Journal of Sustainable Development of Transport and Logistics
journal home page: https://jsdtl.sciview.net

Chiappetta, A. (2017). Hybrid ports: the role of IoT and Cyber Security in the next decade. *Journal of Sustainable Development of Transport and Logistics, 2*(2), 47-56. doi:10.14254/jsdtl.2017.2-2.4.

ISSN 2520-2979

Hybrid ports: the role of IoT and Cyber Security in the next decade

Andrea Chiappetta

Marconi International University,
111 NE 1st street, Miami -33132 Florida, USA
PhD, Professor of Geopolitical Economy

Article history:

Received: September 12, 2017
1st Revision: October 10, 2017
Accepted: October 28, 2017

DOI:
10.14254/jsdtl.2017.2-2.4

Abstract: The next future will be played on a cyber level that imposes the need to merge "physical" with "digital in all fields": phygital will be the future of current world, in many sectors, primarily in the transportation fields. Nowadays ports are doing several investment to provide technical solution to attract freight flows, are they ready to provide an answer to the cyber threat? This paper wish to present an overview of the main implications related to the cyber threats and maritime transports.

Keywords: Cyber Security, ports, Critical Infrastructure Protection, Internet of Things.

1. Introduction

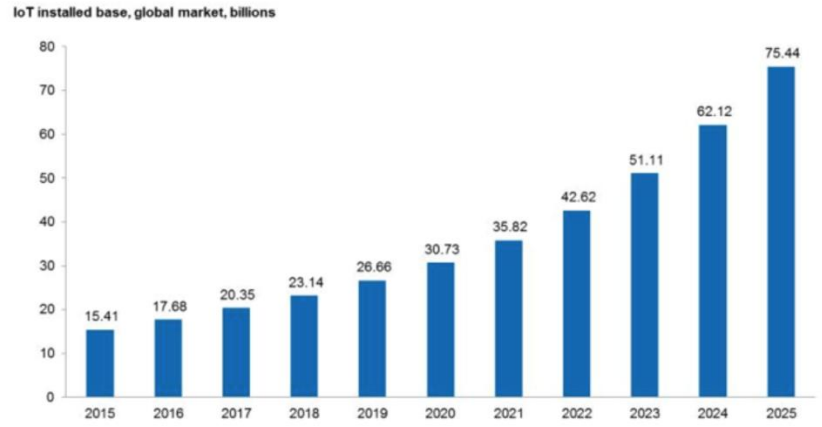
Mobility and transportation have always been playing a crucial role as way to provide economic and social development. The maritime transports, as main player in freight movements, nowadays cover more then 70% of the markets: most of goods are shipped through the sea. Ports are considered, due to their strategical relevance as a Critical Infrastructure, to be protected and the main issues is to guarantee the resilience of transportation infrastructures. The Cyber Security in the sector has become a corner stone that needs to be looked after and raised on a daily basis with continuous improvement. The cyber-attacks are becoming a daily problem showing how the public sector and private sector have to create synergies to provide a more safe and secure conditions: in transportation, this is more true than in any other sector. This article will present a short overview of the main vulnerabilities related to the maritime transport and the impact of a connected community where almost 3 billion of people are online and with a forecast of more then 40 billion devices connected by 2020 (IoT). Beyond the creation of the Hybrid port, that will be a consequence of the Digital Transformation and technology innovation is necessary to enable new services. Ports have to be re-thinked and re-designed in: immaterial and material infrastructure, processes, organization and information exchanged between actors. A safe and secure port is a fundamental component to provide a right answer to the next decade flows. This paper provide an impact assessment approach to check if a port is compliance to the Cybersecurity issues or not.

Today, 2.9 billion people, or 40% of the world's population are online. By 2020 it is predicted that over 40 billion more devices will become "smart" via embedded processors and intelligence. IoT has

Corresponding author: *Andrea Chiappetta*
E-mail: a.chiappetta@miuniversity.edu

already grown beyond niche industrial and medical applications into every market and industry, and growth is anticipated to be exponential without forgetting the SCADA Systems. Future developments will inevitably rely on state of the art platforms and systems that enable advanced semi- autonomous IoT applications. Such applications are anticipated to integrate smart objects, embedded intelligence, and smart networks across distributed heterogeneous systems of systems. The figure 1 shows that the data created and consumed by IoT devices is an ever growing challenge. Estimated the number of IoT devices as shown in the graph. IoT devices are the foundational layer, where data is created. The IoT industry assumes you can trust the data from device, but in most cases, this is not true. The mobile devices of today are essential to decentralized data processing, but that processing can be easily corrupted.

Figure 1: IoT Installed base, global market, billions



Source: IHS – Markit, as reported in Forbes

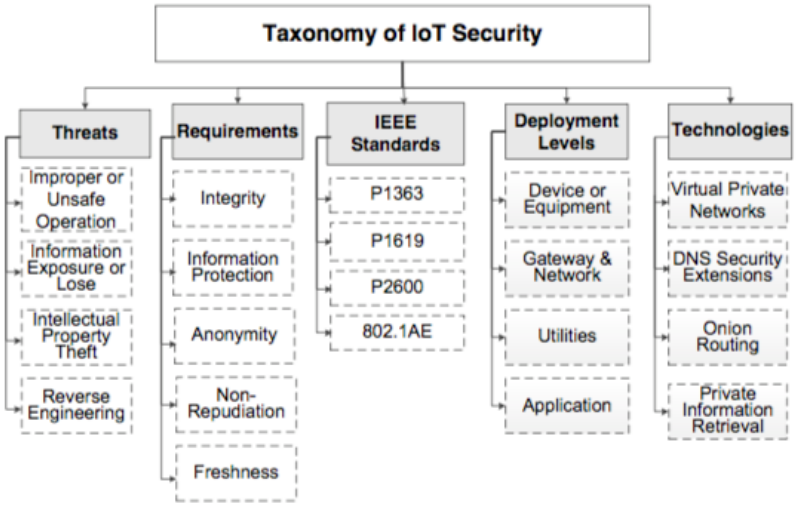
2. From Scada to IoT

SCADA means supervisory control and data acquisition, the first use is started in the 1960's to monitor and control remote gear grew that is part of the Control Systems family, that include ICS (Industrial control system), DCS (Distributed control systems), PCS (process control system) etc. Early systems were built from main frame computers and required human oversight to operate. With the technological development became automated reducing the involvement of human control. These systems are used to monitor and control a plant on industries in many different sectors like energy, transport, waste control etc. In the maritime sector there are several parameters to be monitored like the GPS. Hull opening, hull stress, radar, ship speed, fuel and machinery temperature and so on, from land side SCADA allow the control of Surveillance system until cargo handlings systems.

In recent years, with the 4th industrial revolution, or Industry 4.0, these systems were substitutes by the Cloud Computing and Internet of Things (IoT) have been rapidly advancing as the two fundamental technologies of the "Future Internet" concept, that allows the "connection of thousands of sensors and devices". Different IoT systems are designed and implemented according to the IoT domain requirements, typically not taking into consideration issues of openness, scalability, interoperability, and use case independence. This leads to a variety of new potential risks concerning information security and privacy, data protection and especially safety, all of which need to be considered in unison. Clearly, the risk assessment model is influenced by the circumstances in which each IoT application and system is configured, deployed and used. Large scale connectivity of intelligent objects coupled with complex constraints inevitably leads to many security challenges, which are not included into the classical formulation of security problems and solutions. Consequently, securing data, objects, networks, infrastructure, systems and people in IoT will have a prominent role in the research and standardization activities over the next several years. This imperative is the need to pay close attention to increasing amounts of data, with the associated concerns for security, privacy and protection of personal, proprietary, business and confidential information of all kinds. The costs of cyber-attacks in such

settings is estimated to reach over 2 trillion USD by 2020, and today IoT is just beginning to emerge with exploits reported at a steady pace and suggesting that information security and operational security are already major challenges. Such security threats are broad, and have the potential to incapacitate IoT systems and/or significantly alter their intended operation. Since the IoT ecosystem can have critical infrastructure components, it will inevitably be a target for attack and espionage, as well as vulnerable to denial-of-service and many other types of cyber-attacks. Likewise, the heterogeneous functional and operational nature of interconnected and cooperating IoT systems will evolve to a point where the security threat canvas is of a size and scale that will be difficult (if not impossible) to accurately represent in formalized security threat models, implying a need for compensatory techniques to help guarantee security imperatives are met. IoT, Industry 4.0 and interconnected devices and infrastructures are likely to be a standard in the near future, bringing disruptive changes as we move from the era of personal devices to an era that is promoting large scale inter-connected and highly integrated devices and platforms that support real time monitoring, autonomous adaption, instrumentation, peer-peer/master-slave communications, actuation, control logic and more. The European Bratislava agenda acknowledges that even "modest innovators" need to "adopt the latest smart technologies" in Europe, and to a large extent this is already happening. Early threats and risks identification from a physical and cyber security in port operations is a vital aspect in the overall security concerns of Europe and its member states, not only in terms of homeland security but also in terms of economic and legal interests. However, with ever increasing potential threats and decreasing budgets in the member states physical and cyber security in critical infrastructures need to become efficient and cost-effective. In the figure below it is described the taxonomy of IoT security based in various parameters providing the threats, requirements, IEEE Standards, Deployment levels and technologies. From this taxonomy is clearly showed how the IoT and cyber threats are something that can't be considered as an issue to be solved.

Figure 2: Taxonomy of IoT Security



Source: The rise of ransomware and emerging security challenges in the Internet of Things, - Sep 2017- Computer Networks

3. Cyber threats in the maritime sector

A global study related to the risks rated the cyber risks as the third highest business risk worldwide. Incidents such as the recent increase in illegal migrants entering Europe through the Mediterranean coastal areas as well as smuggling of illicit goods requires increased protection of the critical infrastructures such as port operations. Software systems that support critical infrastructures operations are becoming more and more attractive to outside cyber-attacks from cyber-criminal interested in wreaking havoc in cyber environments. Not only sensitive data needs to be protected from any malicious intentions, but if the overall control that these software systems have on the operational aspects in critical infrastructures is harmed then negative results with high risk, impact and visibility

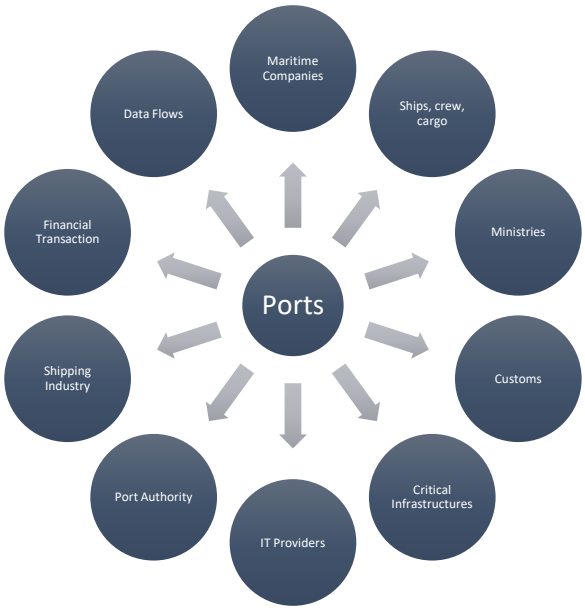
can arise. Innovative physical and cyber security mechanisms have to be created in order to be able to prevent and respond to all potential threats in these critical infrastructures. Transportation is a key economic sector, facilitating the movement of people, food, water, medicines, fuel, etc. Port Authorities play an important role in the international trade and economy environment. Transportation infrastructures face multiple threats, ranging from physical disasters, sabotage, insider threats, terrorist attacks, etc. The increasing need for protecting transport infrastructures is recognized by most countries; the transportation sector is among the sectors recognized as critical. Ports and the maritime industry compete as part of entire supply chains. After 2009 crisis, to strengthen their position, a great number of top container shipping companies are integrating vertically with port terminals, hinterland logistic operators, and shipping agencies. More concentrated volumes of cargo, as well as the need to remain competitive versus other modes of transport, also necessitate speedier execution of formalities and better coordination of logistic operations. Digitalization is considered to be crucial in simplifying administrative processes, enabling efficient management of freight flows through exchange of information on cargo, infrastructure and equipment. Increased pressure on environmental resources has already required corrective action to contribute to the "greening" of shipping. Though infrastructure protection and infrastructure resilience represent complementary elements of a comprehensive risk management strategy, the two concepts are distinct but need to be considered both. Infrastructure protection is the ability to prevent or reduce the effect of an adverse event. Infrastructure resilience is the ability to reduce the magnitude, impact or duration of a disruption. The spread in the continuous discovery of new threats that target Cis, stress the importance of a whole rethinking around the concept of protection. That's where resilience emerges from and becomes important part of the playing field. A resilient approach is a holistic set of procedures and measures that encompasses the entire structure of an institution, from physical parts to the management, to ensure the ability to prevent, absorb, adapt and recover to an attack, either physical or cyber. We need to have in mind without confuse the concepts of resilience, security, business continuity and risk management, crisis and emergency. Concerning the maritime cyber-attacks, they are not too much, at least declared due to reputational damage or because they still don't know to be attacked. The known cyber-attacks are the following, Port of Antwerp were Drugs were hidden in containers and these containers were misled without early recognition (Bateman, 2013); The port of Rotterdam in 2016 the Customs systems were shut down, stopping operations for hours, probably to extort ransom; Disruption of the GPS-signal stopped operations of vessels as well as of terminal cranes that store and locate containers basing on GPS for the same reason (Wagstaff, 2014; Scott, 2015; Hayes, 2016); Piracy attacks use AIS-signals to identify vessels and hack into the shipping companies systems to identify their loaded goods (Allianz Global Corporate & Specialty SE, 2016); Global ransomware campaign known as "WannaCry" and detected on May 12, 2017, affected various organizations with tens of thousands of infections in over 150 countries (US-CERT, 2017a) after the "WannaCry" attack, on June 27, 2017, further threats was launched, using among other attack vectors the same exploit as "WannaCry" (USCERT, 2017b; Fox-Brewster, 2017). It exploited a vulnerability in a Ukrainian tax preparation software update mechanism to propagate and attack entire networks (e.g. Cimpanu, 2017). Besides several Ukrainian ministries, banks and metro systems, large companies became also victim of the attack. Merck Sharp & Dohme (e.g. Holland, 2017) and India's largest container terminal JNPT (e.g. PTI, 2017) were affected and, as a consequence, had to deal with business interruptions. The malware's attack path leading from a Ukrainian software update to several international company networks shows how malware can propagate among the connected ICT systems in supply chains.

4. Cyber ports: Risk and opportunities

Since 2009, initiatives were undertaken to establish a true 'European maritime transport space without barriers', removing unnecessary administrative obstacles to maritime transport, developing into the Union a Maritime Information and Exchange system (Safe Sea Net), simplifying formalities for regular shipping services (Blue Belt), investing in the port sector and in the connection between ports and hinterland (Trans-European Network Transport projects), last but not least Digital Future Port point at improve the economic process of the Mediterranean Area, with the support of Digital Tools, that is, a target of UE Strategy (ports 2030).The ocean and short shipping ports constitute part of the European Critical Infrastructure, as indicated in the Directive 114/2008, and concurrently critical part

of the supply chains and transport routes, transferring goods and passengers. The maritime sector sustains the society and the economy through the movement of people and vital goods, such as energy, food, etc. The ports have a direct impact on connectivity across Europe, enabling the connection of islands and isolated areas while significant proportion of economic activities are occurred in the ports, mainly through the transfer of goods. Currently, the European ports serve around 3,733 million tons of freight flows and 397,506,000 passengers per year (data for year 2012, available by Eurostat). Moreover, 74% of goods entering or leaving Europe go by sea, and Europe boasts some of the finest port facilities in the world while around 90% of EU external trade and more than 43% of the internal trade take place via maritime routes while the gross weight of seaborne goods handled in EU reached in 2014. A part from the above, the ports are significant for the economy in terms of employment, as 1.5 million workers employed in European ports while the number of indirect employed work is almost equal. Finally, the maritime transport has a positive impact on the environment, owe to the reduced amount of GHG emissions per ton or passenger transferred.

Figure 3: Ports interdependencies



Source: Author elaboration

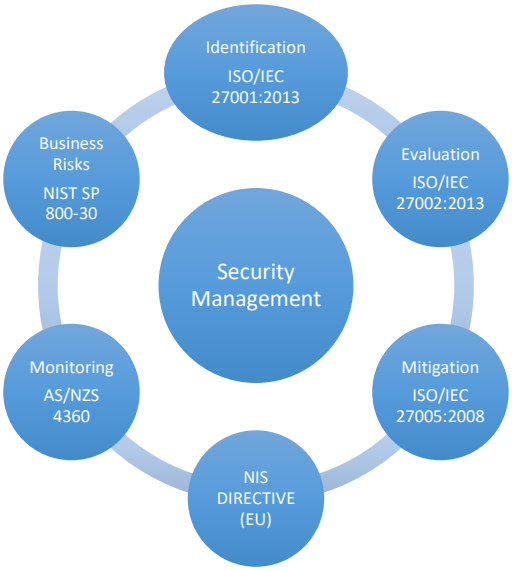
The Figure 3 presented above underline the critical and vital role of maritime transport and consequently ports in the society and economy of EU showing how and why A port is a complex cyber environment that encompasses both land, waterside and economic activities and interdependencies. The enhancement of security, both physical and cyber, at ports is essential in order to ensure the smooth operation, serving the passenger and freight flows. On the other side, the ports are considered as vulnerable infrastructure mainly due to their proximity to the sea and the problems faced in controlling the threats coming through it, the number of operations taking place in the ports and their different nature and the considerable number of people working or involved in several operations in the ports; Internationally the relevant legislation on port security is the ISPS Code (International Ship and Port Facility Security Code), implemented at EU level by the EU / 725/2004 and the EU / 65/2005, which requires the identification of authority, acts skills and objectives to establish and maintain security measures. In this context, it takes the definition of a Port Security Plan, drawn up by the Port Security Officer (PSO), which takes into account the analysis of the risks of ships and the port facility. Also it identifies the Port Facility responsibilities and tasks of the Port Facility Security Officer (PFSO). It is also important to note that many European ports are to all parts of the city and therefore the effects of splitting the areas under Security checks presents greater complexity. Nowadays few countries launched a maritime cyber security strategy or programs, for example US launched in 2014 the port security grant program allowing funds to provide cyber vulnerability assessments and then the ”Information Sharing and Analysis Organizations” (ISAO), e.g., the ”Maritime & Port Security Information Sharing and Analysis Organization” (MPS-ISAO, 2017), a second approach was launched by

the UK, where the Department for Transport, Maritime Sector Issued a guidance on ship security: cyber security code of practice that provide a guidance to assist ship operators to develop a cybersecurity assessment and plan, device the most appropriate mitigation measures and ensure to establish a correct structures with roles and responsibilities. Last but not least is the work done by the IMO (International Maritime Organization that issued a Guidelines on Maritime Cyber Risk Management that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management. At EU level were adopted the Network and Information System (NIS) Directive (EU, 2016). The directive aims to reach a common level of security for NIS in the EU in order to provide a common approach concerning the network security and minimum level to be adopted but each Member states. Nowadays, implemented security solutions within the ports areas aim to achieve the desired security levels through the implementation of a network of active sensors (high-resolution cameras, IR barriers, biometric fingerprint reader, microphone cable, etc.), subsystems functional (vehicular video, license plate reading and container codes units, video over IP, turnstiles, automatic barriers, metal detectors, baggage scanners, radar, etc.) and passive protection systems (metal fences, etc.) for control and protection of the different port areas (perimeter) gates of vehicular / pedestrian access, cruise terminals, parking lots, docks, electrical substations, etc.). Although the above security network seems well structured, the use of modern technology is not enough. With regard to the ENISA report on cyber security challenges in the Maritime Sector seems evident that cyber threats are a growing menace, spreading to all industry sectors that are relying on ICT systems. Such incidents could be prevented by policies that neutralize the various market failures acting as a barrier to optimize private investment in cybersecurity from public and private institutions. Many computers systems store valuable information about entities other than the system's owner. From a legislation point of view in starting from 2018, payments service provider will have to comply with the new payments services directive (PSD2) which mandates very high standards of cyber security for all digital payments where central banks or other regulators can also impose obligations. Something similar will be done in the framework of the NIS Directive that will cover also the critical infrastructure. Cyber-attacks to maritime transports are an issue already consolidated: Infiltrating a port's computers, or transmitting fake GPS signals to alter ship's route, altering a ship's automatic identification system signal to misreport it location, accessing electronic chart display and information systems software to modify maps, as well as pirates listening into AIS transmissions to locate potential victims. Recent deliberate disruptions of critical automation systems, such as Stuxnet, prove that cyber-attacks have a significant impact on critical infrastructures. Disruption of these ICT capabilities may have disastrous consequences for the EU Member States' governments and social well being. The need to ensure ICT robustness against cyber-attacks is thus a key challenge at national and pan-European level. Some key findings of the report emphasized that Maritime cyber security awareness is currently low and a holistic, risk-based approach coupled with an assessment of maritime specific cyber risks, as well as identification of all critical assets within this sector is highly necessary. An answer is represented by the holistic security: Physical and Cyber security of the network, to guarantee Privacy Integration Protocols of the users. There are so many initiatives that come in response to recent computer hacks that enabled containers to be abstracted from the port in an apparently legal manner. For instance, MSC introduced a new Container Release System that enables containers to be collected from the port in a more secure manner. Users have to log into a secure portal site where they must identify themselves in order to gain access to the container release data. This technology has now been made available port wide, thanks to APCS. Furthermore, the Port of LA took a significant step towards reducing its cyber risks with the implementation of a state-of-the-art Cyber Security Operations Center (CSOC). The CSOC includes advanced hardware and software that is used to proactively monitor the computer environment to prevent a breach and be able to quickly detect and respond if a breach does occur. The CSOC is also the technical nerve center, which collects cyber security data that can be analyzed and shared with other agencies.

5. The next port: Hybrid

Ports are known as physical space where trades meets the market needs. Ships are a visible and touchable instrument to transfer goods from an origin to a destination. All these actions, now are managed by a system and or OS. Nowadays, it is fundamental take in account the next challenges, related to the connectivity and to capacity to provide solutions and (cyber) security to guarantee the economic flows and development. Ports and ships now require a multi-level intelligence and surveillance system, aimed at creating a comprehensive Port Hybrid Security System providing real-time, accurate physical & cyber situational awareness and early warning to Ports Stakeholders, as well as decision making in terms of threat & impact assessment and suggested response or mitigation actions. The HYBRID PORT concept is based upon a fusion of inputs from different types of Front End (physical) sensory systems and cyber detection systems - legacy and new innovative - from different security sectors. Such threat events are detected through 'bottom-up' integration of different types of real-time sensors and sub-systems for data collection in a variety of modes, including physic and cyber, and correlate each other to generate (1) hybrid threat prioritized alarm/s, (2) decisions sequence for the security operators. This "fusion" is based upon predefined threat scenarios as determined by the Port Security Operation Centre (P-SOC), as a 'top-down' approach.

Figure 4: Security Management approach



Source: Author elaboration

The hybrid port idea has incorporated the latest technologies, is scalable and empowered with the flexibility to expand and enrich the System by adding new sensors and applications according to specific requirements and future needs. In addition, each sensor can be activated independently and/or fused with other specific sensors to achieve the necessary output. The hybrid port should integrates with ease into the existing Port Front End (F/E) sensors and information systems. Under previous Port Security conditions (security plan schemes), the end user is overwhelmed with the magnitude of data needed to be filtered individually, step-by-step. The hybrid port, through its automatic selection and fusion of the input data, transforms the process into a user friendly interface and presents only relevant alert information to the end user in a straightforward and clear manner. This enables an advanced, more accurate decision making process in the face of the growing multitude of threats and dangers each port is faced with on a daily basis. The hybrid port divides the port security into "security control" sectors (Port Facilities & People, Land Borders & Gates, Last Mile Surface & Underwater, AIS & GNSS and Cyberspace). Each segment is monitored by tailored technologies, which are incorporated into the system creating a multisource labyrinth fusion logic, which enables situational and security awareness of the port anytime, anywhere. These consolidated control segments are accessed through the Port C2 HMI (C2HMI) by running a suite of applications, thus the port security control is centralized, serving all port authorities. Information will be shared and synchronized to generate an integrated, real time,

security overview for the port C2, providing the necessary features to assure a total "no breach" security environment. Most of the technologies that will be fused are already used by port (in-place technologies), yet in a 'stand- alone mode'. This mode is less effective in creating a comprehensive intelligence system compared to the "fused mode". The Hybrid port approach brings the capability to integrate these in-place technologies (mobile and fixed) and the new detection technologies and to fuse their collected data into a central point where it will be analyzed together with data from other sources. Most physical processes within the port community (e.g. vehicles and cargo loading/unloading, LNG distribution and storage) are executed with autonomous or semi-autonomous mechanical physical systems and machineries (e.g. ships, trucks, cranes, electronic gates/fences) under the control of sophisticated logistic software systems (e.g. Industrial Cyber-Physical Systems, SCADA, surveillance systems). Utility networks categorization, threats taxonomy in industrial and utility communication infrastructures, are comprised of a diverse set of technologies and networks topologies that cannot be effectively secured without having categorized the utility networks components and technologies in respect of cyber threats and their impact in terms of service availability. The general utility infrastructure, reported by INTELBLUEPRINT, is shown in the table below, nevertheless a deep security management plan has to take into account the vulnerability of specific components, applications and devices involved within the utility network. A typical solution for the detection of attacks in a network environment consists of leveraging signature- based NIDS (Network Intrusion Detection System) technologies that aim at detecting attacks by recognizing specific patterns in network data streams. However, current signature-based technologies are not effective in Critical Infrastructure systems because there is often little information about system internals (let alone attack vectors). Hence, developing effective signatures is a difficult task. On the other hand, behavior based NIDS technologies are not based on needing complete knowledge of all possible attack vectors. During a training phase, these techniques build a statistical model of the input that is then used in the detection phase to raise an alert when the input does not match the expected statistical profile. Using more than one technical or procedural protection measure is recommended. It is essential to protect critical systems and data with layers of protection measures which take into account the role of personnel, procedures and technology to: increase the probability that a cyber-incident is detected; increase the effort and resources required to protect information, data or the availability of IT and OT systems. This defense in depth approach encourages a combination of: physical security of the ship in accordance with the ship security plan; protection of networks, including effective segmentation; intrusion detection; software white listing; access and user controls; appropriate procedures regarding the use of the removable media and password policies; personnel's awareness of the risk and familiarity with appropriate procedures. Fundamental start with a third party risk assessments. Targets to be considered: Communication Systems, Integrated communication systems; satellite communication equipment, VOIP equipment; WLANs, Public address and general alarm systems. Bridge systems: Integrated navigation system; GPS, Electronic Chart display information system, Dynamic positioning systems; Global maritime distress and safety system, radar equipment; Voyage data recorders, Propulsory and machinery Management and power control systems: Engine governor; power management; integrated control system; alarm system; emergency response system; access control systems: Surveillance system; Bridge navigational each alarm system, Shipboard security alarm systems; Electronic personnel on board systems; cargo management systems: Cargo Control room; Level indication system; valve remote control system; ballast water; passenger servicing and management systems; ship passenger boarding access systems; infrastructure support systems like domain naming system DNS and user authentication/authorization systems; passenger facing networks; passenger Wi-Fi - WLAN; guest entertainment systems; passenger Wi-Fi, core infrastructure Systems; Security gateways; routers; switches; firewalls, VPN, Intrusion or prevention systems; security event logging systems; administrative and crew welfare systems administrative systems; review of the onboard networks.

Different behavior - based NIDS technologies have been devised by researchers, mostly focusing on the modelling of network interactions. However, behavior - based detection systems have been rarely successfully applied to business solutions for a variety of reasons. Firstly, such systems usually raise too many false positives to be of practical use. Secondly, most recent engines have been mainly tailored for and tested against the HTTP protocol. Thus, the effectiveness of current detection engines, when deployed in critical infrastructure networks, could be biased by the fact that a large part of protocols is binary-based, and it might be hard (or infeasible) to adapt the detection algorithm to a different lower

layer protocol. Artificial Immune System (AIS) is a relatively new bio-inspired model, which is applied for solving various problems in the field of information security. The unique features AIS encourage the researchers to employ these techniques in variety of applications and especially in intrusion detection systems. Originally created for applications in immune networks, the application of its ideas is mainly focused in anomaly detection in computer networks connected to internet, exposed to many kinds of cyber-crimes. Over the years, it has become a fertile and wider research field. In particular, it is of great interest its application in isolated networks as those of critical infrastructures (communication and control systems), promoting active research on efficient Intrusion Detection Systems (IDS). Some of the research is oriented to a specific kind of infrastructure, for example, modern and future electrical grid.

6. Conclusion

Cybersecurity is becoming a vital concern for the functioning of a modern economy. There is an urgent need for improvement understanding of microeconomic mechanism in the cybersecurity market and for reliable data upon which policy design can be based: this with particular reference to transportation sector, where the goal of securitization can only be reached by a strong and continuous cooperation between public and private sector.

Every single day cybersecurity software proves unsuccessful in stopping attacks. Malware, malicious users, and targeted attacks create massive risk. For industry, government and consumers to realize cybersecurity success, they must begin with a foundation built on trusted hardware execution.

Appendix A. Supplementary material

Supplementary data associated with this article can be found, in the online version, at https://jsdtl.sciview.net

Funding

The authors received no direct funding for this research.

Citation information

Chiappetta, A. (2017). Hybrid ports: the role of IoT and Cyber Security in the next decade. *Journal of Sustainable Development of Transport and Logistics, 2*(2), 47-56. doi:10.14254/jsdtl.2017.2-2.4.

References

Bou-Harb, E., Kaisar, E. I., & Austin, M. (2017, June). On the impact of empirical attack models targeting marine transportation. In *Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017 5th IEEE International Conference on* (pp. 200-205). IEEE.

Chiappetta, A., & Cuozzo, G. (2017, June). Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In *Models and Technologies for Intelligent Transportation Systems (MT-ITS), 2017 5th IEEE International Conference on* (pp. 206-211). IEEE.

Hosseinpour, F., Bakar, K. A., Hardoroudi, A. H., & Dareshur, A. F. (2010, November). Design of a new distributed model for Intrusion Detection System based on Artificial Immune System. In *Advanced Information Management and Service (IMS), 2010 6th International Conference on* (pp. 378-383). IEEE.

Michel, D. (2017). United States Coast Guard – Dep. of Homeland Security – 2017 – Cyber Risks in the Marine Transportation System The U.S. Coast Guard Approach , U.S. Coast Guard Rear Admiral Paul F. Thomas, U.S. Coast Guard Captain Andrew E. Tucci, U.S. Coast Guard.

Pishva, D. (2017, February). Internet of Things: Security and privacy issues and possible solution. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on* (pp. 797-808). IEEE.

Schauer, S., Stamer, M., Bosse, C., Pavlidis, M., Mouratidis, H., König, S., & Papastergiou, S. (2017). An adaptive supply chain cyber risk management methodology. In *Digitalization in Supply Chain Management and Logistics* (Eds.). ISBN 9783745043280.

Tsamboulas, D., Chiappetta, A., Moraiti, P., & Karousos, I. (2015). Could Subsidies for Maritime Freight Transportation Achieve Social and Environmental Benefits? The Case of Ecobonus. *Transportation Research Record: Journal of the Transportation Research Board*, (2479), 78-85. https://doi.org/10.3141/2479-10

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks*.

Journal of Sustainable Development of Transport and Logistics (ISSN: 2520-2979) is published by **Scientific Publishing House "CSR", Poland, EU** and **Scientific Publishing House "SciView", Poland, EU**
Publishing with JSDTL ensures:
• Immediate, universal access to your article on publication
• High visibility and discoverability via the JSDTL website
• Rapid publication
• Guaranteed legacy preservation of your article
• Discounts and waivers for authors in developing regions
Submit your manuscript to a JSDTL at http://jsdtl.sciview.net/ or submit.jsdtl@sciview.net