TOWARDS SECURE MARITIME TRANSPORT IN SOUTH AFRICA: AN INVESTIGATION OF CYBERSECURITY READINESS OF ORGANISATIONS

K MURONGA[1], M LETEBELE[2]*, P BINDA[2] and S SMITH[2]*****

[1]University of South Africa and CSIR Smart Logistics and Infrastructure
Tel: 012 841-2337; Email: kmuronga@csir.co.za
[2]CSIR Smart Logistics and Infrastructure, PO Box 395, Pretoria, 0001
*Tel: 012 841-3393; Email: mletebele@csir.co.za
**Tel: 012 841-3355; Email: pbinda@csir.co.za
***Tel: 012 841-3455; Email: SSmith1@csir.co.za

ABSTRACT

Transport is an important sector for the economic development of South Africa. The maritime environment plays a very important role as it sustains other sectors in the economy. A sustainable transport system requires that all systems operate efficiently and continuously with minimum failure. Cyber-attacks are disruptive and may destruct the functions and operations of any sector including that of transport and more specifically maritime transport. This paper provides feedback regarding an investigation which was conducted with maritime transport organisations in South Africa to understand if any cybersecurity measures, policies, strategies etc. are in place and are successfully implemented to prevent cyber-attacks. A systematic literature review and a qualitative content analysis research technique was used to assess the status of maritime organisation's ability to identify and prevent such attacks. The results of the study indicate that the South African government has put relevant structures in place to ready the country for cyber-attacks, what is lacking is how these structures are used by organisations. This study also provides a brief overview of the existence of cybersecurity activities in the maritime transport industry of South Africa.

1. INTRODUCTION

The past decade has seen an increase in the usage of computers as well as the internet by both individuals, business and governments (Jones and Fox, 2009; File and Ryan, 2014). Known as the 4th industrial revolution, this is the digital era, where innovative technologies such as big data, the sharing economy, the internet of everything (also known as the internet of things) and blockchain technology are increasing, connecting the physical world with the information world, at a fast pace (Baller, Dutta and Lanvin, 2016). The World Economic Forum (WEF) estimates that the number of connected devices will increase from 13.4 billion in 2015 to 38.5 billion by the year 2020. This increase in connected devices will bring with it a rise in cyber risks and data breaches (WEF, 2016).

1.1 Important definitions

Maritime Transport, "*can simply be defined as the transportation and/or shipping of people and goods between two or more ports by making use of waterways and/or the sea*" (Hoffmann Jan, 2017). According to the *Review of Maritime Transport in 2017*, about 80%

in volume of the global trade is transported by ships and pass through sea ports, which makes maritime transport an important player in the transportation of goods.

Maritime Security, has many definitions depending on whom the security is affecting, but in general it can be defined as "*the protection of fishing spots; securing of offshore oil and gas production; protecting the maritime trade operations, as well as the development of ocean governance and regional operations including tourism, shipping of goods and deep sea mining"* (Siebels, no date)*.*

Cybersecurity, can be defined as "*the protection of cyberspace itself, the electronic information, the Information and Communication Technologies that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace*" (Von Solms and Van Niekerk, 2013) and expands further "*to the the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wireless communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation*" (Toth and Paulsen, 2016).

For the purpose of this study we had to combined all three definitions to come up with one definition of maritime cybersecurity and defined it as: (The protection of the national environment in which information and communication occurs via computerised networks, in order to facilitate the transportation of people and goods by making use of waterways and the sea, including the protection of the users of these networks in their personal and national capacity).

1.2 Background

The digital era is opening up positive possibilities to all industries with its interconnectivity, but with these possibilities cyber risk is also on the rise (Clemente, 2013; Jensen, 2015). The maritime industry, especially the shipping of goods and the transportation of passengers via luxury cruises, is no exception. In the past five years, there has been evidence of an increase in cyber-attacks on the shipping industry (Hubmann, Polke-Markmann and Vanheyden, 2018), when this happens transportation plans are revealed to the hackers, exposing the location and movement of the containers, and goods could be rerouted to the wrong recipients. The maritime industry experienced an event illustrating this hazard, when it fell victim to the "*Ransomware Petya cyber-attack*", which disrupted many industries in the world since 2016.

The Petya attack to Maersk, made its first infection through an end-user. Maersk being the biggest and largest maritime shipping company in the world, moving about 12 million containers each year, to deliver all over the world was a victim of the cyber-attack on 27 June 2017 (Moller, 2017). It is no secret that users of computers and the internet are the easy and simple target for initiating a cyber-attack. Maersk is credited for being reliable, flexible, eco-efficient and logistics company since its inception in 1928, but with over 33 000 employees worldwide, one wrong click from an employee can have their computerised environment affected, which is what happened with the Petya Attack.

The company's facilities in South Africa, Port Elizabeth and USA, New Jersey, had to be completely shut down until the ransomware ordeal was over. The whole ordeal was estimated to cost the maritime giant close to 300 million us dollars (Palmer, 2017). The morale of the story is that a simple click from one employee could cost a company millions of dollars, both in disrupted services; recovering from the attack and/or paying the ransom.

1.3 Problem statement

In South Africa, in 2013, it was evident that approximately a third (30.8%) of internet users accessed the internet mainly on their mobile devices, followed by users accessing the internet at work (16.1%), public places (10%) and at home (10%) (STATS-SA, 2014). The 2013 Household Survey shows that 40.9% of South Africans have access to the internet, translating into about 21 million internet users, based on the population of 52 million people in 2013 (Statistics South Africa, 2014). This means that in 2013, there were 21 million users who could have fallen prey to cyber-attacks and cyber breaches, and this number is increasing rapidly based on the predictions made by the WEF in 2016.

The global marine community managed to stay out of sight of computer hackers for decades until about five years ago when the number of cyber intrusion incidents reportedly increased (Hubmann, Polke-Markmann and Vanheyden, 2018). There is evidence that organisations are increasingly acknowledging incidents of cyber intrusions, as well as loss of computer devices whilst in the care of employees either outside and/or during working hours (Mitchley, 2017; Msimanga, 2017).

1.4 Objectives of the paper

With the realisation of the disruptive nature of cyber intrusions and their increase in the maritime industry. It was deemed important by the researchers to conduct a study to investigate the status of maritime transportation in South Africa with regards to cybersecurity measures, policies, strategies etc. and understand if any are in place and/or successfully implemented to prevent cyber-attacks, by South African organisations. The purpose of this paper is to provide feedback on what the study has found so far, and further give the status of the country in relation to the readiness to combat cybersecurity issues.

2. METHODOLODY

The research process in this study was divided into two phases, with phase one focusing on scientific process of identifying relevant content. To achieve the objectives of the study, a qualitative content analysis method was followed. To make sure that the content to be studied was scientific and relevant to the study, a Systematic Literature Review (SLR) was applied, where reputable databases and search engines were used. The second phase involved direct content search from government databases and international organisations for work published by relevant structures, this was used to find content relevant to cybersecurity as well as those relevant to maritime cybersecurity.

2.1 Content selection

For the SLR in this study, two databases and one search engine were used as listed in Table 1 and a number of publications were selected for further review.

The keywords used to search the database were simple, (maritime cybersecurity), but the results thereof were impressive as per Table 1 below.

Table 1: Content selection from databases and search engines

Database & Search engine	Year sort (2010 to current)	Downloaded (granted access)	Excluded	Reviewed
ScienceDirect	368	76	58	11
Scopus	189	24	14	6
Google Scholar	753	213	132	6
Total	**1 310**	**227** (- 86 Dup)	**204**	**23**

From the government databases the relevant documents are as listed in Table 2 below:

Table 2: Government and organisational documents

Document	Citation
ISO Standard 27001 (Information Security)	(ISO, 2005)
Cybercrimes	(National Assembly (RSA), 2017)
South African National Cybersecurity Policy Framework	(State Security Agency (RSA), 2015)
Electronic Communications and Transactions Act 25 of 2002	(National Assembly (RSA), 2011)
Notice of Intention to Make South African National Cybersecurity Policy	(Department of Communications (RSA), 2010)
Implementation Guideline for ISO/IEC 27001:2013	(ISACA, 2016)
South African Maritime Safety Authority Notice No. 18 of 2017	(SAMSA, 2017b)
Maritime Transport in the Context of the Maritime Sector in South Africa	(Deacon, 2006)

2.2 Exclusion criteria

To select the relevant articles to be included in the review an article was considered relevant if it complied with the following:

- It was published in 2010 or later and consisted of primary research
- It included “maritime cybersecurity” or “Cybersecurity in shipping” or “Transportation cybersecurity, that included maritime”. All these articles were further reviewed for relevance.

To exclude irrelevant articles, a further review was conducted, were articles that discussed physical marine security and warfare were excluded. Also, articles that focused on maritime security but not necessarily cyber security were excluded. Lastly articles that were not peer reviewed or published in an academic process were excluded and only peer reviewed articles that had five or more citations were included.

3. RESULTS

The results of this study will be presented as per data collection phases, starting with phase 1 were a systematic literature review process was followed and phase two were relevant organisational and government databases were searched for valuable content.

3.1 Phase 1 (Systematic literature review)

The search and selection processes were successful with 1 310 articles found, out of that only 313 were downloaded as per access to publication privileges. From the 313 downloaded, about 86 were duplicates and 204 were excluded via the exclusion process. After the completion of all the processes only 23 articles (see Table 3) were left as part of the review. During the review the articles where grouped according the similarities or their discussions in the studies. The groupings were numbered zero (0) to three (3), group (0) recorded articles that were found to not really discuss issues that are related to cybersecurity in the maritime industry, the assumptions are that they slipped through the cracks during the exclusion criteria, because their introduction and abstract gave an impression that they were going to discuss relevant topics. From this, five articles were found and therefore not included in the citation table (Table 3) even though the articles where reviewed.

Table 3: Selected articles for final review

	Discussion Topic	Selected Articles
0	Not relevant for this study (5)	five studies reviewed and excluded from citations
1	Collaboration and Information Sharing (4)	(Settanni *et al.*, 2017); (Ilves *et al.*, 2016); (Fitton, Oliver D.Prince, B Germound, 2015); (Hathaway *et al.*, 2012).
2	Risk assessment of maritime technologies (12)	(Hoyhtya *et al.*, 2017); (Polemi and Papastergiou, 2016); (Polatidis, Pavlidis and Mouratidis, 2018); (Kostopoulos, 2018); (Caponi, Steven L; Belmont, 2018); (Wiseman, 2014); (You, Zhang and Cheng, 2018); (Murphy, 2010); (Direnzo, Goward and Roberts, 2016); (Jones, Tam and Papadaki, 2016); (Johnson, 2016); (Peterman, Elias and Frittelli, 2013).
3	Cybersecurity Readiness (2)	(Peter, 2017); (Kramek, 2013)

What is of interest and encouraging is that most of the studies reviewed, twelve (12) to be exact, focused their discussions on maritime technology and risk assessments. Which could be interpreted that most researchers are realising the importance of assessing cyber risks in the maritime industry. A brief description of all the groupings is discussed in the following paragraphs.

3.1.1 Collaboration and information sharing (4)

After the countries in Europe experienced cyber threats, they decided to make use of the European Union (EU) and North Atlantic Treaty Organisation (NATO) to coordinate and collaborate cybersecurity strategies that are based on similar policies and standards, for a stronger European cyber defence. Since then other researcher have encouraging the use of collaborative technological tools, for improving cyber defences. These researchers believed that collaborating and sharing of cyber related information could assist the parties in identifying new and more modern cyber-attacks. Some researcher went as far as suggesting that during law making and policy formulation, organisations should consider the laws and policies of all organisations in the collaboration group. Formulating similar laws and policies, will make the fight against cybercrimes global and easily dealt with, as the operating laws will be similar. The value derived from these studies, also include, the provision of the attributes that form maritime cyber operations framework, those, being: Information, Technology and People.

3.1.2 Risk assessment of maritime technologies (12)

The studies in this group, discussed more similar and related issues and only the ones that were deemed important to this study will be discussed. These studies acknowledge the complexity of technology used in maritime industry. To name but few, the studies identified technology that the modern maritime operations depend on: **a)** Electronic Chart Display and Information System (ECDIS); **b)** Automatic Identification System (AIS); **c)** Radio Direction and Ranging (Radar); **d)** Compass; **e)** Computerised Automatic Steering Systems; and **f)** Global Maritime Distress and Safety System (GMDSS). The researchers also acknowledged that all these systems require human machine interaction for them to operate optimally, and all are susceptible to cyber-attacks.

With all the complexity of the maritime technologies and their vulnerabilities to cyber-attacks, which poses a challenge for any maritime operations. Because of the challenges it is advisable that the three layers of a cyber defence system be used, being, risk assessment; risk evaluation and risk mitigation. With human machine interaction, the users of these technologies should also form part of the risk assessments. The value that these studies added to our study is that they support the notion that maritime operations are now dependent on cyber systems, that are used for navigation; communication; cargo handling etc. and cybersecurity vulnerability assessment should be conducted.

3.1.3 Cybersecurity readiness (2)

Cybersecurity readiness can be managed under organisational governance, with governance defined as "*the process of establishing chains of accountability, authority and communication, indicating clearly the measurement, policies, standards and control mechanisms to enable entities to perform their roles and responsibilities"* (Mueller *et al.*, 2008). For this study, will focus on the readiness of government and organisations by looking at the establishment of Responsible, Accountable, Consulted and Informed (RACI) model, as used by other countries (Department of Communications (RSA), 2009; Kral, 2019).

After the September 11 attacks in the United States of America (USA), the USA government decided to increase their security measures including cybersecurity in their maritime ports. This was motivated by the USA, understanding that most of the authorities that are landlords of the maritime ports don't always know what networked systems are being used and the kind of cybersecurity measures that are being taken (Kramek, 2013). This study raised a very important aspect about maritime ports landlords and them not always knowledgeable of systems and technologies being used by those renting the space in the ports.

In an African perspective a study was conducted to find out which African countries have managed to put structures in place to ready themselves for cyber related attacks (Peter, 2017). This study went as far as rating and ranking the countries for their readiness by making use of the following attributes: **a)** legislation, regulations, policies and how the cybersecurity strategy is communicated; **b)** Collaborations, cooperation and partnerships; **c)** Technical measures (e.g. CERT/CSIRT[1]); **d)** Information sharing mechanisms; **d)** Capacity building (e.g. training programs). Based on these attributes South Africa rated number 1 in terms of a grouping of "Networked readiness" (investment in ICT infrastructure and Telecommunications), and number 2, just behind Egypt in terms of Growth Domestic Products (GDP) (the contribution of ICT to GDP). This could be interpreted that South African have invested enough on the growth of ICT infrastructure and that is also visible in the contribution it makes in GDP.

<u>3.2 Phase 2 (Organisational and government databases)</u>

In 1998, the South African government established under Act 5 of 1998, a maritime safety authority, namely South African Maritime Authority (SAMSA). SAMSA's objectives are to "*provide safe, reliable, effective, efficient, and fully integrated transport operations and infrastructure which will best meet the needs of freight and passenger customers at improving levels of service and cost in a fashion which supports government strategies for economic and social development whilst being environmentally and economically sustainable*" (SAMSA, 2017a). Transnet on the other hand, a State-Owned Company is a

[1] Computer Emergency Response Team (CERT) and Cyber Incident Response Team

public entity that is solely owned by the South African government, with an objective to both operate and control the major transport infrastructures. Transnet is also responsible for ensuring that the country's transport industries operate according to world-class standards and that they form an integral part of the overall economy (Transnet, 2018).

Worldwide organisations have grown to have faith and trust in various standardisation organisations and the "*International Organization for Standardization*" (ISO) and the "*International Electrotechnical Commission*" (IEC) are amongst the reputable and respected organisations. The ISO/IEC formed a specialised system for standardising a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) (ISO, 2005). This standard (ISO/IEC 27001), can be adopted by any organisation and customized to align with strategic objectives. This standard follows the simple process of PDCS (Plan-Do-Check-Act), which is applied to all processes.

For organisations to be able to ready themselves for cybersecurity issues, it is advisable to have an ISMS, which is a comprehensive set of policies and processes that an organization creates and maintains to manage risk to information assets. In 2013, the Information Systems Audit and Control Association (ISACA), developed a guideline for offering practical support and strategies for anyone interested and/or responsible for setting up and/or operating an ISMS (ISACA, 2016). ISACA is recognised as the leader in the information systems environment, with about 140 000 members in more than 180 countries, who work in the Information Technology (IT) space.

The South African government in 2001, was challenged by the United Nations General Assembly Resolution 56/183 to put their house in order when it comes to Cybersecurity issues and they relied on the ISO/IEC standards (Department of Communications (RSA), 2010). The Figure 1 shows the progress of South Africa since 2001 in terms of the implementation of regulatory support for cybersecurity and Table 4 shows the structures that were created and their roles, since then.

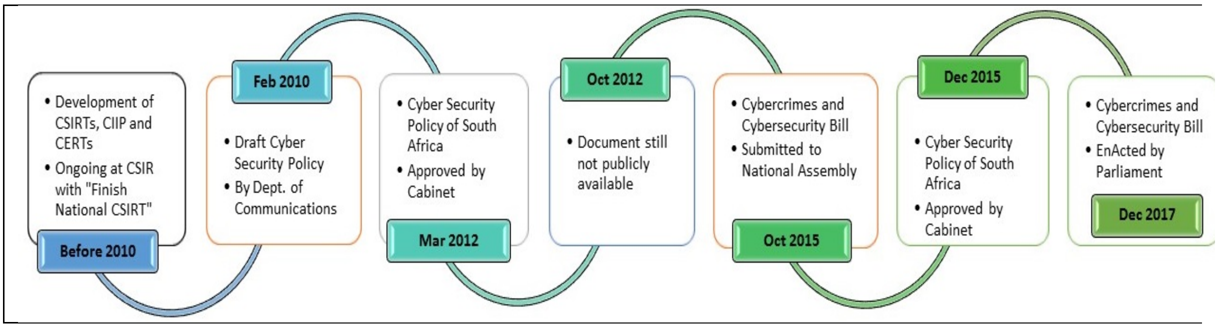
• Development of CSIRTs, CIIP and CERTs
• Ongoing at CSIR with "Finish National CSIRT"
Before 2010
Feb 2010
• Draft Cyber Security Policy
• By Dept. of Communications
• Cyber Security Policy of South Africa
• Approved by Cabinet
Mar 2012
Oct 2012
• Document still not publicly available
• Cybercrimes and Cybersecurity Bill
• Submitted to National Assembly
Oct 2015
Dec 2015
• Cyber Security Policy of South Africa
• Approved by Cabinet
• Cybercrimes and Cybersecurity Bill
• EnActed by Parliament
Dec 2017

Figure 1: Cybersecurity regulatory progress in South Africa

The ISO/IEC 27001 standard is not limited to a specific organisation or government and therefore covers any entity including commercial enterprises, government agencies and non-profit organisations. In order to achieve the objectives or recommendations from the standard South Africa implemented a Cybersecurity Response Committee, as enacted in the Cybercrimes and Cybersecurity Bill (Republic of South Africa, 2016) and listed as follows. The cyber response committee is lead by the Director General of State Security Agency, with the objective of implementing the government policy and act as a driving body of other structures and further included are all government departments and agencies represented.

Table 4: South African structures to deal with cybersecurity

Structure name	Responsible body	Role to play
Cybersecurity Centre	State Security Agency	• Cybersecurity impact and national security. • Effectively deal with Critical Information Infrastructure Protection (CIIP).
Government Security Incident Response Teams (GSIRT)	State Security Agency	• Develop and implement measures to deal with cybersecurity matters affecting national intelligence and national security. • Provide proactive and reactive incident management
National Cybercrime Centre	The cabinet member of Policing	• Cybersecurity law enforcement • Detect, prevent and investigate cybercrimes
Cyber Command Centre	The cabinet member of Defence	• Cybersecurity national defence • Establish a cyber offensive and defensive capacity for the South African National Defence Force
Cybersecurity Hub	Department of Telecommunications and Postal Services	• Coordinate general cyber security activities in the private sector • Cybersecurity awareness campaigns • Provide cybersecurity expertise to government and private sector
Private Sector Security Incident Response Teams (PSSIRT)	Department of Telecommunications and Postal Services	• Establish Private Sector Security Incident Response Teams • Provide a contact point for specific sector on cyber security matters • Establish minimum standards for the specific sector.

These structures have the main aim of promoting a cybersecurity culture and encourage compliance with minimum cybersecurity standards, and further centralise the coordination of cybersecurity activities. By putting relevant structures in place, as supported, initiated and lead by government, the South African government has done a great job and its now mainly in the hands of implementors to facilities and make use of these initiatives.

4. CONCLUSIONS

This study was divided into two phases, with phase 1 making use of an SLR to understand the discussions of other researchers with regards to cybersecurity in the maritime industry and phase 2 making use of content available in government databases, with the main aim of understand the readiness of the South African government with regards to cybersecurity issues. The SLR helped us understand that other researchers are in agreement that, the complexity of technologies used in the maritime industry requires that risk assessments be conducted and that regulations, standards and policies should be consistent worldwide, which fosters organisations to form collaborative efforts to deal with cybersecurity matters.

Government documents helped us understand that in South Africa there are two major players mandated to look after our maritime infrastructure from the government point of view and these are Transnet and South African Maritime Safety Authority (SAMSA). On SAMSA’s Strategic Programme 3, their maritime operations programs, is stated as aiming to ensure observance of safe marine practices including but not limited to Maritime security. Maritime security is “*the prevention of damage and disturbance to the South African and global maritime supply chain network, trade security, elimination of sabotage in the sea environment, acts of piracy, illegal exploitation of South African sea-based resources, vessel security, etc*” (SAMSA, 2017a). Which can only be achieved in collaboration with other security structures. This places SAMSA as a good stakeholder to collaborate with in order to investigate the readiness of South African based organisations in relation to cybersecurity.

On the other hand, Transnet has five operational division and only two were found to be relevant for this study. Namely; the Transnet National Ports Authority (TNPA), which is responsible for the safe, effective and efficient economic functioning of the national port system, which it manages in a capacity of a landlord; and Transnet Port Terminals (TPT), which plays a key role in supporting the South African government's export-led growth strategy. Most Southern African import and export commodities are handled through South Africa's ports, which makes the work of TPT to expand to other countries. With TNPA managing the ports and TPT on the terminal's operations, Transnet becomes a good stakeholder as well, for the maritime cybersecurity study. Customers, that are catered for in the ports include but not limited to the shipping industry, vehicle manufacturers, agriculture, timber and forestry products, the mining industry and exporters of minerals, metals and granite. All this customer's one way or the other interact with ICT systems, which are vulnerable to cyber-attacks.

From all the information provided in this study, we can conclude that South Africa is ready to combat cyber related attacks and crimes. The cybersecurity structures that government has put in place are in line with international standards, based on the studies from regions like the USA and Europe.

5. RECOMMENDATIONS

What is not clear from the studies and documents reviewed is how organisations are making use of all the structures that the South African government has put in place. What is also lacking is relevant studies that indicate a good understanding of the contribution or lack thereof, of users of maritime technologies and/or employees that work for these relevant structures identified. For these reasons, this study recommends that a further readiness study be conducted aiming at evaluating users of maritime technologies and employees of organisations involved with maritime operations, to understand their readiness of cybersecurity.

6. REFERENCES

Baller, S, Dutta, S and Lanvin, B, 2016. 'The global information technology report 2016', in *World Economic Forum, Geneva*, pp. 1-307.

Caponi, SL and Belmont, KB, 2018. 'Maritime Cybersecurity: A Growing Threat Goes Unanswered', *Socio-Economic Review*, 16(3), pp. 637-655. doi: 10.1093/ser/mwy024.

Clemente, D, 2013. *Cyber security and global interdependence: what is critical?* Chatham House, Royal Institute of International Affairs.

Deacon, H, 2006. 'Maritime Transport in the Context of the Maritime Sector in South Africa', (July), pp. 169-174.

Department of Communications (RSA), 2009. 'CYBERSECURITY POLICY OF SOUTH AFRICA August 2009', (August).

Department of Communications (RSA), 2010. *Notice of intention to make South African National cybersecurity policy*, *Government Gazette No. 32963*.

Direnzo, J, Goward, DA and Roberts, FS, 2016. ‘The little-known challenge of maritime cyber security’, *IISA 2015 - 6th International Conference on Information, Intelligence, Systems and Applications*. doi: 10.1109/IISA.2015.7388071.

File, T and Ryan, C, 2014. ‘Computer and Internet use in the United States: 2013’, *American Community Survey Reports*, 28, pp. 1-16.

Fitton, OD, Prince, B and Germound, ML, 2015. ‘The Future of Maritime Cyber Security’, p. 32.

Hathaway, OA *et al.,* 2012. ‘The law of cyber-attack’, *California Law Review*, 100(4), pp. 817-885. doi: 10.15779/Z38CR6N.

Hoffmann Jan, SSJW, 2017. *Review of Maritime Transport 2017*.

Hoyhtya, M *et al.,* 2017. ‘Connectivity for autonomous ships: Architecture, use cases, and research challenges’, *International Conference on Information and Communication Technology Convergence: ICT Convergence Technologies Leading the Fourth Industrial Revolution, ICTC 2017*, 2017–Decem, pp. 345-350. doi: 10.1109/ICTC.2017.8191000.

Hubmann, C, Polke-Markmann, H and Vanheyden, P, 2018. ‘Allianz Risk Barometer’.

Ilves, LK *et al.,* 2016. ‘Institute for National Strategic Security , National Defense University European Union and NATO Global Cybersecurity Challenges : A Way Forward Source : PRISM , Vol . 6 , No . 2 (2016), pp . 126-141 Published by : Institute for National Strategic Securi’, 6(2), pp. 126-141.

ISACA, 2016. ‘Implementation Guideline ISO/IEC 27001:2013’, *Isaca*, p. 64.

ISO, 2005. *ISO/IEC 27001:2005*.

Jensen, L, 2015. ‘Challenges in Maritime Cyber-Resilience’, *Technology Innovation Management Review*, 5(4), p. 35.

Johnson, C, 2016. ‘Why We Cannot (Yet) Ensure the Cyber-Security of Safety-Critical Systems’, pp. 1-13.

Jones, KD, Tam, K and Papadaki, M, 2016. ‘Threats and Impacts in Maritime Cyber Security’, *Engineering & Technology Reference*, pp. 1-12.
doi: 10.1049/etr.2015.0123.Published.

Jones, S and Fox, S, 2009. ‘Generations Online’, *Generations online in 2009. Washington DC: Pew Internet & American Life Project*.

Kostopoulos, G, 2018. *Cyberspace and Cybersecurity*, *Taylor & Francis Group*.

Kral, P, 2019. ‘Information Security Reading Room Incident Handler’s Handbook’.

Kramek, J, 2013. ‘The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabiliies’, (July).

Mitchley, A, 2017. ‘Centurion Licensing Centre robbed of computers, camera equipment’, *News24*.

Moller, A, 2017. *Cyber attack*. Available at: http://investor.maersk.com/releasedetail.cfm?ReleaseID=1031559 (Accessed: 23 July 2018).

Msimanga, S, 2017. ‘String of break-ins at Tshwane Licensing centres’, *Times Live*.

Mueller, L *et al.,* 2008. ‘IBM IT Governance Approach: Business Performance through IT Execution’, *International Technical Support Organisation*, pp. 1-132.

Murphy, T, 2010. ‘Security Challenges in the 21 st Century Global Commons’, *Yale Journal of International Affairs*, (Spring/Summer), pp. 28-43.

National Assembly (RSA), 2011. ‘Electronic Communication and Transaction Act 25 of 2002’, 2005(28619), pp. 1-176.

National Assembly (RSA), 2017. *Cybercrimes Bill*.

Palmer, D, 2017. *Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk | ZDNet*. Available at: https://www.zdnet.com/article/petya-ransomware-cyber-attack-costs-could-hit-300m-for-shipping-giant-maersk/ (Accessed: 23 July 2018).

Peter, AS, 2017. ‘Cyber resilience preparedness of Africa’s top-12 emerging economies’, *International Journal of Critical Infrastructure Protection*. Elsevier B.V., 17, pp. 49-59. doi: 10.1016/j.ijcip.2017.03.002.

Peterman, DR, Elias, B and Frittelli, J, 2013. ‘Transportation Security : Issues for the 113 th Congress’.

Polatidis, N, Pavlidis, M and Mouratidis, H, 2018. ‘Cyber-attack path discovery in a dynamic supply chain maritime risk management system’, *Computer Standards and Interfaces*. Elsevier B.V., 56(July 2017), pp. 74-82. doi: 10.1016/j.csi.2017.09.006.

Polemi, N and Papastergiou, S, 2016. ‘Current efforts in ports and supply chains risk assessment’, *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*. Infonomics Society, pp. 349-354. doi: 10.1109/ICITST.2015.7412119.

Republic of South Africa, 2016. ‘Cybercrimes and Cybersecurity Bill’, (27031).

SAMSA, 2017a. ‘Maritime Safety for a Sustainable Future’, *SAMSA Annual Report*, 91, pp. 399-404.

SAMSA, 2017b. ‘South African Maritime Safety Authority Marine Notice No 18 of 2017’, Marine Not (September), pp. 1-5.

Settanni, G *et al.,* 2017. ‘A collaborative cyber incident management system for European interconnected critical infrastructures’, *Journal of Information Security and Applications*. Elsevier Ltd, 34, pp. 166-182. doi: 10.1016/j.jisa.2016.05.005.

Siebels, D, no date. ‘Privatisation of maritime security: Implications for governments, navies and other security agencies’.

Von Solms, R and Van Niekerk, J, 2013. ‘From information security to cyber security’, *Computers and Security*. Elsevier Ltd, 38, pp. 97-102. doi: 10.1016/j.cose.2013.04.004.

State Security Agency (RSA), 2015. *South African National Cybersecurity Framework*.

STATS-SA, 2014. *General Household Survey 2013*.

Toth, PR and Paulsen, C, 2016. *Small Business Information Security: The Fundamentals*.

Transnet, 2018. ‘Integrated Report 2018’.

WEF, 2016. *Global Agenda Council on Cybersecurity*, *Whitepaper*.

Wiseman, Y, 2014. ‘Protecting Seaport Communication System by Steganography Based Procedures’, *International Journal of Security and Its Applications*, 8(4), pp. 25-36. doi: 10.14257/ijsia.2014.8.4.03.

You, B, Zhang, Y and Cheng, L, 2018. ‘Review on Cybersecurity Risk Assessment and Evaluation and Their Approaches Review on Cybersecurity Risk Assessment and Evaluation and Their Approaches on Maritime Transportation’, *University of Houston*, (October).