CyberShip Project Cyber resilience for the shipping industry - Final Project Report

Sepúlveda Estay, Daniel Alberto

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

CyberShip Project: Cyber resilience for the shipping industry – Final Project Report

Daniel Sepúlveda Estay[1]

[1]*Department of Technology, Management and Economics, Technical University of Denmark*

June 30, 2020

Abstract

This report describes the final state of the research performed as a part of the CyberShip project. In particular it details the results of its Work Package #5, this is, the application of methods and measures identified in work packages 3 and 4 to case studies. This report therefore closes the research process that was scoped for the project.

Additionally, this project report updates the information presented in previous Work Package reports, updating the performance measures and Cybership model (Work Package #2), the methods and measures for the prevention of cyber-attacks in shipping (Work Package #3), and the methods and measures for the reaction to cyber-attacks in shipping (Work Package #4). These are presented in the Appendix.

All the publications associated with this project are available at the DTU Orbit web page for the CyberShip project. [1]

[1]https://orbit.dtu.dk/en/projects/cyber-resilience-for-the-shipping-industry-cybership

Contents

Nomenclature

BFT++ Byzantine Fault Tolerant++, page 25

BIMCO Baltic and International Maritime Council, page 9

CPS Cyber Physical Systems, page 35

CRF Cyber Resilience Frameworks, page 11

DMF Danish Maritime Find, page 7

HBR Human Behavior Resilience, page 25

HIL Hardware-in-the-loop, page 25

ICT Information and Communication Technologies, page 7

IMO International Maritime Organization, page 5

ISM International Safety Management Code, page 5

ISPS International Ship and Port Facility Security Code, page 5

KPI Key Performance Indicator, page 7

NIST National Institute of Standards, page 26

NRL Naval Research Laboratory, page 25

PRISMA Preferred Reporting Items for Systematic Reviews and Meta-Analyses, page 87

SCCRM Supply Chain Cyber Risk Management, page 75

SDN Software-Defined Network, page 72

SLR Structure Literature Review, page 72

SLR Structured Literature Review, page 11

STAMP Systems Theoretic Accident Model and Process, page 32

STPA Systems Theoretic Process Approach, page 32

WP Work Package, page 7

Acknowledgements

This work is profoundly grateful to the multiple persons that have contributed to its advancement.

A number of different MSc. students took part in developing parts of this study. The wave analogy model was first proposed by Pablo Guerra (detailed in Appendix A), who also later participated as advisor for the special course that tested this framework, as shown in Case Study 2 of this report. Sotiria Lagouvardou developed the first models that used SDN for testing a simple control network in a ship, as shown in Appendix B. Bartlomiej Hyra developed the risk analysis of a CyberShip through the use of Asset Based Risk methods as shown in the Study 5 of this report. James Osborn developed the comparison of the wave analogy framework with other cyber resilience frameworks, as shown in the Study 2 of this report.

The Advisory Committee continuously has provided advice particularly to include the focus of industrial relevance. Their comments and suggestions have been crucial to the development of the project.

Finally, the Cyber Ship project team was a crucial group to direct and define how this project was developed. Both Professors Harilaos Psaraftis and Christian D. Jensen continuously provided helpful advice to the project. Particular thanks to Rishikesh Sahay, who has collaborated intensely both as postdoc at CyberShip and later as he continued with his career in industry. Finally, the project leadership of Professor Michael B. Barfod has been fundamental, and one of clear support, guidance and advice.

-

Daniel A. Sepulveda Estay
Postdoc.

1 Introduction

1.1 Virtues and problems of Cyber-ships

International entities such as the International Maritime Organization (IMO) have had maritime security and safety as one of their the main objectives, reflected through different norms and measures that have been issued, such as The International Safety Management Code (ISM) and International Ship and Port Facility Security Code (ISPS). These aim to ensure safety in the operation of ships and harbours, and the working environment including personnel on board vessels and on shore.

These codes focus on risk identification, accident prevention and emergency situations in order to help shipping operations to prevent hazardous situations with significant consequences such as loss of life at sea or environmental disaster. However, the prevalence and increasing use of ICT in shipping operations reveals that security concerns in this industry are not limited to the physical sources of potential crises. Historically, the physical isolation of a ship once it left the port validated the assumption that any potential risks would only be a matter of human error or mechanical failure.

ICT has changed this paradigm. With the introduction of interconnected infrastructure that enables communication with onshore facilities, the shipping industry entered a new, increasingly promising, but also highly risky digital era. Digitalization has transformed the shipping industry by including digital information collected throughout the physical voyage in the decision making process.

Higher IT automation and integration with cyber-technologies in shipping also is resulting in new risks. Advanced shipping systems are not secure in the same way as traditional shipping operations were, since cyber risks differ from traditional risks in at least 7 dimensions, as indicated in Table 1 (based on [Sepúlveda Estay, 2017a]):

It is therefore becoming increasingly clear that the abilities to avoid and detect cyber-attacks (cyber-security) and to react efficiently once cyber-attacks have been detected (cyber-resilience) have become critical for the success of smart shipping operations. IoT enabled cyber-physical systems are regularly threatened by a broad range of potential cyber-attacks coming from criminals, terrorists or hacktivists [He et al., 2016]. Cyber-attackers use any available channel to exploit poorly-secured systems for different purposes, giving way to threats like harassment, corporate espionage, extortion, stock market manipulation, or the planning and carrying out of terrorist activities. In parallel, there is the risk that failing to ensure continuous IT systems may also cause disruptions in operations [Järveläinen, 2013], and consequent challenges for mission assurance of the enterprise [Bodeau et al., 2010]. Rand has estimated that the global cost of cyber-crime can range from US$799 billion to over US$2 trillion[Dreyer et al., 2018] and, as recent examples like the Wannacry and Petya viruses have shown, effects include not only disruption of industrial operations, but also lives put at risk.

The modern shipping industry thus faces cyber-risks associated with their own data and control systems, and also to their supply chains [He et al., 2016], as processes connected both with suppliers and customers through the internet form part of a shared network. As a result, cyber-attackers access and impact actors sharing a common network and gaining access to IT systems through the weakest link in the supply network [He et al., 2016], [Khan and Sepulveda Estay, 2015].

Considering their effects and the urgency of a problem that is continuing to unfold, it is sensible to ask how should risks derived from the use of IT systems be managed in shipping operations to increase detection and reaction to cyber-attacks.

ICT has been adopted in many operational systems in ships, allowing for greater sensing

Figure 1: Dimensions where traditional and cyber-risks differ for shipping operations[Sepúlveda Estay, 2017a]

Dimensions / Risk Types	Dimension Description	Non Cyber-risks	Cyber-risks
Latency	Delay between when the attacker accesses the ship and when the effects of the attack start	Low to medium	High latency, extending to years between penetration and action of the cyber-attack.
Physical location	Place where the attacks happen in the ship and shipping network	Localized. Geography is relevant.	Affects multiple connected locations. Geography is less relevant
Complexity	Operation units where the attack can have consequences, and the number of ways in which the attack takes place.	Limited complexity	Virtually unlimited complexity. Can affect many shipping systems simultaneously
Replication	Possibility and accuracy in which the attack can be repeated in the same location or elsewhere	No replication to highly imperfect replication	Perfect replication
Perpetuity	The amount of time during which the attack continue to take place	Limited duration.	Continuous effect until counter-acted or self-ending
Component versus interaction	Unit of attack, ranging from an attack to units in the system, to an attack happening to the communication between connected units	Shipping component risks	Interaction risks - Component communication risks
Anonymity	The identification of the source of the attacks	Traceable perpetrator	Anonymous perpetrator unless explicit hacker declaration.

and analysis of operational data that results in better operation and remote, networked control. This connectivity has also led, however, to a greater vulnerability in these systems resulting in higher degrees of uncertainty due to the lack of understanding of the exposure of shipping operations to cyber-risks.

This opens the opportunity for researchers to focus on the security properties in the shipping industry to understand, for example, how security breaches within ship's technologies will result in a variety of harmful impacts on ship operation and its crew members. This hopefully can highlight requirements for system design that will prevent cyber attacks or help cyber-ships react better to cyber-attacks once these are taking place.

According to the BIMCO survey as presented in the Figure 2, respondents suggest that most vulnerable systems are Positioning system, ECDIS (Electronic Chart Display and Information System), and Engine control, and monitoring. This maritime cyber security survey on 22 July 2016. As indicated by The survey, which ran for four weeks, was promoted on social media and via email. More than 300 industry players responded. Of the 300 respondents, 65 had been a victim of a cyber attack.

This information is a reflection of the need for improved knowledge about the shipping systems and their vulnerability to cyber-attacks, and this project is a contribution towards obtaining improved insights for better decision making.

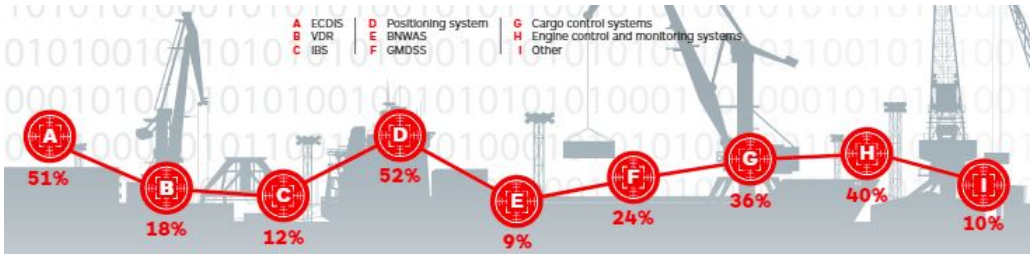

Figure 2: Ship borne systems are most vulnerable to cyber attacks ["IHS Fairplay", 2016]

1.2 The CyberShip Project

The CyberShip project, "Cyber resilience for the shipping industry", is a project financed by the Danish Maritime Fund (DMF) and Orients Fund, for 33 months from September 2017 to June 2020, and it is aimed at proposing a theoretical framework to aid the decision making process for preventing and reacting to cyber-attacks in the shipping industry. The unit of analysis is a CyberShip operation system, this is, a ship composed of elements connected through Information and Communication Technologies (ICT), including humans interacting with the ICT, the connections existing between these elements and the policies regarding how these connections result in a decisions.

This project is divided into six work packages that are developed sequentially. These work packages are:

- Work Package 1 (WP1): The first WP has the objective of achieving an adequate management of the CyberShip project, by coordinating technical activities and assuring quality of results through activities such as the production of regular status reports, and the creation the Advisory Committee.

- Work Package 2 (WP2): The second work package of the CyberShip project has two main objectives. First, it defined a generic cyber ship model through the identification of all systems, cyber components, and their communication requirements in a modern commercial ship. The resulting model defined what is understood as the "attack surface" of the ship. As such, a ship is seen as a system composed of several sub-systems that have individual and independent characteristics. Such a CyberShip model thus consist of all systems and cyber components in a ship, their capabilities for computation and interaction with the environment, and the interactions between components in a modern ship. Second, WP2 defined a set of Key Performance Indicators (KPIs) to measure the degree of cyber resilience performance of any ship system under investigation. These KPIs are qualitative and quantitative measures of the ship system's resilience towards cyber attacks. These indicators come from areas such as risk of cyber attacks, degree of resource redundancy, response and recovery times, and implementation costs.The results for WP#2 were presented in a report in April 2018, and this final report adds to the information presented with further research results. This can be seen in Appendix E.

- Work Package 3 (WP3): The third WP has the objective of defining cyber attack prevention measures and tools at a strategic (design) level. The proposal of these measures is developed from an analysis of the CyberShip structure and the relationships that exist between these structures, particularly related to the way in which these relationships can lead to disruptions in the expected operation of the system. These results were presented in the CyberShip report for WP3 and WP4 [Sahay and Sepúlveda Estay, 2018b], and a summary of the results for this part of the project are contained in Appendix A.

- Work Package 4 (WP4): The fourth WP has the objective of defining cyber attack response and recovery measures and tools if and once the cyber attack occurs. The proposal of these measures is developed from an analysis of a simplified CyberShip structure and the use of Software-defined networking to detect cyber attacks and trigger appropriate procedures when an attack is likely. These results were presented in the CyberShip report for WP3 and WP4 [Sahay and Sepúlveda Estay, 2018b], and a summary of the results for this part of the project are contained in Appendix B.
- Work Package 5 (WP5): Evaluation and application to specific case studies, to define and evaluate the case studies, and to propose recommendations for the shipping industry and regulators. This is the content of this report.
- Work Package 6 (WP6): The sixth WP has the objective of disseminating the project and its results and of linking colleagues and stakeholders with the project, its findings and its proposals. The dissemination that has resulted so far from this work, includes 11 publications and 19 presentations of this project, detail that is presented in Appendix F.

2 Related work

The research into ship security is still in its early stage and much work focus on identifying potential threats and vulnerabilities [IMO, 2017a, BIMCO, 2017, Deloitte, 2017].

These reports highlight the risks that result from the use of ICT to critical systems in ships. In particular, BIMCO guidelines draw special attention to the different types of cyber attacks affecting the ships and exploiting the vulnerabilities in the critical components [BIMCO, 2017].

These reports are fundamentally management guidelines on how to approach cybersecurity in the context of shipping, and as such can be used as an input for traditional the cyber risk assessments. An example of the assessment of these vulnerabilities is the examination of the importance of critical infrastructure on shipboard systems, as can be found in [Bensing, 2009].

Moreover, these guidelines have established threats and vulnerabilities with the aim of developing countermeasures to protect the system. However, to the best of our knowledge, there are very few works dealing with the protection of the communication infrastructure of ships to cyber attacks. Some of these proposals are mentioned next.

Babineau [Babineau et al., 2012] proposed the periodical diversion of communication traffic between different switches in a network to protect the critical components of the ship from cyber attacks. This proposal relies on the redundancy of the design of the ship's communication network to divert the traffic through different paths while forwarding it to the destination. ABB a leading company in industrial automation proposed to place the critical components of the ship in the core of the network that typically requires firewalls to enter from outside [ABB, 2014].

Yunfei [Yunfei et al., 2015] and Chen [Yuanbao et al., 2015] have proposed architectural solutions to protect the warship system from cyber attacks. Their mechanisms rely on statically deployed access controls, firewall and intrusion detection system (IDS) in the network to mitigate the attacks.

Penera [Penera and Chasaki, 2015] identifies the packet scheduling attack on the shipboard network controlled system for mitigation. However, it fails to explain how switches can be configured in an automated way to mitigate the attacks dynamically.

The project CyberShip aims at proposing a framework to mitigate the attacks in an automated way to improve the resilience of the ship control system. A requirement is therefore the need for a comprehensive literature review to gather information about frameworks for cyber resilience that have been published in the scientific literature, included in this report as Study 1.

3 Case studies - Work Package 5 results

This section presents the results of the application of the methods mentioned in Work package #3 and #4 and the results of a comprehensive Literature Review about published Cyber Resilience Frameworks. The methods were first presented in the Report for Work Package #3 and Work Package #4 in 2018, and updates have been made to these reports. These updates are presented in the Appendix A section 8 and Appendix B section 9 of this report. Additionally, a review of existing cyber resilience frameworks applicable to cyber attacks, and their applicability to shipping were also explored.

The following studies are shared in this section of the report:

1. The literature review of existing cyber resilience frameworks applicable to cyber attacks in ships. This work as been reflected as a research paper, and it has been submitted to a scientific journal.

2. The evaluation of the Wave Analogy Model for cyber resilience with respect to other selected cyber resilience frameworks. This work has been reflected as a research paper submitted to scientific conference.

3. The application of the Wave Analogy Model to Cyber attacks in shipping. This work has been reflected as a research paper published as book chapter.

4. The Application of the Systemic Risk Analysis Framework to a Ship System Research Published as book chapter.

5. The comparison of the Systemic Risk Analysis Framework with other industrial standards.

3.1 Study 1 - Existing Cyber-resilience frameworks

Note: This subsection presents work that is reflected as a journal paper that is under review at a scientific journal at the time of issuing of this report.

Despite efforts to better manage unexpected breakdowns, scientific literature highlights the inadequacy of existing models for understanding and predicting breakdown in complex systems [Hollnagel et al., 2006], resulting from a lack of tools for designing an adequate system response that will avoid, or limit the consequences of, operational disruption.

This inadequacy is further expanded by the problem of cyber attacks, as breakdowns of interconnected systems can be triggered from anywhere in the world with little to no traceability, known as the problem of *"intractability of digital attribution"* [Rid and Buchanan, 2015].

Coherent and efficient future collaborative research can be aided greatly by understanding the Cyber Resilience Frameworks (CRFs) that have already been proposed, through aspects such as the types of attacks these frameworks address, the methods that these CRFs use, the institutes and countries where these CRFs are investigated, and the proportion of collaborative research being performed by country about CRFs, for example.

As a result, this part of the research presents the results of using a reproducible method to gather and synthesise information about the cyber resilience frameworks ((CRF) that have been proposed by the scientific community, in order to reveal the characteristics of published CRF by providing answers to the following questions:

1. What types of attacks are addressed by CRFs proposed in literature?
2. Which methods do these proposed CRFs use?
3. Which countries and institutions have proposed CRFs?", and
4. Which research and industrial areas do existing CRFs cover?

Answers to these questions are expected to help identify the potential use of these frameworks in the design cyber resilience in ships, and to facilitate the understanding about the present CRF research landscape, promote cross-pollination between research approaches, and provide ideas for potential research areas and industries including shipping, by highlighting potential networking between CRF research groups.

The methodology followed for this part of the research is a structured literature review process (SLR) as per the process outlined in Figure 3. The methodology is detailed in Appendix C section 10 in this report.

The number of published articles about CRFs has increased exponentially, as shown in Figure 4. The main journals where these CRFs have been published are shown in Table 1.

Most journals in the sample have published only one or two articles about CRFs as can be seen in Figure 5. This represents a highly disperse yet diverse publication landscape. A notable exception is the journal *IEEE Transactions on Smart Grid*, with ten publications related to CRF.

The authors of these papers are also from diverse nationalities. Authors from 47 different countries were represented in the sample. Figure 6 represents the proportion of the number of collaborating countries found in the synthesis sample papers. Collaboration was determined by the number of distinct countries to which the paper authors have been registered. Over 70% of papers represented in the sample, are the result of single authorship or national collaboration, while close to 1% of the papers in the sample result of researchers in 4 countries collaborating, the highest number of distinct collaborating countries [Li et al., 2016]. [Lv et al., 2017].

Countries in the sample produced papers in collaboration with other countries, without collaboration with other countries, or both. Tables 2 and 3 reflect the countries that were predominantly collaborative and non-collaborative ordered by the number of papers from

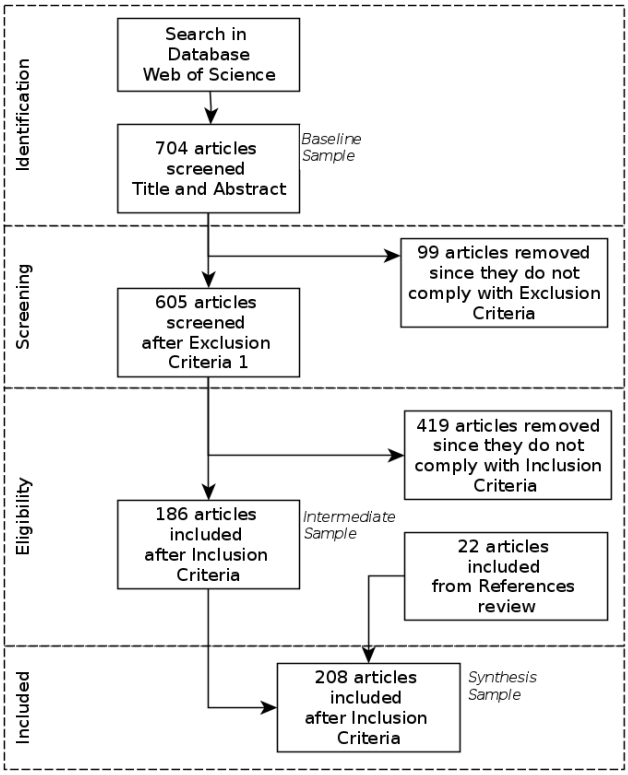

Figure 3: PRISMA set for the Systematic Literature Review

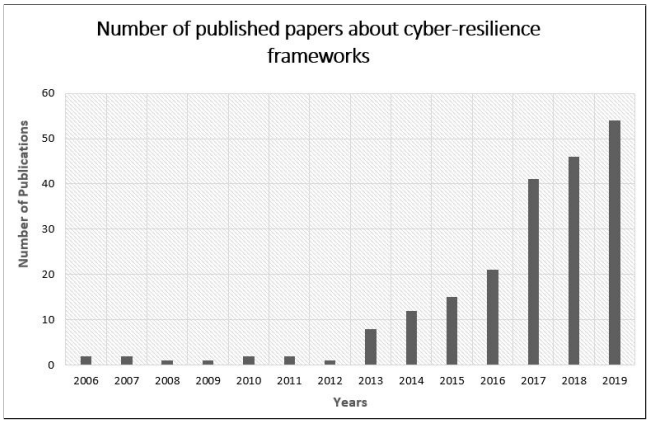

Figure 4: Number of articles published about CRF

Table 1: Main journals that have published a CRF

Journal	Num. of Publications
IEEE Transactions on Smart grid	10
Sensors	6
Future generation computer systems	6
Computers & Security	5
IEEE Systems Journal	4
IEEE Transactions on Industrial Informatics	4
IEEE Access	4
Journal of Defense modeling and simulation	4
International journal of cyber warfare and terrorism	4
International journal of critical infrastructure protection	4
Computers in industry	3
Security and communication networks	3
IEEE transactions on power systems	3
IEEE transactions on automatic control	3
International journal of security and its applications	3
Information sciences	3
IEEE transactions on systems man cybernetics - Systems	3
Other journals	136
Total publications	**208**

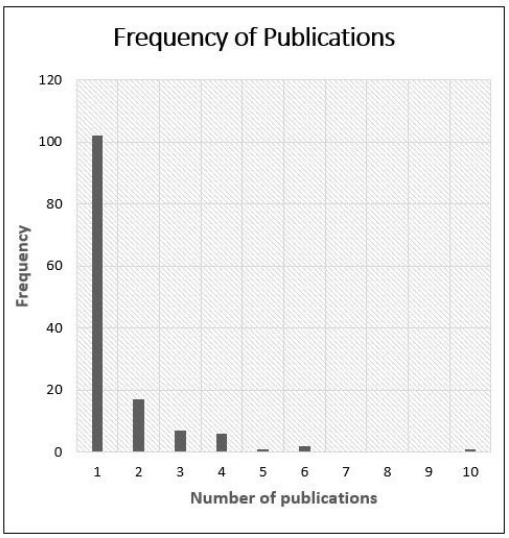

Figure 5: Frequency of CRF journal article publication

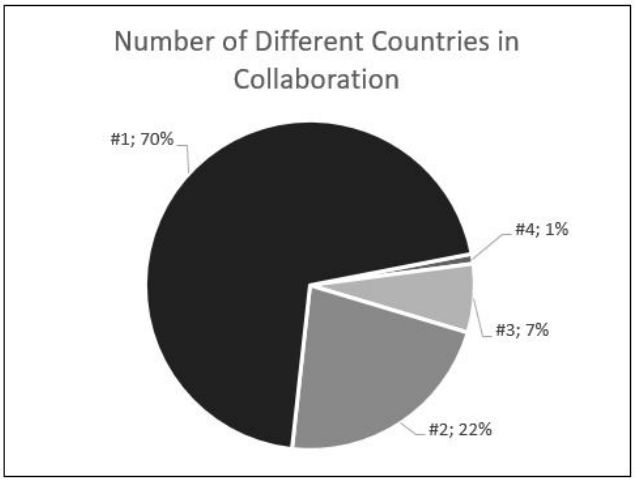

Figure 6: Number of distinct collaborating countries for papers in the synthesis sample

Table 2: Number of authors in mainly non-collaborating country

Country	Coll.	Non-Coll.	Total
USA	25	48	73
England	6	9	15
India	6	7	13
France	4	4	8
Japan	0	4	4
Ireland	1	2	3
Greece	1	2	3
Iran	1	2	3
Jordan	0	2	2
Thailand	1	1	2
Malaysia	0	2	2
North Ireland	0	1	1
Macedonia	0	1	1
Turkey	0	1	1
Romania	0	1	1
South Africa	0	1	1
Wales	0	1	1
Mexico	0	1	1

that country in the synthesis sample. For this analysis, if an article has been published by scientists in two countries for example, it will appear once for each country. The total number therefore reflects the number of distinct researchers that authored the papers in the synthesis sample.

As shown in Table 2, USA is the country that has produced the most papers about cyber-resilience framework with 73, with almost two-thirds of them authored by researchers associated with institutions in the USA. As a result, USA is the country with the least proportion of research collaboration in our sample. On the other hand, as seen from Table 3, Chinese researchers have produced slightly more articles through international collaboration than through research merely between Chinese researchers.

The country with the highest number of completely non-collaborating authors is Japan (4 non-collaborating authors against zero collaborating authors), as per Table 2. On the other hand the country with the highest number of completely collaborating authors is Israel, with 5 authors collaborating against zero with non collaborative publications, as per Table 3.

The network representation of the authors involved in the production of articles in the synthesis sample is shown in Figure 7, through use of an undirected graph. The main parameters that describe this network are listed in Table 4.

A clustering analysis of this network of authors shows one big cluster around the US and China, smaller peripheral clusters of European countries collaborating with south-east Asia, and several countries that have not collaborated internationally, and appear as isolated islets in a network representation. Notable examples of these lack of collaboration include Japan with four CRF papers [Nower et al., 2014], [Li et al., 2014b], [Chakhchoukh and Ishii, 2014] and [Tarao and Okamoto, 2016].

Figure 8 shows a measure of the efficiency in the article production process per country, represented through the relationship between articles produced and citations per article. The US is positioned as the country with both a high production of CRF articles and a high number of average citations, followed closely by China, with Australia and England following further behind.

The thematic analysis in this work categorizes the articles in the `synthesis sample` according to characteristics of the frameworks these articles present and/or implement, as a way of answering the research questions of this paper. The categorizations that have been used for this analysis are:

- Resilience time frame and hierarchy category to which the frameworks belong,

Table 3: Number of authors in mainly collaborating country

Country	Coll.	Non-Coll.	Total
Peoples R China	22	21	43
Australia	7	6	13
Singapore	7	3	10
Canada	5	4	9
Germany	7	2	9
South Korea	4	3	7
Italy	5	2	7
Sweden	4	2	6
Saudi Arabia	3	2	5
Israel	5	0	5
Portugal	2	1	3
Denmark	3	0	0
Switzerland	2	1	3
Brazil	2	1	3
Taiwan	2	0	2
Luxembourg	2	0	2
Pakistan	2	0	2
Spain	2	0	2
Poland	1	0	1
Kazakhstan	1	0	1
Qatar	1	0	1
Netherlands	1	0	1
Norway	1	0	1
Ukraine	1	0	1
Austria	1	0	1
Hungary	1	0	1
U Arab Emirates	1	0	1
Ghana	1	0	1
Myanmar	1	0	1

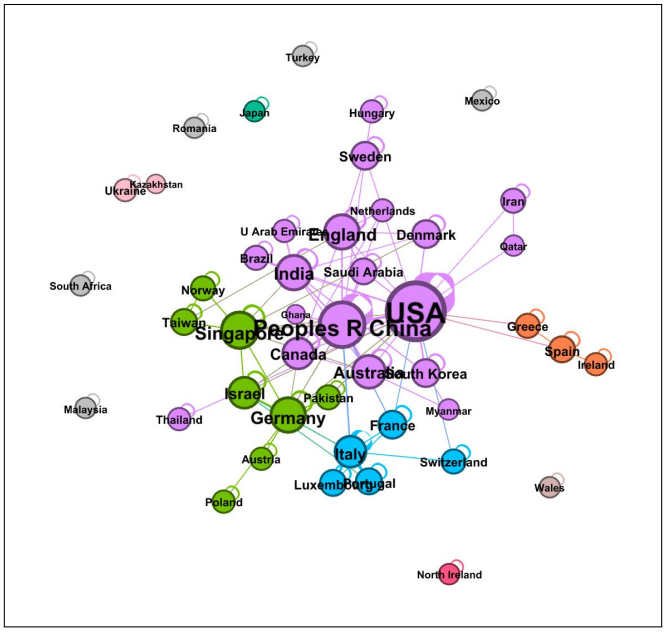

Figure 7: Network representation of author collaborations

Table 4: Basic network parameters

Measure	Value
Number of Nodes	45
Number of Edges	116
Average Degree	5,156
Avg. Weighted Degree	136,356
Network Diameter [?]	4
Graph Density	0,117
Modularity [Blondel et al., 2008]	0,442
Number of Communities	12
Avg. Clustering Coef.	0,497
Avg. Path Length	2,341

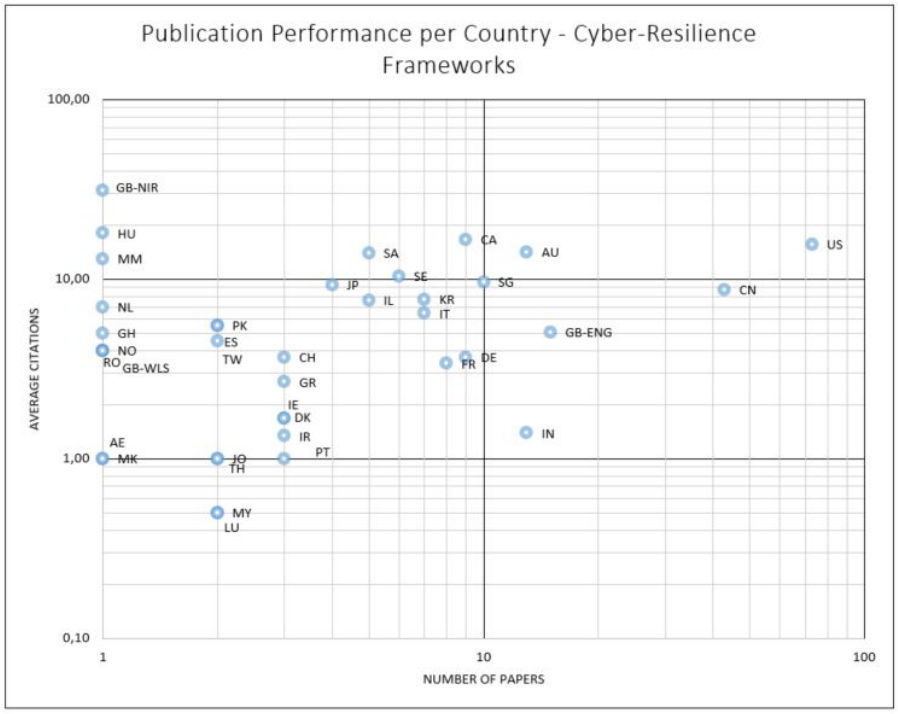

Figure 8: Articles versus citations per country in the sample

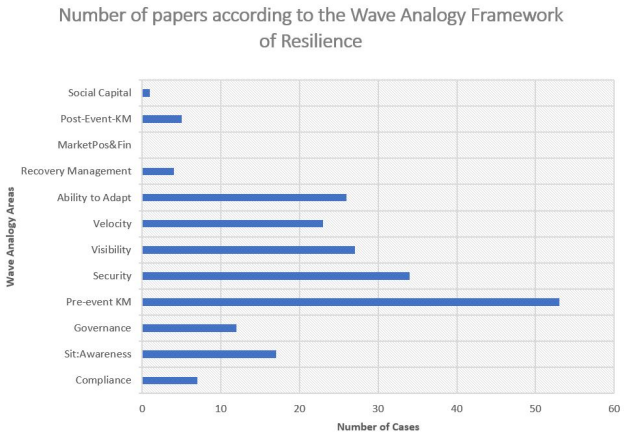

Figure 9: Papers in the synthesis sample according to the *Wave Analogy* for resilience

- The industrial area where the cyber resilience frameworks are applied,
- The types of attacks that each of these frameworks address,
- The methods used in these frameworks, and
- The countries and organizations (e.g., institutes, universities) where this research is taking place.

A first categorization used corresponds to the resilience framework presented by Guerra & Sepulveda Estay [Guerra and Sepulveda Estay, 2019], corresponding to the `"Wave Analogy"` for resilience, explained in Appendix A section 8.1.3 in this report, which categorizes resilience frameworks along an event timeline which has a disruption event at its center, with categories grouping frameworks lead to the disruption and categories grouping frameworks that follow from the disruption, from operational to strategic.

The categorization proposed by Guerra & Sepulveda-Estay considers twelve categories according to a dynamic and a hierarchical dimension. The dynamic dimension groups articles according to the time at which decisions can be made about resilience for each category, either before, during, or after the disruption. The hierarchical dimension categorizes the level at which the decisions are made about resilience, either at a strategic or at an operational level.

Figure 9 shows the number of articles in the synthesis sample for each of the *Wave Analogy* categories. One paper may have had more than one category, although in those cases categories are normally hierarchically close to each other. The biggest share of the papers in the sample are in the category of Pre-event Knowledge Management, and concerning risk analysis, simulation and modeling. Examples of papers in the different Wave Analogy categories are shown in Table 5. The category with most papers is the *Pre-event Knowledge Management* followed by *Security*, *Velocity*, and *Ability to Adapt*.

The research areas represented in the `synthesis sample` papers are listed in Table 6, with examples of papers for the main research areas and application areas found in the synthesis sample.

Several of the papers in the `synthesis sample` indicated a specific cyber-attack. The types of attacks that have been addressed in the papers in the `synthesis sample` are presented in Table 7.

The attack type that is mentioned the most in the papers in the sample are are the False Data Injection Attacks (FDIA), followed by the Distributed Denial of Service (DDoS).

Table 5: CRF examples from synthesis sample for every Wave Analogy Category

Wave Analogy Category	**Example papers**
Compliance	[Srinivas et al., 2019] [Porcedda, 2018] [Ruan, 2017]
Situational Awareness	[Shakibazad, 2019] [Yadegar et al., 2019] [Paradise et al., 2017] [Raulerson et al., 2015] [Cardoza and Wagh, 2017]
Governance	[Irwin and Dawson, 2019] [Januário et al., 2019] [Abraham and Nair, 2018] [Zhang et al., 2017] [Kumar et al., 2014] [Hathaway et al., 2012] [Le and Hoang, 2017]
Pre-event Knowledge Management	[Shakibazad, 2019] [Noor et al., 2019] [Rodofile et al., 2019] [Tam and Jones, 2019] [Baig and Zeadally, 2019] [Rongrong et al., 2019] [Park and Lee, 2019][Huang et al., 2018b] [Moslemi et al., 2018] [Al-Dabbagh et al., 2017] [Su, 2018] [Wang et al., 2018a] [Taormina et al., 2017] [Awan et al., 2016] [Agrafiotis et al., 2018] [Hemanidhi and Chimmanee, 2017] [Yunos et al., 2015] [Ashtiani and Abdollahi Azgomi, 2014]
Security	[Kim et al., 2019] [Ju et al., 2019] [Lei et al., 2019] [Adamsky et al., 2018] [Alsaleh et al., 2017] [Chittister and Haimes, 2011] [Agnarsson et al., 2016] [Chen et al., 2018] [Ashok et al., 2017]
Visibility	[Chakhchoukh and Ishii, 2014] [Rege, 2014] [Pasqualetti et al.,] [Spyridopoulos et al., 2013] [Canepa and Claudel, 2013]
Velocity	[Barenji et al., 2019] [Peng et al., 2019] [Al-Gburi and Mohd Ariff, 2019] [Comert et al., 2018] [Bretas et al., 2019]
Ability to Adapt	[Babiceanu and Seker, 2019] [Bretas et al., 2019] [Wu et al., 2018] [Haque et al., 2018] [Yong et al., 2018] [Mo and Sansavini, 2017]
Recovery Management	[Barreto and Costa, 2019] [Wagner et al., 2017] [Khan and Sepulveda Estay, 2015] [Davis, 2015]
Market Position and Finance	*No papers found in sample*
Post-event Knowledge Management	[Chhabra et al., 2018] [Akhmetov et al., 2018] [Chejerla and Madria, 2017] [Nower et al., 2014] [Katos and Bednar, 2008]
Social Capital	[Paradise et al., 2017]

Table 6: CRF examples from synthesis sample for research and application areas

Research Areas	**Application Areas**
Computer Science	Cloud Technology [Le and Hoang, 2017] [Chejerla and Madria, 2017] Cyber attack outsourcing [Huang et al., 2018a] Manufacturing [Li et al., 2019] [Babiceanu and Seker, 2019] [Khalid et al., 2018] Military Operations [Barreto and Costa, 2019] [Hemanidhi and Chimmanee, 2017] [Denning, 2014] [Tang et al., 2015] [Jaquire and von Solms, 2015] [Mo and Sansavini, 2017] [Chen, 2016] [Atoum and Otoom, 2017] [Wagner et al., 2017] [Raulerson et al., 2015] [Bergin, 2015] [Hadji-Janev and Bogdanoski, 2017] [Alqahtani, 2015] Networks [Spyridopoulos et al., 2013] [Ashtiani and Abdollahi Azgomi, 2014] [Awan et al., 2016] [Sun and Yang, 2018a] [Li et al., 2015] [Abraham and Nair, 2018] [Rongrong et al., 2019] Social Networks [Paradise et al., 2017] Software Development [Tang et al., 2018] Web-based platforms [Russo et al., 2019] [Tarao and Okamoto, 2016]
Engineering	Electrical Grids [Sahoo et al., 2018] [Beg et al., 2017] [Tan et al., 2018] Food Production [West, 2018] Pharmaceutical [Barenji et al., 2019] Nuclear Plants [Wang et al., 2018b] [Park and Lee, 2019] [Lee and Lim, 2016] Oil and Gas [Shakibazad, 2019] Power Systems (Electrical) [Gao et al., 2016] [Farraj et al., 2015] [Chakhchoukh and Ishii, 2014] [Hahn and Govindarasu, 2011] [Wang et al., 2017a] [Al-Gburi and Mohd Ariff, 2019] [Chung et al., 2019] [Jin et al., 2019] [Liang et al., 2019] [Wu et al., 2018] [Taha et al., 2018] [Wang et al., 2017b] [Lei et al., 2019] [Ashok et al., 2017] [Liu et al., 2013] Smart Grid [Bretas et al., 2019] [Wang et al., 2018a] [Sani et al., 2019] [Moslemi et al., 2018] [Xiang et al., 2018] Water Distribution [Taormina et al., 2017]
Telecommunications	Communication Network [Januário et al., 2019] [Nower et al., 2014] [Canepa and Claudel, 2013] [Foglietta et al., 2019] Cyber Forensics [Chhabra et al., 2018] Healthcare [Sharma et al., 2019] Wireless Networks [Al-Dabbagh et al., 2017] [Yuan and Xia, 2018] [Kim et al., 2019] [Li et al., 2014b]
Automation & Control Systems	Adaptive Control [Yadegar et al., 2019] Distributed Control [Peng et al., 2019] General Control [Bezzaoucha et al., 2018] [Chejerla and Madria, 2017] [Li et al., 2016] [Sun and Yang, 2019] [Rodofile et al., 2019] [Adamsky et al., 2018]
Government & Law	Critical Infrastructure [Baig and Zeadally, 2019] [Chittister and Haimes, 2011] [Hadji-Janev and Bogdanoski, 2017] Finance [Noor et al., 2019] [Irwin and Dawson, 2019] Foreign Policy [Brown III, 2019] Legal [Hathaway et al., 2012] Regulation [Kumar et al., 2014] [Srinivas et al., 2019] [Porcedda, 2018]
Business and Economics	Economics [Ruan, 2017] Insurance [Zhang et al., 2017] [Young et al., 2016] Intellectual Property [Andrijcic and Horowitz, 2006] Supply Chains [Khan and Sepulveda Estay, 2015] [Davis, 2015]
Public Administration	Public Sector [Wirtz and Weyerer, 2017] National Power Systems [Rege, 2014] Critical Infrastructure [Chittister and Haimes, 2011]
Transport	Autonomous Vehicles [Sheehan et al., 2019] [Ratasich et al., 2019] Shipping [Tam and Jones, 2019] [Sahay et al., 2019c] Transportation Networks [Comert et al., 2018] [Akhmetov et al., 2018]

Table 7: CRF examples from synthesis sample for cyber attack types and application areas

Attack Type	**Application areas**
Actuator Attacks	Manufacturing [Li et al., 2019]
	Adaptive Control [Yadegar et al., 2019]
Advanced Persistence Attacks	Social Networks [Park and Lee, 2019]
Alter and Hide	Power Systems (electrical) [Wang et al., 2017a]
Authentication & Availability	Manufacturing [Khalid et al., 2018]
Black Hole & Grey Hole	Healthcare [Sharma et al., 2019]
Deception	Non-specific CPS [Li et al., 2018] [Rodofile et al., 2019]
	Power Systems (electrical) [Chung et al., 2019]
	Smart Grid [Bretas et al., 2019]
	Switching [Liu et al., 2013]
Distributed Denial of Service	General Control [Sun and Yang, 2019] [Wang and Xu, 2019]
(DDOS)	Government Regulation [Srinivas et al., 2019]
	Networks [Sun and Yang, 2018a] [Li et al., 2015] [Spyridopoulos et al., 2013] [Sahay et al., 2019c]
	Non-specific [Sun and Yang, 2018b]
	Wireless Networks [Yuan and Xia, 2018]
False Data Injection	Electrical Grids [Sahoo et al., 2018] [Tan et al., 2018] [Beg et al., 2017]
(FDIA)	Non-Specific CPS [Li and Yang, 2019] [Yong et al., 2018]
	Power Systems (electrical) [Jin et al., 2019] [Liang et al., 2019] [Wu et al., 2018] [Tan et al., 2018] [Taha et al., 2018] [Wang et al., 2017b]
	Smart Grid [Moslemi et al., 2018] [Xiang et al., 2018]
Ransomware	Finance [Irwin and Dawson, 2019]
Replay	Non-specific CPS [Chen et al., 2018]
Sensor-related	Alterations [Li et al., 2018] [Su, 2018]
Spoofing	Communication Networks [Canepa and Claudel, 2013]
Stealth	Electrical Grids [Sahoo et al., 2018]
Zero-Day	Power Systems (electrical) [Al-Gburi and Mohd Ariff, 2019]
	Software Development [Tang et al., 2018]

The cyber-resilience frameworks presented in the papers in the `synthesis sample` use a number of different methods in the CFR's that are proposed. Table 8 lists the methods that have been found in the `synthesis sample` and the institutions that are using these methods, referencing example papers. The categorization structure is based on the main method used for each paper in the sample. The number of methods used have been categorized as either related to Algorithms, Game theory, Architecture, Optimization, Machine learning, Statistical methods, Qualitative methods and Simulation. Machine learning and Optimization were shown separately to be able to include sub-classes of these categories. The same reasoning is applied for separating game theory from algorithms, for example.

The research institutions with the highest number of CRF-related paper publications in the sample are headed by the University of Illinois in the US with 6 publications, followed by Northeastern University located in China and the University of Wisconsin in the US with 5 publications each. The methods that present the highest number of references is *General risk Assessment*, followed by *Bayesian Networks* and *Machine Learning*.

Table 8: CRF examples from synthesis sample for methods used and organizations using them

General Method	Specific Method	Research Institution
Algorithms	Attack graphs and attack trees	Univ Warwick,UK[Lallie et al., 2018]
	Attack resilient	PNNL,US & Iowa state Univ,US & Argoinne Nar Lab,US[Ashok et al., 2017]
	Candidate in-variants	Univ texas,US & Vanderbilt Univ,US[Beg et al., 2017]
	Contradiction Methods	Yangzhou Univ,CN & Brunel Univ,UK & King Adbulaziz Univ,SA[Zhang et al., 2018]
	Control based mitigation	Univ Toronto,CA & TELUS Comun,CA[Farraj et al., 2015]
	Cooperative Observer-based detection	NUS,SG & IIT Dehli,IN & Aalborg,DK[Sahoo et al., 2018]
	Doubly weighted trees	George Mason Univ,US & US NAval Acad,US & Chiang Mai Univ,TH[Agnarsson et al., 2016]
	Dynamic State Estimator	Univ Texas,US & Argonne Nat Lab,US & Purdue Univ,US[Taha et al., 2018]
	Dynamic Watermarking	Texas A&M Univ,US[Huang et al., 2018b]
	Efficient Data Recovery	Japan Adv Inst Sci&Tech,JP[Nower et al., 2014]
	Graph Theoretic characterization	Univ California St Barbara,US[Pasqualetti et al.,]
	Inference system synthesis	Univ Hong-Kong,CN & Michigan Tech Univ,US & Waterfall Secur Solut,IL[Wang et al., 2017a]
	Kullback Leibler divergence	Northeastern Univ,CN[Li and Yang, 2019]
	Matrix decomposition & Factorization	Shanghai Jiao Tong Univ,CN & Chinese Acad Sci,CN & Xian Jiaotong Liverpool Univ,CN & Univ Coll Eng,IN[Wang et al., 2018a]; Rensselaer Polytech Inst,US & Exponent Inc.,US & New York Power Author,US[Gao et al., 2016]
	Real time traffic analysis	Cardiff Univ,UK[Awan et al., 2016]
	Software Defined Networking (SDN)	Embry Riddle Aeron Univ,US[Babiceanu and Seker, 2019]; Tech Univ Danmark,DK[Sahay et al., 2019c]
Architecture	Adaptive base corrective signal	Amirkabir Univ Tech,IR & Qatar Univ,QA & Georgia Inst Tech,US[Yadegar et al., 2019]
	Artificial Immune server	Kanagawa Inst Tech,JP[Tarao and Okamoto, 2016]
	Co-design	Daegu Gyeongbuk Inst Sci Tech,KR[Kim et al., 2019]
	Discrete event triggered communication	Lanzhou Univ Tech,US[Li et al., 2019]
	Dist. Kalman Fusion Estimator	City Univ Hong-Kong,CN & Nanyang Tech Univ,SG & Zhejiang Univ Tech,CN[Chen et al., 2018]
	Systems Design	Carnagie Mellon Univ,US & Univ Virginia,US[Chittister and Haimes, 2011]
	Three-layered reference architecture	Washington State Univ,US & MITRE Corp,US & Univ Texas,US[Hahn and Govindarasu, 2011]
	Variable structure system theory	Commun Univ China,CN & Texas A&M Univ,US & Univ Toronto,CA[Liu et al., 2013]

Continued on next page

Table 8 – continued from previous page

General Method	Specific Method	Research Institution
Game Theory	Bi-linear differential quality	Caspian State Univ,KZ & European Univ,UA [Akhmetov et al., 2018]
	Nash Equilibrium	Univ Sydney,AU & Univ New South Wales,AU[Sani et al., 2019]; Hong-Kong Univ,CN & Zhejiang Univ,CN & Univ. Newcastle,UK [Li et al., 2015]; Univ Bristol, UK[Spyridopoulos et al., 2013]
	Two-stage Min-Max	ETH,CH & Univ Tech Sydney,AU[Mo and Sansavini, 2017]
Literature Review	General	Tech Univ Denmark,DK[Khan and Sepulveda Estay, 2015]; Univ Murcia,ES & Univ Aegean,GR[Nespoli et al., 2018]; Univ of Tech,MY[Yunos et al., 2015]
	Regulation	Jundal Global Univ,IN & Int Inst Informat Technol,IN[Srinivas et al., 2019]; Macquarie Univ,AU[Irwin and Dawson, 2019]
	Security Objectives	Beijing Univ,CN[Lu et al., 2015]
	Taxonomy & Propagation	Univ Oxford,UK[Agrafiotis et al., 2018]
Machine	General	NUST,PK & Fontbonne Univ,US & IIUI,PK[Noor et al., 2019]; Zhengzhou Int Informat Sci & Tech,CN[Ju et al., 2019]; UTP Univ Sci Technol,PL & Fern Univ,DE[Kozik et al., 2019]; Thapar Univ,IN[Chhabra et al., 2018]; Northeastern Univ, CN[Sun and Yang, 2018b]
Learning	Data Mining and Classification	Univ Tun Hussein Onn,MY[Al-Gburi and Mohd Ariff, 2019]
	Deep Learning	Illinois State Univ, US & Univ Texas, US[Fang et al., 2019]
	Robust Regression	Takyo Inst Tech,JP[Chakhchoukh and Ishii, 2014]
	Text Analysis - Nat. Lang. Proc.	Christ Univ,IN[Cardoza and Wagh, 2017]
Maturity Model	Cloud Based	Univ Tech Sydney,AU[Le and Hoang, 2017]
Optimization	Bi-level MILP	Hunan Univ,CN & Illinois Inst Tech,US[Tan et al., 2018]; New York Univ,USA[Zhang et al., 2017]
	Markov chains - Dyn Prog	Beijing Inst Tech,CN[Yuan and Xia, 2018]; Univ Wisconsin,US & Univ Toledo,US & ATSEC Informat Secur Corp,US[Xiang et al., 2018]
	Min-Max Multi-obj	Queen Mary Univ London,UK[Khouzani et al., 2019]
	Parametric fb linearization	Univ Toronto,CA[Farraj et al., 2015]
	Semi-Definite Programming	Univ Calif Berkeley,US & KTH Royal Inst Tech,SE [Jin et al., 2019]
	Stochastic model	IBM Corp,US & Southern Method Univ, US[Abraham and Nair, 2018]
Qualitative	Rational Choice perspective	Temple Univ,US[Rege, 2014]
	Vulnerability detection	Rangsit Univ,TH[Hemanidhi and Chimmanee, 2017]
Risk Assess.	General	Univ Roma,IT[Russo et al., 2019]; Univ Plymouth,UK[Tam and Jones, 2019]; Deakin Univ,AU & Univ Kentucky,US[Baig and Zeadally, 2019]; Chinese Acad Sci,CN[Rongrong et al., 2019]; Univ Roma,IT & Univ Coimbra,IT & Israel Elect Corp Ltd, IL[Foglietta et al., 2019]; UNIST,KR[Park and Lee, 2019]; Air Force Inst Tech,US & Appl Res Solut,US & LGS Innovat,US[Young et al., 2016]; DoD Nat Def Univ,US[Chen, 2016]
	Economic Evaluation	Univ Virginia,US[Andrijcic and Horowitz, 2006]
	Satisfiability Module theory	Univ North Carolina,US[Alsaleh et al., 2017]
	Tallin Manual	Korea Univ,KR[Lee and Lim, 2016]
	Vulnerability Management	Univ Luxembourg,LU & Itrust Consulting,LU & Roma Tre Univ,IT & CRAT,IT & Univ Coimbra,IT & Leonardo SpA,IT[Adamsky et al., 2018]
	Interdependency	Univ Newcastle,AU & Chinese Univ Hong-Kong,CN & China Southern Power Grid,CN & Univ Sydney,AU & Chongquing Univ,CN & Univ New South Wales,AU[Liang et al., 2019]
Simulation	Agent-based system	Hacettepe Univ,TR[Barenji et al., 2019]
	Ad hoc on demand distance vector	Jaypee Univ Inf Tech,IN & Vellore Inst Tech,IN & Soonchunhyang Univ,KR & La Trobe Univ,AU[Sharma et al., 2019]
	Bayesian Max. Likelihood Est.	Univ Georgia,US[Moslemi et al., 2018]

Continued on next page

Table 8 – continued from previous page

General Method	Specific Method	Research Institution
	Bayesian Networks	Univ Limerick,IE[Sheehan et al., 2019]; George Mason Univ,US[Barreto and Costa, 2019]; Benedict Coll,US & Univ Illinois,US[Comert et al., 2018]; Missouri Univ Sci Tech,US[Chejerla and Madria, 2017]; World Islamic Sci Edic Univ,JO & Royal Jordanian Air Forces,JO[Atoum and Otoom, 2017]
	Block-chain	Chinese Univ Hong-Kong,CN & Univ Sci Tech China,CN & Univ Newcastle,AU & Univ Sydney,AU & Chongqing Univ,CN & Elect Power Res Inst,US & Univ South Wales,AU[Liang et al., 2019]
	BMI Control	Univ Luxembourg,LU & Univ Lorraine,FR[Bezzaoucha et al., 2018]
	Bounded sensor reading	Nanyang Tech Univ,SG[Su, 2018]
	Convex Optimization	South China Univ Tech,CN[Wang and Xu, 2019]
	Distributed Attack	Iran Sci Univ Tech,IR[Ashtiani and Abdollahi Azgomi, 2014]
	Hierarchical Modeling	MIT,US[Wagner et al., 2017]
	LiSM: Land in Sand Miner	NEC Labs Amer,US & Univ Illinois,US & BBN Tech,US[Tang et al., 2015]
	Montecarlo	Politech Milan,IT & Univ Paris,FR[Wang et al., 2018a]
	Penetration Testing	Malek Ashtar Univ Tech,IR & NIOPDC,IR[Shakibazad, 2019]; US Air Force,US[Raulerson et al., 2015]
	Process	Northeastern Univ,CN[Sun and Yang, 2018b]; Singapore Univ Tech Design,SG & Optiwater,IL & Technion Israel Inst Tech,IL[Taormina et al., 2017]; Shenandoah Res Tech,US[Bergin, 2015]
	Reliability	Univ Idaho,US & Texas A&M Univ,US[Lei et al., 2019]
	Robust predictive control	Northeastern Univ,CN[Sun and Yang, 2019]
	Stochastic methods	Arizona State Univ,US & Penn State Univ,US & Swiss Fed inst Tech,CH[Yong et al., 2018]; Jiangnan Univ,CN & Northeastern Univ,CN[Li et al., 2018]
	Swarming Based Cyber Defense	Mil Acad Gen Mihailo Apostolski,MK[Hadji-Janev and Bogdanoski, 2017]
	Traffic Flow - Lighthill-Whitham-Richards	King Abdullah Univ Sci Tech,SA & Univ Califonia Berkeley,US[Canepa and Claudel, 2013]
Statistical	Honeypot	Univ Texas,US & Illinois State Univ,US[Zhan et al., 2013]; Ben gurion Univ,IL & Deutsch Telekom,DE & Bosch Ctr Artif Intel,DE[Paradise et al., 2017]
	Hypothesis Testing	Univ Florida,US & Univ Sao Paulo,BR[Bretas et al., 2019]
	Modeling	Charles Darwin Univ,AU & Univ Melbourne,AU & Commonwealth Bank,AU[Tang et al., 2018]
Strategy	Attack Strategy	Singapore Univ Tech Design,SG & Univ Oslo,NO & Nat Tsing Hua Univ,TW & Nat Chiao Tung Univ,TW & Nat Sun Yat Sen Univ,TW[Chung et al., 2019]
	Criminal Law	Yale Univ,US & Princeton Univ,US[Hathaway et al., 2012]
	Critical infrastructure Regulation	Univ Petr&En Studies,IN & Wipro tech,IN[Kumar et al., 2014]
	Cyber-crime	Univ Portsmouth,UK & Lund Univ,SE & Athabasca Univ,CA[Katos and Bednar, 2008]
	Hierarchical Contracts	Nanyang Tech Univ,SG & Delta Elect,SG[Haque et al., 2018]
	Regulation Instrument Comparison	Univ Leeds,UK[Porcedda, 2018]
	Two-pronged	CUST,PK & Univ Bremen,DE & BIBA Bremer Int Prod,DE & Bahria Univ,PK[Khalid et al., 2018]
Survey	General	Shanghai Univ,CN[Peng et al., 2019]; Univ Hull,UK[Alqahtani, 2015]; MIT,US[Huang et al., 2018a]

3.2 Study 2 - Comparison of Wave Analogy Model to other Frameworks

Note: This subsection is based on the work performed by James Osborne, Master level student at the Technical University of Denmark [Osborn, 2020].

Cyber Resilience Frameworks are being developed to meet the growing cyber threats posed to organisations and governments, but frameworks differences in structures and

methodologies give them variable applications. The Impact-Wave Analogy is a newly developed cyber resilience framework; how it compares to other resilience frameworks is unknown. Cyber resilience frameworks are structured guidelines in which organisations and governments can plan accordingly, to create defences and to create strategies for cyber events.

Based on a SLR, five other cyber resilience frameworks were identified and compared using two analyses. The first analysis aimed to understand the flexibility and adaptability of the framework. The second identified how the frameworks compared to one another based on statistical information about them, such as publications written citing them, implementation in industry, and which stage of cyber resilience is addressed. The results from this culminate in an evaluation and discussion to identify which frameworks met the stated criteria and how the Impact-Wave Analogy compared in this analysis.

This work identifies three questions after comprehensive analysis, and a detailed evaluation in relation to the chosen cyber resilience models:

1. Which Cyber Resilience Frameworks have been proposed in literature that can be Compared with the Wave Analogy Framework?

2. How does the Wave Analogy Compare to other Cyber Resilience Frameworks and Analogies?

3. Is the Wave Analogy Framework a capable Cyber-Resilience Model?

Five frameworks were chosen for comparison with the Wave Analogy Model, the AWaRE framework, Byzantine Fault tolerant framework, the Human Behavior Resilience Framework, the NIS Directive, and the NIST Framework.

Framework 1 - AWaRE (AWR)

The first framework selected for the comparison is called AWaRE and was first published in 2018 at the International Conference on Engineering of Complex Computer Systems (ICECCS). The introductory paper is titled "AWaRE – Towards Distributed Self-Management for Resilient Cyber Systems" [Chhetri et al., 2018]. The paper defines AWaRE's capabilities as *"...the use of a conceptual, state-space-based design and reconstitution framework, combined with run-time models and distributed constraint satisfaction/optimization techniques for decision-making and coordination of system re-configurations"* [Chhetri et al., 2018].

The AWaRE framework consists of five layers - Management, Knowledge, Interoperability, Messaging and Storage.

1. *The Management layer* follows the MAPE-K reference model, which includes monitoring, execution, performing constraint solving to detect inconsistencies from constraint-solver agents, and self-manager agents used to bring system back to required state.

2. *The knowledge layer*, also follows the MAPE-K reference model, and it also includes two self-representing, light-weight models: design-time and run-time.

3. *The Interoperability layer* is described as *"Wrapper Facade pattern to provide a consistent API facade that abstracts away the various middleware platforms."*

4. *The Messaging and Storage layer* contains middleware platforms for communication and distributed storage [Chhetri et al., 2018].

Framework 2 - Byzantine Fault Tolerant++ (BFT)

The next framework identified for this comparison is the Byzantine Fault Tolerant++ (BFT++), which was first published in 2019 by the Office of Naval Research, and was part of a fault tolerance initiative to safeguard Cyber Physical Systems (CPS). BFT++ is a *"cyber resilient architecture that engineers the cyber components to be brittle against attack, which consequently forces cyber-attacks and related disruptions to be short-lived and within tolerance of the physical system's inertia"* [Mertoguno et al., 2019].

The base implementation of BFT++ uses triple redundancy, artificial software diversity applied across the replicas, and delayed input sharing with the replicas designated as backups. Additionally, the diversification transformations can employ FastCrash techniques to increase cyber brittleness to attack and entice the crash signal to be generated as early as possible.

Being a newly developed framework/ analogy, its use in industry is limited; although *"BFT++ has been implemented in a hardware-in-the-loop (HIL) testbed at the Naval Research Laboratory (NRL) for a shipboard chilled water system"* [Mertoguno et al., 2019].

Framework 3 - Human Behaviour Resilience (HRB)

The next cyber resilience strategy to be discussed is Human Behaviour Resilience (HBR).HBR is described in the "Advances in Human Factors in Cybersecurity" journal which was most recently updated in 2020. The HBR framework can be defined as a principal adopted by industry which is implemented slowly into an organisation. Organisations core values should encourage a culture where employees are all responsible to achieve an effective cyber resilience by monitoring, responding, anticipating, and learning functions to maintain resilience in cyber capabilities are vital for this model to be effective.

The cyber resiliency of an organization is in part determined by employees' motivation, opportunity, and ability to perform the four generic resilience functions - monitoring, responding, anticipating, and learning. This is having its own framework, with ability and opportunity regulating the motivation, which together creates the employee behaviour [Hughes, 2007]. For this to be achieved in the workforce, there must be a strong managerial and leadership motivation to encourage an ethos of continual improvement and cyber resilience [McCarthy and Milner, 2020].

This framework is completely dependent on the ability and participation of employees. Employees can be capable and motivated to behave in a resilient manner, but when there is no opportunity to do so within the organization these intentions remain in vain. However, as a criterion for cyber resilience and alongside a technical defence it could be suggested this is an opportunity for development and responsiveness which is more flexible and adaptable than the other frameworks already described.

Framework 4 - NIS Directive (NIS)

The Network and Information Systems (NIS) Directive [Markopoulou et al., 2019] were implemented by the European Parliament in 2016. The NIS Directive creates a "Cooperation Group" to facilitate strategic cooperation and exchange of information; with this groups work being centred around planning, steering, sharing information, best practices, and reporting. A key part of the NIS Directive involves greater cooperation and collaboration between all member states; this allows transparency and for all new threats and weaknesses to be shared and fixed as one.

The NIS Directive achieves this by having all member organisation undertake strategies to improve their cyber resilience. The NIS Factsheet states that each member state follows

"Identification of measures on preparedness, response and recovery", *"Strategic objectives, priorities and governance framework"* and *"Member States will designate one or more national competent authorities for the NIS Directive, to monitor the application of the Directive"*, as well as the creation of a "Computer Security Incident Response Teams (CSIRTs)". These teams will be responsible for responding to cyber incidents, but also their functions include *"providing dynamic risk and incident analysis and situational awareness"*, *"providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents"*, and *"participating in the network of the national CSIRTs (CSIRTs network)"*.

All member states of the EU were asked to "transpose" the standards into their critical infrastructure, as well as laws by 2018. The NIS Directive [Markopoulou et al., 2019] is made up of 27 articles, which defines its scope and clarifies its definitions. The legislation was made to ensure all cyber infrastructure was adequately protected from cyber events.

However, this framework is dependent on each state's interpretation of both the framework and the need to for transparency and collaboration, whilst observing it is a national strategy.

Framework 5 - NIST

The (NIST) (National Institute of Standards and Technology) SP 800 series, is a guideline created by the United States government. NIST impacts organisations that interact with Federal Government by storing, transmitting, processing, or protecting Controlled Unclassified Information (CUI).

Contractual organisations have access to information such as "financial services… processing security clearances… providing cloud services; and developing communications, satellite, and weapons systems" (Ross et al. 2020). The series includes many of publications (last count on 27/02/2020 was 185), which cover a broad array of cyber resilience systems and risks. These include subjects such as developing security plans (800-18), conducting risk assessments (800-30), and guides on contingency planning (800-34). The documents have been created and updated since the series creation in 1990.

Results

Comparing the frameworks effectively started with how an identified tool can be incorporated into the framework. These tools, seen in Table 16, are split into proactive and reactive resilience tools; five for each. For each tool and framework, it is determined how well they would be able to be incorporated, and this is achieved via a scoring system, from 1 to 5; details of which can be found in Table 15 in the Appendix D.

This analysis was chosen because it can demonstrate desirable qualities about the frameworks. If a tool can be effectively incorporated into the framework, it shows it is flexible, as it has the ability to reconfigure itself in a resilience and security orientated manner, and demonstrates the flexibility of what the framework can achieve defensively. Therefore, the more tools the framework can incorporate into its structure, the more effective and well-rounded it is.

If the framework can incorporate more proactive resilience tools, than reactive resilience tools (based on higher scoring), then it would suggest the framework is more proactively orientated, than re-actively. This could be important information for organisations looking for frameworks which have these certain strengths.

The analysis undertaken was a comparative research method [Esser and Vliegenthart, 2017]. The comparison chosen heightens our awareness of other systems and understand their patterns of thinking, enabling a critical contrast. As each tool is compared, you must look at the features and characteristics of the frameworks to evaluate its compatibility.

Cyber Defensive Strategies / Resilient Analogies	Proactive 1: Segmentation, Isolation, Containment	Proactive 2: Diversity & Randomness	Proactive 3: Moving Target and Distributedness	Proactive 4: Non-persistence	Proactive 5: Data and System Integrity & Availability	Reactive 1: Dynamic Reconfiguration	Reactive 2: Deception	Reactive 3: Dynamic Reconstitution	Reactive 4: Dynamic Composition	Reactive 5: Alternative Operations
Human Resilient Behaviour	4	3	3	5	2	3	2	5	4	4
BFT++	2	4	4	1	4	4	2	3	4	2
AWaRE	3	1	1	2	4	4	5	4	4	5
NIS Directive	2	3	2	3	4	3	2	3	2	3
NIST	3	2	3	3	4	3	2	3	3	3
Impact-Wave Analogy	4	3	3	3	4	4	3	3	5	3

Figure 10: Table of scores attained in the first Analysis

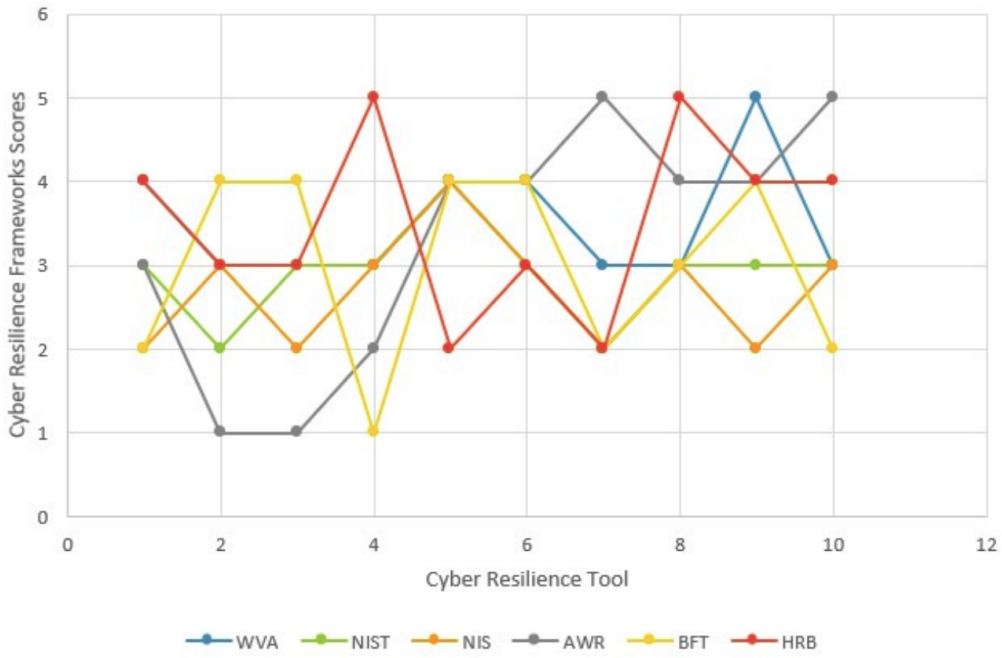

Figure 11: Graphical representation of the scores attained in the first analysis

Factors / Frameworks	Strategic	Operational	Emphases on Pre-Event Resilience	Emphases on During Event Resilience	Emphases on Post Event Resilience	Implemented in Industry	Tested	Ease of Implementation. (1 Difficult to 5 Easy)	No. of Publications Associated	Year of Creation/ Publication	Number of Recorded uses in Industry or Tests	**Final Score based on Information in the table**
Human Resilient Behaviour	✓		✓	✓	✓	✓	✓	5	19	2020	Many	**22**
BFT++	✓		✓		✓		✓	4	4	2019	1	**12.5**
AWaRE	✓				✓			3	8	2018	0	**10**
NIS Directive	✓		✓			✓	✓	3	36	2016	>27	**15**
NIST	✓		✓			✓	✓	4	327	1990	>1	**16**
Impact-Wave Analogy	✓		✓	✓	✓			3	2	2018	0	**10**

Figure 12: Results of the second analysis

The use of scoring also gives us quantitative data of which can be used to create visual representations of the comparisons, for further use in the evaluation and reflection of the frameworks. The results from the first analysis can be seen in Figure 10 and were then plotted, which can be seen in Figure 11. The detail of the score assignment is presented in detail according to the Explanation Keys shown in Table 17 and the analysis detail shown in section in Appendix D.

A second detailed analysis and comparison was performed to tabulate the characteristics of each framework with one another. This is seen in Figure 12. This means, when observing these characteristics, you may see the strengths in some and weaknesses in other and allowing the reader to determine which they deem to be a more important characteristics, by giving them the unbiased, raw information.

The characteristics determined to be suitable for this analysis were predominantly from the sources themselves. These included number of publications written about them, number of uses in industry, whether they had been tested or not, and if they were strategic or operational based frameworks. What this does is present the main traits of each framework and standard being compared in a user friendly way. The only characteristics not taken from the source is which frameworks have emphasis on pre, during, or post resilience methods, as this is to be taken from the results of the first analysis.

From the strengths identified for each characteristic, scores were given based on ranks. For instance, the year of publication column, the oldest framework was given a 6 through to the youngest which is given a 1, as it is believed the older frameworks would have had longer to develop and improve over time, hence deserving higher scores. This was the case for the latter columns. In the former columns, if they gain a tick, they gain one point.

All these were added up, and the final column is the final score of the frameworks; with all columns seen in Figure 12.

All descriptions are contained in Appendix D, including Descriptions about the reasoning's behind column "Ease of Implementation. (1 Difficult to 5 Easy)" , cells in the table and the reasoning's behind some of the choices, values for the column titled "No. of Publications Associated" with a description on the method used, the cell which meets the column "Number of Recorded uses in Industry or Tests" and the row "Human Resilient Behaviour", the column "Number of Recorded uses in Industry or Tests" with a description about the "NIS Directive" and the "NIST" rows , an explanations on the scoring and calculations.

The scores achieved in Analysis 2 can be graphically represented, seen in Figure 13.

Figure 13: Scoring graph of second analysis

3.3 Study 3 - Application of Wave Analogy Model to Shipping Operations

Note: This subsection is reflected as a book chapter in the process of publication at the time of issuing of this report.

The nature of cyber risks is distinctively different in several dimensions from other risks in shipping and transport. Some of these dimensions are indicated in Figure 14 [Sepúlveda Estay, 2017a This study explores these differences and describes the results of a research process to categorize published literature about cyber-risks in supply chain and shipping, by using the Wave Analogy of Resilience as explained in Appendix A. By using the Wave Analogy, this study describes a way of organizing this categorization, and describes how it can be used to understand both how a shipping system failure results in a cyber-attack, and how this cyber-attack will increasingly affect areas in the shipping system, from operational to strategic, until the attack is stopped.

The applicability of this framework for shipping operations can be explored by using it to identify the elements present pre- and post-event, in the case of a cyber-attack to a shipping company such as the *NotPetya* attack, which affected the shipping company AP Moller-Maersk (Maersk) in 2017 [Van Niekerk, 2018]. This attack, despite having the initial appearance of being a Ransomware, resulted to be a Wiper [Furnell and Emm, 2017], where no data recovery was possible, even if the required Bitcoin payment was carried out.

The Wave Analogy framework themes, as applied to the facts of the NotPetya attack, result in the following analysis, supported by journalistic data [Greenberg, 2018].

1. **Compliance**: Norms and regulations in the shipping industry include Global norms like ISO 27000 [Disterer, 2013], NIST SP-800-53 [Bodeau and Graubart, 2013], industry-related norms like the Danish Cyber and Information Security Strategy for the Maritime Sector [Danish-Maritime, 2019], the BIMCO Guidelines on cyber security on board ships [BIMCO, 2018], the IMO Guidelines on maritime cyber risk management [IMO, 2017b], as well as any internal guidelines of the company.

2. **Situational Awareness**: NotPetya made use of a then recently discovered Windows vulnerability (known as EternalBlue) which allowed to extract passwords when combined with another tool known as Mimikatz. Earlier in 2017, EternalBlue was known to the public after a breach of NSA files, and some time later Windows released a patch

Dimensions / Risk Types	Dimension Description	Non Cyber-risks	Cyber-risks
Latency	Delay between when the attacker accesses the ship and when the effects of the attack start	Low to medium	High latency, extending to years between penetration and action of the cyber-attack.
Physical location	Place where the attacks happen in the ship and shipping network	Localized. Geography is relevant.	Affects multiple connected locations. Geography is less relevant
Complexity	Operation units where the attack can have consequences, and the number of ways in which the attack takes place.	Limited complexity	Virtually unlimited complexity. Can affect many shipping systems simultaneously
Replication	Possibility and accuracy in which the attack can be repeated in the same location or elsewhere	No replication to highly imperfect replication	Perfect replication
Perpetuity	The amount of time during which the attack continue to take place	Limited duration.	Continuous effect until counter-acted or self-ending
Component versus interaction	Unit of attack, ranging from an attack to units in the system, to an attack happening to the communication between connected units	Shipping component risks	Interaction risks - Component communication risks
Anonymity	The identification of the source of the attacks	Traceable perpetrator	Anonymous perpetrator unless explicit hacker declaration.

Figure 14: Dimensions where traditional and cyber-risks differ for shipping operations

to EternalBlue's vulnerability. Although it has been reported that issues such as network segmentation - which contributed to the company-wide outreach of NotPetya - had been internally pointed out before [Greenberg, 2018], it seems reasonable to think that the risk of a cataclysmic cyber-event spanning their entire IT infrastructure was underestimated by Maersk, considered as either not probable or even feasible in the short-term as to prompt immediate, subsequent action. Additionally, there is no documented existence of the identification of cyber-threats to their shipping operations.

3. **Governance**: Maersk has had a Chief Information Security Officer since the year 2015, and it was one of the first major shipping companies to do so, based on its *digitalization strategy*. Maersk has therefore a hierarchy for the decision-making process of its IT infrastructure, located in England and overseeing the digital needs of the almost 80.000 employees at the company. Therefore, even though Maersk had resources to manage this governance structure, an incorrect situational awareness did not seem to trigger enough actions to prevent and mitigate the risk of a global IT meltdown.

4. **Pre-Event Knowledge Management**: The vulnerability-exploiting application EternalBlue and Mimikatz were known, but the first one was relatively recent, and a combined use of both was not widely observed before. Because of this, there was no initial knowledge on how to prevent or deal with this specific threat until it was reverse-engineered some time afterwards.

5. **Cyber-Security**: it might have been possible to prevent or reduce the impact of NotPetya from a more technical perspective, had Maersk had in place elements such as more thorough software patching policies, up-to-date operating systems and network segmentation [Greenberg, 2018]. Nonetheless, the lack of awareness regarding this specific threat made it arguably more difficult to be prepared against it. For example, Maersk reportedly managed around 150 domain controllers (servers that work as maps of the network at Maersk, and which store and communicate the rules regarding which users can access what systems) before NotPetya, which were supposed to act

as a backup for each other. Nonetheless, this did not seem to foresee the scenario in which all of them were taken down simultaneously [Greenberg, 2018]. There was no evidence found of any cyber-security or response to cyber-attack training at Maersk before the events. Additionally, as it was later found in the attack analysis, the two vulnerability-exploiting applications integrated by NotPetya were recent, but known: EternalBlue and Mimikatz.

6. **Agility**: It took two hours to disconnect Maersk's systems from the network. The recovery team at Maidenhead using clean equipment, searched for backup images of servers and domain controllers. The only unaltered (not been affected by NotPetya) copy image of this domain controller was found in a server in Ghana, due to a fortuitous power outage. This fortunate discovery was regarded as a key piece in the relatively quick reconstruction of Maersk IT infrastructure.

7. **Ability to Adapt**: Before the reconstruction brought the IT infrastructure back online, orders were reportedly being taken through improvised channels like Whatsapp, and kept track via written notes or spreadsheets instead of the previous systems used. However, without IT systems many employees were left without any means to carry out their jobs, as there was no "analogical" alternative to carry out their tasks. Moreover, many ships could not continue operations as there was no readily available way to manage the cargo. Therefore, this cyber-event severely impacted and disrupted Maersk's operations.

8. **Recovery Management**: While the NotPetya attack left Maersk's IT systems unavailable for business, there did not seem to be backup plans for alternate processes to maintain business activities without these IT systems. In order to deal with this new situation, the Group Infrastructure Services building in Maidenhead, UK, was transformed into an emergency center with a very clear purpose: rebuilding Maersk's global network as a result of the actions of the NotPetya attack.

9. **Market Position and Financial Strength**: Customers and public image were affected by this attack. Maersk estimates the costs brought by NotPetya to be valued over US$300 million. Nonetheless, their ability to survive this event can be at least partly explained thanks to their sheer size. Maersk made in 2017 a net profit of US$517 million, and their activity accounts for over 17% of the world share in container transportation, making it the biggest sea freight provider in the world.

10. **Post-Event Knowledge Management**: The mechanics of the attack became clear, as it was found that NotPetya used two system vulnerabilities, both known at the time of the attack. Maersk CEO indicated that cyber-security is viewed by the company, and after the NotPetya attack, as a competitive advantage. IT makeover is still underway. For example, Some servers in the company are still running the unsupported operative system Windows 2000. Incentives are not all aligned either. For example, IT makeover has not been carried out completely as it has not been aligned to IT executive's pay.

11. **Social Capital**: Customers and public image was affected by this attack. Some containers became lost in the system for over 3 months due to the attack and subsequent recovery process. The online Maersk reservation and status monitoring system for customers was out for several days, and the ports recovered an acceptable level of operation after more than a week from the attack. Maersk reportedly tried to reinforce customer relationships by covering at least part of the additional costs carried by their disrupted business [Greenberg, 2018]. However, not all stakeholders were treated equally as collateral damage from Maersk's disrupted operations spanned broadly.

3.4 Study 4 - Application of STPA Analysis to a CyberShip System

Note: This work in this subsection has been reflected as a journal paper in the process of publication at the time of issuing of this report.

This study explores the vulnerabilities that can be exploited, beyond component failure, by understanding the interaction between the components in a ship, through the use of the system theoretic process analysis (STPA) method, which considers both physical and cyber components.

From this analysis, two main advantages of STPA are highlighted. First, STPA uncovers more hazardous situations at the design level. Second, STPA analysis results in design recommendations to secure shipping system against cyber attacks, and independent of the source of the attacks, by focusing on the system structure.

The case

In June 2017, A.P. Moller-Maersk was the subject of an attack by a malware known as non-Petya that left its IT systems inoperable for several weeks. Beyond the immediate effects that this attack had on Maersk's bottom line, and which sources calculate as over US$300 million, this attack was another clear evidence that cyber attacks that can go beyond the loss or corruption of data to result in operational disruptions, are also a reality in the shipping industry. Authors indicate that attacks like these result in two important trends. First, remote cyber-attacks on industrial control systems have the potential for physical damage and second, the number of cyber security laws and regulations continue to increase as a result of attacks growing more severe [Tonn et al., 2019].

The non-Petya attacks is by no means an isolated event. Many other less visible attacks are happening to shipping operations every day, in a trend that is showing no signs of slowing down. Companies in the shipping industry, formerly inclined to invest mainly in cyber security, have increasing evidence that failing to avert a cyber-attack is more and more likely. Cyber-resilience, the capacity to react to cyber-attacks, becomes thus desirable, through for example, designing a system with the ability to cope with a cyber-attack already under way through DCRA resilience, namely Detection, Contention, Recovery and Adaptability.

A CyberShip is the system composed of the physical ship, human operators, all its constituent sub-systems and components, their capabilities for computation and interaction with the environment, and the interactions between these components and systems. By gathering information about present ship configurations a CyberShip model was proposed, consisting of components categorized as either critical or non-critical. A Cyber-ship model was proposed during this project and its most updated form is presented in Appendix E.

The method of analysis is the Systems Theoretic Process Approach (STPA) based on the Systems Theoretic Accident Model and Process (STAMP) framework. This is explained in section 8.2.1 in Appendix A.

The Cybership model in our study is represented by a hierarchical control structure as shown in Figure 15. This representation is consistent with literature [Hyra, 2019] [Sahay et al., 2019a]. Such a model includes cyber-physical systems that are important for the safe operation of the ship.

- **Bridge Devices:** These sense the surrounding environment and provide this information to the ship controller for centralized process control and decision making. Bridge devices can be connected to shore-side networks for software updates, or be updated through removable media such as USB. Radar, Automatic Identification System (AIS), Electronic Chart Display System (ECDIS), Global Maritime Distress System

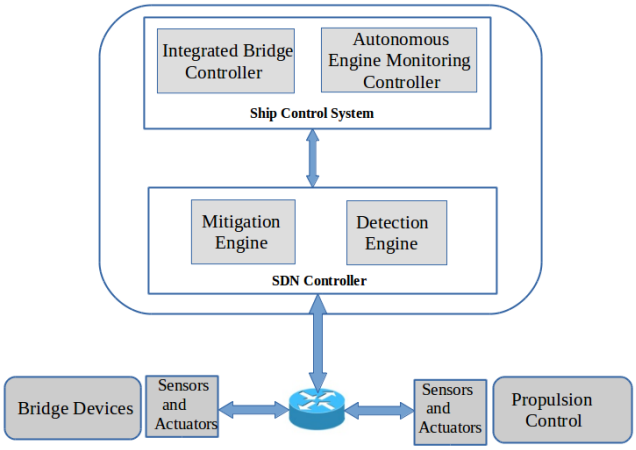

Figure 15: Basic CyberShip Framework

(GMDSS), Global Navigation Satellite System (GNSS), and Echo Sounding are examples of bridge devices on the ship.

- **Integrated Bridge Controller (IBC):** It supervises the operation of bridge devices [BIMCO, 2017] by receiving data from sensors in these devices and providing a centralized interface to the crew on-board to access the data and to make decisions. The IBC also issues control commands to the engine controller, such as start/stop of the propulsion control system, rerouting the ship, and increase/decrease water level in the ballast, depending on the information from the bridge devices.

- **Engine Controller:** It controls all the system related to power generation and propulsion [aut, 2015b]. It gathers data related to speed, rudder angle, and propeller, and it monitors the engine load, fuel consumption, and water level in the ballast compartment. Depending on the information from the integrated bridge controller, the engine controller commands and controls the to propulsion control system to increase or decrease the speed of the ship. Furthermore, it also sends the command to increase or decrease the level of water in the ballast compartment depending on the information from the bridge system.

- **Ballast Water Control:** It supervises the operation of the the ballast tank system in the ship used for draft and balance control. Ballast tanks are compartments within a ship that hold water, and which is used to provide stability, by adjusting the ship balance. If the water in the ballast tanks is pumped out temporarily, this reduces the draft of the vessel. Depending on the model of the ship, the ballast water control is independent of the engine system.

- **Propulsion Control:** It controls the propeller, rudder and steering of the ship. Propulsion control acts on the inputs from the engine control and provides the information to the engine controller such as speed of the ship, fuel level, engine load, etc.

- **Cargo Management System:** Computer systems used for the management and control of cargo may interface with a variety of other systems ashore [BIMCO, 2017]. These systems may include shipment tracking details available to shippers via the Internet. Interfaces of this kind make cargo management systems and data in cargo vulnerable to cyber attacks.

- **Human factors** also have to be considered in a cyber-ship model, as only in highly automated shipping systems there is no expected interaction between human opera-

tors and the shipping system. Examples of human factors that can have a disruptive effect through cyber-attacks include events such as unauthorized system entry (software level) or rewiring (hardware level).

A high level control diagram is represented in Figure 16. In the first step, we identify unacceptable losses/accidents (A) and hazards (H) that can lead to these accidents, followed by the identification the inadequate/unsafe control actions (UCA) designed in the system that can lead to these H and A [Leveson, 2011]. Table 9 the identified A and H, and some UCA are listed in Table 10,referring to the control actions (CA) `start pump` from Engine Controller (EC) to the ballast pump.

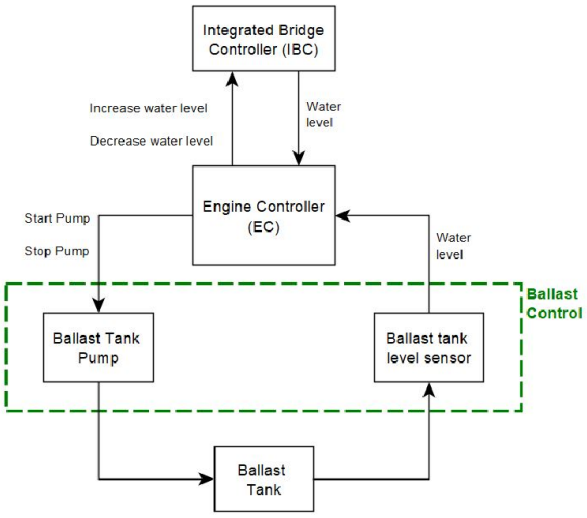

Figure 16: High-level Structure of the ballast control

Table 9: Undesirable Accidents (A) and Hazards(H)

A1	Shipment late or non arriving	H1	Uncontrolled maneuvering of the ship
A2	Loss/harm to life of passengers/crew	H2	Unidentified cargo items/wrong cargo data
A3	Wrong or non delivery to customers	H3	Incorrect functioning of ship components
A4	Damage to the ship	H4	Uncontrolled transmission of data
A5	Damage to the cargo	H5	Uncontrolled data being transmitted
A6	Reputational loss		

For instance, `start pump` action leads to increase or decrease of the level of water in the ballast tank. Increase or decrease of the water to a wrong level in the ballast tank can imbalance the ship (H1), which can damage the ship (A4). This may be caused by the EC having received wrong parameters from the Integrated Bridge Controller which can cause EC to initiate `start pump` action with the wrong parameters. The `Start pump` action can cause hazards in different conditions. For instance, if the ship is sailing through a shallow or deep water, then it may require to increase or decrease the level of water in the ballast tank to balance the ship depending on the scenario.

However, if the `Engine Controller` is compromised by an external adversary or is not functioning properly because of the component failure then it can damage the ship. This example highlights a main advantage of this methodology that the individual components are working well but the vulnerability lies in the interaction between different components.

The analysis of unsafe control actions is used to suggest design requirements and constraints. These suggestions result from the conditions where the control actions become

unsafe. For example the following constraint should be specified: the `start pump` action must not be provided if the water level information is not received from `Integrated Bridge Controller`. This responds directly to **UCA1.4**. The specific implementation of this constraint is not specified, as it can be achieved in different ways.In the same way, a requirement (a risk boundary) should be set to avoid the increase or decrease of water level in the ballast tank to a dangerous level. This boundary will provide protection against commands issued from a compromised `Integrated Bridge Controller` to `Engine Controller` with wrong water level information, or avoid damage caused in case the `start pump` action is applied for too long or too short time.Table 11 contains system constraints and requirements that can be proposed for scenarios derived from this analysis.

3.5 Study 5 - Compare the STPA frameworks with other industrial frameworks

This part of the work presents the partial results of an empirical study to determine the fitness of the use of STPA method for cyber risk evaluation with respect to other following risk analysis frameworks. Specifically STPA is evaluated against the CORAS method.

By detailing the STPA's fitness to other standards, this paper highlights the critical factors for the use of STPA for industrial compliance, details the opportunities for STPA development, and provides evidence for the potential of more extensive use of STPA in the evaluation of cyber-risks in Cyber-Physical Systems (CPS).

The CORAS method is a modelling language and procedure for the discovery of risks and threats [Den Braber et al., 2007] through the use of the Unified Modeling Language (UML). The use of UML aids in the description of the evaluation target at an appropriate level of abstraction, facilitates communication and interaction between stakeholders, and serves as an explicit method for documenting assumptions and the analysis of result for subsequent improvement or maintenance [den Braber et al., 2003].

The CORAS method has been successfully used in the risk analysis of web applications [Dimitrakos et al., 2002], social networks[Larionovs et al., 2015], tele-medicine services [Stamatiou et al Internet of things-IoT [Jensen, 2018], in the analysis of the risk and threats of systems over time [Lund et al., 2011], and in the risk assessment of SCADA systems [Cherdantseva et al., 2016].

The analysis is performed on part of the CyberShip Model presented in Appendix B. The method comparisons are indicated in Table 12, Table 13.

Table 12: Comparison of method phases

Phase	STPA	CORAS
Preparation	*System objective*: identify the goal for which the system is designed and system boundaries	*Preparation for the Analysis*: clarify the target of the analysis
Definitions	*Define Unacceptable Losses*: list the outcomes which have to be avoided *Identify System Structure*: list the controls, process models, processes and operators and their connections, including hierarchy	*Customer Presentation of Target*: Customer presents the system to be analyzed and the purpose of this analysis. *Refine the Target*: description of the system using asset diagrams
Identifications	*Identify Hazards*: list system state or conditions that with environmental worst-case scenario, lead to an unacceptable loss *Identify requirements and constraints*: list the controls by presence (passive) and the controls by action (active) through detection, measurement, diagnosis or response	*Approval of Target Description*: agreement about scales for likelihood and consequences, and risk evaluation criteria. *Risk identification*: workshop with experts to identify unwanted incidents, threats, vulnerabilities and threat scenarios, and reflect them in a threat diagram.
Estimation	*Describe Unsafe Control Actions (UCA)*: list conditions when each control action or their lack creates a hazard. List hazards through degradation over time	*Risk estimation*: quantify likelihoods through a structured brainstorming session and reflecting this in a threat diagrams
Evaluation	*Evaluate Unsafe Control Actions*: list causal scenarios and additional constraints from the UCA analysis	*Risk evaluation*: determine acceptable risks from those that should be further evaluated in direct and indirect assets
Treatment	*Additional requirements*: list the additional design requirements to implement the additional constraints	*Risk treatment*: identify and analyze treatments for unacceptable risks

Table 13: Comparison of methods characteristics

Characteristic	STPA	CORAS
Applicability	It can be used at any stage of the system lifecycle [Leveson, 2011]	Not identified
Level of expertise required	Knowledge about the system components, and connections	Knowledge about structure component, connections and external threats

Table 14: Comparison of tools for each method and phase

Phase	STPA Tools	CORAS Tools
Preparation	No specific tool	No specific tool
Definition	Hierarchical Control Diagram	Asset Diagrams
Identification	Hierarchical Control Diagram	Threat Diagrams
Estimation	Unsafe Control Action Matrix	Brainstorming & Threat Diagrams
Evaluation	Unsafe Control Action Matrix	Risk Diagrams
Treatment	No specific tool	Treatment Diagrams

4 Discussion

The papers in the sample evidence both the increasing interest that cyber resilience frameworks is receiving in academic research, and the variety of approaches that are being proposed to understand how a CRF can be designed and implemented. The approach variety is reflected at least in the the number of different attacks that are addressed in the CRFs proposed, and in the methodologies that are used.

Out of the 136 journals included in the paper sample, 20% of the journals only contain 92 articles (44,2% of the total). This high dispersion in the publication density is an indication that there is as yet no clear focus for the research of CRF. This can also be understood from the number of different areas (25) where this research is taking place.

The categories proposed by the *wave Analogy* model as presented in Figure 19 facilitate a relevant structure for the description, from the papers in the `synthesis sample`, of the current state of CRF research. According to Figure 9 the category with most `synthesis sample` publications is *Pre-event knowledge Management*, which considers the risk analysis of vulnerabilities and their economic, legal and operational implications. The categories that follow it in number of `synthesis sample` papers addressing the *Security* of Cyber-Physical systems, the *Visibility* of cyber-Physical systems and their *Adaptability* once the events have occurred.

This category analysis also shows that most of the research have been focused in operational aspects of cyber resilience, with only a few articles in the `synthesis sample` about the more strategic *Governance* or *Social Capital*. The relative difference in numbers between CRF papers about Strategy with respect to Operations is a reflection of the preferred approach for containment of disruptions from cyber-attacks by using a CRF, this is mainly in the operational plane rather than an approach of design for avoidance or for the response to disruptions.

Multiple operational disruptions originating from cyber-attacks are strong evidence that response and recovery from a cyber-disruption is not the last resource when prevention has failed, but in many cases is a strategy in itself, particularly when dealing with systems that are so complex that it is infeasible to analyze and prevent every way in which the system can fail.

The collaboration between countries in the development of CRFs was also found to be a relevant difference between the papers in the `synthesis sample`. A majority of the researcher countries in the sample, 61,7%, have chosen to collaborate in the development of CRFs, as can be seen in Table 3. Only 17% of the researcher countries carried out exclusively non-collaborative papers, while in contrast 31% of the researcher countries delivered exclusively collaborative research. It is the understanding of this team that a de-centralized problem such as cyber-attacks with operational disruption not only needs a global approach to respond to the effects of these attacks, but also will benefit from multiple points of view in order to propose effective and innovative CRFs.

In regard to the opportunities for collaboration, this paper provides both an introductory overview of the CRFs as proposed in literature and a categorization of these CRFs, as enablers for collaboration. The industry areas are presented in Table 6 , Table 7 presents the attacks that are addressed in current CRFs, and Table 8 lists the methods used and the research institutions using these methods.

The analysis shown in this paper makes evident that in future a deeper look is possible, for an analysis of CRFs in specific methodological areas, industrial applications or related to specific attack types, for example.

The network analysis that has been explored in this paper is a way of representing the relationships between countries and their collaborations in Figure 7 or countries represent

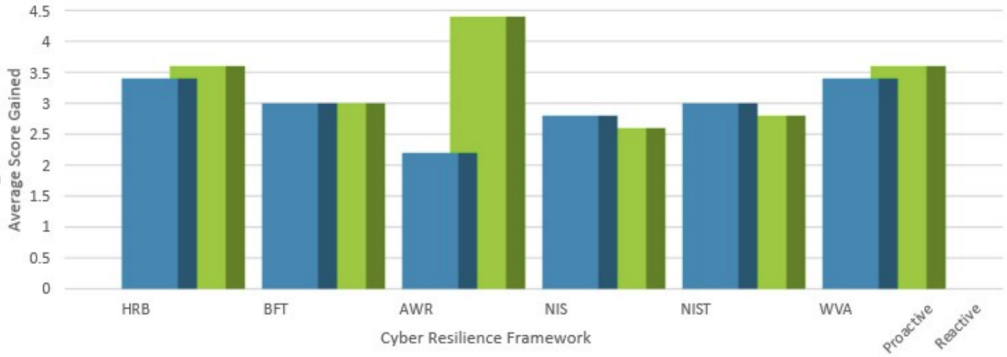

Figure 17: Average Scores for First Analysis

quantitatively the current state of the relationships found in the `synthesis sample`. As shown in Table 4, a network analysis found 12 relevant communities, with an *Average Clustering Coefficient* of 0,497, meaning that on average nodes are connected to 49% of all the nodes in the network. This average connectivity is driven by highly connected nodes (countries) like USA and China, which compensate for isolated nodes such as South Africa or North Ireland, for example. This contrast between highly connected nodes and nodes with a low connection can be seen in the *Graph Density* measure with a value of 0,117, meaning that only 11,7% of all possible connections are present in the network.

The work presented in this paper has followed a rigorous, structured approach to the gathering and analysis of information to advance the knowledge about CRFs. However, in future other sources of knowledge should be used, particularly when considering a rapidly developing area such as cyber-resilience. In the process of gathering the sample that has been analyzed and presented in this paper, our team found numerous reports by private institutions about the proposal of CRFs. These data sources have not been included in this review, as they are not peer reviewed. However, these are important references to the industrial application of CRFs. It is not clear how these reports eventually become scientific, published, peer-reviewed work. Due to the rapid development of the topic of cyber resilience, future scientific work should both address the proposal of methods to use information contained in industrial reports, to counter act the existing relatively slow publishing cycles.

As identified in Analysis 1 and illustrated in Figure 17, the results that some frameworks and standards can proactively protect infrastructures and systems better than reactive protection are seen. This is only seen for the NIST and NIS Directive standards, as the remaining frameworks appear to react to cyber events more effectively than prepare and try to stop them. This, is seen evidenced in the AWaRE framework, which is reactive; however, it is poor on its proactive defence.

For the remaining three frameworks, they are well balanced between reactive and proactive techniques for cyber resilience. Combining the proactive and reactive averages, displays the greatest frameworks and standards; this being displayed in Figure 4.2. Whilst all frameworks and standards could be considered the best, the joint best frameworks from this analysis are the human behavioural resilience strategy and the wave analogy framework. Figure 17 and Figure 18 place emphasis on the differences between proactive and reactive techniques. The ones which can deal with both will be the most useful of the models.

Only one stands out as being unsuitable for a balanced resilience system; that being AWaRE. As it does not appear to place enough emphasis on preventative measures, it will be susceptible to a cyber event; but, with a greater focus on reactive resilience, it has the capacity to positively recover.

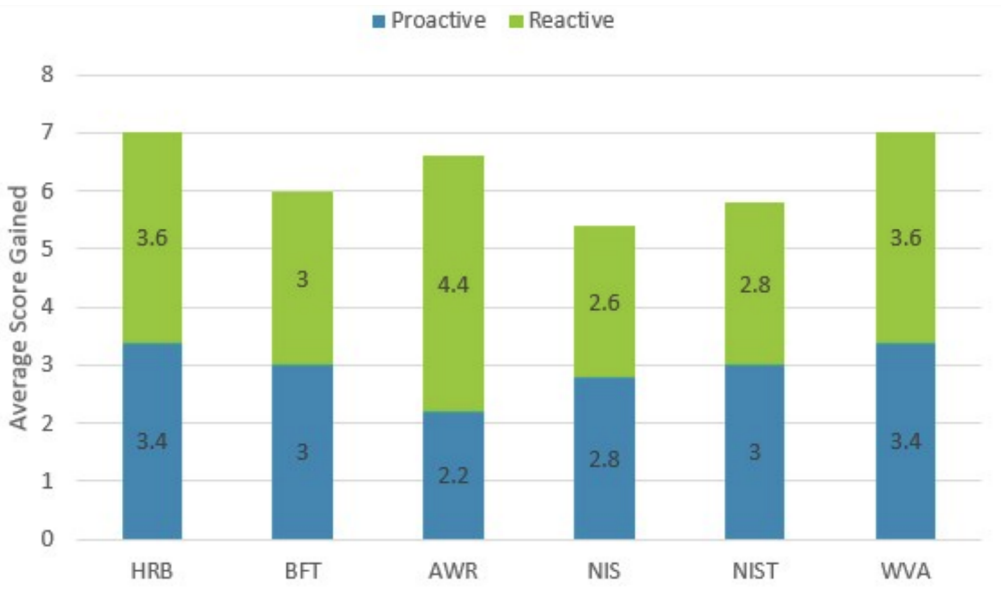

Figure 18: Scoring graph of second analysis

The second Analysis described the characteristics of each identified framework and standard used in this part of the study. A final score was assigned to each framework, and the results from this can be seen in Figure 13.

To begin with, AWaRE and the Wave Analogy have scored the joint lowest of 10 each. This is primarily due to them being new frameworks with little to no publications, no industry uses, and neither have had much of an opportunity for development or to prove themselves.

BFT++ scores a bit better, but has similar problems, as it is new on the cyber security scene. Its score of 12.5 is gained due to it being tested and ease of implementation. The next highest scoring framework or standard is the NIS Directive and NIST, with scores of 15 and 16 respectively.

With a lot of information available about them, being well developed over time, and having a ease of implementation; they gain good scores. The highest-ranking framework is the Human Resilient Behaviour with a respectable score of 22. Although, being the newest of the whole selection of frameworks and evidencing little development in terms of actual cyber resilience, the link between quality and resilience is central for its success here. It has a good amount of publications linked to it, and has a comprehensive implementation strategy. The analysis has shown which frameworks have been comprehensively developed and tested. Analysis 2 verifies and gives trust to all organisations thinking of implementing the framework into their system.

The Wave Analogy scores well in comparison to the identified frameworks and standard in the first analysis. It has the joint highest score average and is consistently high in mostly all categories, as shown in Figure 11.

Its other factors, such as social capital, governance, and velocity, make the Wave Analogy Model a very effective framework in which organisations, governments, and institutions can build cyber resilience into its structure. This, in the end, may mean greater profits, higher rates of efficiency, and general growth of the industry.

The Wave Analogy does not score well in the second analysis, primarily due to its lack of development and having only been created two years prior to this study being written.

The positives, however, are that it displays a well-rounded approach to cyber resilience compared to its counterparts in this study, it follows the trend of being a strategic framework. When compared to a operational framework its ability to fit in in the field is high.

Furthermore, it is well described and clearly defined, making its use by organisations and implementation easier.

Unfortunately, the Wave Analogy's weaknesses are its lack of recognition in the industry and scientific community, due to its recent appearance and being underdeveloped and untested. This analysis identifies the areas for improvement for all the frameworks being compared here, especially the Wave Analogy, with its need for greater name recognition being its greatest barrier to becoming a practical, effective, and distinguished cyber resilient tool.

Strengths of the Wave Analogy Model

- **Detailed understanding of a Cyber Event**: The Impact-Wave Analogy gives the user of the framework a detailed understanding of the before, during, and after stages of a cyber event, and the actions to be considered to mitigate the negative consequences of it.
- **Use of Non-Technical Strategies in its Framework**: Different organisations will have differing levels of technological capabilities and understandings. The Impact-Wave Analogy has given all users the ability to understand what they need to consider to maximise the effectiveness of their cyber defence. For example, considering compliance standards or developing a pre-event knowledge management plan which may not have been considered.
- **Flexibility**: As seen in the results of the first analysis (which can be found in subsection 3.2), the Wave Analogy consistently scores highly for implementation of the tools. This is useful for a variety of organisations offering differing needs and requirements meaning a flexible framework is needed such as the Impact-Wave Analogy.
- **Accounting of During a Cyber Event**: Shown in the second analysis (which can be found in subsection3.2), the Wave Analogy is one of the few frameworks which takes the "during" section of a cyber event into account as being part of the strategy for defence. Organisations which take this type re-activeness as a priority will be able to deal with such incidents, and not have to wait for them to end, and then deal with the aftermath.

Weaknesses of the Wave Analogy Model

- **Lack of Technical Detail**: Although there is potential for its implementation for low technological organisation, the Wave Analogy does not make clear which of its stages are technical and which are not. This could be achieved by clarifying what types of resources should be allocated to each stage. For example stating the legal department is responsible for the compliance and governance stages, or pre and post knowledge management to specialised departments or contractors; could make implementation of this framework a lot easier. On the other hand, the ambiguity of the directions of use widen the applicability for some industries, which is similar to the NIST SP 800 and NIS Directive Standards.
- **Underdeveloped**: Clearly displayed in the results of the second analysis (in subsection 3.2) the Wave Analogy suffers from a lack of development and implementation in organisations, a requirement for further validation.

In general, the ripple effect of the NotPetya attack to Maersk can be clearly drawn out from the perspective of this framework, where it can be observed how the elements preceding the cyber-event were not adequately aligned to face the incoming threat, while an intensive use of resources was necessary to absorb the impact of that event on Maersk. Moreover, this analysis presents the following advantages:

- The data about a cyber-attack is organized into the different themes, providing a structure.
- This framework structure organizes the knowledge about a company and the attack into aspects that range from tactical to strategic.
- By following the framework from the point of attack towards the outer mitigation levels, it is possible to understand the progression of an attack. For example, market position was fundamental to their survival because of ineffective "ability to adapt" in the short term, and to support the extensive Recovery Management measures for this scenario.
- By identifying measures in each level, a record of best and worst practices can be created.

The increased vulnerabilities due to the multiple control systems present in modern CyberShips challenge security and continuity of operations in new ways. Traditional methods for risk analysis present relevant shortcomings when applied to complex systems and when considering risks that do not involve the failure of components, features own to CyberShip systems. The application of the Systems Theoretic Process Analysis method (STPA) helps address these points.

By focusing the risk analysis on the CyberShip design structure rather than on the threat, a number of different threats, both known and unknown, are addressed through the design-by-requirement process that results from the STPA analysis.

By considering different levels of aggregation, STPA is used to analyse a complex CyberShip system for risk and response, all the way from restrictions and requirements that are system-wide, drilling down to requirements that are control-system-specific, whenever necessary.

Finally, by analyzing the CyberShip system structure to determine risk and response instead of focusing on the threats, STPA both delivers results without the need for historical information to identify risks and requirements, and detects risks that result from faulty design beyond the need of component failure.

5 Potential Future Work

The structured literature review of cyber resilience frameworks published in peer-reviewed journals presents a number of limitations.

First, the publication process in peer-reviewed journals results in a time lag between the CRFs included in this work and the ones actually available in extant scientific literature. Future work to address this is therefore regular updates to this analysis.

Second, the use of peer-reviewed journals excludes a number of sources of information, particularly papers and reports about CRFs that have been published either in moderated or non-peer reviewed journals (e.g., ArXiv [Ginsparg, 2011]) or that have been published as reports by research institutions (e.g., MITRE Corporation [Taub, 1993], RAND Corporation [Fisher and Walker, 1994]), despite their reputation. Related future work is therefore the

inclusion of these works alongside a discussion about the validity of including research that has not been peer-evaluated before publication. Additionally, future related work could thus consider innovative dimensions for validation of non-peer reviewed publications, such as measures of reputation of the entity that produced them, or the number of citations of such publications.

Third, the search process considered specific keywords. This selection can be broadened. For example, future related work could include the identification of the main terms used in the publication of CRFs, for the refinement of paper sample selection.

Finally, this work has not been concerned with defining what a CRF should contain, but rather with the description and content analysis of the CRFs that have been proposed. Through the analysis developed in this paper, common themes are highlighted to promote collaboration. Future work lies in the analysis of the requirements that a CRF should fulfill and the evaluations of existing CRFs with respect to such requirements.

6 Conclusion

The SLR and subsequent analysis to identify existing research on cyber-resilience frameworks for cyber attacks identified the main research areas, the application areas, the attack types which are addressed by the CRFs, and the main methodologies used by these CRFs to understand different threat types.

This part of the work will assist cyber security community to know the Universities, organizations, countries and people working on designing and developing cyber resilience frameworks, particularly i their application to CyberShips. Furthermore, it will help the cyber security community to collaborate and and work towards addressing the existing challenges faced by cyber resilience frameworks.

The conclusion of the Wave Analogy comparison CRFs suggests the strengths and weaknesses of the Wave Analogy and recommendations for the use of the reviewed frameworks. The findings indicate that the Impact-Wave Analogy suffers from a lack of testing and implementation to prove its capabilities. That was its primary weakness compared to the other frameworks. However, it was adaptable, clear, and accounted for all stages of cyber resilience. Overall, the Wave Analogy is a very good cyber resilience model, but until it can be tested in some capacity, it will lack being a completely capable cyber resilience framework.

7 References

[ABB, 2014] (2014). Cyber threat to ships – real but manageable. Technical report, ABB. 2

[Mun, 2014] (2014). Process map for Autonomous Navigation. Technical report, MUNIN:Maritime Unmanned Navigation through Intelligence in Network.

[aut, 2015a] (2015a). Final Report:Autonomous Bridge. Technical report, MUNIN:Maritime Unmanned Navigation through Intelligence in Network.

[aut, 2015b] (2015b). Final Report:Autonomous Engine Room. Technical report, MUNIN:Maritime Unmanned Navigation through Intelligence in Network. 3.4, 5

[llo, 2016] (2016). Cyber-enabled ships:Deploying information and communications technology in shipping. Technical report, Lloyd Register.

["a10networks - Ahmad Nassiri", 2018] "a10networks - Ahmad Nassiri" (2018). "5 MOST FAMOUS DDOS ATTACKS".

[Abraham and Nair, 2018] Abraham, S. and Nair, S. (2018). Comparative analysis and patch optimization using the cyber security analytics framework. *Journal of Defense Modeling and Simulation*, 15(2):161–180. 5, 6, 8

[Adamsky et al., 2018] Adamsky, F., Aubigny, M., Battisti, F., Carli, M., Cimorelli, F., Cruz, T., Di Giorgio, A., Foglietta, C., Galli, A., Giuseppi, A., Liberati, F., Neri, A., Panzieri, S., Pascucci, F., Proenca, J., Pucci, P., Rosa, L., and Soua, R. (2018). Integrated protection of industrial control systems from cyber-attacks: the atena approach. *International Journal of Critical Infrastructure Protection*, 21:72–82. 5, 6, 8

["Adremsoft", 2019] "Adremsoft" (2019). "Essential Free Tollkit For Network Professionals That Runs On Windows".

["Adverse events dangerous but preventable", 2010] "Adverse events dangerous but preventable" (2010). "SNSPMS - Carmen Angheluta".

["AFP news agency", 2009] "AFP news agency" (2009). "Canadian crew foils Somali pirate attack.".

[Agnarsson et al., 2016] Agnarsson, G., Greenlaw, R., and Kantabutra, S. (2016). On cyber attacks and the maximum-weight rooted-subtree problem. *Acta Cybernetica*, 22(3):591–612. 5, 8

[Agrafiotis et al., 2018] Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., and Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1). 5, 8

[Ahmed et al., 2015] Ahmed, K., Blech, J. O., Gregory, M. A., and Schmidt, H. (2015). Software defined networking for communication and control of cyber-physical systems. In *2015 IEEE 21st International Conference on Parallel and Distributed Systems (ICPADS)*, pages 803–808.

[Akhmetov et al., 2018] Akhmetov, B. B., Lakhno, V. A., and Malyukov, V. P. (2018). Model of cyber security financing within the framework of the bilinear differential quality game scheme. *Radio Electronics, Computer Science, Control*, 0(3). 5, 6, 8

[Al-Dabbagh et al., 2017] Al-Dabbagh, A. W., Li, Y., and Chen, T. (2017). An intrusion detection system for cyber attacks in wireless networked control systems. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 65(8):1049–1053. 5, 6

[Al-Gburi and Mohd Ariff, 2019] Al-Gburi, Q. A. and Mohd Ariff, M. A. (2019). Dynamic security assessment for power system under cyber-attack. *Journal of Electrical Engineering and Technology*, 14(2):549–559. 5, 6, 7, 8

["Aleksei Fjodorov", 2017] "Aleksei Fjodorov" (2017). "Software defined radio implementation of marine AIS".

[Ali et al., 2017] Ali, A., Mahfouz, A., and Arisha, A. (2017). Analysing supply chain resilience: integrating the constructs in a concept mapping framework via a systematic literature review. *Supply Chain Management: An International Journal*, 22(1):16–39.

[Alqahtani, 2015] Alqahtani, A. (2015). Towards a framework for the potential cyber-terrorist threat to critical national infrastructure. *Information and Computer Security*, 23(5):532–569. 6, 8

[Alsaleh et al., 2017] Alsaleh, M. N., Al-Shaer, E., and Husari, G. (2017). Roi-driven cyber risk mitigation using host compliance and network configuration. *Journal of Network and Systems Management*, 25(4):759–783. 5, 8

[Alsmadi and Xu, 2015] Alsmadi, I. and Xu, D. (2015). Security of software defined networks: Asurvey. *Computers & Security*, 53:79 – 108.

[Altabbakh et al., 2014] Altabbakh, H., AlKazimi, M. A., Murray, S., and Grantham, K. (2014). Stamp–holistic system safety approach or just another risk model? *Journal of loss prevention in the process industries*, 32:109–119. 8.2.1

["Amazing Inventions", 2018] "Amazing Inventions" (2018). "Somali Pirates vs USA & Russian private security guards 2018 #4".

[Andrijcic and Horowitz, 2006] Andrijcic, E. and Horowitz, B. (2006). A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property. *Risk analysis*, 26(4):907–923. 6, 8

[Antoine, 2013] Antoine, B. (2013). *Systems Theoretic Hazard Analysis (STPA) applied to the risk review of complex systems: an example from the medical device industry*. PhD thesis, Massachusetts Institute of Technology. 8.2.1

[Arbor Networks, 2016] Arbor Networks (2016). Worldwide Infrastructure Security Report. Technical report, Arbor Networks.

["Army Intelligance",] "Army Intelligance". "Why Systems are Vulnerable. There are many reasons why systems are vulnerable to attack.".

["ARS Technica - Peter Bright", 2018] "ARS Technica - Peter Bright" (2018). "Here's how, and why, the Spectre and Meltdown patches will hurt performance".

["ArsTechnica - Sean Gallagher", 2015a] "ArsTechnica - Sean Gallagher" (2015a). "Hacked at sea: Researchers find ships' data recorders vulnerable to attack".

["ArsTechnica - Sean Gallagher", 2015b] "ArsTechnica - Sean Gallagher" (2015b). "Navy re-ups with Microsoft for more Windows XP support".

[Ashok et al., 2017] Ashok, A., Govindarasu, M., and Wang, J. (2017). Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proceedings of the Ieee*, 105(7):7936473, 1389–1407. 5, 6, 8

[Ashtiani and Abdollahi Azgomi, 2014] Ashtiani, M. and Abdollahi Azgomi, M. (2014). A distributed simulation framework for modeling cyber attacks and the evaluation of security measures. *Simulation*, 90(9):1071–1102. 5, 6, 8

["ASIC",] "ASIC". "Safety Management and Control System". 12

[Atoum and Otoom, 2017] Atoum, I. and Otoom, A. (2017). Effective belief network for cyber security frameworks. *International Journal of Computers*, 11:117–22, 117–122. 6, 8

["Attainable Adventrue Crusing", 2013] "Attainable Adventrue Crusing" (2013). "NMEA 2000—Missing the Obvious".

[Awan et al., 2016] Awan, M. S. K., Burnap, P., and Rana, O. (2016). Identifying cyber risk hotspots: A framework for measuring temporal variance in computer network risk. *computers & security*, 57:31–46. 5, 6, 8

[Babiceanu and Seker, 2019] Babiceanu, R. F. and Seker, R. (2019). Cyber resilience protection for industrial internet of things: A software-defined networking approach. *Computers in Industry*, 104:47–58. 5, 6, 8

[Babineau et al., 2012] Babineau, G. L., Jones, R. A., and Horowitz, B. (2012). A system-aware cyber security method for shipboard control systems with a method described to evaluate cyber security solutions. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pages 99–104. 2

[Baig and Zeadally, 2019] Baig, Z. and Zeadally, S. (2019). Cyber-security risk assessment framework for critical infrastructures. *Intelligent automation and soft computing*, 25(1):121–129. 5, 6, 8

[Banda et al., 2019] Banda, O. A. V., Kannos, S., Goerlandt, F., van Gelder, P. H., Bergström, M., and Kujala, P. (2019). A systemic hazard analysis and management process for the concept design phase of an autonomous vessel. *Reliability Engineering & System Safety*, 191:106584. 8.2.1

[Banghart et al., 2018] Banghart, M., Babski-Reeves, K., Bian, L., and Strawderman, L. (2018). Subjectivity in failure mode effects analysis (fmea) severity classification within a reliability centered maintenance (rcm) context. *International Journal of Aviation, Aeronautics, and Aerospace*, 5(1):2.

[Barenji et al., 2019] Barenji, R. V., Akdag, Y., Yet, B., and Oner, L. (2019). Cyber-physical-based pat (cpbpat) framework for pharma 4.0. *International journal of pharmaceutics*. 5, 6, 8

[Barreto and Costa, 2019] Barreto, A. B. and Costa, P. C. (2019). Cyber-argus-a mission assurance framework. *Journal of Network and Computer Applications*, 133:86–108. 5, 6, 8

["BBC News - Chris Baraniuk", 2017] "BBC News - Chris Baraniuk" (2017). "How hackers are targeting the shipping industry".

[Becker and Gould, 2019] Becker, L. T. and Gould, E. M. (2019). Microsoft power bi: Extending excel to manipulate, analyze, and visualize diverse data. *Serials Review*, 45(3):184–188. 10.2

[Beg et al., 2017] Beg, O. A., Johnson, T. T., and Davoudi, A. (2017). Detection of false-data injection attacks in cyber-physical dc microgrids. *IEEE Transactions on industrial informatics*, 13(5):2693–2703. 6, 7, 8

["Belltower Hrc", 2015] "Belltower Hrc" (2015). "Seagull Maritime Security".

[Ben-Itzhak et al., 2015] Ben-Itzhak, Y., Barabash, K., Cohen, R., Levin, A., and Raichstein, E. (2015). Enforsdn: Network policies enforcement with sdn. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 80–88.

[Bensing, 2009] Bensing, R. (2009). An assessment of vulnerabilities for shipbased control systems. Master's thesis, Naval Postgraduate School. 2

[Bergin, 2015] Bergin, D. L. (2015). Cyber-attack and defense simulation framework. *Journal of Defense Modeling and Simulation*, 12(4):383–392. 6, 8

["Better Embedded System SW - Phil Koopman - Carnegie mellon University", 2012] "Better Embedded System SW - Phil Koopman - Carnegie mellon University" (2012). "Controller Area Network (CAN) Protocol Vulnerabilities".

[Bezzaoucha et al., 2018] Bezzaoucha, S., Voos, H., and Darouach, M. (2018). Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems. *European Journal of Control*. 6, 8

[BIMCO, 2017] BIMCO (2017). The Guidelines on Cyber Security Onboard Ships. Technical report, BIMCO. 2, 3.4, 6

["BIMCO", 2018] "BIMCO" (2018). "Cyber Security Survey Shows More Action is Needed In The Industry".

[BIMCO, 2018] BIMCO (2018). The guidelines on cyber security on board ships, version 3. 1

["BIMCO, CLIA, ICS, and others", 2018] "BIMCO, CLIA, ICS, and others" (2018). "The Guidelines On Cyber Security Onboar Ships". 12

[Björck et al., 2015] Björck, F., Henkel, M., Stirna, J., and Zdravkovic, J. (2015). Cyber resilience–fundamentals for a definition. In *New contributions in information systems and technologies*, pages 311–316. Springer.

["Blank Rome LLP - American Association of Port Authorities - Kate B. Belmont", 2016] "Blank Rome LLP - American Association of Port Authorities - Kate B. Belmont" (2016). "Maritime Cybersecurity: Cyber Cases in the Maritime Enviornment".

["Blog of Lasse Karstensen - Varnish, Sailing and occasional weekend hacks", 2016] "Blog of Lasse Karstensen - Varnish, Sailing and occasional weekend hacks" (2016). "NMEA2000 and CANbus".

[Blondel et al., 2008] Blondel, V. D., Guillaume, J.-L., Lambiotte, R., and Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of statistical mechanics: theory and experiment*, 2008(10):P10008. 4

[Bodeau and Graubart, 2013] Bodeau, D. and Graubart, R. (2013). Cyber resiliency and nist special publication 800-53 rev. 4 controls. *MITRE, Tech. Rep.* 1

[Bodeau et al., 2010] Bodeau, D. J., Graubart, R., and Fabius-Greene, J. (2010). Improving cyber security and mission assurance via cyber preparedness (cyber prep) levels. In *2010 IEEE Second International Conference on Social Computing*, pages 1147–1152. IEEE. 1.1

[Boyes, 2015] Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, 5(4):28.

[Bretas et al., 2019] Bretas, A. S., Bretas, N. G., and Carvalho, B. E. (2019). Further contributions to smart grids cyber-physical security as a malicious data attack: Proof and properties of the parameter error spreading out to the measurements and a relaxed correction model. *International Journal of Electrical Power and Energy Systems*, 104:43–51. 5, 6, 7, 8

["Brookings - Jack Karsten and Darrel M. West", 2016] "Brookings - Jack Karsten and Darrel M. West" (2016). "A brief history of U.S encrytpion policy".

[Brown III, 2019] Brown III, H. (2019). Spcta: An analytical framework for analyzing cyber threats by non-state actors. In *Multigenerational Online Behavior and Media Use: Concepts, Methodologies, Tools, and Applications*, pages 135–158. IGI Global. 6

[Canepa and Claudel, 2013] Canepa, E. S. and Claudel, C. G. (2013). Spoofing cyber attack detection in probe-based traffic monitoring systems using mixed integer linear programming. In *2013 International Conference on Computing, Networking and Communications (ICNC)*, pages 327–333. IEEE. 5, 6, 7, 8

[Cardoza and Wagh, 2017] Cardoza, C. and Wagh, R. (2017). Text analysis framework for understanding cyber-crimes. *International Journal of Advanced and Applied Sciences*, 4(10):58–63. 5, 8

[Carey et al., 2011] Carey, S., Lawson, B., and Krause, D. R. (2011). Social capital configuration, legal bonds and performance in buyer–supplier relationships. *Journal of operations management*, 29(4):277–288.

["Carnegie Endowment For International Peace - A.VAEZ, K. SADJADPOUR", 2013] "Carnegie Endowment For International Peace - A.VAEZ, K. SADJADPOUR" (2013). "Iran's Nuclear Odyssey: Costs and Risks".

["Carnegie Mellon University - Eushiuan Tran", 1999] "Carnegie Mellon University - Eushiuan Tran" (1999). "Multi-Bit Error Vulnerabilities in theController Area Network Protocol".

["Carnigie Mellon University - Software Engineering Institute", 2001] "Carnigie Mellon University - Software Engineering Institute" (2001). "2001 CERT Advisories".

["CBS News - Jonathan Berr", 2017] "CBS News - Jonathan Berr" (2017). "WannaCry ransomware attack losses could reach $4 billion".

[Chakhchoukh and Ishii, 2014] Chakhchoukh, Y. and Ishii, H. (2014). Coordinated cyber-attacks on the measurement function in hybrid state estimation. *IEEE transactions on power systems*, 30(5):2487–2497. 3.1, 5, 6, 8

[Chandra and Shang, 2017] Chandra, Y. and Shang, L. (2017). An rqda-based constructivist methodology for qualitative research. *Qualitative Market Research: An International Journal*. 10.2

[Chejerla and Madria, 2017] Chejerla, B. K. and Madria, S. K. (2017). Qos guaranteeing robust scheduling in attack resilient cloud integrated cyber physical system. *Future Generation Computer Systems*, 75:145–157. 5, 6, 8

[Chen et al., 2018] Chen, B., Ho, D. W., Hu, G., and Yu, L. (2018). Secure fusion estimation for bandwidth constrained cyber-physical systems under replay attacks. *Ieee Transactions on Cybernetics*, 48(6):1862–1876. 5, 7, 8

[Chen, 2016] Chen, J. Q. (2016). Deception detection in cyber conflicts: A use case for the cybersecurity strategy formation framework. *International Journal of Cyber Warfare and Terrorism*, 6(3):31–42, 31–42. 6, 8

[Cherdantseva et al., 2016] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., and Stoddart, K. (2016). A review of cyber security risk assessment methods for scada systems. *Computers & security*, 56:1–27. 3.5

[Chhabra et al., 2018] Chhabra, G. S., Singh, V., and Singh, M. (2018). Hadoop-based analytic framework for cyber forensics. *International Journal of Communication Systems*, 31(15):e3772. 5, 6, 8

[Chhetri et al., 2018] Chhetri, M. B., Uzunov, A., Vo, Q. B., Kowalczyk, R., Docking, M., Luong, H., Rajapakse, I., and Nepal, S. (2018). Aware-towards distributed self-management for resilient cyber systems. In *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, pages 185–188. IEEE. 3.2, 4

[Chiesi, 2016] Chiesi, S. S. (2016). Stpa application for safety assessment of generic missile systems. In *2016 Annual Reliability and Maintainability Symposium (RAMS)*, pages 1–7. IEEE. 8.2.1

[Chittister and Haimes, 2011] Chittister, C. G. and Haimes, Y. Y. (2011). The role of modeling in the resilience of cyberinfrastructure systems and preparedness for cyber intrusions. *Journal of Homeland Security and Emergency Management*, 8(1). 5, 6, 8

["Christophe Claramunt, Yvon Leroux, Rene Garello, G.Landrac, F.Vallee, Yin Ping", 2006] "Christophe Claramunt, Yvon Leroux, Rene Garello, G.Landrac, F.Vallee, Yin Ping" (2006). "MITS for Safer Seas".

[Christopher and Peck, 2004] Christopher, M. and Peck, H. (2004). Building the resilient supply chain. *The international journal of logistics management*, 15(2):1–14.

[Chung et al., 2019] Chung, H. M., Li, W. T., Yuen, C., Chung, W. H., Zhang, Y., and Wen, C. K. (2019). Local cyber-physical attack for masking line outage and topology attack in smart grid. *IEEE Transactions on Smart Grid*, 10(4):8435933, 4577–4588. 6, 7, 8

["CIS - The Center for Internet and Society - Riana Pfefferkorn", 2018] "CIS - The Center for Internet and Society - Riana Pfefferkorn" (2018). "Security Risks of Government Hacking".

["CISA - Cyber Infrastructure", 2017] "CISA - Cyber Infrastructure" (2017). "CAN Bus Standard Vulnerability".

["Cloudflare",] "Cloudflare". "Famous DDoS Attacks, The Largest DDoS Attacks Of All Time".

["Comae - Matt Suiche", 2017] "Comae - Matt Suiche" (2017). "Petya.2017 is a wiper not a ransomware".

[Comert et al., 2018] Comert, G., Pollard, J., Nicol, D. M., Palani, K., and Vignesh, B. (2018). Modeling cyber attacks at intelligent traffic signals. *Transportation research record*, 2672(1):76–89. 5, 6, 8

["Computer hope", 2018] "Computer hope" (2018). "When was the first computer invented?".

["Computer Weekly - Ron Condon", 2009] "Computer Weekly - Ron Condon" (2009). "Conficker worm update: How does Conficker spread?".

["Computer Weekly - Warwick Ashford", 2016] "Computer Weekly - Warwick Ashford" (2016). "Half of vehicle cyber vulnerabilities could give hackers control, study shows".

["Corero",] "Corero". "How Mirai Works".

["Corero", 2018] "Corero" (2018). "The Rise Of The Intelligent Machine In Cybersecurity".

["Crazy Hippo", 2018a] "Crazy Hippo" (2018a). "How Cruise Ship Stabilisers Work". 12

["Crazy Hippo", 2018b] "Crazy Hippo" (2018b). "How Cruise Ship Stabilisers Work".

["CRFS",] "CRFS". "How to deal with GPS jamming and spoofing".

["CrowdStrike - Karan Sood and Shaun Hurley", 2017] "CrowdStrike - Karan Sood and Shaun Hurley" (2017). "NotPetya Technical Analysis – A Triple Threat: File Encryption, MFT Encryption, Credential Theft".

["Cruise deals Expert - Robert Grant", 2015] "Cruise deals Expert - Robert Grant" (2015). "How Cruise Ship Stabilisers Work".

["CSO - Josh Fruhlinger", 2018] "CSO - Josh Fruhlinger" (2018). "What is WannaCry ransomware, how does it infect, and who was responsible?".

["CSO - Ms.Smith", 2015] "CSO - Ms.Smith" (2015). "Maritime cybersecurity firm: 37% of Microsoft servers on ships vulnerable to hacking".

["CSO from IDG - Josh Fruhlinger", 2017] "CSO from IDG - Josh Fruhlinger" (2017). "Petya ransomware and NotPetya malware: What you need to know now".

["CSO from IDG - Marin Ivezic", 2018a] "CSO from IDG - Marin Ivezic" (2018a). "Defeating 21st Century pirates: the maritime industry and cyberattacks".

["CSO from IDG - Marin Ivezic", 2018b] "CSO from IDG - Marin Ivezic" (2018b). "Stuxnet: the father of cyber-kinetic weapons".

["CSO from IDG - Smith", 2017] "CSO from IDG - Smith" (2017). "NotPetya ransomware hits hospitals, while Shadow Brokers touts its July VIP service".

["CVE - Common Vulnerabilities and exposures", 2019] "CVE - Common Vulnerabilities and exposures" (2019). "About CVE".

["CVE Details", 2019] "CVE Details" (2019). "Browse Vulnerabilities By Date".

["CyberBit/Volpe/US department of transportaion", 2013] "CyberBit/Volpe/US department of transportaion" (2013). "ICS Security in Maritime Transportation.". 29

[da Silva et al., 2015] da Silva, E. G., Knob, L. A. D., Wickboldt, J. A., Gaspary, L. P., Granville, L. Z., and Schaeffer-Filho, A. (2015). Capitalizing on sdn-based scada systems: An anti-eavesdropping case-study. In *2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, pages 165–173.

["DailyPost - Chijioke Jannah", 2019] "DailyPost - Chijioke Jannah" (2019). "Onnoghen: N-Delta militants warn S'South govs".

[Dallat et al., 2017] Dallat, C., Salmon, P. M., and Goode, N. (2017). Risky systems versus risky people: To what extent do risk assessment methods consider the systems approach to accident causation? a review of the literature. *Safety Science*. 8.2.1

[Damianou et al., 2001] Damianou, N., Dulay, N., Lupu, E., and Sloman, M. (2001). The ponder policy specification language. In *Proceedings of the International Workshop on Policies for Distributed Systems and Networks*, POLICY '01, pages 18–38, London, UK, UK. Springer-Verlag.

["Daniele Borio, Joaquim Fortuny-GuaschandCillian O'Driscoll", 2013] "Daniele Borio, Joaquim Fortuny-GuaschandCillian O'Driscoll" (2013). "Spectral and Spatial Characterization of GNSS Jammers".

[Danish-Maritime, 2019] Danish-Maritime (2019). Cyber and information security strategy for the maritime sector, 2019-2022. 1

["Danish Shipping",] "Danish Shipping". "Members".

["Dark Reading - Jai Vijayan", 2016] "Dark Reading - Jai Vijayan" (2016). "The 10 Worst Vulnerabilities of The Last 10 Years".

["DarkTrace", 2018] "DarkTrace" (2018). "The Next Paradigm Shift - AI-Driven Cyber-Attacks".

[Davis, 2015] Davis, A. (2015). Building cyber-resilience into supply chains. *Technology Innovation Management Review*, 5(4). 5, 6

[Deloitte, 2017] Deloitte (2017). Cyber Security in the Shipping Industry. Technical report, Deloitte. 2

[den Braber et al., 2003] den Braber, F., Dimitrakos, T., Gran, B. A., Lund, M. S., Stolen, K., and Aagedal, J. O. (2003). The coras methodology: model-based risk assessment using uml and up. In *UML and the Unified Process*, pages 332–357. IGI Global. 3.5

[Den Braber et al., 2007] Den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., and Vraalsen, F. (2007). Model-based security analysis in seven steps—a guided tour to the coras method. *BT Technology Journal*, 25(1):101–117. 3.5

[Denning, 2014] Denning, D. E. (2014). Framework and principles for active cyber defense. *Computers & Security*, 40:108–113. 6

["Department of Production and Quality Engineering NTNU - Marvin Rausand",] "Department of Production and Quality Engineering NTNU - Marvin Rausand". "Fault Tree Analysis".

["Digital Trends - Geoff Duncan", 2013] "Digital Trends - Geoff Duncan" (2013). "Here's why your email is insecure and likely to stay that way".

[Dimitrakos et al., 2002] Dimitrakos, T., Ritchie, B., Raptis, D., and Stølen, K. (2002). Model-based security risk analysis for web applications: The coras approach. In *Proceedings of the EuroWeb*. Citeseer. 3.5

[Disterer, 2013] Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. 1

["DLA Piper", 2019] "DLA Piper" (2019). "GDPR Data Breach Survey: February 2019A report by DLA Piper's cybersecurity team".

[Dong et al., 2015] Dong, X., Lin, H., Tan, R., Iyer, R. K., and Kalbarczyk, Z. (2015). Software-defined networking for smart grid resilience: Opportunities and challenges. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, CPSS '15, pages 61–68. ACM.

["Dr. Marco Balduzzi", 2014] "Dr. Marco Balduzzi" (2014). "AIS ExposedUnderstanding Vulnerabilities and Attacks 2.0".

[Dreyer et al., 2018] Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., and Winkelman, Z. (2018). Estimating the global cost of cyber risk. *Methodology and Examples. RAND*. 1.1

["DTU - CyberShip", 2018] "DTU - CyberShip" (2018). "Partners".

["DTU - Sotiria Lagouvardou", 2018] "DTU - Sotiria Lagouvardou" (2018). "Maritime Cyber Security:concepts, problems and models".

["Dualog", a] "Dualog". "Dualog AntiVirus Distribution".

["Dualog", b] "Dualog". "Dualog Business Mail".

[Dupont, 2019] Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, 5(1):tyz013.

[Durach et al., 2017a] Durach, C. F., Kembro, J., and Wieland, A. (2017a). A new paradigm for systematic literature reviews in supply chain management. *Journal of Supply Chain Management*, 53(4):67–85. 8.1.1, 10.2

[Durach et al., 2017b] Durach, C. F., Kembro, J., and Wieland, A. (2017b). A new paradigm for systematic literature reviews in supply chain management. *Journal of Supply Chain Management*, 53(4):67–85. 10.2

["East China University of Science and Technology Shanghai - Xiang Ji, Huiqun Yu, Guisheng Fan, Wenhao Fu", "East China University of Science and Technology Shanghai - Xiang Ji, Huiqun Yu, Guisheng Fan, Wenhao Fu" (2016). "Attack-defense trees based cyber security analysis for CPSs".

[Ebata et al., 2006] Ebata, K., Watanabe, Y., Nezu, Y., and Tanimura, S. (2006). Cyber attack countermeasures based on websam incidentguard and authentication switches. *NEC technical journal*, 1(1):28–31.

["EDIdEv - EDI Development",] "EDIdEv - EDI Development". "Acknowledging a UN/EDIFACT D01B ORDERS EDI file".

["Egil Haaland, Ornulf Jan Rodseth", 1993] "Egil Haaland, Ornulf Jan Rodseth" (1993). "MiTS: Maritime Information Technology Standard".

["Equasis", 2017] "Equasis" (2017). "The World Merchant Fleet in 2017".

[Esser and Vliegenthart, 2017] Esser, F. and Vliegenthart, R. (2017). Comparative research methods. *The international encyclopedia of communication research methods*, pages 1–22. 3.2

[Estefan et al., 2007] Estefan, J. A. et al. (2007). Survey of model-based systems engineering (mbse) methodologies. *Incose MBSE Focus Group*, 25(8):1–12. 8.2.1

["EU GDPR", 2018] "EU GDPR" (2018). "The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years.".

["European Parliament and Council of the European Union", 2016] "European Parliament and Council of the European Union" (2016). "General Data Protection Regulation".

[Fang et al., 2019] Fang, X., Xu, M., Xu, S., and Zhao, P. (2019). A deep learning framework for predicting cyber attacks rates. *Eurasip Journal on Information Security*, 2019(1):5. 8

[Farraj et al., 2015] Farraj, A., Hammad, E., Al Daoud, A., and Kundur, D. (2015). A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems. *IEEE Transactions on Smart Grid*, 7(4):1846–1855. 6, 8

[Fayaz et al., 2015] Fayaz, S. K., Tobioka, Y., Sekar, V., and Bailey, M. (2015). Bohatei: Flexible and elastic ddos defense. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 817–832, Washington, D.C. USENIX Association.

[Feinstein et al., 2015] Feinstein, B., Curry, D., and Debar, H. (2015). The Intrusion Detection Message Exchange Format (IDMEF). RFC 4765.

["Financial Post", 2014] "Financial Post" (2014). "Printers can be a hacker's gateway to your network".

[Fisher and Walker, 1994] Fisher, G. and Walker, W. (1994). *Operations Research and the RAND Corporation*. Rand Corporation. 5

["Fleet Mon - Maritime Security - Mikhail Voytenko", 2019] "Fleet Mon - Maritime Security - Mikhail Voytenko" (2019). "Container ship MSC MANDY attacked, Russian crew kidnapped".

[Foglietta et al., 2019] Foglietta, C., Masucci, D., Palazzo, C., Santini, R., Panzieri, S., Rosa, L., Cruz, T., and Lev, L. (2019). From detecting cyber-attacks to mitigating risk within a hybrid environment. *Ieee Systems Journal*, 13(1):8352138, 424–435. 6, 8

[for Engoineering and Technology,] for Engoineering, I. and Technology. Code of Practice Cyber Security for Ships. Technical report, IET Standards.

["Fortinet - Raul Alvarez", 2017] "Fortinet - Raul Alvarez" (2017). "Key Differences Between Petya and NotPetya".

["Fortune - Robert Hackett", 2016] "Fortune - Robert Hackett" (2016). "Hackers release source code for a powerful DDoS app called Mirai".

["FoxNews", 2018] "FoxNews" (2018). "Biggest DDoS attack on record hits Github".

[Furnell and Emm, 2017] Furnell, S. and Emm, D. (2017). The abc of ransomware protection. *Computer Fraud & Security*, 2017(10):5–11. 3.3

["Future Maritime Nautics", 2018] "Future Maritime Nautics" (2018). "Crew Connectivity2018 Survey Report maritime".

[Gao et al., 2016] Gao, P., Wang, M., Chow, J. H., Ghiocel, S. G., Fardanesh, B., Stefopoulos, G., and Razanousky, M. P. (2016). Identification of successive "unobservable" cyber data attacks in power systems through matrix decomposition. *IEEE Transactions on Signal Processing*, 64(21):5557–5570. 6, 8

["gCaptain", 2017] "gCaptain" (2017). "Maritime Security Incidents".

[Ginsparg, 2011] Ginsparg, P. (2011). Arxiv at 20. *Nature*, 476(7359):145–147. 5

[Goerlandt and Montewka, 2015] Goerlandt, F. and Montewka, J. (2015). Maritime transportation risk analysis: review and analysis in light of some foundational issues. *Reliability Engineering & System Safety*, 138:115–134.

[Google Trends, 2019] Google Trends (2019). Google trends report for term "cyber resilince". `https://trends.google.com/trends/explore?date=all&q=%2Fg%2F11c3ypk3jn`, Last accessed on 2019-11-26.

[Greenberg, 2018] Greenberg, A. (2018). The untold story of notpetya, the most devastating cyberattack in history. *Wired, August*. 3.3, 2, 5, 11

[Guerra and Estay, 2018] Guerra, P. and Estay, D. S. (2018). An impact-wave analogy for managing cyber risks in supply chains. In *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, pages 61–65. IEEE.

[Guerra and Sepulveda Estay, 2019] Guerra, P. and Sepulveda Estay, D. A. (2019). An impact-wave analogy for managing cyber risks in supply chains. In *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*. IEEE. 3.1

[Hadji-Janev and Bogdanoski, 2017] Hadji-Janev, M. and Bogdanoski, M. (2017). Swarming-based cyber defence under the framework of collective security. *Security Journal*, 30(1):39–59. 6, 8

[Hahn and Govindarasu, 2011] Hahn, A. and Govindarasu, M. (2011). Cyber attack exposure evaluation framework for the smart grid. *IEEE Transactions on Smart Grid*, 2(4):835–843. 6, 8

["HAL - Chao Fang", 2014] "HAL - Chao Fang" (2014). "Modeling and Analysing Propagation Behavior inComplex Risk Network : A Decision Support System forProject Risk Management".

[Haque et al., 2018] Haque, M. S., Jun Xian Ng, D., Easwaran, A., and Thangamariappan, K. (2018). Contract-based hierarchical resilience management for cyber-physical systems. *Computer*, 51(11):8625911, 56–65. 5, 8

[Hardy and Guarnieri, 2011] Hardy, K. and Guarnieri, F. (2011). Modelling and hazard analysis for contaminated sediments using stamp model. 8.2.1

[Hathaway et al., 2012] Hathaway, O. A., Crootof, R., Levitz, P., and Nix, H. (2012). The law of cyber-attack. *Calif. L. Rev.*, 100:817. 5, 6, 8

[Hayes, 2016] Hayes, H. R. (2016). Maritime cybersecurity: the future of national security. Master's thesis, Naval Postgraduate School.

[He et al., 2016] He, H., Maple, C., Watson, T., Tiwari, A., Mehnen, J., Jin, Y., and Gabrys, B. (2016). The security challenges in the iot enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In *2016 IEEE Congress on Evolutionary Computation (CEC)*, pages 1015–1021. IEEE. 1.1

["Heartbleed", 2014] "Heartbleed" (2014). "The Heartbleed Bug".

["Heinzmann Automation", 2013] "Heinzmann Automation" (2013). "Reducing operating costs and complying with emissions legislation are of key interest to marine carriers.".

["Heinzmann Automation", 2019a] "Heinzmann Automation" (2019a). "Alarm & Monitoring".

["Heinzmann Automation", 2019b] "Heinzmann Automation" (2019b). "Power Management Systems".

[Hemanidhi and Chimmanee, 2017] Hemanidhi, A. and Chimmanee, S. (2017). Military-based cyber risk assessment framework for supporting cyber warfare in thailand. *Journal of ICT*, 16(2):192–222. 5, 6, 8

["Hexagon - Positioning Intelligence", 2013] "Hexagon - Positioning Intelligence" (2013). "Understanding the difference between anti-spoofing and anti-jamming".

[Hollnagel et al., 2006] Hollnagel, E., Woods, D. D., and Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Ashgate Publishing, Ltd. 3.1

["Hongkiat", 2017] "Hongkiat" (2017). "10 Most Destructive Computer Viruses".

[Huang et al., 2018a] Huang, K., Siegel, M., and Stuart, M. (2018a). Systematically understanding the cyber attack business: A survey. *ACM Computing Surveys (CSUR)*, 51(4):70. 6, 8

[Huang et al., 2018b] Huang, T., Satchidanandan, B., Kumar, P. R., and Xie, L. (2018b). An online detection framework for cyber attacks on automatic generation control. *Ieee Transactions on Power Systems*, 33(6):8345676, 6816–6827. 5, 8

[Hughes, 2007] Hughes, J. (2007). The ability-motivation-opportunity framework for behavior research in is. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 250a–250a. IEEE. 3.2

["Humans At Sea", 2017] "Humans At Sea" (2017). "Somali Pirates VS Ship's Private Security Guards".

["Huston Chronicle - Zain Shauk", 2013] "Huston Chronicle - Zain Shauk" (2013). "Malware on oil rig computers raises security fears".

[Hyra, 2019] Hyra, B. (2019). Analyzing the Attack surface of ships. 3.4, 8.2.1, 12, 12

["ICC - Commercial Crime Services", 2018] "ICC - Commercial Crime Services" (2018). "IMB Piracy & Armed Robbery Map 2018.".

["IEEE Spectrum - David Kushner", 2013] "IEEE Spectrum - David Kushner" (2013). "The Real Story of Stuxnet".

["IHS Fairplay", 2016] "IHS Fairplay" (2016). "2016 Cyber Security Survey". 2

[IMO, 2017a] IMO (2017a). Guidelines on Maritime Cyber Risk Management. Technical report, IMO. 2

[IMO, 2017b] IMO (2017b). Guidelines on maritime cyber risk management, msc-fal.1/circ.3. 1

["IMO", 2018] "IMO" (2018). "IMO publications". 12

["IMO", 2019] "IMO" (2019). "IMO web page". 12

["Independent - Keith Martin Rory Hopcraft", 2018] "Independent - Keith Martin Rory Hopcraft" (2018). "50,000 Ships worldwide are vulnerable to cyberattacks.".

["Institution of Engineering and Technology", 2017] "Institution of Engineering and Technology" (2017). "Code of Practice - Cyber Security of Ships".

["International Holographic Organisation", 2017] "International Holographic Organisation" (2017). "S66 - Facts About Electronic Charts And Carriage Requirements".

["International Maritime Organization", 2010] "International Maritime Organization" (2010). "International Safety Management Code".

["International Shipsuppliers and Services Association", 2016] "International Shipsuppliers and Services Association" (2016). "International Ship and Port Facility Security Code".

[Irwin and Dawson, 2019] Irwin, A. S. and Dawson, C. (2019). Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help. *Journal of Money Laundering Control*, 22(1):110–131. 5, 6, 7, 8

["ISACA", 2016a] "ISACA" (2016a). "Cybersecurity Threat Modeling".

["ISACA", 2016b] "ISACA" (2016b). "Cybersecurity Threat Modeling".

["ISACA", 2017] "ISACA" (2017). "IT Asset Valuation, Risk Assessment and Control Implementation Model - Shemlse Gebremedhin Kassa, CISA, CEH".

[ISO, 2008] ISO, I. (2008). Iec 27005: Information technology–security techniques–information security risk management. *ISO/IEC*, 66.

["ISSN - Department of Defense Analysis - D. E. Denning", 2012] "ISSN - Department of Defense Analysis - D. E. Denning" (2012). "Stuxnet: What Has Changed?".

["Jahshan Bhatti and Todd E. Humphreys",] "Jahshan Bhatti and Todd E. Humphreys". "Hostile Control of Ships via False GPS Signals:Demonstration and Detection".

[Januário et al., 2019] Januário, F., Cardoso, A., and Gil, P. (2019). A distributed multi-agent framework for resilience enhancement in cyber-physical systems. *IEEE Access*, 7:31342–31357. 5, 6

[Jaquire and von Solms, 2015] Jaquire, V. and von Solms, B. (2015). A strategic framework for a secure cyberspace in developing countries with special emphasis on the risk of cyber warfare. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, 5(1):1–18. 6

[Järveläinen, 2013] Järveläinen, J. (2013). It incidents and business impacts: Validating a framework for continuity management in information systems. *International journal of information management*, 33(3):583–590. 1.1

[Jayaram, 2016] Jayaram, A. (2016). Lean six sigma approach for global supply chain management using industry 4.0 and iiot. In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pages 89–94. IEEE.

[Jensen, 2018] Jensen, C. D. (2018). Analyzing the communication security between smartphones and iot based on coras. In *Network and System Security: 12th International Conference, NSS 2018, Hong Kong, China, August 27-29, 2018, Proceedings*, volume 11058, page 251. Springer. 3.5

[Jin et al., 2019] Jin, M., Lavaei, J., and Johansson, K. H. (2019). Power grid ac-based state estimation: Vulnerability analysis against cyber attacks. *IEEE Transactions on Automatic Control*, 64(5):8403288, 1784–1799. 6, 7, 8

[Johnson et al., 2013] Johnson, N., Elliott, D., and Drake, P. (2013). Exploring the role of social capital in facilitating supply chain resilience. *Supply Chain Management: An International Journal*, 18(3):324–336.

["Jones Walker", 2018a] "Jones Walker" (2018a). "Jones Walker LLP 2018 - Maritime Cybersecurity Survey".

["Jones Walker", 2018b] "Jones Walker" (2018b). "Jones Walker LLP Releases Inaugural Maritime Cybersecurity Survey".

[Ju et al., 2019] Ju, A., Guo, Y., Ye, Z., Li, T., and Ma, J. (2019). Hetemsd: A big data analytics framework for targeted cyber-attacks detection using heterogeneous multisource data. *Security and Communication Networks*. 5, 8

["K-Force - Computer Solutions", 2016] "K-Force - Computer Solutions" (2016). "New at K-Force: Cloud Backup".

[Karami et al., 2015] Karami, E., Goodarzi, Z., Hosseinzadeh, T., and Shirali, G. (2015). Analyzing hazards using system theoretic process analysis (stpa) methodology: A case study in the emergency extinguishing systems of thermal power plant. *Health and Safety at Work*, 5(1):13–24. 8.2.1

["Kaspersky", 2005] "Kaspersky" (2005). "The biggest virus epidemic since Sasser and Mydoom? Kaspersky Lab comments on the current situation".

["Kaspersky", 2018] "Kaspersky" (2018). "Modern yacht hacking".

["Kaspersky - GReAT", 2014] "Kaspersky - GReAT" (2014). "Stuxnet: Zero victims".

["Kaspersky - Kate Kochetkova", 2015] "Kaspersky - Kate Kochetkova" (2015). "Maritime industry is easy meat for cyber criminals".

["Kaspersky Lab", 2014a] "Kaspersky Lab" (2014a). "Stuxnet Patient Zero: First Victims of the Infamous Worm Revealed".

["Kaspersky Lab", 2014b] "Kaspersky Lab" (2014b). "Stuxnet: Victims Zero".

["Kaspersky Lab", 2018] "Kaspersky Lab" (2018). "Virus.MSWord.Melissa-based".

["Kaspersky Lab - Nikolay Pankov", 2017] "Kaspersky Lab - Nikolay Pankov" (2017). "WannaCry: What you need to know".

["Kaspersky Lab - Nikolay Pankov", 2018] "Kaspersky Lab - Nikolay Pankov" (2018). "WannaCry: Not dead yet".

[Katos and Bednar, 2008] Katos, V. and Bednar, P. M. (2008). A cyber-crime investigation framework. *Computer Standards & Interfaces*, 30(4):223–228. 5, 8

[Kavallieratos et al., 2018] Kavallieratos, G., Katsikas, S., and Gkioulos, V. (2018). Cyber-attacks against the autonomous ship. In *Computer Security*, pages 20–36. Springer.

[Khalid et al., 2018] Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K.-D., and Pannek, J. (2018). Security framework for industrial collaborative robotic cyber-physical systems. *Computers in Industry*, 97:132–145. 6, 7, 8

[Khan and Sepulveda Estay, 2015] Khan, O. and Sepulveda Estay, D. A. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, (April):6–12. 1.1, 5, 6, 8

[Khouzani et al., 2019] Khouzani, M. H., Liu, Z., and Malacaria, P. (2019). Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. *European Journal of Operational Research*, 278(3):894–903. 8

[Kim et al., 2019] Kim, D., Won, Y., Eun, Y., and Park, K.-J. (2019). Resilient architecture for network and control co-design under wireless channel uncertainty in cyber-physical systems. *Transactions on Emerging Telecommunications Technologies*, 30(4):e3499. 5, 6, 8

["KNect365 - Leah Kinthaert", 2017] "KNect365 - Leah Kinthaert" (2017). "8 Experts Weigh In on Cybersecurity in Shipping & Maritime".

["Kongsberg", 2019] "Kongsberg" (2019). "Kongsberg web page". 12

["Korea University - Young-Gab Kim, Dongwon Jeong, Soo-Hyun Park, Jongin Lim, and Doo-Kwon Baik", 2007] "Korea University - Young-Gab Kim, Dongwon Jeong, Soo-Hyun Park, Jongin Lim, and Doo-Kwon Baik" (2007). "Modeling and simulation for security risk propagation in critical information systems".

[Kowalski and Sergot, 1986] Kowalski, R. and Sergot, M. (1986). A logic-based calculus of events. *New Gen. Comput.*, 4(1):67–95.

[Kozik et al., 2019] Kozik, R., Choraś, M., and Keller, J. (2019). Balanced efficient lifelong learning (b-ella) for cyber attack detection. *Journal of Universal Computer Science*, 25(1):2–15. 8

["Krebs On Security", 2017] "Krebs On Security" (2017). "Petya - Ransomware Outbreak Goes Global".

[Kreutz et al., 2015] Kreutz, D., Ramos, F. M. V., Veríssimo, P. E., Rothenberg, C. E., Azodolmolky, S., and Uhlig, S. (2015). Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76.

[Kuhn, 2014] Kuhn, T. (2014). A survey and classification of controlled natural languages. *Comput. Linguist.*, 40(1):121–170.

[Kumar et al., 2014] Kumar, V. A., Pandey, K. K., and Punia, D. K. (2014). Cyber security threats in the power sector: Need for a domain specific regulatory framework in india. *Energy Policy*, 65:126–133. 5, 6, 8

[Lallie et al., 2018] Lallie, H. S., Debattista, K., and Bal, J. (2018). Evaluating practitioner cyber-security attack graph configuration preferences. *Computers and Security*, 79:117–131. 8

[Langner, 2011] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security and Privacy*, 9(3):49–51.

[Larionovs et al., 2015] Larionovs, A., Teilans, A., and Grabusts, P. (2015). Coras for threat and risk modeling in social networks. *Procedia Computer Science*, 43:26–32. 3.5

[Le and Hoang, 2017] Le, N. T. and Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. *Scalable Computing*. 5, 6, 8

[Lee and Lim, 2016] Lee, K.-b. and Lim, J.-i. (2016). The reality and response of cyber threats to critical infrastructure: A case study of the cyber-terror attack on the korea hydro & nuclear power co., ltd. *KSII Transactions on Internet & Information Systems*, 10(2). 6, 8

[Lei et al., 2019] Lei, H., Chakhchoukh, Y., and Singh, C. (2019). Framework of a benchmark testbed for power system cyber-physical reliability studies. *International Transactions on Electrical Energy Systems*, 29(1):e2692. 5, 6, 8

[Leveson, 2004] Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science*, 42(4):237–270. 8.2.1

[Leveson, 2011] Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT press. 3.4, 13, 8.2, 8.2.1, 8.2.1, 8.2.1, 3

[Li et al., 2014a] Li, J., Berg, S., Zhang, M., Reiher, P., and Wei, T. (2014a). Drawbridge: Software-defined ddos-resistant traffic engineering. *SIGCOMM Comput. Commun. Rev.*, 44(4):591–592.

[Li et al., 2014b] Li, R., Li, J., and Asaeda, H. (2014b). A hybrid trust management framework for wireless sensor and actuator networks in cyber-physical systems. *IEICE TRANSACTIONS on Information and Systems*, 97(10):2586–2596. 3.1, 6

[Li et al., 2019] Li, W., Shi, Y., and Li, Y. (2019). Research on secure control and communication for cyber-physical systems under cyber-attacks. *Transactions of the Institute of Measurement and Control*, page 0142331219826658. 6, 7, 8

[Li et al., 2018] Li, Y., Liu, X., and Peng, L. (2018). An event-triggered fault detection approach in cyber-physical systems with sensor nonlinearities and deception attacks. *Electronics (basel)*. 7, 8

[Li et al., 2016] Li, Y., Quevedo, D. E., Dey, S., and Shi, L. (2016). A game-theoretic approach to fake-acknowledgment attack on cyber-physical systems. *IEEE Transactions on Signal and Information Processing over Networks*, 3(1):1–11. 3.1, 6

[Li et al., 2015] Li, Y., Shi, L., Cheng, P., Chen, J., and Quevedo, D. E. (2015). Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control*, 60(10):7172466, 2831–2836. 6, 7, 8

[Li and Yang, 2019] Li, Y. G. and Yang, G. H. (2019). Optimal stealthy false data injection attacks in cyber-physical systems. *Information Sciences*, 481:474–490. 7, 8

[Liang et al., 2019] Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y. (2019). A framework for cyber-topology attacks: Line-switching and new attack scenarios. *IEEE Transactions on Smart Grid*, 10(2):8118126, 1704–1712. 6, 7, 8

[Liang and Menghong, 2012] Liang, Q. and Menghong, Y. (2012). Research on ship cpp networked control system based on svm, gpc and qs. In Jiang, L., editor, *Proceedings of the 2011, International Conference on Informatics, Cybernetics, and Computer Engineering (ICCE2011) November 19–20, 2011, Melbourne, Australia*, pages 177–184, Berlin, Heidelberg. Springer Berlin Heidelberg.

[Lim et al., 2018] Lim, G. J., Cho, J., Bora, S., Biobaku, T., and Parsaei, H. (2018). Models and computational algorithms for maritime risk analysis: a review. *Annals of Operations Research*, pages 1–22.

[Liu et al., 2013] Liu, S., Mashayekh, S., Kundur, D., Zourntos, T., and Butler-Purry, K. (2013). A framework for modeling cyber-physical switching attacks in smart grid. *Ieee Transactions on Emerging Topics in Computing*, 1(2):6695779, 273–285. 6, 7, 8

[Lu et al., 2015] Lu, T., Zhao, J., Zhao, L., Li, Y., and Zhang, X. (2015). Towards a framework for assuring cyber physical system security. *International Journal of Security and Its Applications*, 9(3):25–40. 8

[Lund et al., 2011] Lund, M. S., Solhaug, B., and Stølen, K. (2011). Risk analysis of changing and evolving systems using coras. In *International School on Foundations of Security Analysis and Design*, pages 231–274. Springer. 3.5

[Lv et al., 2017] Lv, C., Wang, H., Zhao, B., Cao, D., Huaji, W., Zhang, J., Li, Y., and Yuan, Y. (2017). Cyber-physical system based optimization framework for intelligent powertrain control. *SAE International Journal of Commercial Vehicles*. 3.1

["Machinery Spaces", a] "Machinery Spaces". "Fuel oils treatment for marine use - The refining process". 12

["Machinery Spaces", b] "Machinery Spaces". "The fuel oil system for a marine diesel engine - Internal combustion engine procedure". 12

[Mahimkar et al., 2007] Mahimkar, A., Dange, J., Shmatikov, V., Vin, H., and Zhang, Y. (2007). dfence: Transparent network-based denial of service mitigation. In *4th USENIX Symposium on Networked Systems Design & Implementation (NSDI 07)*, Cambridge, MA. USENIX Association. 3

[Manners-Bell, 2017] Manners-Bell, J. (2017). *Supply chain risk management: understanding emerging threats to global supply chains*. Kogan Page Publishers.

["Marine Electronics", 2016] "Marine Electronics" (2016). "NMEA 0183 vs 2000: What's the difference?".

["Marine Insight", 2017] "Marine Insight" (2017). "BMT To Launch Unique Fleet Management System". 12

["Marine Insight", 2018a] "Marine Insight" (2018a). "Marine Heavy Fuel Oil (HFO) For Ships – Properties, Challenges and Treatment Methods". 12

["Marine Insight", 2018b] "Marine Insight" (2018b). "Understanding Capacity Control in Ship's Air Conditioning and Refrigeration System". 12

["Marine Insight - Anish", 2017a] "Marine Insight - Anish" (2017a). "8 Common Problems of Ship's Incinerator Mariners Should Know". 12

["Marine Insight - Anish", 2017b] "Marine Insight - Anish" (2017b). "General Overview of Central Cooling System on Ships". 12

["Marine Insight - Anish", 2017c] "Marine Insight - Anish" (2017c). "Understanding Turbocharger Bearings and Lubrication On Ships". 12

["Marine Insight - Anish", 2018a] "Marine Insight - Anish" (2018a). "Everything You Ever Wanted to Know About Container Refrigeration Unit".

["Marine Insight - Anish", 2018b] "Marine Insight - Anish" (2018b). "Marine Heavy Fuel Oil (HFO) For Ships – Properties, Challenges and Treatment Methods". 12

["Marine Insight - Chief Office Abhishek Bhanawat", 2019] "Marine Insight - Chief Office Abhishek Bhanawat" (2019). "Important Points Seafarers Must Consider For Clean Drinking Water System On Ships". 12

["Marine Insight - KaranC", 2016] "Marine Insight - KaranC" (2016). "Intelligent Cylinder Lubrication for Modern Marine Engines - Part 1". 12

["Marine Insight - KaranC", 2017] "Marine Insight - KaranC" (2017). "Converting Seawater to Freshwater on a Ship: Fresh Water Generator Explained". 12

["Marine Insight - Mayur Agrawal", 2018] "Marine Insight - Mayur Agrawal" (2018). "An Overview Of Sludge And Bilge Management Onboard Ships". 12

["Marine Insight - Shalabh Agarwal", 2017] "Marine Insight - Shalabh Agarwal" (2017). "8 Things Marine Engineers Must Know About Starting Air System On Ship". 12

["Marine Insight - Shilavadra Bhattacharjee", 2019] "Marine Insight - Shilavadra Bhattacharjee" (2019). "What is Electronic Chart Display and Information System (ECDIS)?".

["Marine Knowledge", 2013] "Marine Knowledge" (2013). "What Are SART And EPIRB Used For?". 12

["MarineInsight", 2019] "MarineInsight" (2019). "Main web page". 12

["MarineInsight - Shilavadra Bhattacharjee", 2017] "MarineInsight - Shilavadra Bhattacharjee" (2017). "What is Integrated Bridge System (IBS) on Ships?". 12

["MarineInsight - Shilavarda Bhattacharjee", 2017] "MarineInsight - Shilavarda Bhattacharjee" (2017). "What is An Emergency Position Indicating Radio Beacon (EPIRB)?". 12

["MarineInsight - Shilavarda Bhattacharjee", 2019] "MarineInsight - Shilavarda Bhattacharjee" (2019). "What is Search and Rescue Transponder (SART)?". 12

["Marintek - MiTS", 2012a] "Marintek - MiTS" (2012a). "Communication between ship and shore".

["Marintek - MiTS", 2012b] "Marintek - MiTS" (2012b). "MariComputer networks on board and shore".

["Marintek - MiTS", 2012c] "Marintek - MiTS" (2012c). "MiTS: Maritime Information Technology Standard".

["Marintek - MiTS", 2015a] "Marintek - MiTS" (2015a). "Communication between ship and shore".

["Marintek - MiTS", 2015b] "Marintek - MiTS" (2015b). "Maritime Information Technology Standard".

["Maritime and Coastguard Agency", 2002] "Maritime and Coastguard Agency" (2002). "SOLAS Chapter V". 12

["Maritime Digitalisation and Communications", 2018] "Maritime Digitalisation and Communications" (2018). "Maritime industry has 'false sense of preparedness' for cyber attacks, survey shows".

["Maritime Inury Lawsuit - Gordon, Seely", 2018] "Maritime Inury Lawsuit - Gordon, Seely" (2018). "Types of Serious Maritime Accidents".

["MaritimeInsight - KaranC", 2018] "MaritimeInsight - KaranC" (2018). "30 Types of Navigation Equipment and Resources Used Onboard Modern Ships". 12

["MaritimeTraffic", 2019] "MaritimeTraffic" (2019). "The Live map of vessels position.".

[Markopoulou et al., 2019] Markopoulou, D., Papakonstantinou, V., and de Hert, P. (2019). The new eu cybersecurity framework: The nis directive, enisa's role and the general data protection regulation. *Computer Law & Security Review*, 35(6):105336. 3.2

["Marorka", 2017] "Marorka" (2017). "Marorka Onboard - Reference Guide".

["Marquard and Bahls", 2015] "Marquard and Bahls" (2015). "Marine Diesel Oil (MDO) and Intermediate Fuel Oil (IFO)". 12

["Mashable - Emma Hinchliffe", 2016] "Mashable - Emma Hinchliffe" (2016). "Sites across the internet suffer outage after cyberattack".

["McAfee", 2004] "McAfee" (2004). "Virus Profile: W32/Mydoom@MM".

[McCarthy and Milner, 2020] McCarthy, G. and Milner, J. (2020). Ability, motivation and opportunity: managerial coaching in practice. *Asia Pacific Journal of Human Resources*, 58(1):149–170. 3.2

[McKeown et al., 2008] McKeown, N., Anderson, T., Balakrishnan, H., Parulkar, G., Peterson, L., Rexford, J., Shenker, S., and Turner, J. (2008). Openflow: Enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74.

["Meltdown and Spectre", 2018] "Meltdown and Spectre" (2018). "Meltdown and Spectre - Vulnerabilities in modern computers leak passwords and sensitive data.".

["Mendel University in Brno - M. Jukl, J.Cupera",] "Mendel University in Brno - M. Jukl, J.Cupera". "Using of tiny encryption algorithm in CAN-Bus communication".

[Mertoguno et al., 2019] Mertoguno, J. S., Craven, R. M., Mickelson, M. S., and Koller, D. P. (2019). A physics-based strategy for cyber resilience of cps. In *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*, volume 11009, page 110090E. International Society for Optics and Photonics. 3.2

[Meskell,] Meskell, J. P. "Merchant shipping and the marine engineering technology revolution". 12, 30

["Military Embedded Systems - Sally Cole", 2015] "Military Embedded Systems - Sally Cole" (2015). "Securing military GPS from spoofing and jamming vulnerabilities".

["MIT Lincol Labolatory - Kevin M. Carter, Nwokedi Idika, William W. Sterilein", 2013] "MIT Lincol Labolatory - Kevin M. Carter, Nwokedi Idika, William W. Sterilein" (2013). "Probabilistic Threat Propagation For Malicious Activity Detection".

[Mitka,] Mitka, E. Safety-guided design towards standardization of mowing robots. 8.2.1

[Mo and Sansavini, 2017] Mo, H. and Sansavini, G. (2017). Dynamic defense resource allocation for minimizing unsupplied demand in cyber-physical systems against uncertain attacks. *Ieee Transactions on Reliability*, 66(4):1253–1265. 5, 6, 8

[Moher et al., 2009] Moher, D., Liberati, A., Tetzlaff, J., and Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: the prisma statement. *Annals of internal medicine*, 151(4):264–269. 10.2

[Moslemi et al., 2018] Moslemi, R., Mesbahi, A., and Velni, J. M. (2018). A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids. *Ieee Transactions on Smart Grid*, 9(5):7867093, 4930–4941. 5, 6, 7, 8

[Mousavi et al., 2016] Mousavi, M., Ghazi, I., and Omaraee, B. (2016). Risk assessment in the maritime industry. *Engineering, Technology & Applied Science Research*, 7(1):1377–1381.

[Mulrow, 1987] Mulrow, C. D. (1987). The medical review article: state of the science. *Annals of internal medicine*, 106(3):485–488. 10.2

[Murtagh and Legendre, 2014] Murtagh, F. and Legendre, P. (2014). Ward's hierarchical agglomerative clustering method: which algorithms implement ward's criterion? *Journal of classification*, 31(3):274–295.

["My friend shared with me",] "My friend shared with me".

["Nan Feng, Harry Jiannan Wang, Minqiang Li", 2014] "Nan Feng, Harry Jiannan Wang, Minqiang Li" (2014). "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis".

["NASA", 2002] "NASA" (2002). "Fault Tree Handbook with Aerospace Applications".

["National Aerospace Laporatory NLR - S. Storm van Leeuwen",] "National Aerospace Laporatory NLR - S. Storm van Leeuwen". "Electromagnetic Interference on Low Cost GPS Receivers".

["National Institute of Standards and Technology", 2018] "National Institute of Standards and Technology" (2018). "Framework for Improving Critical Infrastructure Cybersecurity".

["National instruments", 2019] "National instruments" (2019). "Controller Area Network (CAN) Overview".

["National maritime College of Ireland - Damien Lavelle", 2017] "National maritime College of Ireland - Damien Lavelle" (2017). "An Analysis of Cyber Security Awareness Onboard Cruise Ships".

["Naval Dome", 2019] "Naval Dome" (2019). "WORLD'S LEADING Maritime Cyber Defense Solution".

["NCC Group - Yevgen Dyryavyy", 2014] "NCC Group - Yevgen Dyryavyy" (2014). "Preparing for Cyber Battleships –Electronic Chart Display and Information System Security".

[Nespoli et al., 2018] Nespoli, P., Papamartzivanos, D., Goacutemez Maacutermol, F., and Kambourakis, G. (2018). Optimal countermeasures selection against cyber attacks: A comprehensive survey on reaction frameworks. *Ieee Communications Surveys and Tutorials*, 20(2):1361–96, 1361–1396. 8

["Network World form IDG - Matt Conran", 2018] "Network World form IDG - Matt Conran" (2018). "Overcoming kludges to secure web applications".

["NewScientist", 2017] "NewScientist" (2017). "Ships fooled in GPS spoofing attack suggest Russian cyberweapon".

["Newsweek - Babak Dehganpisheh", 2018] "Newsweek - Babak Dehganpisheh" (2018). "Stuxnet worm, latest attack in growing cyberwar".

["NIST", 2018a] "NIST" (2018a). "NIST Releases Version 1.1 of its Popular Cybersecurity Framework".

["NIST", 2018b] "NIST" (2018b). "The Framework for Improving Critical Infrastructure Cybersecurity".

["Nmap.org", 2019] "Nmap.org" (2019). "Nmap - the Network Mapper - Free Security Scanner".

["NMEA Standards Comittee - Frank Cassidy", 1999] "NMEA Standards Comittee - Frank Cassidy" (1999). "NMEA 200 Explained - The Latest Word?".

["NMEA Standards Committee - Franks Cassidy", 1997] "NMEA Standards Committee - Franks Cassidy" (1997). "NMEA 2000 and the Controller Area Network (CAN)".

[Nogal and O'Connor, 2017] Nogal, M. and O'Connor, A. (2017). Cyber-transportation resilience. context and methodological framework. In *Resilience and Risk*, pages 415–426. Springer.

["Nomadic Research labs", 2008] "Nomadic Research labs" (2008). "NMEA 2000 – The Journey Begins".

["Noonsite", 2015] "Noonsite" (2015). "Maritime Security Incident Report".

[Noor et al., 2019] Noor, U., Anwar, Z., Amjad, T., and Choo, K.-K. R. (2019). A machine learning-based fintech cyber threat attribution framework using high-level indicators of compromise. *Future Generation Computer Systems*, 96:227–242. 5, 6, 8

["Northrop Grumman", 2005] "Northrop Grumman" (2005). "Satellite Compas". 12

["Norton by Symantec",] "Norton by Symantec". "What you need to do about the WPA2 Wi-Fi network vulnerability".

["Norton Team", 2016] "Norton Team" (2016). "The 8 Most Famous Computer Viruses of All Time".

[Nower et al., 2014] Nower, N., Tan, Y., and Lim, A. O. (2014). Traffic pattern based data recovery scheme for cyber-physical systems. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 97(9):1926–1936. 3.1, 5, 6, 8

[Nunes et al., 2014] Nunes, B., Mendonca, M., Nguyen, X.-N., Obraczka, K., and Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. *Communications Surveys Tutorials, IEEE*, 16(3):1617–1634.

["Offshore Energy Today - Bartlomiej Tomić", 2018] "Offshore Energy Today - Bartlomiej Tomić" (2018). "Pirates board offshore vessel in Nigeria".

[Open Networking Foundation, 2013] Open Networking Foundation (2013). SDN Architecture Overview. Technical report, ONF.

["OPSWAT - Bryan Vale", 2014] "OPSWAT - Bryan Vale" (2014). "Have Printers Become a Gateway for Malware?".

[Osborn, 2020] Osborn, J. (2020). Comparison of the impact-wave analogy to published cyber resilience models. Technical report, DTU Technical University of Denmark. 3.2, 11

[Paradise et al., 2017] Paradise, A., Shabtai, A., Puzis, R., Elyashar, A., Elovici, Y., Roshandel, M., and Peylo, C. (2017). Creation and management of social network honeypots for detecting targeted cyber attacks. *IEEE Transactions on Computational Social Systems*, 4(3):65–79. 5, 6, 8

[Park and Lee, 2019] Park, J. W. and Lee, S. J. (2019). Probabilistic safety assessment-based importance analysis of cyber-attacks on nuclear power plants. *Nuclear Engineering and Technology*, 51(1):138–145. 5, 6, 7, 8

[Pasqualetti et al.,] Pasqualetti, F., Dörfler, F., and Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE transactions on automatic control*, 58(11). 5, 8

[Patnayakuni and Patnayakuni, 2014] Patnayakuni, R. and Patnayakuni, N. (2014). Information security in value chains: a governance perspective.

["PC World - Brad Chacos and Michael Simon", 2018] "PC World - Brad Chacos and Michael Simon" (2018). "Meltdown and Spectre FAQ: How the critical CPU flaws affect PCs and Macs".

["PC World - Robert Strohmeyer", 2008] "PC World - Robert Strohmeyer" (2008). "The 7 Worst Tech Predictions of All Time".

["PCmag - Larry Seltzer", 2010] "PCmag - Larry Seltzer" (2010). "I Love You - Virus Turns Ten: What Have We Learned?".

["PCWorld from IDG - Henryl Tur", 2018] "PCWorld from IDG - Henryl Tur" (2018). "700 razy na godzinę podejmowane są próby przeprowadzenia cyberataków na Polskę".

["Pen Test Partners - Ken Munro", 2017a] "Pen Test Partners - Ken Munro" (2017a). "Sinking bulk carrier ships by hacking HSMS".

["Pen Test Partners - Ken Munro", 2017b] "Pen Test Partners - Ken Munro" (2017b). "Sinking container ships by hacking load plan software".

["Pen Test Partners - Ken Munro", 2018a] "Pen Test Partners - Ken Munro" (2018a). "Hacking, tracking, stealing and sinking ships".

["Pen Test Partners - Ken Munro", 2018b] "Pen Test Partners - Ken Munro" (2018b). "So, you've got 5 minutes over a coffee, what should you do about your fleet security?".

[Penera and Chasaki, 2015] Penera, E. and Chasaki, D. (2015). Packet scheduling attacks on shipboard networked control systems. In *2015 Resilience Week (RWS)*, pages 1–6. 2

[Peng et al., 2019] Peng, C., Sun, H., Yang, M., and Wang, Y.-L. (2019). A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 5, 6, 8

["PenTestPartners - Ken Munro", 2017a] "PenTestPartners - Ken Munro" (2017a). "Making prawn espressos, or hacking ships by deciphering BAPLIE EDIFACT messaging".

["PenTestPartners - Ken Munro", 2017b] "PenTestPartners - Ken Munro" (2017b). "OSINT from ship satcoms".

["PenTestPartners - Ken Munro", 2018] "PenTestPartners - Ken Munro" (2018). "Hacking maritime IFTFCC messaging for invoice fraud".

[Pettit et al., 2013] Pettit, T. J., Croxton, K. L., and Fiksel, J. (2013). Ensuring supply chain resilience: development and implementation of an assessment tool. *Journal of Business Logistics*, 34(1):46–76.

[Porcedda, 2018] Porcedda, M. G. (2018). Patching the patchwork: appraising the eu regulatory framework on cyber security breaches. *Computer Law and Security Review*, 34(5):1077–1098. 5, 6, 8

["Processing - Sridhar Srinivasan", 2013] "Processing - Sridhar Srinivasan" (2013). "Risk-Based Asset Management Enhanced Through Real-Time Modeling Tools".

["Project leader - Bruno Blanchet", 2019] "Project leader - Bruno Blanchet" (2019). "ProVerif: Cryptographic protocol verifier in the formal model".

[Puisa et al., 2018] Puisa, R., Lin, L., Bolbot, V., and Vassalos, D. (2018). Unravelling causal factors of maritime incidents and accidents. *Safety science*, 110:124–141. 8.2.1

["Quality Progress - ASQ", 2002] "Quality Progress - ASQ" (2002). "What Is a Fault Tree Analysis?".

["Quality Progress ASG - Simha Pilot", 2002] "Quality Progress ASG - Simha Pilot" (2002). "What Is a Fault Tree Analysis?".

["Rapid1 - Christian Kirisch", 2014] "Rapid1 - Christian Kirisch" (2014). "Security Advisory: OpenSSL Heartbleed Vulnerability (CVE-2014-0160) in Metasploit".

[Rasmussen, 1983] Rasmussen, J. (1983). Position paper for nato conference on human error. august 1983. *Bellagio, Italy*.

[Ratasich et al., 2019] Ratasich, D., Khalid, F., Geissler, F., Grosu, R., Shafique, M., and Bartocci, E. (2019). A roadmap toward the resilient internet of things for cyber-physical systems. *IEEE Access*, 7:13260–13283. 6

[Raulerson et al., 2015] Raulerson, E. L., Hopkinson, K. M., and Laviers, K. R. (2015). A framework to facilitate cyber defense situational awareness modeled in an emulated virtual machine testbed. *Journal of Defense Modeling and Simulation*, 12(3):229–239. 5, 6, 8

["RedStag Fulfillment", 2016] "RedStag Fulfillment" (2016). "DYN infographic".

[Rege, 2014] Rege, A. (2014). A criminological perspective on power grid cyber attacks: Using routine activities theory to rational choice perspective to explore adversarial decision-making. *Journal of Homeland Security and Emergency Management*, 11(4):463–487. 5, 6, 8

["ResearchGate - Maria Papadaki, Kimberly Tam, Kevin D. Jones", 2016] "ResearchGate - Maria Papadaki, Kimberly Tam, Kevin D. Jones" (2016). "Threats and Impacts in Maritime Cyber Security".

["Reuters - Jonathan Saul", 2017] "Reuters - Jonathan Saul" (2017). "Global shipping feels fallout from Maersk cyber attack".

[Rid and Buchanan, 2015] Rid, T. and Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1-2):4–37. 3.1

[Rodofile et al., 2019] Rodofile, N. R., Radke, K., and Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *School of Electrical Engineering and Computer Science; Science and Engineering Faculty*. 5, 6, 7

[Rokseth et al., 2018] Rokseth, B., Utne, I. B., and Vinnem, J. E. (2018). Deriving verification objectives and scenarios for maritime systems using the systems-theoretic process analysis. *Reliability Engineering & System Safety*, 169:18–31. 8.2.1

[Rongrong et al., 2019] Rongrong, X., Xiaochun, Y., and Zhiyu, H. (2019). Framework for risk assessment in cyber situational awareness. *Iet Information Security*, 13(2):149–156. 5, 6, 8

[Ruan, 2017] Ruan, K. (2017). Introducing cybernomics: A unifying economic framework for measuring cyber risk. *Computers & Security*, 65:77–89. 5, 6

[Russo et al., 2019] Russo, P., Caponi, A., Leuti, M., and Bianchi, G. (2019). A web platform for integrated vulnerability assessment and cyber risk management. *Information*, 10(7):242. 6, 8

["Safety4Sea", 2018a] "Safety4Sea" (2018a). "Emergency Shutdown (ESD)".

["Safety4Sea", 2018b] "Safety4Sea" (2018b). "Emergency shutdown for tankers". 12

[Sahay et al., 2019a] Sahay, R., Meng, W., Sepúlveda Estay, D., Jensen, C., and Barfod, M. (2019a). Cybership-iot: A dynamic and adaptive sdn-based security policy enforcement framework for ships. *Future Generation Computer Systems*, 100:736–750. 3.4

[Sahay et al., 2019b] Sahay, R., Meng, W., Sepúlveda Estay, D., Jensen, C., and Barfod, M. (2019b). Cybership-iot: A dynamic and adaptive sdn-based security policy enforcement framework for ships. *Elsevier*, 100:736–750.

[Sahay et al., 2019c] Sahay, R., Meng, W., Sepúlveda Estay, D. A., Jensen, C. D., and Barfod, M. B. (2019c). Cybership-iot: A dynamic and adaptive sdn-based security policy enforcement framework for ships. *Elsevier*, 100:736–750. 6, 7, 8

[Sahay and Sepúlveda Estay, 2018a] Sahay, R. and Sepúlveda Estay, D. (2018a). *Work Package 2 Report - Cyber resilience for the shipping industry*. 12

[Sahay and Sepúlveda Estay, 2018b] Sahay, R. and Sepúlveda Estay, D. (2018b). *Work Package 3 and 4 Report - Cyber resilience for the shipping industry*. 1.2, 8, 9

[Sahoo et al., 2018] Sahoo, S., Mishra, S., Peng, J. C.-H., and Dragičević, T. (2018). A stealth cyber-attack detection strategy for dc microgrids. *IEEE Transactions on Power Electronics*, 34(8):8162–8174. 6, 7, 8

["Samid Mulla", 2016] "Samid Mulla" (2016). "Ships Bridge equipment". 12

[Sani et al., 2019] Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., and Dong, Z. Y. (2019). Cyber security framework for internet of things-based energy internet. *Future Generation Computer Systems*, 93:849–859. 6, 8

["SC Media - The Cyber Security Source - Doug Drinkwater", 2015] "SC Media - The Cyber Security Source - Doug Drinkwater" (2015). "Stuxnet-style attack on US smart grid could cost government $1 trillion".

["Schaltbau - Pintsch Aben",] "Schaltbau - Pintsch Aben". "MCU Control and Monitoring Unit".

[Schryen et al., 2015] Schryen, G., Wagner, G., and Benlian, A. (2015). Theory of knowledge for literature reviews: an epistemological model, taxonomy and empirical analysis of is literature. In *Proceedings of the Thirty Sixth International Conference on Information Systems, Fort Worth*.

[Scott-Hayward et al., 2013] Scott-Hayward, S., O'Callaghan, G., and Sezer, S. (2013). Sdn security: A survey. In *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, pages 1–7.

["Search Security - Margaret Rouse", 2001] "Search Security - Margaret Rouse" (2001). "CodeRed".

["Search Security - Margaret Rouse", 2005] "Search Security - Margaret Rouse" (2005). "Melissa virus".

["Search Security - Peter Dizikes", 2001] "Search Security - Peter Dizikes" (2001). "Nimda Disables Florida Court Computers".

["Search Security - Peter Dizikes", 2018] "Search Security - Peter Dizikes" (2018). "Warning: Code Red Virus Returning".

["Seattle Pacific University - Jennifer A. Martin", 2017] "Seattle Pacific University - Jennifer A. Martin" (2017). "Encryption Backdoors: A Discussion of Feasibility,Ethics, and the Future of Cryptography".

["Sebastian Modersheim and Luca Vigano", 2019] "Sebastian Modersheim and Luca Vigano" (2019). "The Open-source Fixed-point Model Checker for Symbolic Analysis of Security Protocols".

["Sebastian Modersheim, Luca Vigano, Omar Almousa, Riis Hanne Nielson", 2016] "Sebastian Modersheim, Luca Vigano, Omar Almousa, Riis Hanne Nielson" (2016). "Security Protocols: Specification, Verification, Implementation, and Composition".

["Seed Labs", 2014] "Seed Labs" (2014). "Hearbleed Attack Lab".

[Sepúlveda Estay, 2017a] Sepúlveda Estay, D. (2017a). *Managing cyber-risk and security in the global supply chain: a systems analysis approach to risk, structure and behaviour*. PhD thesis. 1.1, 1, 3.3

[Sepúlveda Estay, 2017b] Sepúlveda Estay, D. (2017b). *Managing cyber-risk and security in the global supply chain: a systems analysis approach to risk, structure and behaviour*. PhD thesis.

["Sertica", 2019] "Sertica" (2019). "Module Overview".

["Sgarks - Smart Grid Protection Against Cyber Attacks", 2015] "Sgarks - Smart Grid Protection Against Cyber Attacks" (2015). "Threat and Risk Assessment Methodology".

[Shah et al., 2013] Shah, S. A., Faiz, J., Farooq, M., Shafi, A., and Mehdi, S. A. (2013). An architectural evaluation of sdn controllers. In *2013 IEEE International Conference on Communications (ICC)*, pages 3504–3508.

[Shakibazad, 2019] Shakibazad, M. (2019). A framework to create a virtual cyber battlefield for cyber maneuvers and impact assessment. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, pages 1–11. 5, 6, 8

[Sharma et al., 2019] Sharma, A., Rathee, G., Kumar, R., Saini, H., Vijaykumar, V., Nam, Y., and Chilamkurti, N. (2019). A secure, energy-and sla-efficient (sese) e-healthcare framework for quickest data transmission using cyber-physical system. *Sensors*, 19(9):2119. 6, 7, 8

[Sheehan et al., 2019] Sheehan, B., Murphy, F., Mullins, M., and Ryan, C. (2019). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A: Policy and Practice*, 124:523–536. 6, 8

[Sheffi and Rice Jr, 2005] Sheffi, Y. and Rice Jr, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan management review*, 47(1):41.

[Sheridan, 2008] Sheridan, T. B. (2008). Risk, human error, and system resilience: fundamental ideas. *Human factors*, 50(3):418–426.

[Shin et al., 2013] Shin, S., Porras, P. A., Yegneswaran, V., Fong, M. W., Gu, G., and Tyson, M. (2013). FRESCO: Modular Composable Security Services for Software-Defined Networks. In *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*.

["Shippipedia", 2010] "Shippipedia" (2010). "Ship Automation and Control System".

["Singal K",] "Singal K". "Singal K - introduction".

["SKEMA",] "SKEMA". "Cybersecurity Threat Modeling". 12

["Skema - Interactive Knwoledge Platform For Transport And Logistics", 2019] "Skema - Interactive Knwoledge Platform For Transport And Logistics" (2019). "Navigation systems including developments in e-navigation".

["SKEMA Coordination Action", 2009] "SKEMA Coordination Action" (2009). "Navigation systems including developments in e-Navigation".

["Smithsonian - Sharon Weinberger", 2012] "Smithsonian - Sharon Weinberger" (2012). "Top Ten Most-Destructive Computer Viruses".

["Sodena",] "Sodena". "GECDIS - Operating Manual".

["Softpedia News - Lucian Constantin", 2011] "Softpedia News - Lucian Constantin" (2011). "McAfee Names MyDoom 'Exploit' of the Decade".

["Solace News", 2018] "Solace News" (2018). "Week 04 – Maritime Security Weekly Snapshot".

["Solarwinds MSP", 2018] "Solarwinds MSP" (2018). "Top Computer Security Vulnerabilities". 12

[Spyridopoulos et al., 2013] Spyridopoulos, T., Karanikas, G., Tryfonas, T., and Oikonomou, G. (2013). A game theoretic defence framework against dos/ddos cyber attacks. *Computers & Security*, 38:39–50. 5, 6, 7, 8

[Srinivas et al., 2019] Srinivas, J., Das, A. K., and Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. *Future Generation Computer Systems*, 92:178–188. 5, 6, 7, 8

["Stack Exchange - haimg", 2013] "Stack Exchange - haimg" (2013). "Which remote printing protocol to use?".

["Stack Exchange - Information Security - oldmud0", 2016] "Stack Exchange - Information Security - oldmud0" (2016). "How can I encrypt my print jobs?".

["Stack Exchange - mfinni", 2013] "Stack Exchange - mfinni" (2013). "How secure is traffic between domain members?".

[Stamatiou et al., 2003] Stamatiou, Y., Skipenes, E., Henriksen, E., Stathiakis, N., Sikianakis, A., Charalambous, E., Antonakis, N., Stølen, K., den Braber, F., Lund, M. S., et al. (2003). The coras approach for model-based risk management applied to a telemedicine service. *Proc. Medical Informatics Europe (MIE'2003)*. 3.5

["Statista", 2018] "Statista" (2018). "Number of pirate attacks against ships worldwide from 2009 to 2017.".

[Su, 2018] Su, R. (2018). Supervisor synthesis to thwart cyber attack with bounded sensor reading alterations. *Automatica*, 94:35–44. 5, 7, 8

[Sun and Yang, 2018a] Sun, Y. C. and Yang, G. H. (2018a). Event-triggered resilient control for cyber-physical systems under asynchronous dos attacks. *Information Sciences*, 465:340–352. 6, 7

[Sun and Yang, 2018b] Sun, Y. C. and Yang, G. H. (2018b). Periodic event-triggered resilient control for cyber-physical systems under denial-of-service attacks. *Journal of the Franklin Institute*, 355(13):5613–5631. 7, 8

[Sun and Yang, 2019] Sun, Y. C. and Yang, G. H. (2019). Robust event-triggered model predictive control for cyber-physical systems under denial-of-service attacks. *International Journal of Robust and Nonlinear Control*, 29(14):4797–4811. 6, 7, 8

["Symantec", 2017] "Symantec" (2017). "Ransom.Petya".

["Symantec", 2018] "Symantec" (2018). "VBS.LoveLetter.Var".

["Symantec - Security Response Team", 2017] "Symantec - Security Response Team" (2017). "Petya ransomware outbreak: Here's what you need to know".

[Taha et al., 2018] Taha, A. F., Qi, J., Wang, J., and Panchal, J. H. (2018). Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. *IEEE Transactions on Smart Grid*, 9(2):886–899. 6, 7, 8

[Tam and Jones, 2019] Tam, K. and Jones, K. (2019). Macra: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1):129–163. 5, 6, 8

[Tan et al., 2018] Tan, Y., Li, Y., Cao, Y., and Shahidehpour, M. (2018). Cyber-attack on overloading multiple lines: A bilevel mixed-integer linear programming model. *Ieee Transactions on Smart Grid*, 9(2):1534–1536. 6, 7, 8

[Tang et al., 2015] Tang, L.-A., Yu, X., Gu, Q., Han, J., Jiang, G., Leung, A., and Porta, T. L. (2015). A framework of mining trajectories from untrustworthy data in cyber-physical system. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 9(3):16. 6, 8

[Tang et al., 2018] Tang, M., Alazab, M., Luo, Y., and Donlon, M. (2018). Disclosure of cyber security vulnerabilities: time series modelling. *International Journal of Electronic Security and Digital Forensics*, 10(3):255–275. 6, 7, 8

[Taormina et al., 2017] Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., and Ostfeld, A. (2017). Characterizing cyber-physical attacks on water distribution systems. *Journal of Water Resources Planning and Management*, 143(5):04017009. 5, 6, 8

["Tap TV", 2017] "Tap TV" (2017). "ALL TIME BEST Somali Pirates VS Ship Security Compilation HD 2017".

[Tarao and Okamoto, 2016] Tarao, M. and Okamoto, T. (2016). Toward an artificial immune server against cyber attacks: enhancement of protection against dos attacks. *Procedia Computer Science*, 96:1137–1146. 3.1, 6, 8

[Taub, 1993] Taub, A. E. (1993). The mitre corporation. *Analytical Methods in Software Engineering Economics*, page 171. 5

["Team Viewer", 2017] "Team Viewer" (2017). "TeamViewer Security Statement".

["Team Viewer", 2018] "Team Viewer" (2018). "How secure is TeamViewer?".

["Team Viewer", 2019] "Team Viewer" (2019). "Remote Desktop".

["Tech World - Tamlin Magee", 2018] "Tech World - Tamlin Magee" (2018). "Can you hack a ship? Global maritime industry ripe for hacking".

["TechCrunch - John Biggs", 2016] "TechCrunch - John Biggs" (2016). "Why a Hacker Dumped Code Behind Colossal Website-Trampling Botnet".

["TechRepublic - James Sanders", 2018] "TechRepublic - James Sanders" (2018). "5 biggest security vulnerabilities of 2018".

["TechTarget What Is - Margaret Rouse", 2009] "TechTarget What Is - Margaret Rouse" (2009). "Conficker".

["Tempre Univeristy of Technology - Petteri Vistiaho", 2017] "Tempre Univeristy of Technology - Petteri Vistiaho" (2017). "Maritime Cyber Security Incident Data Reporting For Autonomous Ship".

["The Guardian - Alex Hern", 2018] "The Guardian - Alex Hern" (2018). "What is GDPR and how will it affect you?".

["The Guardian - Nadia Khomami and Olivia Solon", 2017] "The Guardian - Nadia Khomami and Olivia Solon" (2017). "Accidental hero - halts ransomware attack and warns: this is not over".

["The Guardian - Tom McCarthy", 2015] "The Guardian - Tom McCarthy" (2015). "NSA director defends plan to maintain 'backdoors' into technology companies".

["The Hacker News - Swati Khandelwal", 2017] "The Hacker News - Swati Khandelwal" (2017). "WannaCry Kill-Switch(ed)? It's Not Over! WannaCry 2.0 Ransomware Arrives".

["The maritime Executive", 2015] "The maritime Executive" (2015). "Maritime Cyber Attacks: Changing Tides".

["The New Your Times - Nicole Perlroth", 2016] "The New Your Times - Nicole Perlroth" (2016). "Hackers Used New Weapons to Disrupt Major Websites Across U.S.".

["The Register - Christopher Williams", 2009] "The Register - Christopher Williams" (2009). "Conficker seizes city's hospital network".

["The Register - Richard Chirgwin", 2018] "The Register - Richard Chirgwin" (2018). "IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz".

[Tjahjono et al., 2017] Tjahjono, B., Esplugues, C., Ares, E., and Pelaez, G. (2017). What does industry 4.0 mean to supply chain? *Procedia Manufacturing*, 13:1175–1182.

[Tonn et al., 2019] Tonn, G., Kesan, J. P., Zhang, L., and Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport Policy*. 3.4

[Torabi et al., 2016] Torabi, S. A., Giahi, R., and Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, 89:201–218.

["Tototheo",] "Tototheo". "Ships Movement Information Display System". 12

["Tototheo Maritime",] "Tototheo Maritime". "BNWAS Basic (Sam Electronics)". 12

["Tototheo Maritime", 2019a] "Tototheo Maritime" (2019a). "Bon Voyage System (BVS) delivered by NAVTOR". 12

["Tototheo Maritime", 2019b] "Tototheo Maritime" (2019b). "Products". 12

[Tranfield et al., 2003] Tranfield, D., Denyer, D., and Smart, P. (2003). Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *British journal of management*, 14(3):207–222. 10.2

["Transaction On Maritime Science - Dean Sumića, Dragan Perakovićb, Marinko Jurčević", 2014] "Transaction On Maritime Science - Dean Sumića, Dragan Perakovićb, Marinko Jurčević" (2014). "Contribution to ECDIS Reliability using Markov Model".

["TransNav - S.Žuškin, D.Brčić, S.Valčić", 2017] "TransNav - S.Žuškin, D.Brčić, S.Valčić" (2017). "ECDIS Possibilities for BWE Adoption".

["Trend Micro - Marco Balduzzi, Kyle Wilhoit, Alessandro Pasta", 2014] "Trend Micro - Marco Balduzzi, Kyle Wilhoit, Alessandro Pasta" (2014). "A Security Evaluation of AIS".

[Tzannatos, 2003] Tzannatos, E. (2003). A decision support system for the promotion of security in shipping. *Disaster Prevention and Management: An International Journal*, 12(3):222–229.

["UN/EDIFACT", 1999] "UN/EDIFACT" (1999). "United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport".

["United Nations", 2018] "United Nations" (2018). "REVIEWOF MARITIMETRANSPORT".

["Univerity of Illionois Press - John von Neumann", 1966] "Univerity of Illionois Press - John von Neumann" (1966). "Theory of Self-Reproducing Automata".

["University of Arkansas - Zachary King, Shucheng Yu", 2017] "University of Arkansas - Zachary King, Shucheng Yu" (2017). "Investigating and securing communications in the Controller Area Network (CAN)".

["University of Ljubljana Portoro - Daneiele Borio, Ciro Gioia, Franc Dimic, Matej Bazec, Joaquim Fortuny, Gianr "University of Ljubljana Portoro - Daneiele Borio, Ciro Gioia, Franc Dimic, Matej Bazec, Joaquim Fortuny, Gianmarco Baldini, Marco Basso" (2015). "An Experimental Evaluation of the GNSS Jamming Threat".

["University of Luxembourg - Marlon Fraile, Margaret Ford, Olga Gadyatskaya, Rajesh Kumar, Marielle stoeling "University of Luxembourg - Marlon Fraile, Margaret Ford, Olga Gadyatskaya, Rajesh Kumar, Marielle stoelinga, Rolando Trujillo-Rasua" (2016). "Using attack-defense trees to analyze threats and countermeasures in an ATM: A case study".

["University of Luxembourg - Patrick Schweitzer", 2013] "University of Luxembourg - Patrick Schweitzer" (2013). "Attack–Defense Trees".

["University of Luxemburg - Barbara Kordy",] "University of Luxemburg - Barbara Kordy". "Attack–Defense Tree Methodology for SecurityAssessment".

["University of Malta - Robert Buttigieg, Mario Farrugia, Clyde Meli", 2018] "University of Malta - Robert Buttigieg, Mario Farrugia, Clyde Meli" (2018). "Security issues in controller area networks in automobiles".

["University of Wroclaw - Kinga Gancarek", 2018] "University of Wroclaw - Kinga Gancarek" (2018). "Celowe zagłuszanie sygnału GNSS jako zagrożenie dla pracy stacji permanentnych (Intentional interfering GNNS signal as threat to permament station's work)".

["University of Wroclaw - Piotr Bryłka", 2017] "University of Wroclaw - Piotr Bryłka" (2017). "Test odporności odbiornika GNSSna celowe zakłócanie sygnału satelitarnego (Resistance test of the GNSS receiver on indented interference of satellite signal)".

["University of York - Muhammed Mustafa Aydin", 2016] "University of York - Muhammed Mustafa Aydin" (2016). "Engineering Threat Modelling Tools forCloud Computing".

["UPI", 2009] "UPI" (2009). "Virus strikes 15 million PCs".

[Van Niekerk, 2018] Van Niekerk, B. (2018). Information warfare as a continuation of politics: An analysis of cyber incidents. In *2018 Conference on Information Communications Technology and Society (ICTAS)*, pages 1–6. IEEE. 3.3

["Veem Gyro",] "Veem Gyro". "Gyro Solution".

["Venom Crowdstrike - Jason Geffner and CrowdStrike", 2015] "Venom Crowdstrike - Jason Geffner and CrowdStrike" (2015). "Venom - Virtualized Environment Neglected Operations Manipulation".

["Venturebeat - Brian Fox", 2018a] "Venturebeat - Brian Fox" (2018a). "The tech supply chain is more vulnerable than ever".

["Venturebeat - Brian Fox", 2018b] "Venturebeat - Brian Fox" (2018b). "The tech supply chain is more vulnerable than ever".

[Wagner et al., 2017] Wagner, N., Şahin, C., Winterrose, M., Riordan, J., Hanson, D., Peña, J., and Streilein, W. W. (2017). Quantifying the mission impact of network-level cyber defensive mitigations. *Journal of Defense Modeling and Simulation*, 14(3):201–216. 5, 6, 8

[Wang et al., 2017a] Wang, C., Ten, C. W., Hou, Y., and Ginter, A. (2017a). Cyber inference system for substation anomalies against alter-and-hide attacks. *Ieee Transactions on Power Systems*, 32(2):7484326, 896–909. 6, 7, 8

[Wang et al., 2018a] Wang, C., Zhu, Y., Shi, W., Chang, V., Vijayakumar, P., Liu, B., Mao, Y., Wang, J., and Fan, Y. (2018a). A dependable time series analytic framework for cyber-physical systems of IoT-based smart grid. *ACM Transactions on Cyber-physical Systems*, 3(1):7 (18 pp.), 7 (18 pp.). 5, 6, 8

[Wang et al., 2017b] Wang, J., Hui, L. C., Yiu, S. M., Zhou, G., and Zhang, R. (2017b). F-DDIA: A framework for detecting data injection attacks in nonlinear cyber-physical systems. *Security and Communication Networks*, 2017:9602357. 6, 7

[Wang et al., 2004] Wang, J., Sii, H., Yang, J., Pillay, A., Yu, D., Liu, J., Maistralis, E., and Saajedi, A. (2004). Use of advances in technology for maritime risk assessment. *Risk Analysis: An International Journal*, 24(4):1041–1063. 8.2.1

[Wang and Xu, 2019] Wang, M. and Xu, B. (2019). Observer-based guaranteed cost control of cyber-physical systems under dos jamming attacks. *European Journal of Control*, 48:21–29. 7, 8

[Wang et al., 2018b] Wang, W., Cammi, A., Di Maio, F., Lorenzi, S., and Zio, E. (2018b). A monte carlo-based exploration framework for identifying components vulnerable to cyber threats in nuclear power plants. *Reliability Engineering & System Safety*, 175:24–37. 6

[Wang and Wagner, 2016] Wang, Y. and Wagner, S. (2016). Towards applying a safety analysis and verification method based on stpa to agile software development. In *2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED)*, pages 5–11. IEEE.

["Wartsila",] "Wartsila". "Navigation Automation Control System". 12

["Wartsila Encyclopedia of Marine Technology", a] "Wartsila Encyclopedia of Marine Technology". "Central Cooling Water System". 12

["Wartsila Encyclopedia of Marine Technology", b] "Wartsila Encyclopedia of Marine Technology". "Fuel oil system". 12

["We Live Security by ESET - Miguel Ángel Mendoza", 2018] "We Live Security by ESET - Miguel Ángel Mendoza" (2018). "Vulnerabilities reached a historic peak in 2017".

[West, 2018] West, J. (2018). A prediction model framework for cyber-attacks to precision agriculture technologies. *Journal of Agricultural & Food Information*, 19(4):307–330. 6

["Who Is Hosting This - KeriLynn Engel", 2015] "Who Is Hosting This - KeriLynn Engel" (2015). "Which Computer Viruses Caused The Most Damage Around The World?".

["Wierd - Andy Greenberg", 2018] "Wierd - Andy Greenberg" (2018). "The untold story of NotPetya, The most devastating cyberattack in history".

["Wiki Dot", 2004] "Wiki Dot" (2004). "My Doom".

["Wireshark", 2019] "Wireshark" (2019). "Wireshark is the world's foremost and widely-used network protocol analyzer".

[Wirtz and Weyerer, 2017] Wirtz, B. W. and Weyerer, J. C. (2017). Cyberterrorism and cyber attacks in the public sector: How public administration copes with digital threats. *International Journal of Public Administration*, 40(13):1085–1100. 6

["World Economic Forum - Thomas Holt", 2017] "World Economic Forum - Thomas Holt" (2017). "Why is software so vulnerable, and what can be done?".

["World Maritime News", 2017] "World Maritime News" (2017). "Nightmare Scenario: Ship Critical Systems Easy Target for Hackers".

["World Maritime News", 2019] "World Maritime News" (2019). "Nightmare Scenario: Ship Critical Systems Easy Target for Hackers".

[Wróbel et al., 2018] Wróbel, K., Montewka, J., and Kujala, P. (2018). System-theoretic approach to safety of remotely-controlled merchant vessel. *Ocean Engineering*, 152:334–345. 8.2.1

[Wu et al., 2018] Wu, G., Sun, J., and Chen, J. (2018). Optimal data injection attacks in cyber-physical systems. *Ieee Transactions on Cybernetics*, 48(12):3302–3312. 5, 6, 7

[Xiang et al., 2018] Xiang, Y., Wang, L., and Zhang, Y. (2018). Adequacy evaluation of electric power grids considering substation cyber vulnerabilities. *International Journal of Electrical Power and Energy Systems*, 96:368–379. 6, 7, 8

[Yadegar et al., 2019] Yadegar, M., Meskin, N., and Haddad, W. M. (2019). An output-feedback adaptive control architecture for mitigating actuator attacks in cyber-physical systems. *International Journal of Adaptive Control and Signal Processing*, 33(6):943–955. 5, 6, 7, 8

[Yelan and Hui, 2014] Yelan, H. and Hui, C. (2014). Study on the architecture of intelligent warship's tsce based on multi-view. In *2014 13th International Symposium on Distributed Computing and Applications to Business, Engineering and Science*, pages 220–223.

[Yong et al., 2018] Yong, S. Z., Zhu, M., and Frazzoli, E. (2018). Switching and data injection attacks on stochastic cyber-physical systems: Modeling, resilient estimation, and attack mitigation. *Acm Transactions on Cyber-physical Systems*, 2(2):9 (2 pp.), 9 (2 pp.). 5, 7, 8

[Young et al., 2016] Young, D., Lopez Jr, J., Rice, M., Ramsey, B., and McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. *International Journal of Critical Infrastructure Protection*, 14:43–57. 6, 8

[Yousefi et al., 2018] Yousefi, A., Rodriguez Hernandez, M., and Lopez Peña, V. (2018). Systemic accident analysis models: A comparison study between accimap, fram, and stamp. *Process Safety Progress*. 8.2.1

[Yuan and Xia, 2018] Yuan, H. and Xia, Y. (2018). Resilient strategy design for cyber-physical system under dos attack over a multi-channel framework. *Information Sciences*, 454:312–327. 6, 7, 8

[Yuanbao et al., 2015] Yuanbao, C., Shuang, H., and Yunfei, L. (2015). Intrusion tolerant control for warship systems. In *4th International Conference on Computer, Mechatronics, Control and Electronic Engineering (ICCMCEE 2015)*, pages 165–170. 2

[Yunfei et al., 2015] Yunfei, L., Yuanbao, C., Xuan, W., Xuan, L., and Qi, Z. (2015). A framework of cyber-security protection for warship systems. In *2015 Sixth International Conference on Intelligent Systems Design and Engineering Applications (ISDEA)*, pages 17–20. 2

[Yunos et al., 2015] Yunos, Z., Ahmad, R., and Mohd Sabri, N. A. (2015). A qualitative analysis for evaluating a cyber terrorism framework in malaysia. *Information Security Journal*, 24(1-3):15–23. 5, 8

["ZDnet - Danny Palmer", 2017] "ZDnet - Danny Palmer" (2017). "Petya ransomware: Cyberattack costs could hit $300m for shipping giant Maersk".

[Zhan et al., 2013] Zhan, Z., Xu, M., and Xu, S. (2013). Characterizing honeypot-captured cyber attacks: Statistical framework and case study. *Ieee Transactions on Information Forensics and Security*, 8(11):6587320, 1775–1789. 8

[Zhang et al., 2013] Zhang, J., Seet, B.-C., Lie, T.-T., and Foh, C. H. (2013). Opportunities for software-defined networking in smart grid. In *2013 9th International Conference on Information, Communications Signal Processing*, pages 1–5.

[Zhang et al., 2017] Zhang, R., Zhu, Q., and Hayel, Y. (2017). A bi-level game approach to attack-aware cyber insurance of computer networks. *IEEE Journal on Selected Areas in Communications*, 35(3):779–794. 5, 6, 8

[Zhang et al., 2018] Zhang, W., Wang, Z., Liu, Y., Ding, D., and Alsaadi, F. E. (2018). Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks. *International Journal of Robust and Nonlinear Control*, 28(1):53–67. 8

8 Appendix A - The prevention of cyber-attacks in the Cybership Model (WP3)

Note: This Section is based on the report for WP3 and WP4 of the project CyberShip [Sahay and Sepúlveda Estay, 2018b]

The first section of the WP3 and WP4 report is related to Work Package #3, and it has to do with the prevention of cyber-attacks for the case of a CyberShip. This section of the report is divided into three parts, representing three levels in which prevention of cyber-risks has been studied in this research.

A first level is strategic-managerial. This is an analysis of the current frameworks found in literature for the management of cyber-risks in supply operations and the derivation of a proposed encompassing framework for cyber attack prevention based on the consequences of such an attack. This framework is presented by using an analogy of a seismic or flood wave.

A second level of analysis is tactical, through the analysis of different risk evaluation frameworks and their applicability to the analysis of a CyberShip system. For this analysis, four different risk evaluation frameworks are presented.

The third level of analysis is operational. In this level of analysis, the detection phase of the Software-Defined Network (SDN) framework as a way to actively monitor the traffic of information to detect suspicious or fraudulent traffic. This research thus presents a real-time tool to reduce the likelihood of cyber-attacks.

8.1 Strategic Managerial - Prevention framework

8.1.1 Introduction

Cyber risk management is a relatively novel field with only few frameworks available that have been specifically adapted and/or validated for the management of this kind of risks in CyberShip operations.

This part of the report contributes to closing this gap by proposing a framework derived from existing literature on cyber-risks. Initially, a structured literature review reveals the approaches used to manage the risks associated to the use of information and communication technologies (ICT). These approaches are categorized and a framework is proposed to give a structure to this categorization.

We followed the structured literature review (SLR) as proposed by Durach et al. [Durach et al., 2017a], details of which can be found in the appendix of this report.

As a result of this SLR analysis, recurrent themes are identified during the literature review process. These themes are knowledge areas under which the paper contents can be clustered. This process of theme identification and categorization results in a list of twelve knowledge areas in the field of supply chain cyber risk management according to the times these were found in the papers that were analyzed. Each of these categories is listed with a brief description to the concepts it contains, and with some reference examples of the papers that refer to these concepts. For a full list of the papers, please refer to the Appendix.

1. **Compliance:** In the context of supply chain cyber risk management, risk compliance is understood as the identifying of the legislation affecting this area and the standards that must be met, and meeting these regulations and standards [4].

2. **Situational Awareness:** It involves the identification of potential cyber threats, vulnerabilities and risks associated to the supply chain, as well as the ability to assess the probability and impacts of occurrence of potential cyber risk events.

3. **Governance:** IT governance defines who, where and how decisions affecting IT are made [7]. Moreover, it can be used to provide adequate authority to cyber security to affect decisions in other managerial areas which have an impact on or are impacted by cyber risks.

4. **Pre-Event Knowledge Management:** it is understood as making the best use of the knowledge available to achieve organizational objectives. Supply chain resilience can be improved by

cultivating knowledge management in a situation previous to a risk-event, due to bringing a better general understanding of the supply chain and the human resources [6]. In this regard, the practices recommended are related to education and training with respect to cyber risks, and the creation of a resilience/risk management culture.

5. **Cyber-Security:** it refers to the protection of the assets and systems (physical or digital) involved with the storing and processing of information in digital format. Once the risks have been identified and assessed, then countermeasures must be put in place. Proactive measures and techniques used to prevent previously identified cyber risks, before the risk event takes place. In general, information security measures tend to focus on the protection of the confidentiality, integrity and availability of information [8].

6. **Visibility:** refers to generating knowledge and awareness on the current status of supply chain operating assets and the environment [6],[9]. It involves being able to detect risk events on the supply chain (i.e. affecting supply chain partners) which also have the potential of impacting the focal company. Finding issues as soon in the lifecycle as possible provide for time and better availability of resources to deal with them.

7. **Velocity:** supply chain velocity is defined as "distance over time" [10], referring to how rapidly the supply chain reacts to disruptive events.

8. **Ability to Adapt:** The ability to adapt can be understood as being able to manage critical resources and operations in the supply chain and adjust them in response to challenges and opportunities [6],[9]. This ability is also covered in the supply chain resilience literature through two elements: flexibility and redundancy [6]. In this case, flexibility refers to flexibly use of processes, supply and/or demand management. Redundancy, on the other hand, builds on maintaining excess capacity as a mechanism to adapt to disruptive events [6].

9. **Recovery Management:** it involves the identification of critical vulnerabilities and risks that the firm should prepare for, the development of contingency plans for recovery and mission assurance after a risk event, planning for the availability of resources needed for the execution of post-disruption plans, and the effective and efficient execution of those plans when needed [6].

10. **Market Position and Financial Strength:** In the context of supply chain resilience, market position refers to the status of an organization and/or its products in specific markets, while financial strength reflects its capacity to absorb variations in cash flow [9]. Both concepts are instrumental in increasing a firm's chance of recovering from supply chain disruptions [6]. This way, market share, product differentiation and customer loyalty are some sub-factors understood to form part of the market position, while financial reserves, liquidity, portfolio diversification and insurance are elements under the broader concept of financial strength [9].

11. **Post-Event Knowledge Management:** Post-event knowledge management focuses on enhancing the ability of the supply chain to learn from past events, through elements like post-event feedback, improvement through education and training, and gathering of cost/benefit knowledge [6], which can be used for updating contingency plans and innovating by improving or changing resilience mechanisms [11]. Some elements proposed for pre-event knowledge management are also useful in post-event knowledge management, like education and training about information security, and the embeddedness of key learnings in the organizational security culture.

12. **Social Capital:** Social capital involves the network of relationships formed with suppliers, which can also be seen as a valuable asset, and an enduring source of advantage. Social capital contains "the information, trust and norms of reciprocity inhering within social networks" and is linked to the resilient concepts of absorbing shock and adapting to change [12], as well as a strengthened ability among the supply chain partners to learn from each other [6].

8.1.2 A structure for the effects of cyber-attacks

A dynamic approach is followed to classify the themes described in the previous section. A dynamic approach as one that considers time as the main variable of study. In the case of a cyber-attack, the occurrence of a hypothetical event related to a cyber-attack is taken as the point of reference in time, and themes found in literature are clustered and presented as belonging to a moment in time that can be 1) before, 2) during or 3) after (post) the realization of this hypothetical event. A representation of this perspective can be seen in figure 19.

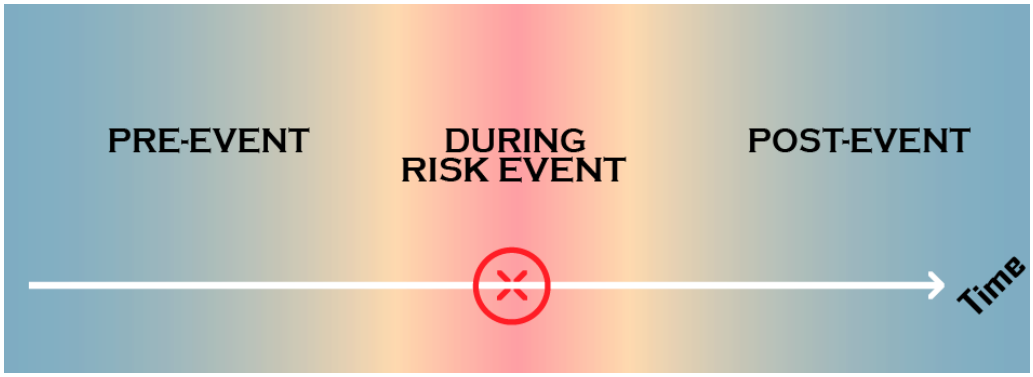

Figure 19: A dynamic representation of a cyber-attack

In published literature, other authors have used similar approaches, especially in the area of supply chain resilience. For example, Herrera & Janczewski [11] and Ali et al. [6] present frameworks where the different themes belong to one of the three stages in a disruption event: pre-disruption, during-disruption and post-disruption. Additionally, their positions differ in relation to how far they are from the moment in time in which a risk event occurs, and whether they take place before or after a risk event.

This proposed dynamic approach positions all the identified themes in a sort of timeline, position related to how each element interacts in time, both 1) with the prevention of, response to, and recovery from cyber risk events, as well as with their 2) short, medium or long-term effects. As a result, the main elements from section III are represented on a timeline as shown in figure 20.

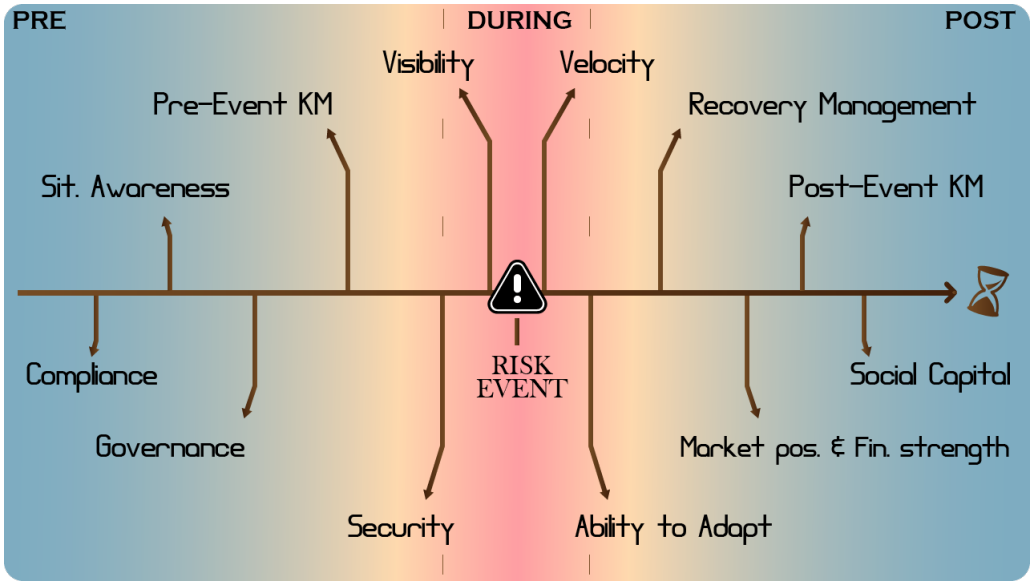

Figure 20: Main themes on the timeline framework

The order of the elements shown in the timeline is derived from literature, as it has been argued that *Compliance* can be regarded as the precedent for the management of cyber risks, where the risks

and security standards to conform to exert influence into the risk assessment process [4], which forms part of *Situational Awareness*. Good situation awareness in the context of supply chain resilience leads to the understanding of the vulnerabilities of the supply chain and the planning for risk events, allowing for the elaboration of early warning strategies or continuity planning and the identification of supporting elements needed for them, like information sharing, coordination, and the availability of knowledge [6]. Therefore, it is understood that situation awareness is also needed early in the process of Supply Chain Cyber Risk Management (SCCRM).

Governance, on the other hand, feeds on the outcomes from *Compliance* and *Situation awareness* [4], defining how IT-related decisions should be made across the organization and the supply chain to manage cyber risks. Subsequently, the previous elements define what knowledge should be created and nurtured among the members of the organization and the supply chain when it comes to managing cyber risks, which is achieved through proper Knowledge Management prior to the realization of the risk event [6].

Cyber Security mechanisms must be in place to prevent the exploitation of vulnerabilities from adversaries and to protect the goals of the supply chain from incoming threats [13]. However, if the security in place is not enough to stop the cyber-threat, then enough supply chain *Visibility* is needed to ensure that a cyber-attack is discovered before it has caused significant damage [9].

If the cyber event is spotted, then *Velocity* mechanisms are needed to allow for a fast response [10]. In the chaos of a disruption, the *Ability to Adapt* is instrumental to allow continuity of operations, through for example a flexible redistribution of resources through different processes and the use of previously redundant capacity [6].

The existence of *Recovery Management* programs helps in prioritizing the resources and coordinated actions needed throughout the supply chain to recover from a cyber-disruption, by providing valid contingency plans and ensuring the availability of resources needed to return the enterprise to the normal state [14]. If it turns out that there are no contingencies available, or these are inadequate, then the company will rely solely on absorbing the damage through its *Market Position and Financial Strength* [9].

As operations recovers from the disruption, it is important to use the very valuable lessons gained through the experience to update and improve the practices across the different SCCRM mechanisms previously described, through proper *Post-Event Knowledge Management* [6].

Finally, the *Social Capital* that is formed in turbulent times is also a valuable asset, that can enhance collaborative attitudes across different levels in the supply chain, towards a better management of the common risks faced and the exploitation of new opportunities [12].

This sense of distance in time allows for alternate approaches to the problem of managing cyber risks in the supply chain, through the introduction of concepts like strategic and tactical elements, as depicted in figure 21.

Strategic elements, understood as those elements that look at the problem from a more long-term point of view, and tactical mechanisms as those that approach it from a shorter time span, then this division allows to identify mechanisms that are more relevant in either the short (tactical) or the long (strategical) term, before and/or after the realization of a risk event, and how they can complement each other in a supply chain cyber-risk management plan.

8.1.3 Impact-Wave analogy for cyber risk effects

The themes found in literature and their places in the timeline as proposed by the framework in the previous section, can be better understood through the use of an analogy, which considers the ripple or wave created by an impact against a surface (e.g. like ripples on the water, or the seismic waves after an earthquake).

As part of this analogy, the timeline represents the perspective of a focal organization, which forms part of a supply chain. The point of reference is the "point of impact" in which a cyber-event "hits" the organization, as in figure 22.

From an analysis using this framework, for a risk to successfully impact the organization, it must cut across a number of defensive mechanisms on the left side, located either far in time (strategic

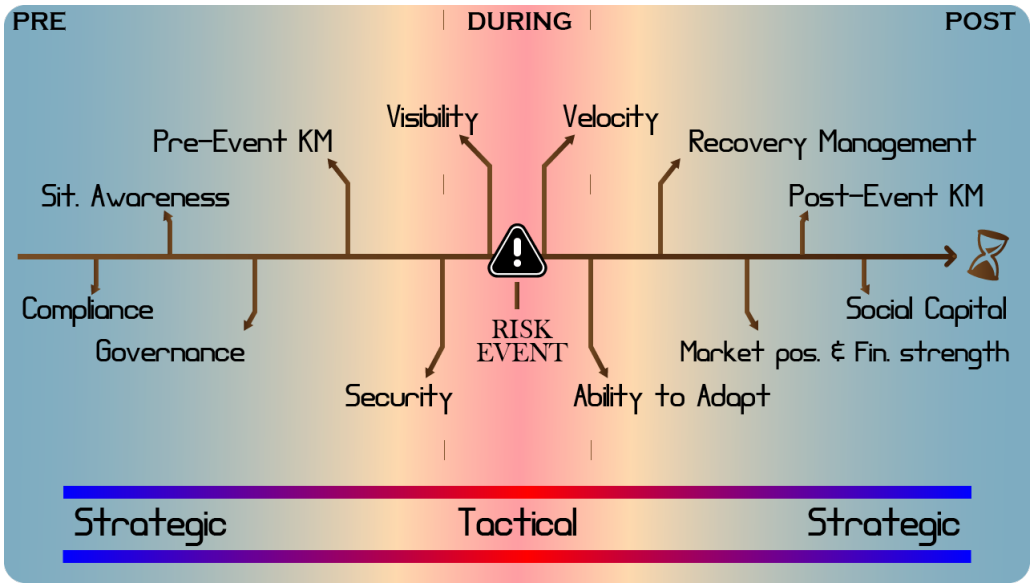

Figure 21: Strategic and Tactical view of the timeline framework

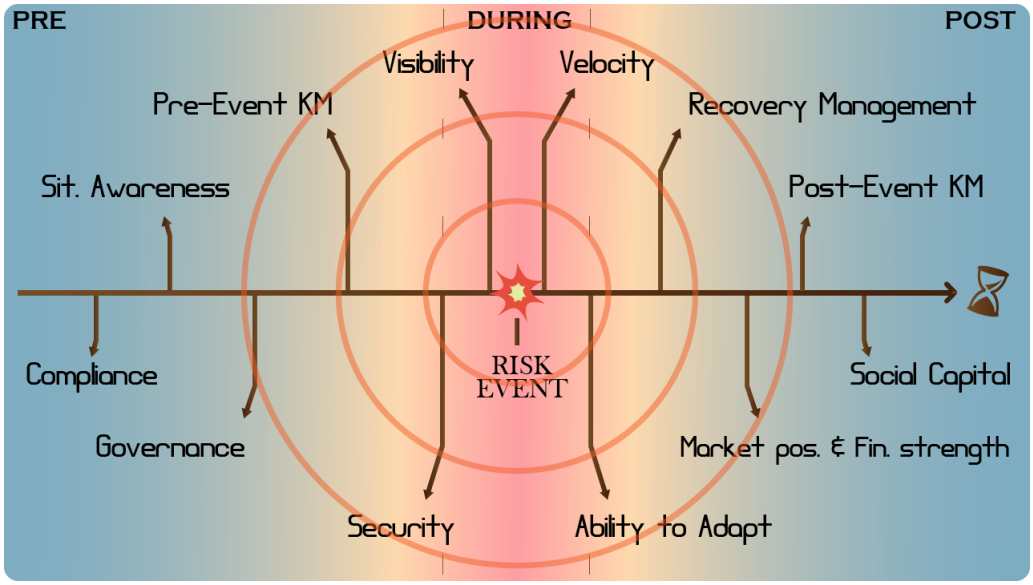

Figure 22: Point of impact for the timeline framework

mechanisms) or close (tactic/operational mechanisms). These can also be understood as lines of defense.

When the lines of defense are not able to stop a cyber-event, an impact takes place. This impact then creates a "shock wave", or a "ripple", that can expand in time as shown in figure 23. The magnitude of those waves and their reach will depend on a number of factors.

On the left side of the framework, there are the elements that can reduce the strength of (or even stop) the impact (i.e., in this analogy the speed at which the cyber-bullet impacts the system), which will directly affect the magnitude of the shock wave on impact. However, the function of the elements placed on the right side of the framework is to mitigate the "disastrous" effects of those waves by absorbing them.

For the sake of this analogy, it can be understood that these waves are able to reach as far as the next absorption mechanism in place is able to absorb a shock wave of equal or bigger magnitude. If a wave is stronger than what a certain mechanism can absorb, then its effects will continue to spread and the next mechanism in time will have to actuate, until the shock wave is stopped.

As an example of the time line use, consider the the left side of the time line from the time of

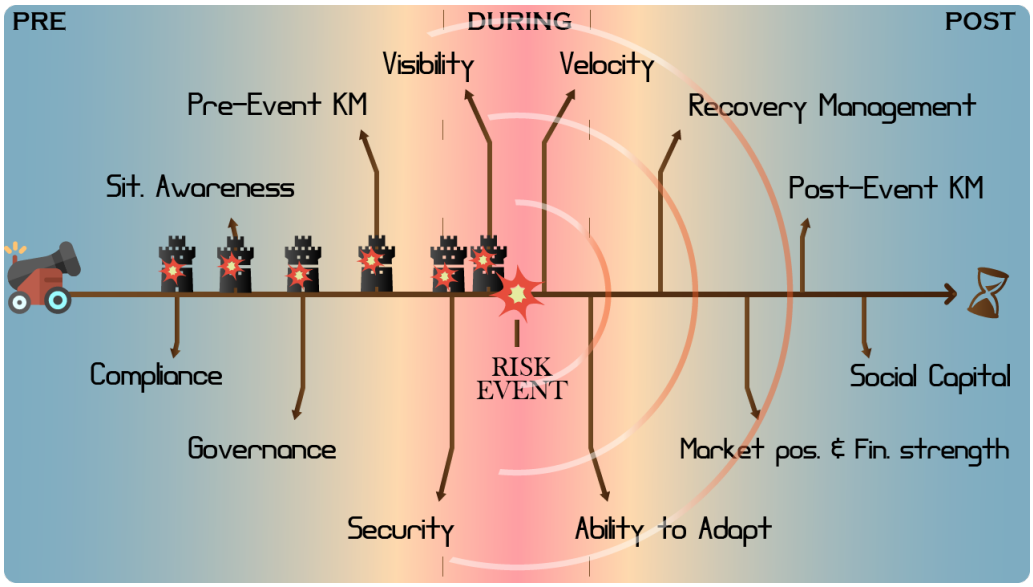

Figure 23: Defenses and ripple effects of a cyber-attack with the time line framework

the risk event. It could be the case that the regulatory requirements (*Compliance*) are not enough to adequately address a certain cyber-threat. If this threat is not made aware of as part of the risk identification and assessment process, then different governing processes and structures may not be in place to correctly address them, and the knowledge management (KM) needed to treat it will not be there either.

It could also happen that this cyber-attacker, making use of an inherent vulnerability in the system, is able to avoid the cyber security in place. Then, if the *Visibility* mechanisms are not designed to detect the actions of a cyber-attack whose possibility had not been identified before, the organization might have been hit by a cyber-event without (maybe) being able to notice it.

For example, if a cyber-breach occurs and the *Visibility* and *Velocity* mechanisms in place are not able to detect and react to the attack fast enough, then *Adaptive mechanisms* could also be not enough to contain and stop it from spreading and/or allowing the attackers to access the IT systems of the organization. If such a breach escalates, then the organization starts relying on the existence of contingency plans to recover from the disruption, together with facing a test on its financial and market strength. If an organization is not able to stop this "wave", then the "disaster" could become comparable to that of a "cyber-tsunami", in which the continuity of the company's mission is at stake.

Even though the effects of a cyber-tsunami (figure 24) are not the same as an actual tsunami, since an organization's physical assets might still be there for some more time, their business model could have been affected critically, due to financial un-sustainability as a consequence of, for example, loss of competitive advantage (e.g., from IP theft), reputation loss, increased costs or the technical impossibility of continuing critical operations within a reasonable time frame.

In such a condition, the only things left for the organization might be *Social Capital* such as the personal and collective knowledge contained in the organization or the value of the network of personal relations formed within the value chain, and learning from past experiences (*Post-Event KM*), which could be used to innovate and build a new start for the organization after the risk event.

8.2 Tactical - Risk analysis frameworks

All risk analysis methods to some extent relate to a more generic process of identifying, quantifying and reducing risk and traditional approaches have followed the "analytic reduction" method of separating a problem into smaller sub-units, understanding the behaviour of each unit separately and then integrating this understanding into an understanding of the whole.

Traditional notions of risk consider it to be the probability of failure of a system, as derived from two characteristics of the system, the probability of occurrence of a specific mode of failure that leads

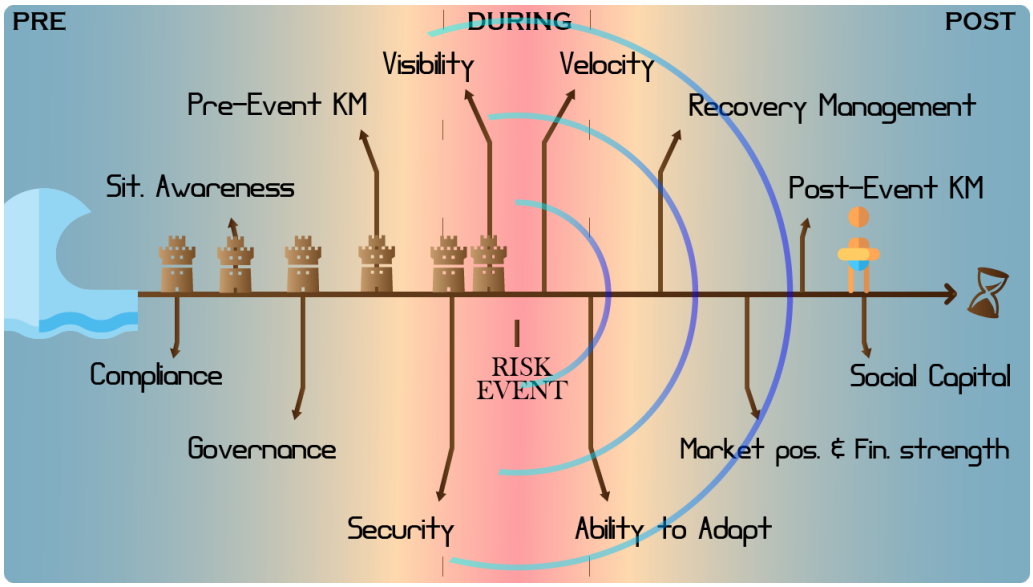

Figure 24: Cyber-tsunami wave analogy with the timeline framework

to an unwanted event, and the consequence or severity of the failure mode materializing. These ways in which the mode of failure can materialize have been identified normally through methods such as fault tree analysis, event tree analysis, the HAZard and OPerability analysis (HAZOP), and the Failure Mode and Effects Analysis (FMEA). These methods link a cause with an undesirable effect, but *"are unable to include aspects such as design errors, such as software flaws, component interaction accidents, cognitively complex human decision-making errors, and social, organizational and management factors contributing to an unwanted event"* [Leveson, 2011]. In order to address this gap, this work considers the following risk analysis frameworks:

- Systems Theoretic Process Analysis
- Attack fault tree
- Attack defense tree, and
- Priced-timed automata

8.2.1 STPA - Systems theoretic process analysis

The STPA is a risk analysis methodology for safety and security, based on systems theory rather than traditional analytic reduction and reliability theories.It conceptualizes losses as a result of the inadequate interaction between components in the system due to a lack of adequate safety constraints. Consequently, safe and secure operation is seen as an emergent property resulting from the interactions between system components and the environment [Leveson, 2011].

STPA is a model based on systems theory rather than traditional analytic reduction and reliability theory. A safe operation is seen as an emergent property resulting from the interactions between the system components and with the environment. The problem of avoiding "accidents" (i.e., unplanned loss events) thus becomes a dynamic control problem of limiting the ways in which the system can behave. Figure 25 is a representation of a generic controlled process.

This representation includes a controlled process that converts inputs to outputs, sensors that convert the state of the system into a signal that is understood by a controller, which then triggers some type of actuator to influence the controlled process. In this way a circular loop of control is formed, which allows for *continuous monitoring and adjustment* of a process.

Representing cyber risks through a control system is not trivial, since from this perspective cyber-attacks are not events that happen from external sources, but rather events which systems such as CyberShip are "mis-designed" to experience. In this context, risky cyber-events are an *unintended*

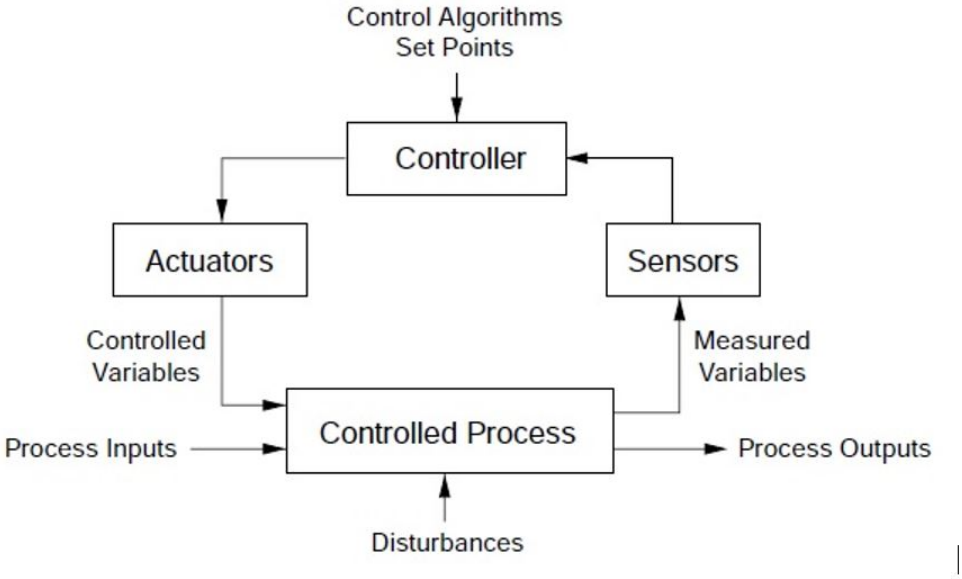

Figure 25: Basic control system

consequence that results from incomplete requirements at the time of system design. A systemic analysis seeks to identify this "unrequested" design that creates cyber-vulnerability, and determine design changes through which a cyber-vulnerable behavior is less likely to occur or no longer possible.

Extensive literature has been published about the description of the STPA methodology. The systems theoretic Accident Model and Process (STAMP) method with its hazard analysis version STPA (Systems Theoretic Process Analysis) [Leveson, 2004] has been identified as the most cited model for systemic risk analysis [Yousefi et al., 2018]. Extensive literature has been published about the description of the STAMP methodology framework for risk analysis [Estefan et al., 2007], [Leveson, 2011], [Dallat et al., 2017], [Altabbakh et al., 2014], with examples of application in different industries, such as medical [Antoine, 2013], environmental [Hardy and Guarnieri, 2011], robotics [Mitka,], power production [Karami et al., 2015], software development [Wang et al., 2004], and defense [Chiesi, 2016].

The use of systemic methods to understand risk in maritime systems has also been advanced by different groups of researchers. For example, STPA has been used to derive verification objectives and hazardous scenarios in maritime systems [Rokseth et al., 2018], to identify causal scenarios and factors that drive maritime incidents and accidents [Puisa et al., 2018] and it has been advanced in the conceptual design autonomous vessels [Banda et al., 2019].

In connection to cyber risks, STPA has been used to identify the conditions of risk for the case of remotely-controlled merchant vessels [Wróbel et al., 2018], work that has focused mainly on the overall shipping operation, considering the vessel, the shore facilities, the environment and the organizational environment, all in an aggregated level. However, recent research that describes the multiple control systems on board standard commercial ships [Hyra, 2019], reflects a need for greater detail in the systemic analysis of risks, a suggestion that is developed in this work.

The systems theoretic process analysis (STPA) application is outlined in figure 26.

The proposed analysis is an adaptation of the analysis proposed by Leveson [Leveson, 2011], and can be separated into five main steps:

1. System identification and description. System goals have to be described, and the boundaries of the system have to be explicitly defined, members of the system (controllers), the information flows that occur between these controllers, accumulation of information that may happen along the process, and the existing control loops in the present state of the system.

2. Boundary identifications in three domains: Unacceptable losses and accidents, hazards, and control actions. The unacceptable losses or accidents (A) should reflect undesirable or un-

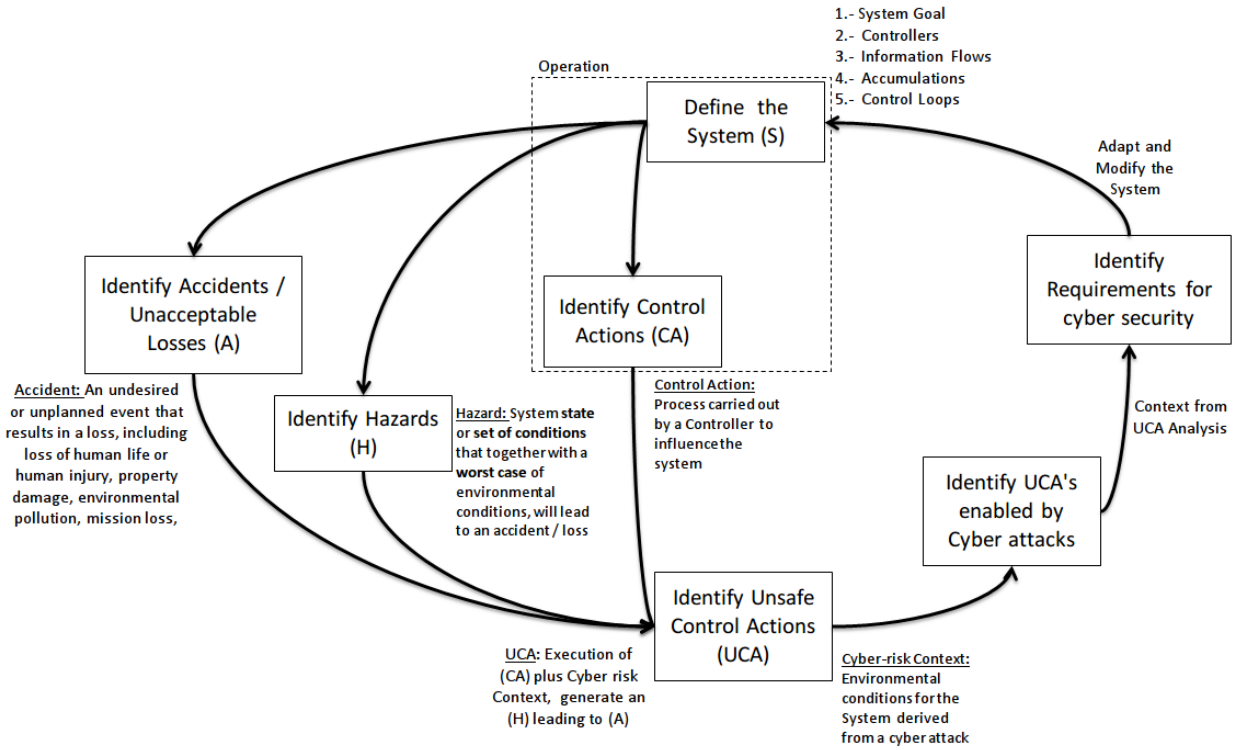

Figure 26: Systems theoretic process analysis sequence

planned events which derive in the loss of a system mission, defined in the previous step, and should include any relevant dimension such loss or damage of property, loss of human life or environmental pollution, for example. In the case of a buyer-seller system, unacceptable losses could include late or wrong deliveries, for example. The hazards (H) are all those states of the systems or sets of conditions that combined with a worst case scenario can end up causing one of the defined A.

3. Unsafe control action (UCA) identification (all those CAs that lead to a H as identified in Step 2, through the use of a structured scenario analysis, and in the form of a descriptive phrase. Leveson [Leveson, 2011] and her team identified four main ways in which a CA can lead to H.
   (a) CA is performed and this leads to H,
   (b) CA is not performed, and this leads to H,
   (c) CA is performed to early or too late,
   (d) CA is performed too long for too short a time, and this creates H.
4. Identify the UCAs from Step 3 that can be enabled by cyber-attacks.
5. Translate the contexts into requirements

Figure 27 shows the representation of a CyberShip STPA analysis.

Table 10: Unsafe Control Actions for Start Pump Action from Engine Controller (EC) to Ballast Tank Pump

Control Action	Performed	Not performed	Timing	Execution length
CA1: Start Pump	**UCA1.1**: when EC has provided wrong parameter (Velocity, Level) to Pump. **UCA1.2**: when EC receives the wrong parameters from IBC **UCA1.3**: when Ballast tank Pump is not functioning. **UCA1.4**: when Due to network failure control action is not received by Ballast tank. **UCA1.5**: when EC is compromised because of human in the loop. **UCA1.6**: when EC is compromised because of component failure. **UCA1.7**: when EC is compromised because of external hacker **UCA1.8**: when it was not required.	**UCA1.9**: when EC is compromised because of human in the loop. **UCA1.10**: when EC is compromised because of component failure. **UCA1.11**: when EC is compromised because of external hacker. **UCA1.12**: when EC did not receive command from IBC.	**UCA1.13**: when `requirement` was for a shorter period and the pump acted for too long. **UCA1.14**: when `requirement` was for a longer period and the pump acted for too short.	**UCA1.15**: when there are communication channel congestion. **UCA1.16**: when there is a feedback delay between Actuator to Ballast tank. **UCA1.17**: when EC action was performed too early or too late.

Table 11: Requirement and constraint examples

Constraints	
C1	`start pump` action must not be provided if the water level information is not received from `Integrated Bridge Controller`
C2	Parameters communicated for `action` needed before execution
C3	User interface limited to required `actions`
C4	`Action` requirement confirmation must be defined and included
C5	A receipt confirmation must be sent of required `actions`
Requirements	
R1	A risk boundary should be set to avoid the increase or decrease of water level in the ballast tank to a dangerous level.
R2	A risk boundary should be set to define and confirm channel integrity.

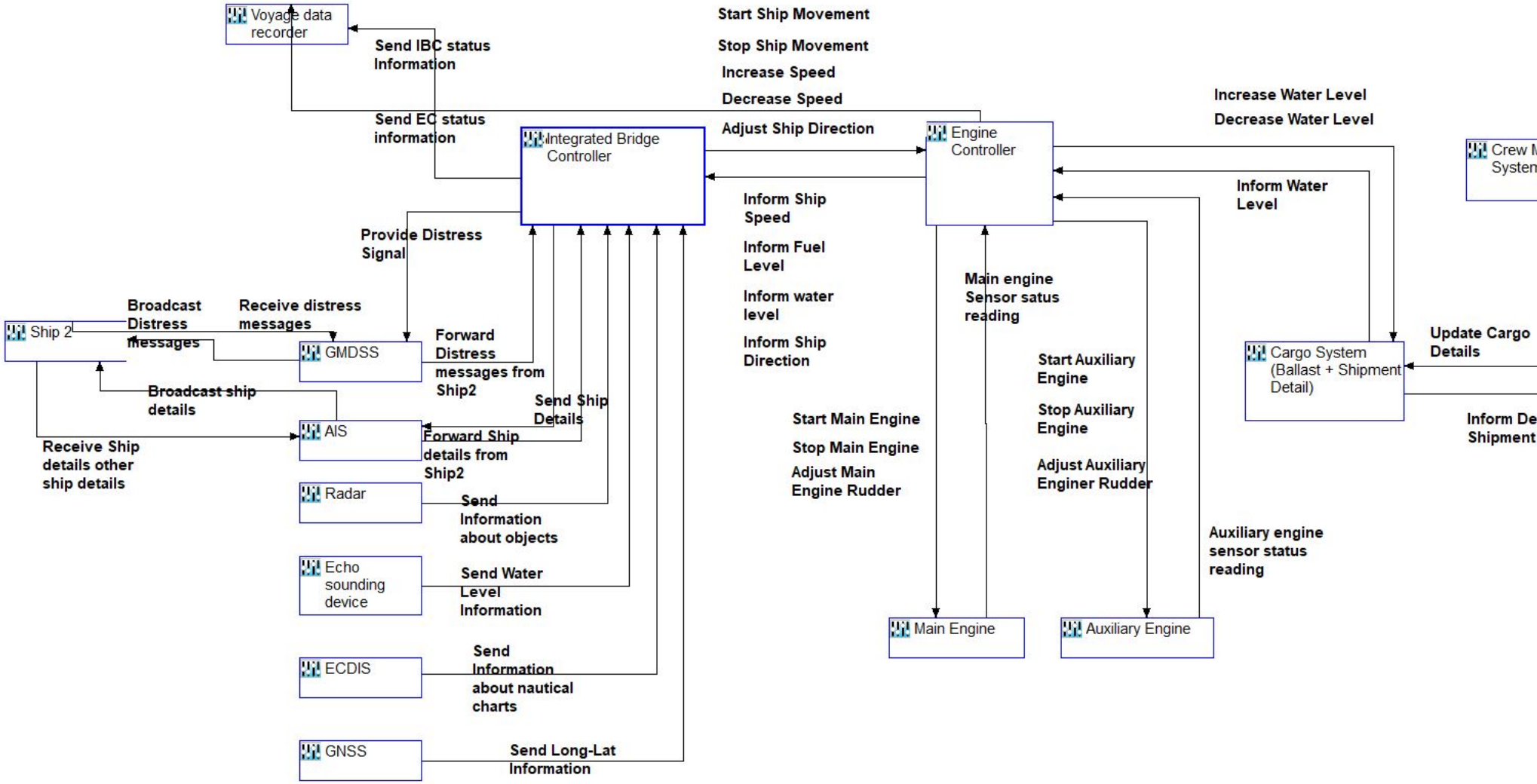

Figure 27: STPA representation of a CyberShip system

9 Appendix B - The reaction to cyber-attacks in the CyberShip Model (WP4)

Note: This Section is based on the report for WP3 and WP4 of the project CyberShip [Sahay and Sepúlveda Estay, 2018b].

In this section, we propose our CyberShip framework to mitigate the attacks in an automated way in the ship communication network. The major components are shown in Fig. 28, while the details are given next:

9.1 Components of the Framework

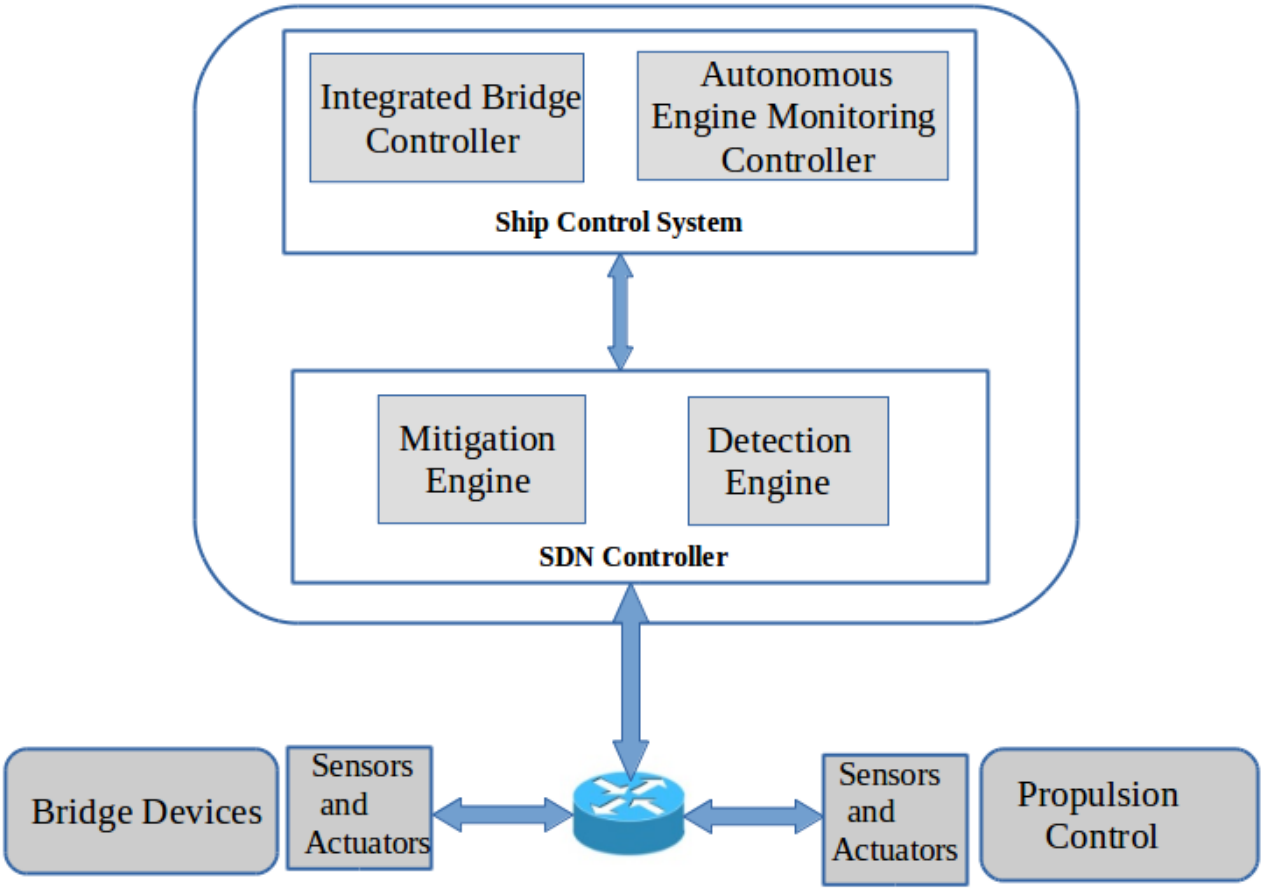

Figure 28: CyberShip Framework

In this section, we describe the components of our framework. It consists of five different cyber physical components as follows:

1. **Sensors and Actuators:** Sensors and actuators are attached to the different physical components of the ship related to the bridge, engine and propulsion control devices. These sensors forward the data related to these physical devices to *Integrated Bridge Controller* and the *Autonomous Engine Monitoring Controller* for analysis.

2. **SDN Controller:** It is a software platform deployed in external entity able to provide the network abstractions needed to manage the network [8]. It provides centralized intelligence and global visibility to manage the network. Southbound API in the SDN controller enables us to deploy the rules in the switches through a centralized location based on the need when it arises.

3. **Detection Engine:** It examines the network traffic to identify suspicious and malicious activities. Network operators can deploy mechanisms to classify the suspicious and malicious flows according to their requirements [Mahimkar et al., 2007]. Upon detection of the suspicious or malicious traffic, it reports a security alert to the mitigation engine.

4. **Mitigation Engine:** It is responsible to take appropriate countermeasures to mitigate the attacks in the framework. It contains a repository consisting of security and network policies defined in high-level language to mitigate the attacks. Depending on the security alert, countermeasure policy is instantiated to mitigate the suspicious or malicious traffic. Furthermore, it maintains a list of network paths to reach the different middleboxes (firewalls, IDS, etc.) or to reroute the traffic through different path.

5. **Autonomous Engine Monitoring Controller (AEMC):** It manages the propulsion control, main engine, propeller devices of the ship [aut, 2015b]. Depending on the scenario, it issues the control command to start or stop the propulsion system, increase or decrease the speed of the ship, reroute the ship through different routes. Moreover, it periodically analyses the data received from the sensors of the propulsion, propeller and other components of the engine to check the status of the devices, i.e. whether they are working properly or not.

6. **Integrated Bridge Controller (IBC):** It supervises the functioning of the different bridge components of the ship such as a GNSS, ECDIS, radar, and AIS [BIMCO, 2017]. It receives the data from the sensors of these devices and provide a centralized interface to the crew on-board to access the data. Moreover, it also issues control commands to the *AEMC* to start/stop the propulsion control system, reroute the ship to different routes depending on the information from the bridge devices. In case, it detects the fault or failure on the bridge devices, it notifies the **Mitigation engine** to divert the network traffic through another route to start the auxiliary bridge devices.

10 Appendix C - Structured literature review (SLR)

A systematic literature review is a special type of literature review that uses an explicit method and comprehensive strategy that has been defined before the review takes place.

10.1 Advantages of a SLR

The relevance of a systematic approach to literature reviews is reflected in the structure and social significance of its final results, with implications for explicitness, transparency, comprehensiveness, trustworthiness, relevance, and synthesis of the results.

First, a systematic approach makes an explicit description of the protocols used before the actual data collection starts. This helps to reflect and reduce hidden bias in the data collection process. The philosophical position of the research determines if and to what extent the researcher is a subjective or objective part throughout the research process. Greater bias is expected for a subjective researcher position, and less so if the researcher position is more objective. Yet, regardless of the level of accepted bias in the research process, an explicit description of the process creates greater transparency and improves reproducibility and comparability.

Second, through the use of explicit protocols, a systematic approach creates transparency about how the analysis is carried out and how the conclusions are generated. This reduces the misrepresentation of the available knowledge collected for the review, promotes critique that is more focused, and results in more efficient improvement of any future SLR process.

Third, a systematic approach attempts to gather as much of the available research as possible by reducing the excessive influence of studies that are simply easier to find through the use of inclusion criteria. Inclusion criteria describe the way in which to assess how much each study addresses the research question. A systematic review does not need to be exhaustive as some reviews only attempt to gather representative examples of evidence to answer the research question. These types of reviews benefit nonetheless from being explicit in their criteria.

Fourth, a systematic approach to a literature review indicates to the reader how much the conclusions reached by the review can be trusted, i.e., its validity. Science is not only the advancement of the contents of the available body of knowledge but also the process of its diffusion and acceptance by relevant communities (Resttvo, 1988). This makes trust on the results reached by systematic reviews a fundamental part of the research process objectives.

Fifth, as a way of increasing the acceptance of the findings, a systematic approach should include information from relevant communities of interest to the research question.

Finally, a systematic approach presents a synthesis of the results in the form of a structured narrative, summary tables and some type of meta-analysis such as statistical indicators. This analysis then drives recommendations intended to connect the findings from the information that was gathered and the conclusions derived by the researcher.

10.2 Methodology for the SLR

Durach et al. [Durach et al., 2017a] propose a structured literature review (SLR) for the field of supply chain management composed of six steps:

1. defining of the research question,
2. determining of the required characteristics of primary studies,
3. retrieving baseline sample,
4. selecting the pertinent literature from the sample,
5. synthesizing the literature, and
6. reporting and using the results.

The methodology followed for this part of the research is a structured literature review process (SLR) as per the guidelines outlined by Durach et al [Durach et al., 2017b]. Durach builds on both the frameworks by Murlow [Mulrow, 1987] for the medical field and its adaption by Tranfield [Tranfield et al., 2003] to management, resulting in a method that is appropriate for research across different fields where there might be divergence about what is found important.

The resulting SLR is a comprehensive, explicit, and reproducible method for the selection and analysis of scientific publications, providing evidence the identification of published CRFs in order to answer the research questions.

The PRISMA) structure was followed (the Preferred Reporting Items for Systematic Reviews and Meta-Analyses [Moher et al., 2009]). This considers an initial set of articles, the `baseline sample` identified by using keywords in search engines specialized in scientific publications. This sample is completed by first using exclusion and inclusion criteria, creating the `intermediate sample` and then by using backward searches to add articles not identified through the original searches to narrow down the final sample that is used for analysis, known as the `synthesis sample`. The `synthesis sample` is then analyzed first through a descriptive analysis, and finally through a thematic analysis directed towards answering the research questions.

Search criteria were applied to specific publication databases in September 2019, resulting in 704 published articles in the `baseline sample`, 605 articles after the Exclusion Criteria and 208 articles in the `synthesis sample` after the Inclusion Criteria and the review of the references in the intermediate sample.

The descriptive analysis consists of statistics about the synthesis sample, through the use of relational databases to describe the data. This was implemented in Microsoft Excel Power Pivot [Becker and Gould, 2019]. This analysis includes publication dates, origins, publication venues, characteristics such as citations, number of papers published, levels and types of collaboration, collaboration clusters, and the relationship between collaboration, origin, and publication and citation density.

The thematic analysis is based on statistics of qualitative analyses of the synthesis sample. These qualitative analyses include the categorization of articles according to the disruption time where the CRF is applied, the decision level where the CRFs are applied, the type of attacks considered, the methods used and the industry areas where the CRFs are applied, and the research institutions where the research is generated. This was implemented through the use of relational databases in Microsoft Excel Power Pivot and the qualitative data analysis package for the R statistical software [Chandra and Shang, 2017].

In order to maximize the coverage of the synthesis sample, the bibliography of the results in the articles that comply with both the exclusion and inclusion criteria (intermediate sample of 186 articles) were reviewed to identify relevant work that had not been included. This intermediate sample plus additional relevant articles from the bibliography, constitute the synthesis sample (208 articles).

11 Appendix D - Comparison Analysis tools and grading

Note: This subsection is based on the work performed by James Osborne, Master level student at the Technical University of Denmark [Osborn, 2020].

11.1 Tables and Keys

Table 15: Scale for for comparison Analysis

Score	Score Valuation
1	The Analogy/ Framework has no potential to incorporate the Cyber Security Tool into its System. This score is given if there is very little link or logical reasoning connecting the tool and the framework.
2	The Analogy/ Framework has little to some potential to incorporate the Cyber Security Tool into its System. If it can be argued, this score is given if the tool can be implemented into the framework under certain circumstances.
3	The Analogy/ Framework has the potential to incorporate the Cyber Security Tool into its System. The Score is attained if the framework can be significantly linked to the tool with logical reasoning.
4	The Analogy/ Framework can fully incorporate the Cyber Security Tool into its System. The score is given if the reasoning behind it is sound, and there is significant evidence to back up the claims.
5	The Analogy/ Framework has been created with the Cyber Security Tool being able to be integrated into its System. In the related literature, it can be reasonably argued that the tool and the framework has an indisputable link.

Table 16: Scale for for comparison Analysis

Tool	Description
Segmentation, Isolation, Containment	This tool involves the separation of data and resources, isolating them in protected databases, and containing them utilising sensors. This means, the separated information cannot be accessed all at once, and is secure from breaches, as all parts need to be accessed to gain it.
Diversity and Randomness	Adding confusing or surprising architecture within your system may break down a cyber event by exposing its presence or foiling the event all together. Having a variety of these in your system can reduce your risk of a breach.
Moving Target and Degree of Distribution	Like segmentation, the idea of this tool is to distribute the information within the system; but then also to move it around constantly and randomly to avoid being corrupted. It then requires a sophisticated cyber event, capable of getting to all packets of data, spread randomly throughout the system.
Non-persistence	Allowing access to data or a certain critical system for certain times, even for those within the organisation, means that during times of inactivity, the system is inaccessible as it is not connected to the mainframe.
Data and System Integrity, and Availability	Should a system be compromised, some tools and strategies to rectify the situation may cause an escalation of the problem. This tool aims to improve the integrity of the system and adding components which check the system is working as it is meant too.
Dynamic reconfiguration	This tool utilises adaptability to reconfigure the system architecture to complement the cyber event it just underwent. So, the tool changes the system, based on what has just happened to the system. For the tool to be very effective, it must have optimal situational awareness.
Continued on next page	

Table16 – continued from previous page

Tool	Description
Deception	Deception is used if the system is breached; then what happens is the data and resources needing protecting are moved, split and changed to make understanding and obtaining them very difficult.
Dynamic Reconstitution	If found to be breached, a way to flush out the attacker is to strategically reconstruct the system, through methods like shutting down segments of the system.
Dynamic Composition	If your system is broken, the dynamic composition tool utilised different capabilities and methods to replace the weakened system. These new capabilities would be different to the ones they replace, as it is evident the ones in use have some flaws.
Alternative Operations	If it is known a certain function is weakened or at risk, using different systems which give the same services, but have a different architecture which may not be as much at risk could be optimal. It is similar to Dynamic Composition, but in this case, Alternative Operations uses simpler tool transference, like going from email to text for communication within an organisation.

Table 17: First Analysis Explanation Key

Key	Description
P	Proactive
SEG	Segmentation, Isolation, Containment
DIV	Diversity and Randomness
MTD	Moving Target and Distributedness
NPR	Non-persistence
DSA	Data and System Intergrity and Availability
R	Reactive
DRF	Dynamic Reconfiguration
DEC	Deception
DRT	Dynamic Reconstitution
DCP	Dynamic Decomposition
ALO	Alternative Operations
HRB	Human Resilience Behaviour
BFT	BFT++
AWR	AWaRE
NIS	NIS Directive
NIST	NIST SP 800 Series
WVA	Wave Analogy

11.2 Detail of First Analysis

The frameworks were given scores based on their capacity to take on the cyber resilience strategies described before. The score attained was linked to the detail of the description of the frameworks in the their respective publications; but, as some had more detail than others, and some did not mention the strategy at all, then the score was based on opinion and critical thinking. Next are the reasoning's behind most of the scores displayed.

- P1 SEG HRB – It should be easy for organisations to access documents and information as and when required. This ensures that employees are motivated to use the security tool enabling their ability to perform roles effectively, offering an opportunity to participate actively in cyber

security measures. The score of 4 is given as employees can be trained to keep data separated, in isolated systems and mainframes.

- P2 DIV HRB – The score of 3 is given as the employees would have the ability to use different software's and tools within their job to give cyber events a greater challenge at effecting each of them. This can be as simple as using different browsers or differing finance tools.
- P3 MTD HRB – The score of 3 is given as the employees would be able to be trained to keep information in differing locations; but to ensure randomness is impossible with human input. Therefore, if preset before with a random generator, then the employees should be effective at applying the tool; however, as it requires outside non-human behavioural techniques, it is given the score of 3.
- P4 NPR HRB – Organisations work for determined amounts of time and therefore are only given limited access and opportunity to participate in cyber security measures. Utilising a non-persistent technique ensures systems can be protected by effectively cutting them off. This gains it a score of 5.
- P5 DSA HRB – Integrity and availability, along with confidentiality, are the cornerstones of data and system resilience. Although they cannot be integrated into human behaviour, employees can be utilised to aid in the data and system security by activating safeguards themselves. For example, for availability, having certain access points for a system, and having people nearby to watch and see if the users are trusted employees, could be a safeguard against a breach. Therefore, the score of 2 is given as the three factors have little to do with the behaviour of employees, and more to do with system design and access.
- R1 DRF HRB – Training and experience are the greatest factor at achieving high dynamic reconfiguration. As it is based around situational awareness and the ability to react to situations effectively, the score of 3 is given due to human error and reaction time; but humans have the capacity for creative thinking and adapting to unforeseen circumstances better than most plans and systems.
- R2 DEC HRB – Deception is difficult to program into HRB. This is due to it needing to be actively undertaken to confuse adversaries and would need to be implemented through external programs. As deception is a reactive technique, if a breach in the system is detected, then LOB's can have processes and sequences to follow to hide their data and create deception points; however, it also needs experience, training and qualification to be able to effectively implement. As a result, a score of 2 is given.
- R3 DRT HRB – Having procedures in place to rebuild in the case of a cyber event is crucial, and is in the foundation of HRB, as the ability to react effectively is important to minimise the loss of data and information is the main aim of resilience. That is why the score of 5 is given.
- R4 DCP HRB – Similar to previous reactive techniques applications in HRB, DCP can be best implemented in procedures set up before a cyber event. What HRB can do is have procedures which state in certain outcomes to move to using secondary machines or third-party functions to reduce the future breach potential, as if something has already happened a weakness has been exposed and measures need to be taken. Therefore, a 4 is given as HRB is well suited to DCP but could be better if automated.
- R5 ALO HRB – Simple to implement into HRB. ALO would be a list of conditional actions employees take as a reaction to certain cyber event circumstances. This means the score of 4 is given as this would be most effective if done automatically. As the end users and those effected are the employees, it may be worth taking that into account as the other frameworks will not account for human error.

- P1 SEG BFT – Byzantine Fault Tolerance ++ has some capability for segmentation, isolation and containment; but, in its framework, it does not give any assurance around safety or performance; therefore, its capacity for data separation is limited. This, as a result, gives it a score of 2.
- P2 DIV BFT – BFT++ creates replicas and safeguards of its information it protects; and in these, it diversifies the data using artificial software. This means it gets the score of 4 as it has a high ability to implement the tool.
- P3 MTD BFT – With its plethora of replicas and backups holding different data at different times, it then can use moving targets and distributedness in its framework. This then gives it a score of 4.
- P4 NPR BFT – BFT++ cannot implement this tool very effectively as in its principal, it is continuously reactive and needs to be able to persist should the system go down. This means it can never be non-persistent as it goes against its nature. This gives it a score of 1.
- P5 DSA BFT – With its use of replicas and redundancies, BFT++ has a strong capability to use integrity and availability tools within a system. This gives it a score of 4.
- R1 DRF BFT – BFT++ is a good reactive framework. Its capacity for situational awareness is high, as it can create redundancies, showing its understanding of the dangers that are present in the system and what risks may be linked. This gives it a score of 4.
- R2 DEC BFT – A score of 2 is given for deception, as BFT++ shows minimal capacity for this tool. It is stated that it has a FastCrash technique to increase cyber brittleness, to alert organisations of a breach early on in the cyber event. This does not allow the use of deception, although some element of hiding the data would be beneficial.
- R3 DRT BFT – BFT++ is incapable of adapting; however, it is capable at reacting to cyber events. This means, its ability for dynamic reconstitution is limited. This gives it a score of 3.
- R4 DCP BFT – Emphasising its use of artificial software diversity, BFT++ can implement dynamic composition to give the system new capabilities and functions. This gives it a score of 4.
- R5 ALO BFT – Unless set in the reactive procedure, BFT++ would not have the ability to effectively implement ALO without minor adjustments to its priorities. This gives it a score of 2.
- P1 SEG AWR – Through its management and messaging and storage levels, AWR has the capacity for segmentation and containment of data and information. This gives it a score of 3.
- P2 DIV AWR – AWR has little to no resource to utilise DIV. It may have the potential for moving the data and the creation and maintenance of “honeypot” like defences. This means it scores a 1.
- P3 MTD AWR – As with P2 DIV AWR, the framework does not have the ability to incorporate MTD into its system. This gives it a score of 1.
- P4 NPR AWR – AWR can be configured to give access at certain times and at certain locations but is against its main function. It gains a score of 2 because of this.
- P5 DSA AWR – The framework of AWaRE is equipped for the adaptive preventative measure of DSA. This gives it a score of 4, as it can adapt to the circumstances given and offers more integrity.

- R1 DRF AWR – As AWaRE is a predominantly reactive framework, it scores a 4 in this category. This is due to AWaRE's characteristics, such as a leader-based problem solving. Leader-based is useful as following a status quo during a cyber event would be a good strategy for pulling all system agents to a common ground understanding.
- R2 DEC AWR – As well as strong management, messaging and storage in its primary system, AWaRE also has sub-solutions which have the capacity to deceive attackers, such as distributed communication and data storage. As this creates a high fault tolerance, this gains the score of 5.
- R3 DRT AWR – AWaRE is effective at incorporating dynamic reconstitution into its framework. This is due to its state space solution; therefore, in the case of a breach it has the capability to reconfigure itself into a new form to hide from attackers. This gives it a score of 4.
- R4 DCP AWR – AWaRE uses DSL semantic models to support its self-representation. This in turn makes three sub-models which have the capacity to implement dynamic composition, such as a problem structure model and an agent architecture model. This gives it a score of 4.
- R5 ALO AWR – Alternative Operations can be utilised well with AWaRE as its management and adaptive capabilities allow it to transition functions whilst maintaining organisational cohesion. This gives it a score of 5. For each of the NIS Directive use of tools, the score was determined based on if the broad standards it makes, covers those tools. For example, the P2 DIV was given a good score of 3 as it is effective when organisations and parties communicate with one another to provide tips and updates on weaknesses; but as the standards are not very specific the score is lowered to a 3. This is similar with the NIST framework and standards; but, due to them being specific in certain areas, it gains higher scores in some categories and lower in others.
- P1 SEG WVA – The Wave Analogy use of cyber security resources means it has the capacity to implement segmentation, isolation and containment. This gives it a score of 4.
- P2 DIV WVA – Use of good communications and learning from the past events meansthe data changes location and can be randomised. But this is not directly linked to DIV so gets a score of 3.
- P3 MTD WVA – Using cyber security means the wave analogy covers this tool but is not as effective with MTD. This gives it a score of 3.
- P4 NPR WVA – Adhering to governance and visibility means the wave analogy should be capable of limiting access to systems. As this is not a directly linked to NPR it gains the score 3.
- P5 DSA WVA – With "Velocity" considered and applied well, the availability of data once an attack is detected should be very low. This means a score of 4 is given as the frameworks adaptability is high.
- R1 DRF WVA – Focusing on the wave analogy's capability to adapt to many cyber situations it is faced with means it has a high reconfiguration capacity. That gains it a score of 4.
- R2 DEC WVA – The frameworks flexible use of processing to recover, means it has a capacity for deception. Although it is not directly linked, this gains it a score of 3.
- R3 DRT WVA – If applied correctly, recovery management would be suitable for reconstitution; but directly. This means it has a score of 3.
- R4 DCP WVA – Emphasising the importance of markets, social capital and finance shows the consideration of secondary safeguards away from normal practice (e.g. second servers and backup systems); i.e. it is more well-rounded. As a result, the score of 5 is chosen.

- R5 ALO WVA – The ability to adapt should encompass redirection of resources, so the alternative options are considered. This means it gets the score of 3 as it is not primarily capable of achieving good ALO.

11.3 Detail of Second Analysis

1. (*) Each framework title was entered into the Web of Science search engine. As the system looks for the terms used, individually, it meant skew results as some of the names of the frameworks can be associated to different subjects. Therefore, other words like "cyber", "framework", or "resilience" have been used to refine the results. The values in subsection 3.3.2 are the results. Note: not all refining keywords were used, only an amount which gave an indication of the analogy's publication usage.

2. (**) The Human Cyber/ Behaviour Resilience used in industry and standards is applied using MOA (Motivation, Opportunity, and Ability). These characteristics are also the three important features companies need to promote for a happy workforce, who produce high quality products. As a result, it could be suggested that companies which have records of high-quality products or services could be subjected to less or no cyber incidents as their employees are trained in the three fundamental aspects which make a good company. An assumption can be made that the application of these features in industry is already vast; and would possibly be tied to the industries and companies who have adopted international quality standards. It is difficult, therefore, to determine the integration of human behaviour resilience, but should some of the links mentioned above are true, then they are widely used in the most effective industries. It is important to note that the training employees receive for improved quality is different than that for behavioural resilience; but the skills and mindsets that are required are apparent in both, substantiating the idea that there is a link between the two. This suggests, the number of uses in industry is high when it comes to Human Behaviour Resilience implementation.

3. NIS Directive is compulsory for each member state of the EU (27), and for critical systems within the Union; therefore, must have a minimum number of uses of over 27 (27 being the current number of member states who are obliged to use the standard). The NIST SP 800 Series is used within the Federal Government, and is the primary user, although companies can adopt the standards. Due to the numbers of implementations not being known, but a minimum of one user, it is given the score of "greater than one".

The columns are explained next:

- **Human Resilient Behaviour**: There is a link between the main parts of Human Resilient Behaviour and the traits of an employee which produces high quality products and services. Therefore, industry standards (such as ISO 9001:2015 (Standardization n.d.)) which detail the criteria a company or organisation must adhere to, and are the basic guides for implementing effective Human Resilient Behaviour. As a result, a score of 5 is given, as over the past few decades, this process has been improved and made into a guide which should be straight forward for companies and organisations to implement.

- **BFT++**: With its testing being achieved at a Naval Research Laboratory (Mertoguno et al. 2019), BFT++ can be assumed to have some of its implementation flaws identified and rectified. As a result, it gains a score of 4 because of its trials, but does not achieve a 5 due to its lack of use in industry and its lack of development achieved over time and use.

- **AWaRE**: Having a well described and discussed publication written about it, makes AWaRE a good tool for companies and organisations to use and apply to their systems. However, as it is new there is a lack of testing, and little to no experience in industry only gains it a score of 3.

- **NIS Directive and NIST**: Government standards are a general guide to cover all industries and as such are vague but simple to implement. They can be used differently by different government departments or independent organisations. This makes adhering to them relatively easy, so gaining certifications should be straightforward. In this case, therefore, of implementation, government standards should score high. As a result, NIST gains a score of 4, as it is well developed over decades of addendum's, developments, and experience in industry (industry in this case being both governmental and non-governmental organisations). It does not gain a score of 5 as its vagueness can then be misinterpreted and implemented incorrectly. These reasons are similar for the NIS Directive also as it can be misinterpreted but should be easy enough to follow. It only scores a 3 due to its lack of experience and development in industry.
- **Wave Analogy**: Like with AWaRE, the Wave Analogy suffers from a lack of use in industry and in field testing. This is due to its recent procurement and creation, but despite this, it is well developed and clear on how companies and organisations should go about setting up their systems to protect themselves from cyber events. With this, it gains a score of 3, whilst there is much room for validation of its implementation potential but still a good framework to use.

Finally, the scoring criteria are the following:

- Each tick for columns 1 to 5 are worth 1 point
- Each tick for columns 6 and 7 is worth 0.5 points
- Column 8 is worth the value in each cell
- Under the assumption the values in column 9 will stay constant until 2021 (from the date the values were recorded (27Feb2020) the average number of publications was taken (using the formula $Average = (Publications)/(2021 - Year)$. This gave us the averages which were then ranked from 6 to 1, with 6 being the higher value.
- The cells in column 11 will be ranked from 1 to 6, with highest values being scored 6.

12 Appendix E - The CyberShip Model (WP2)

The components of the CyberShip model were presented in the CyberShip Project report of Work Package #2 [Sahay and Sepúlveda Estay, 2018a]. The Model shared in that report has been completed and updated with subsequent research conducted within the context of the CyberShip project.

Hyra [Hyra, 2019] expands this model by expanding the identification of the multiple devices and services that operate in a ship. Many communicate with each other directly, others through special hubs. Every single device or service used on a ship is therefore a potential danger in various ways, even endangering people's lives. Hyra goes on to detail that the services and systems on a ship are divided according to the following categories:

- Cargo management systems - All devices and infrastructure used for loading, control and management cargo. These systems are placed on the ship as well as in onshore facilities such as at the shipper companies or at the ports.
- Bridge systems - These are placed on the vessel and include devices such as `ECDIS`, `VDR`, `AIS`, `ARPA`, and radars. Many of these devices also are interconnected.
- Propulsion, machinery, power control systems - These systems are responsible for driving the ship, delivering electricity and other fundamental functions for the operation of the ship. Nowadays most of these systems are interconnected and controlled from the bridge as well.
- Access control systems - Physical security is partly covered by these systems through registering personnel on board, all requests, registering maintenance actions, security alarms, capturing videos from cameras etc.
- Passenger servicing and management systems - Digital systems used for property management, registering all passengers during boarding, their access.
- Passenger facing public networks - Cable and wireless networks made for passengers access to the internet while traveling and all other entertainment systems.
- Administrative and crew welfare systems - All computers used on board by the crew for their daily tasks, usually with access to the inner network and often to the internet.
- Communication systems - Most important here is equipment which connects the ship with a shore or with other ships, this might be done through different kinds of radios or satellite communication. Within this segment are included protocols used inside and outside of the ship between various services as well.

The weak points of communication systems have been classified ["Solarwinds MSP", 2018], with the most common vulnerabilities in the systems being [Hyra, 2019]:

- Missing data encryption.
- Missing data authentication.
- Download of data/codes without integrity checks.
- Missing mechanism of software/firmware authentication.
- OS command injection.
- SQL injection.
- Buffer overflow.
- Missing user authorization.
- Unrestricted upload of dangerous file types.

- Reliance on untrusted inputs in a security decision.
- Cross-site scripting and forgery.
- Use of broken algorithms.
- URL redirection to untrusted sites.
- Path traversal.
- Other software bugs.
- Weak passwords.
- Software that is already infected with the virus
- Outdated of unsupported operating systems.
- Outdated or missing antivirus.
- Outdated or unsupported maritime software or services.
- Wrong design of a network.
- Lack of protection measures in a network.
- Inadequate access control or lack of it.
- Lack of backup mechanisms.

The list cannot be considered as complete, as it depends on the technologies, software-hardware used, and skills of the hacker to refine their methods. Every year new hacking techniques are developed and new security holes are found.

The Model according to Hyra [Hyra, 2019] is indicated next. The list of equipment presented in this document cannot pretend to be complete, as it is possible that some systems, equipment/hardware, software were omitted due to lack of data. Beyond the references placed along with the text, other major sources of information include:

- International Convention for the Safety of Life at Sea (SOLAS)
- International Maritime Organization (IMO) ["IMO", 2019] ["IMO", 2018]
- Integrative Knowledge Platform For Transport and Logistics (SKEMA) ["SKEMA",]
- Baltic and International Maritime Council (BIMCO) ["BIMCO, CLIA, ICS, and others", 2018]
- Marine Insight ["MarineInsight", 2019] ["MaritimeInsight - KaranC", 2018]
- Totoheo ["Totoheo Maritime", 2019b]
- Engineers Journal [Meskell,]
- Samid Mulla ["Samid Mulla", 2016]
- Kongsberg ["Kongsberg", 2019]
- Maritime and Coastguard Agency ["Maritime and Coastguard Agency", 2002]
- Sperry Marine ["Northrop Grumman", 2005]
- Meeting with UltraShip
- Personal or phone contact with people from maritime environment like Lukasz Pozniak (Master Mariner).

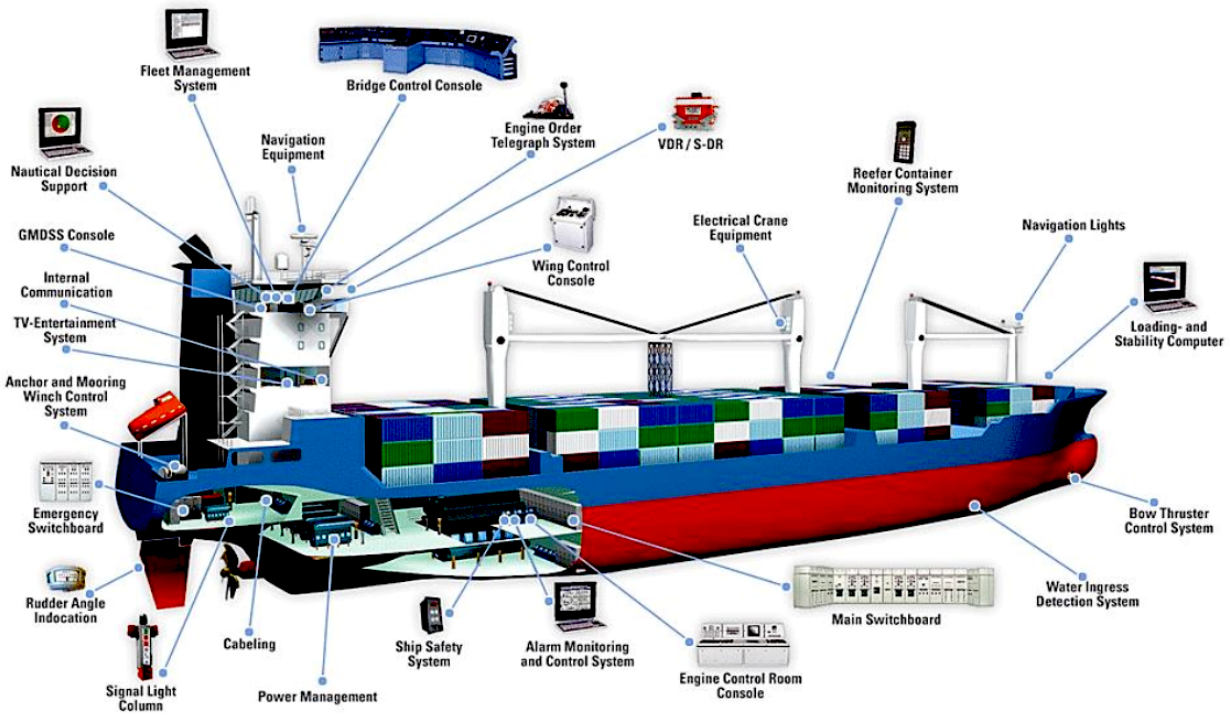

Figure 29: Structure of a ship ["CyberBit/Volpe/US department of transportaion", 2013].

In Figure 29 and Figure 30 various ship system components are presented. Figure 30 focuses mainly on machinery devices which maintain general operation of the ship. Figure 29 focuses on devices that allow control over the ship.

Based on these figures and other sources, the list of ship's components presented by Hyra [Hyra, 2019] is the following:

- Core infrastructure systems - these are main ships equipment and technology allowing devices to communicate with each other.
  - Cabling - in theory:
    - Separate network for crew computers and administrative operations
    - Separate network for ship's sensors, machinery, navigation devices.
    - Separate network for passengers entertainment systems.
  - Security gateways
  - Routers
  - Wireless Access Points (Wi-Fi)
  - Switches
  - Firewalls
  - Virtual Private Network (VPN) - method of encrypted connection to remote network.
  - Intrusion Prevention/Detection Systems, logs of systems
  - Backup and Restore systems
- Communication Systems - All equipment and services allowing to communicate ship with the outside world.
  - Satellite communication - Below is placed a list of services operated by private companies, providing satellite data transfer, they use different usually owned satellite constellations.

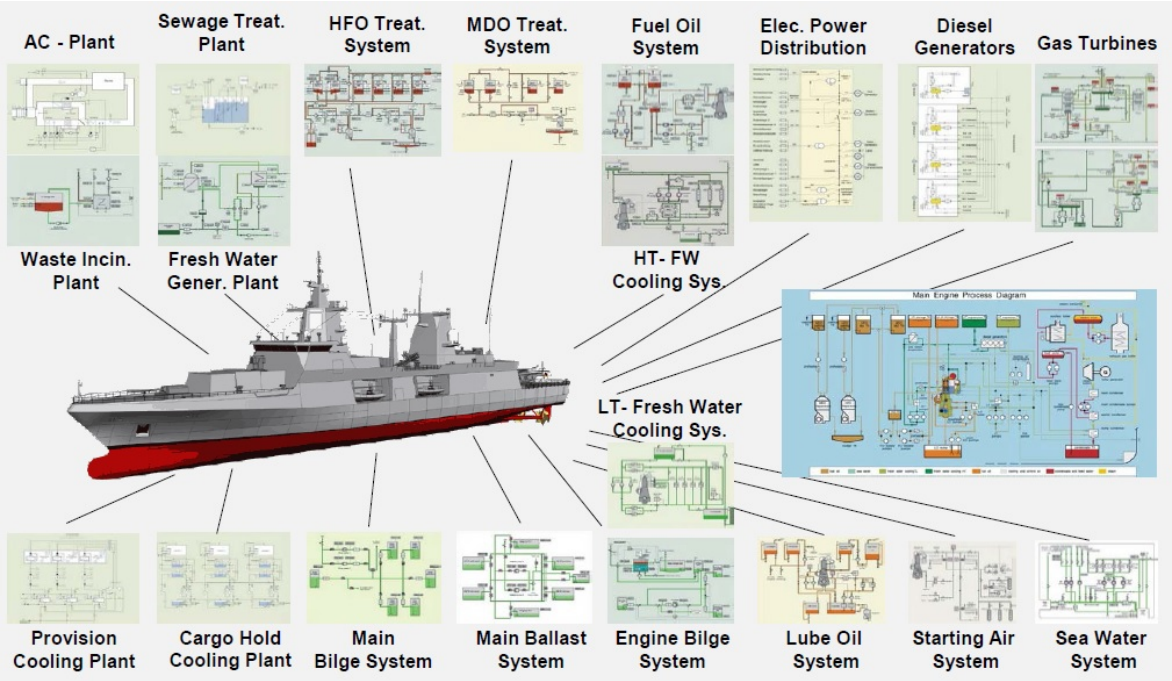

Figure 30: Structure of a ship different view[Meskell,].

  - Iridium
  - Inmarsat
  - Globalstar
  - Thuraya
  - MSAT
  - VSAT
- Voice Over Internet Protocol equipment - special services allowing the crew to make call phone over the internet. This involves inland company special infrastructure to cross-connect internet with phone lines.
- Automatic Identification System (AIS) - It is a system which based on VHF radio automatically send and receives messages between ships, between VTS and ships. It is made for the ship identification, exchanging whether forecast, collision avoidance, search and recuse signals and other complementary information exchange about the position of other ships fed to ECDIS machine, based on messages.
- Long Range Aid to Navigation (LORAN) - Device used for radio location invented before satellite positioning era first version was accurate up to 45km. Last version LORAN-C has accuracy around 460m.
- Enhanced Long Range Aid to Navigation (eLORAN) - Latest version of LOARN with accuracy to 20m
- Vessel Traffic Service (VTS) - It is a marine traffic monitoring system similar to air traffic control. The VTS responsibilities are to track and control vessel traffic around the ports or harbors. They usually use VHF, CCTV, radar, and AIS.
- Long Range Tracking and Identification (LRIT) - It is a system which obligates vessels, according to the SOLAS and IMO regulations, to automatically report their positions over satellite connection to the specially prepared internet platform at least four times a day.
- Global Maritime Distress and Safety System (GMDSS) - This is an international set of regulations and requirements of equipment and procedures which has to be respected. Part of GMDSS is satellite communication, for now, Inmarsat is an official part of this system. In the list below are these required devices/systems.

    * Emergency position-indicating radio beacon (EPIRB) ["Marine Knowledge", 2013] ["MarineInsight - Shilavarda Bhattacharjee", 2017] - It is a device which sends radio beacons as the 406 MHz messages via satellite to alert in case of the event of an emergency. Usually is mounted in emergency boats.
    * Rescue Radar Transponders (SART) ["Marine Knowledge", 2013] ["MarineInsight - Shilavarda Bh
    - Search and rescue locating device mounted on the ship which helps to find a ship when is lost. The SART is waterproof and its battery can operate for over about a hundred hours. It operates in 9 GHz radar band.
    * Navigational Telex (NAVTEX) receiver - international automated service for delivery various of warning to the ship like navigational or meteorological. Works in a range of approximately 370km offshore.
    * Very High-Frequency radio (VHF) - This device operates between 156 MHz to 174 MHz, sometimes connected to the GPS receiver for sending accurate distress signal positions.
        · Digital Selective Calling (DSC) - done over VHF in order to connect to specific other radio units it is required to know Maritime Mobile Service Identity (MMSI) assigned unique 9 digit number to each radio unit. Then it is possible to send the voice or other data.
    * Radiotelex - As far as understood it has similar functionalities to VHF radio but it operates on lower frequency bands HF and MF.

- Integrated Bridge systems ["MarineInsight - Shilavadra Bhattacharjee", 2017] - Devices placed in the bridge often merged in some kind of a integrated control consoles, example products names are: NACOS ["Wartsila",], IMCAS, SMCS ["ASIC",].

  – Global Navigation Satellite Systems (GNSS)
    * Global Positioning System (GPS)
    * Differential Global Positioning System (DGPS)
    * Galileo
    * Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS)
    * BeiDou Navigation Satellite System (COMPASS) (BDS)
    * Indian Regional Navigation Satellite System(NAVIC) (IRNSS)
    * Quasi-Zenith Satellite System (QZSS)
  – Ships Movement Information Display System (SMIDS) ["Tototheo",] - Measures speed over the ground at the Bow and the Stern of the vessel, giving highly accurate speed (it uses GPS/GLONASS receivers).
  – General alarm system - Panel in the bridge where all alarms systems can be managed.
  – Electronic Chart Display and Information System (ECDIS) - It is a system which based on various information from ship's sensors, pre-downloaded maps, and programmed voyage plan displays all necessary nautical information, it is used for better ship navigation and used by autopilot. Among many other devices, it exchanges information with AIS so the other ships get additional information about positioning.
  – Bon Voyage System (BVS) ["Tototheo Maritime", 2019a] - Seems it is a system which might be complementary to the ECDIS, can calculate the fastest route and costs of travel based on weather, wind, type of vessel on which is installed.
  – Transmitting Heading Devices (THD) - An electrical device containing electromagnetic compass that provides information about the true direction of a ship to the other systems on the ship.
  – Anemometer - Device used for measuring wind speed. In maritime these devices nowadays are connected as well to the ship's network.

  - Sonar (or Fishfinder, Fathometer) - Device which scans the underwater area and bottom of the sea. As a result, the sonar can determine what objects are floating in the water and how the sea floor looks like for preventing sandbanks.
  - Gyro Compass - In contrast to electromagnetic compass, this uses gyroscopic properties to determine true north (electromagnetic north is not placed in the north/south pole, it is moved to the side which adds more factors and calculations to consider while navigation).
  - Radar equipment - In contrast to sonar, the radar scans the area above the water level. In result, it can map all objects which are on the water or air.
    * Automatic Radar Plotting Aid (ARPA) - Part of radar equipment in form of a screen with a keyboard, which based on radar inputs can plot scanned area, select moving objects, automatically track them, calculate their speed and course and as result warn if the object is on colliding course with the ship. According to the SOLAS, it can execute automatic ship maneuvers (just connected to the autopilot).
    * Automatic Tracking Aid (ATA) - Similar system to ARPA but has less functionality.
  - Autopilot - Interface between the electronic navigation system and maneuvering system. Essentially it tells the ship where to go.
  - Speed and Distance Log Device - The device which measures and stores various parameters of a voyage from a set point (starting point). Based on various inputs it calculates the ship position. Seems it is a device complementary to the satellite positioning systems.
  - Sound Reception System - For ships with a fully enclosed type of bride. It allows the navigating officer inside the cabin to listen to the sound signals and fog horns from other ships.
  - Ship Whistle - It is just a horn usually there are two of them, one running by air, second electronically.
  - Voyage Data Recorder (VDR/S-DR) - It is an instrument which behaves like a "black box", continuously saves all necessary information about the ship like speed, direction, position, information about the engine, fuel level. Additionally, it has voice recording system saving up to last 12 hours. According to the source, it can be available from the onshore systems.
  - Nautical Decision Support - it is a different name for systems like ECIDS, Radar, Sonar, anemometer, etc.
  - Fleet Management System ["Marine Insight", 2017] - Owners of the ship and management of the ship might have additional systems which allow to keep in touch with all ship and see properties like fuel efficient,
  - Manual Ship Maneuvering
    * Engine Order Telegraph System - Controlling the speed of the ship.
    * Navigation Lights
    * Wing Control Console - extra console placed on the wings of the bridge for a better overview outside the ship (used while docking the ship in the port).
    * Bow Thruster Control System
  - Manual control over water ballast.

- Propulsion, machinery, and power control systems - These are all mechanical and electrical devices of a ship allowing the crew to maintain their operations over an extended period of time. Some of the systems might be accessible from the shore side like engine performance or ESD.

  - Engine Control Room Console - Console placed under the deck centralizing information about machinery.

- Engine Governor System - System which allows controlling the engine properties.
- Power Management System - This is the system which provides stable electrical power for all devices on the ship.
  * Main Switchboard - Equipment which is responsible for main power safety like fuses, circuit breakers, over-current relays.
  * Emergency Switchboard - Backup switchboard to the main one.
  * Diesel Generator or Gas Turbines - Spare devices for generating electrical power if the main engine is damaged or overloaded.
- Emergency Response System - Part of an alarm system with safety properties, probably part of the ESD system.
- Signal Light Column - Part of the alarm system which shows the general condition of mechanical components.
- Ruder Angle Indication - The device which shows a position of the ruder, seen from Engine room as well as from the bridge.
- Anchor and Mooring Winch Control System - This usually is windlass which keeps the ropes controlled offline, electronically by the crew.
- Extra stabilizers of the ship - These are devices prevents the ship from rocking/tilting from side to side on the waves:
  * Electronical controlled fins.
  * Fixed fins.
  * Big gyroscopes.
  * Active extra ballast systems ["Crazy Hippo", 2018a] - Dynamically filling and emptying big tanks with powerful pumps and physical properties with the rhythm of ongoing waves.
- Emergency Shut Down (ESD) ["Safety4Sea", 2018b] - The system which reacts in a given way based on defined dangerous situations. An example can be too big pressure in some of the systems, high tanks levels, too high temperature. Due to an abnormal condition, the system will follow a pre-programmed procedure and shut down some of the subsystems or even the whole ship. It can be activated manually and remotely onshore, as understood from articles. It prevents from physical damages of machinery and might safe life preventing in some situations unwanted explosions and leaks. As far as understood, it might be integrated with other alarm systems on the ship and controlled from one panel.
- Air Condition Plant ["Marine Insight", 2018b]- Some ships might have dedicated own air condition systems, for cooling other systems like cargo, food, the air in the rooms of the ship.
- Sewage Treatment Plant - These systems decompose the raw sewage which after the process is disposed of in the sea.
- Marine Heavy Fuel Oil (HFO) Treatment System ["Marine Insight - Anish", 2018b] ["Marine Insight", 2 - This oil treatment system contained oil used for generating moving force for the ship and generating electrical power. It is the lowest quality fuel comparing with IFO and MDO described below. Usually, HFO oil is solid and need heating in order to be just pumped over the pipes. It is the lowest quality type of oil in industrial production.
- Intermediate Fuel Oil (IFO) Treatment System ["Marquard and Bahls", 2015] - Ratio of HFO and other distillates is smaller than MDO but general quality anyway is better then HFO.
- Marine Diesel Oil (MDO) Treatment System ["Machinery Spaces", a] ["Machinery Spaces", b] - Seems the higher quality than IFO and HFO. It has a very small amount of HFO inside, most of it are blends of other oil distillates.

  - Fuel Oil System ["Wartsila Encyclopedia of Marine Technology", b] - HFO, IFO, and MDO have own tanks and own treatment systems but when these oils are ready to be used (heated up, cleaned, sometimes other processes are done), they are pumped to the settling tanks from which this Fuel Oil System transport it to the engine.
  - Waste Incinerator Plant ["Marine Insight - Anish", 2017a] - It is a piece of machinery on board which burns solid and liquid wastes produced on the ship during normal operations. It is built for reducing overall waste from ships and reduce the costs of waste disposal.
  - Fresh Water Generator Plant ["Marine Insight - KaranC", 2017] ["Marine Insight - Chief Office Abhish - This is system makes fresh water.
  - Central Cooling Water System ["Wartsila Encyclopedia of Marine Technology", a] ["Marine Insight - A - used for cooling main engine and consist of:
    * High Temperature Fresh Water Cooling System
    * Low Temperature - Fresh Water Cooling System
    * Seawater Cooling system
  - Lube Oil System ["Marine Insight - KaranC", 2016] ["Marine Insight - Anish", 2017c] - This system is designed to efficiently spread lubrication/oil around the engine and turbocharger if it is implemented
  - Starting Air System ["Marine Insight - Shalabh Agarwal", 2017] - Specially designed system for starting the ship's engine. Due to the huge inertia of reciprocating masses, it requires lots of energy to be inserted.

- Access control systems - These allow to maintain physical security of a ship as mentioned in previous sections.
  - Surveillance systems like Closed Circuit Television (CCTV) Camera system, might be available from onshore according to the sources.
  - Bridge Navigational Watch Alarm System (BNWAS) ["Totoheo Maritime",]- it is a system which monitors bridge personnel activity by means of user interaction and physical movement in the bride. The system can detect disability of crew and turn on the alarm for backup navigators personnel.
  - Shipboard Security Alarm Systems (SSAS) - It is a silent type of ship security alarm system when activated it sends a message over satellite usually at first to the shipowner. It is used in case of pirate attack or any other terrorist act.
  - Electronic "personnel-on-board" systems - This equipment monitors activity done on the ship like maintenance repairs, who and when got onto the ship and what was the reason for this.

- Cargo management systems - All necessary equipment used for controlling cargo. It happens that the cargo management system is available from onshore as well, it means that all properties as Hull Stress, Ship Planning can be accessible.
  - Cargo Control Room (CCR) - place on the ship either own room or in the bridge where responsible person monitors and controls the process of loading and unloading the vessel. That person controls pumps and valve positions in order to balance the ship if there are not any automatic mechanisms.
  - Water Ingress Detection and Control System (Main Ballast System)
    * Level indication system - As far as understood this system measures the total load of the ship.
    * Valve Control System - Valves which can be open for allowing water to fill ballast tanks.

    * Main Bilge System ["Marine Insight - Mayur Agrawal", 2018]- This system helps with pumping out an excess of water and sludge from spaces like cargo, rooms below the main deck, engine room, other machinery spaces.
    * Water ingress alarm system - as far as understood the system controls how much total amount of water is inside the ship or controls what is the ship level deepness in regards to sea level.
    * Onboard loading computer and other computers used for an exchange of loading information, stability control and load plan updates with the marine terminal and stevedoring company:
        · Reefer Container Monitoring System - Cargo which is transported on the ship either containers or tanks often need an extra power supply. It is important to plan their position in the ship in a way that it is possible to deliver electrical power to them. Such a system might control how much power is sent over the transportation period.
        · Hull Stress Monitoring Systems (HSMS) - System which thanks to its sensors placed around the ship can deliver information about tensile, compressive, torsional, shear/bending forces on the ship's hull in different places due to its load.
        · Ship Planning System (SPS) - System which allows planning how the containers should be spread around the cargo area in order to keep stability. Such systems can cooperate with HSMS so it is possible to make corrections in load. Example software used of this purposes calls IT StowMan, Capstan4, Autship Systems.
  – Electronic Crane Equipment

  Study

- Passenger or visitor services and management systems - Digital systems used for property management, registering all passengers during boarding, their access.
  – Property Management System (PMS) - It takes care of all things connected with baggage tracking, housekeeping, accounting of the customer/passenger, currency exchange, reservation loading and tracking, gangway management.
  – Ship passenger/visitor/seafarer boarding access systems - Complement system for the PMS allowing passengers access to certain parts of ships facilities.
- Passenger-facing networks - Cable and wireless networks made for passengers access to the internet while traveling, all entertainment systems.
  – Passenger segregated Wi-Fi or `LAN` internet access
  – TV Entertainment System and others
- Administrative and crew welfare systems - All computers used on board by the crew for their daily tasks, usually with access to the inner network and often to the internet.
  – Internal Communication - All messages send within the ship.
  – Electronic Health Records
  – Financial Related Systems - For example, management of invoices for delivering transport, passengers, repairs, etc.
  – Infrastructure support systems:
    * Domain Name Service (DNS) (very optional and rare)
    * Active Directory
    * Outlook
    * Mark5

    - Dualog
    - Servers with other services
    - Printers
    - Many other potential software and hardware
- Crew Wi-Fi or LAN

13 Appendix F - List of dissemination activities within the CyberShip project.

The following is a list of 1) the documents generated as a result of the project CyberShip that have either been sent for publication, or that have already been published, and 2) a list of the presentations that have been made of the project and its results.

Publications

Sahay, R., Meng, W., Sepulveda, D. A., Jensen, C. D., & Barfod, M. B. (2019). CyberShip – Systems Theoretic Process approach to the cyber risks in ship systems. Submitted to Reliability Engineering and System Safety.

Sahay, R., Meng, W., Sepulveda, D. A., Jensen, C. D., & Barfod, M. B. (2019). CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. Future Generation Computer Systems.

Sepúlveda Estay, D. A., & Guerra, P. (2019). The wave analogy of resilience as applied to shipping operations. In Risk Analysis for improved resilience

Sahay, R. (2019). CyberShip: Resilience for the shipping industry. In Risk Analysis for improved resilience

Guerra, P. J. G., & Sepúlveda Estay, D. A. (2019). An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains. In 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM) IEEE. DOI: 10.1109/IEEM.2018.8607563

Sahay, R., Sepulveda, D. A., Meng, W., Jensen, C. D., & Barfod, M. B. (2018). CyberShip: An SDN-Based Autonomic Attack Mitigation Framework for Ship Systems. In International Conference on Science of Cyber Security (pp. 191-198). Springer, Cham.

Sahay, R.,& Sepúlveda Estay, D. A. (2018). Work Package 3 & 4 Report - Cyber resilience for the shipping industry.

Sahay, R., & Sepúlveda Estay, D. A. (2018). Work Package 2 Report - Cyber resilience for the shipping industry.

Krull, L. (2018). Det bedste forsvar er en smidig organization. Dynamo Magazine, Nr. 54, pp.20-21.

Lagouvardou, S. (2018). Maritime Cyber Security: concepts, problems and models (MSc. Thesis). Technical University of Denmark DTU.

Barfod, M.B. (2017). New CyberShip project under way. Newsletter of Management Maritime Lighthouse, Newsletter No. 1, fall 2017, pp. 2-3.

Presentations

Sepulveda, D.A. (2019). Status of CyberShip project and Work Package #5. Presentation for the CyberShip Project Advisory Committee, 29 November, 2019.

Sepulveda, D.A. (2019). CyberShip, an example of cyber-resilience research in shipping. Presentation for the DTU Electro, 20 August, 2019.

Sepulveda, D.A. (2019). Cyber-resilience research in shipping. Presentation for the Danish Center for Cyber security, 02 July, 2019.

Sepulveda, D.A. (2019). Cyber-resilience research in shipping. Presentation at the Management Science Seminar series at the Technical University of Denmark, 13 June, 2019.

Sepulveda, D.A. (2019). Cyber-resilience research in shipping. Presentation at the Operations Management Seminar series at the Technical University of Denmark, 10 May, 2019.

Sepulveda, D.A. (2019). CyberShip - Training of cyber-resilience in the shipping industry. Presented to Force Industries, 29 April, 2019.

Sahay, R., Sepulveda, D.A. (2019). Cyber-risk analysis of ship systems using STPA. 2019 STAMP Workshop at the Massachusetts Institute of Technology, 25-28 March, 2019.

Sahay, R., Sepulveda, D.A. (2019). Collaborative Mitigation Approach for a better Response to Disruptions. Presented at the CAMS (Cyber-Security at MIT Sloan) Workgroup in Boston, 08 February, 2019.

Sahay, R. (2019). CyberShip – Cyber resilience for the shipping industry. Governance for Cyber Security and Resilience in the Arctic, North Atlantic Treaty Organization (NATO) Workshop, Rovaniemi, Finland, Jan 27-30, 2019.

Sepulveda, D.A. (2018). CyberShip – Cyber-risks in the shipping industry. CISCO Security Everywhere workshop, Aarhus and Copenhagen, Jan 8 & 9, 2019.

Sepulveda, D.A. (2018). An Impact-Wave Analogy for Managing Cyber Risks in Supply Chains. Presentation at the IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, Dec 16-19, 2019.

Sahay, R. (2018). CyberShip: An SDN-based Autonomic Attack Mitigation Framework for Ship Systems. Presentation at the SciSec conference, Aug 12-14, 2018.

Sahay, R., Sepulveda, D.A. (2018). Cyber-resilience: a structure for reaction to cyber-attacks. Presentation at the DTU Transport Summit, May 31, 2018.

Sepulveda, D.A. (2018). Cyber-resilience: a structure for reaction to cyber-attacks. Presentation at the Danish Maritime Fair, May 04, 2018.

Jensen, C.D. (2017). Cyber Threats for Cyber Ships. Presentation at the first CyberShip workshop at the Technical University of Denmark, December 18, 2017.

Sepulveda, D.A. (2017). Cyber Security vs. Cyber Resilience. Presentation at the first CyberShip workshop at the Technical University of Denmark, December 18, 2017.

Sahay, R. (2017). Cyber Security for Cyber Ships. Presentation at the first CyberShip workshop at the Technical University of Denmark, December 18, 2017.

Barfod, M.B. (2017). The CyberShip project. Presentation at the 139th meeting in the technical committee of Danish Shipping. Copenhagen, September 28, 2017.

Sepulveda, D.A. (2017). Cyber risks and the cyber-ship project, lecture at the Supply Chain Management course (Course 42457) at the Technical University of Denmark, DTU, 22 November 2017.