learners or trainees) are analyzed, their behavior, their environment and their academic basis; because student information greatly influences the integrity of the choice of scientific content.
Identify tools and technology used	In this stage, the learning tools and technology used for students are identified. The technical tools can be divided into two main parts: • Hardware tools: Devices or equipment used inside or outside the classroom to assist in e-learning, i.e. computer types and network connection type. • Software tools: such as applications and the type of software installed in these computers and e- learning management systems. After selecting the learning tools, the techniques that can be used are analyzed, the scientific content designers are consulted with

	technical supervisors to understand the technology limitations, and the restriction developed by the IT department that are responsible.
Information security and privacy	In this stage, a security and privacy mechanisms are identified to prevent the penetration of the e- learning system. It is necessary to have alternative plans in the case of loss of information or damage, and chosen security algorithm; encryption method or the process of making backup copies of information
System & scientific content update and upgrade	In the last stage of the analysis phase, the mechanism for updating the system and upgrading it in the future is identified, such as scalability and the possibility of expansion and increase the number of lecturers, students and subjects, as well as the mechanism of scientific content update and upgrade in an easy and flexible, and how to change the graphical user interface GUI according to suggestions of feedback and change management.
Design Phase	At this phase, the results of the analysis phase are used to form the required schema for e- learning and its scientific content. The results of this phase are the design document. This document covers the objectives and strategies of education as well as the design of scientific content. The document is used to communicate among team members and is important to keep the project track and focus on the real goal of education. Several studies and research have indicated the use of design documents and patterns that are important for development, as well as the importance of developing standards in the design of learning elements as described below Define educational objectives The first stage in the design phase is to study the tasks or sub-goals that are listed in the analysis phase, and then to create a set of behavioral educational objectives. These objectives are specific and testable. For example, you can write final words for website design course such as: After completing this course, the student will be able to: - List types of programming languages available to deal with website design. - List available databases types for dealing with website design. - List and compare available content management systems. - Handle with content management system control panel. - Do own project work. Development of the scientific plan The scientific plan contains the study plan of the courses and its outline, sub-topics, summaries, the scheduling of the practical activities, homework, examinations, projects, research papers and the method of evaluation.

	The process of composing scientific content is the most important in the designing process of educational systems, in addition the importance of the interactive feature of updating, modification and development of content, which must be easy and clear within the interactive environment. Define test questions The design document contains a brief description of students' tests, for example: multiple choice, true or false, fill blanks, simulations, educational games, and exercises.

Conclusion

Maritime and logistic operations are critical to the success of economies in various countries. To ensure maximum returns, there is a need to make the process of maritime transport and logistics digital. However, this creates a new path for challenges to come in as security issues are created through attackers who come with different motives. Thus, there is need to ensure that maritime security is enhanced throughout all ports. The first step to understanding the mechanism to use is knowing the threats that the ports face. This research paper has explained in length the different threats that ports and other logistical firms face and how they can possibly deal with the challenges.

To help digitize port, logistics and supply chain operations, firms have turned to Blockchain as it contains a number of solutions to the current challenges that they face. As explained in the paper, Blockchain is a concept of technology that entails the use of bitcoin, cryptocurrency and is constantly disrupting the growing parts of the economy. Considering the fact that logistics and supply chain sector has been growing rapidly in various parts of the world, the need to have accountability and ease of operations has seen in the report. It is clear that the future of logistics and supply chain lies in the ability of Blockchain to make businesses better and ensure safer and faster transitions that will help eliminate many unnecessary middlemen that make the process of logistics and port operations longer and unsecure than they should be.

For logistics and supply chain to succeed, the paper has stated that there is a need to have a specialized workforce to handle special orders and operations. This, however, has been a great challenge to many institutions as they only have a small number of skilled individuals and many general operations workers. Thus, to ensure that institutions have the right blend of employees working for them, two methods of developing employees are suggested. The first one is employing skilled workers to specific departments where they can do their operations and use their skills to create a better working environment and lead to better results. The second one is developing employees from within the company to get the right skills. This way, organizations will not have to spend exorbitant amounts to employ and train employees. This will ensure the organizations become more competitive and improve their value greatly.

Despite all the changes and need to have human capital adding value to ports in their logistical operations, the digital space presents the greatest threat to their operations.

References

Ahn, Y. S., & McLean, G. N. (2008). Competencies for port and logistics personnel: An application of regional human resource development. Asia Pacific Education Review, 9(4), 542-551.

Allen, D. W., Berg, C., Davidson, S., Novak, M., & Potts, J. (2019). International policy coordination for blockchain supply chains. Asia & the Pacific Policy Studies.

Almotairi, B. (2012). Integrated Logistics Platform The context of the port relational exchanges and systematic integration. Chalmers University of Technology.

Black, W. R., & Van Geenhuizen, M. (2006). ICT innovation and sustainability of the transport sector. European journal of transport and infrastructure research EJTIR, 6 (1).

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342-353.

Burmeister, H. C., Bruhn, W., Rødseth, Ø. J., & Porathe, T. (2014). Autonomous unmanned merchant vessel and its contribution towards the e-Navigation implementation: The MUNIN perspective. International Journal of e-Navigation and Maritime Economy, 1, 1-13.

Caponi, S. L., & Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. Intellectual Property & Technology Law Journal, 27(1), 16.

Carlan, V., Sys, C., Vanelslander, T., & Roumboutsos, A. (2017). Digital innovation in the port sector: Barriers and facilitators. Competition and regulation in network industries, 18(1-2), 71-93.

Chiappetta A. (2017). Hybrid ports: the role of IoT and Cyber Security in the next decade. Journal of Sustainable Development - DOI: 10.14254/jsdtl.2017.2-2.4 .

Christodoulou, P., Christodoulou, K., & Andreou, A. (2018). A decentralized application for logistics: Using blockchain in real-world applications. The Cyprus Review, 30(2), 171-183.

Christopher, M. (2016). Logistics & supply chain management. Pearson UK.

Cimpean, D., Meire, J., Bouckaert, V., Vande Casteele, S., Pelle, A., & Hellebooge, L. (2011). Analysis of cybersecurity aspects in the maritime sector.

Cooper, P. (2015). Transportation & Logistics 2030 Volume 5: Winning the talent race. Website:https://www.pwc.com/gx/en/transportation-logistics/pdf/pwc-tl-2030-volume-5.pdf.

Cristea, D. S., Moga, L. M., Neculita, M., Prentkovskis, O., Md Nor, K., & Mardani, A. (2017). Operational shipping intelligence through distributed cloud computing. Journal of Business Economics and Management, 18(4), 695-725.

De Martino, M., Errichiello, L., Marasco, A., & Morvillo, A. (2013). Logistics innovation in seaports: An inter-organizational perspective. Research in Transportation Business & Management, 8, 123-133.

Di Renzo, J., Goward, D. A., & Roberts, F. S. (2015, July). The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE.

Dujak, D., & Sajter, D. (2019). Blockchain applications in supply chain. In SMART Supply Network (pp. 21-46). Springer, Cham.
Evangelista, P., McKinnon, A., Sweeney, E., & Esposito, E. (Eds.). (2012). Supply chain innovation for competing in highly dynamic markets: challenges and solutions. Business Science Reference.
Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cybersecurity.
Gajšek, B., Kovač, J., & Hazen, B. T. (2018). An Organizational Framework for Logistic Platform and its Subtypes in a Search for More Logistically Attractive Regions. Organizacija, 51(1), 20-34.
Grabara, J., Kolcun, M., & Kot, S. (2014). The role of information systems in transport logistics. International Journal of Education and Research, 2(2), 1-8.
Grawe, S. J. (2009). Logistics innovation: a literature-based conceptual framework. The International Journal of Logistics Management, 20(3), 360-377.
Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: trick or treat? In Proceedings of the Hamburg International Conference of Logistics (HICL) (pp. 3-18). epubli.
Hidalgo, A., & López, V. (2009). Drivers and impacts of ICT adoption on transport and logistics services. Asian Journal of Technology Innovation, 17(2), 27-47.
Inkinen, T., Helminen, R., & Saarikoski, J. (2019). Port Digitalization with Open Data: Challenges, Opportunities, and Integrations. Journal of Open Innovation: Technology, Market, and Complexity, 5(2), 30.
Interreg Adrion. (2018). Report on the transnational best practices concerning OCT tools for improving multimodal transport in Ports at BCPS Know-how transfer. Deliverable d.t2.1.3
Journal of Sustainable Development of Transport and Logistics,2(2),47-56.
Kooistra, W. M. (2008). Drivers and obstacles for innovation in logistics: case studies in dutch logistics (Master's thesis, Open Universiteit Nederland).
Le, T. N. (2015). Factors affecting the competency of domestic logistic Enterprises in Vietnam. 義守大學管理學院碩博士班學位論文, 1-62.
Mansouribakvand, G. (2019). The Impact of Blockchain Technology on Trust in the Supply Chain.
Meyer-Larsen, N., & Müller, R. (2018, February). Enhancing the Cybersecurity of Port Community Systems. In International Conference on Dynamics in Logistics (pp. 318-323). Springer, Cham.
Peansupap, V., & Walker, D. H. (2006). Information communication technology (ICT) implementation constraints: A construction industry perspective. Engineering, construction, and architectural management, 13(4), 364-379.
Perboli, G., Musso, S., & Rosano, M. (2018). Blockchain in logistics and supply chain: A lean approach for designing real-world use cases. IEEE Access, 6, 62018-62028.
Pervez, H., & Haq, I. U. (2019, March). Blockchain and IoT Based Disruption in Logistics. In 2019 2nd International Conference on Communication, Computing and Digital systems (C-CODE) (pp. 276-281). IEEE.

Porathe, T. (2016). A navigating navigator onboard or a monitoring operator ashore? Towards safe, effective, and sustainable maritime transportation: findings from five recent EU projects. Transportation research procedia, 14, 233-242.
PWC. (n.d.). Shifting Patterns. The Future of the logistics industry.
Robert, M. A. R. E. K. A (2016). QUALITATIVE ANALYSIS OF USING SWIBŻ SYSTEM INTO CREATION OF POLISH PORT COMMUNITY SYSTEM.
Robert, M. A. R. E. K. A QUALITATIVE ANALYSIS OF USING SWIBŻ SYSTEM INTO CREATION OF POLISH PORT COMMUNITY SYSTEM.

Saeed, Mustafa & Malallah, Fahad & Alasaady, Maher. (2019). A proposed model for designing E-learning courses. Journal of Theoretical and Applied Information Technology. 97. 1239 -1250.
Shah, S. K. (2004). The evolving landscape of maritime cybersecurity. Review of Business, 25(3), 30.
Skovgaard, J. (2014). European Union's policy on corporate social responsibility and opportunities for the maritime industry. International Journal of Shipping and Transport Logistics, 6(5), 513-530.
Srour, F. J., van Oosterhout, M., van Baalen, P., & Zuidwijk, R. (2008). Port community system implementation: Lessons learned from international scan. In Transportation Research Board 87th Annual Meeting, Washington DC.
Tijan, E., Agatić, A., & Hlača, B. (2012). The necessity of port community system implementation in the Croatian seaports. Promet-Traffic & Transportation, 24(4), 305-315.
Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2019). Blockchain Technology Implementation in Logistics. Sustainability, 11(4), 1185.
Tijan, E., Kos, S., & Ogrizović, D. (2009). Disaster recovery and business continuity in port community systems. Pomorstvo, 23(1), 243-260.
Wagner, S. M., & Sutter, R. (2012). A qualitative investigation of innovation between third--party logistics providers and customers. International Journal of Production Economics, 140(2), 944-958.
Wang, P., Jin, C., Zhu, D., Tang, Y., Loh, P. C., & Choo, F. H. (2014). Distributed control for autonomous operation of a three-port AC/DC/DS hybrid microgrid. IEEE Transactions on Industrial Electronics, 62(2), 1279-1290.
Wilshusen, G. C. (2015). Maritime critical infrastructure protection: DHS needs to enhance efforts to address port cybersecurity (No. GAO-16-116T).
Yadav, D. (2014). Importance of Compliance, Regulations, and Ethics in the wake of Korean Ferry accident. ASA Institute for Risk novation.