Work Package 3 and 4 Report - Cyber resilience for the shipping industry

Sahay, Rishikesh; Sepúlveda Estay, Daniel Alberto

Publication date:
2018

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

CyberShip Project
Cyber resilience for the shipping industry
Work Package 3 & 4 Report

Rishikesh Sahay, PhD
Daniel Sepúlveda Estay, PhD

November 7, 2018

Abstract

This report describes the current state of the research performed as a part of the CyberShip project for its work packages #3 and #4. Work package #3 defines measures of prevention to cyber-attacks, which include frameworks for the strategic and tactical understanding of the effects of a cyber attack, and a number of frameworks that can be used to structure and analyze the existing risk to a cyber attack in a CyberShip system as defined in work package #2. Work Package #4 defines measure of reaction to cyber-attacks and is developed through the use of software-defined networks (SDN) on a simplified Cybership systems to reflect the potential of using such a technology on a complete CyberShip system. This reports provides a theoretical and methodological foundation to be applied in the development of case studies, subject of work package #5.

Contents

1 Introduction

The CyberShip project, "Cyber resilience for the shipping industry", is a project financed by the Danish Maritime Fund (DMF), for 27 months from September 2017 to November 2019, and is 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 system, this is, a ship operation composed of elements connected through Information and Communication Technologies (ICT).

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

- Work Package 1 (WP1): Project Management, to coordinate technical activities and assure quality of results
- Work Package 2 (WP2): Definition of Cyber Resilience KPIs, to define a specific CyberShip model and cyber resilience key performance indicators (KPIs)
- Work Package 3 (WP3): Cyber attack prevention measures, to define measures and tools at a strategic (design) level
- Work Package 4 (WP4): Cyber attack response and recovery measures, to define measures and tools once and if the cyber attack occurs
- 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
- Work Package 6 (WP6): Dissemination, to link colleagues and stakeholders with the project and its findings and proposals.

Currently, the project is developing Work Packages 3 and 4. These work packages build up on the results obtained in Work Package 2, results that are available in a report available publicly at the research site of the project in the Orbit Database of the Technical University if Denmark [14] .

The foundation for this report is therefore Work Package #2 (WP2). The second work package of the CyberShip project had 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.

This paper therefore describes the prevention and the recovery measures that are proposed as a result of the research in the CyberShip project. These are described in detail, and examples of their application are given.

The contributions of this paper are:

- The proposal of prevention measures for the case of CyberShip systems. This proposal 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.

- The proposal of recovery measures for the case of CyberShip systems. This proposal 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.

2 Related Work

The widespread adoption of ICT throughout today's ships has led researchers to focus on security properties of ship 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. However, the research into ship security is in its early stage and much work focus on identifying potential threats and vulnerabilities [8, 9, 7]. All these reports highlights the risks resulting from the use of ICT to critical systems on the ship. 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 [9]. These are basically management guidelines on how to approach the cyber-security issue in the context of shipping that can be used as an input for the cyber risk assessment. Assessment of the vulnerabilities in the control system of the ship is done in [16]. It examines the importance of critical infrastructure on shipboard system. Moreover, it established threats and vulnerabilities with the aim of developing countermeasures to protect the system.

To the best of our knowledge, there are very few works dealing with the protection of the communication infrastructure of the ship from cyber attacks. Babineau et.al. [13] proposed to periodically diverting the traffic between different switches in the network to protect the critical components of the ship from cyber attacks.

It relies on the redundancy in 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 [2].

Yunfei et.al. [43] and Chen et.al [42] 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.

Moreover, Penera et.al. [35] 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.

Our work aims at proposing a framework to mitigate the attacks in an automated way to improve the resilience of the ship control system.

3 The prevention of cyber-attacks in the CyberShip Model

The first section of this 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.

3.1 Strategic Managerial - Prevention framework

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. [20], 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].

3.1.1 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 1.

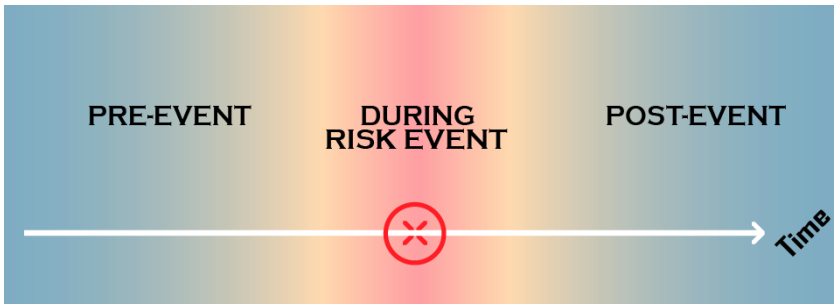

Figure 1: A dynamic representation of a cyber-attack

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 2.

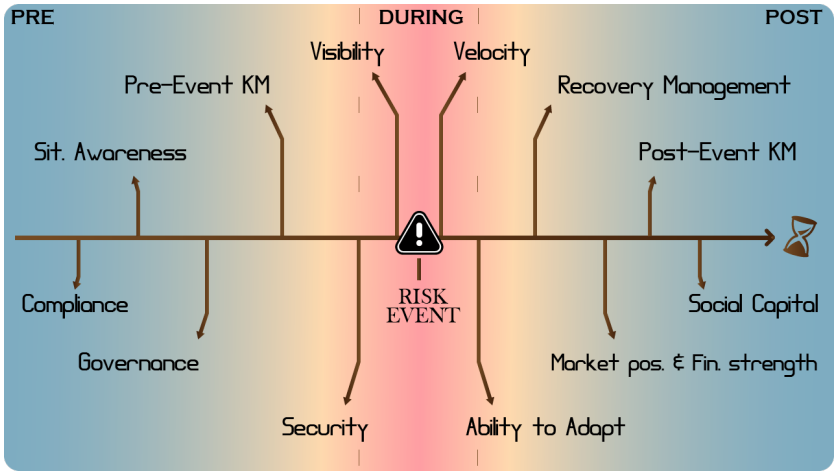

Figure 2: Main themes on the timeline framework

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 learnings 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 3.

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.

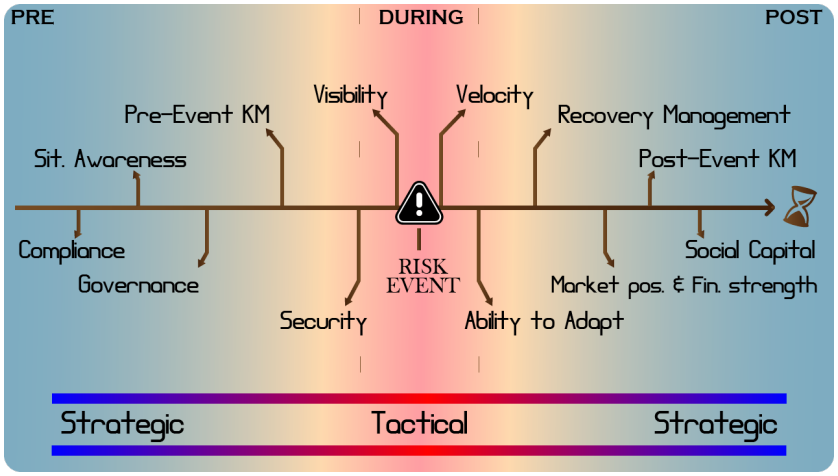

Figure 3: Strategic and Tactical view of the timeline framework

3.1.2 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 4.

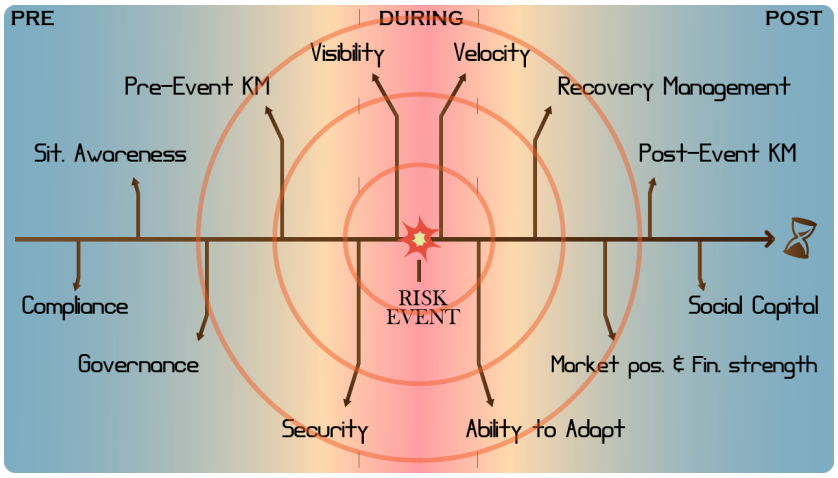

Figure 4: Point of impact for the timeline framework

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 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 5. 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.

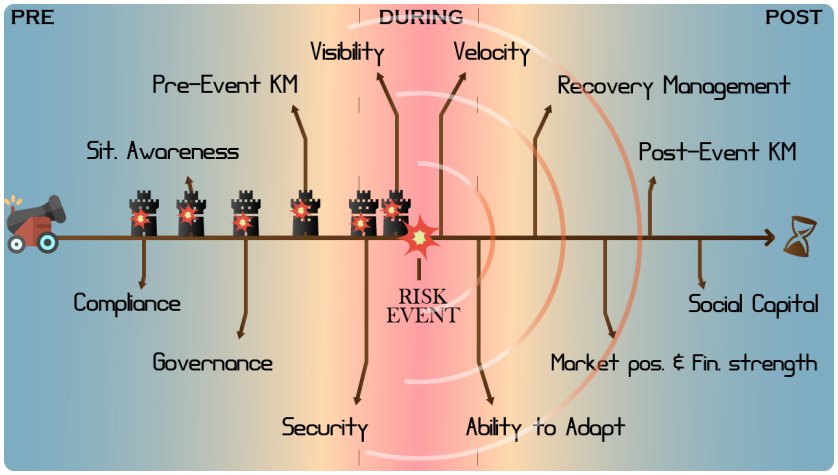

Figure 5: Defenses and ripple effects of a cyber-attack with the time line framework

As an example of the time line use, consider the the left side of the time line from the time of 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 6) 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 unsustainability 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.

3.2 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 sepa-

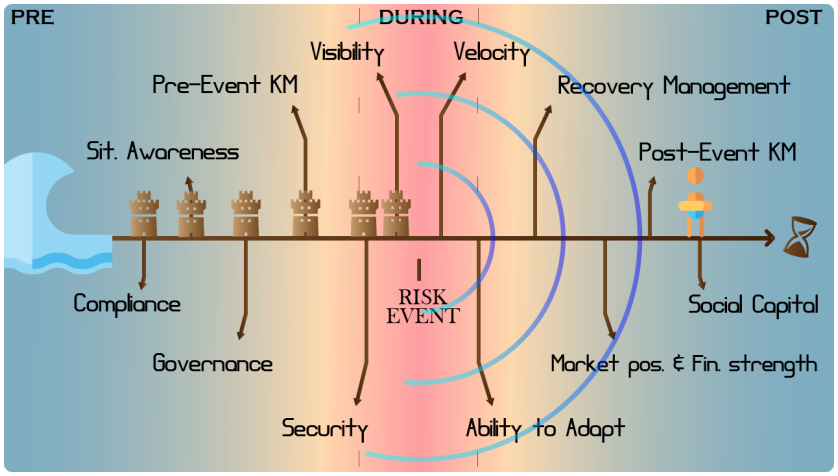

Figure 6: Cyber-tsunami wave analogy with the timeline framework

rately 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 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"* [28]. 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

3.2.1 STPA - Systems theoretic process analysis

This 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 7 is a representation of a generic controlled process.

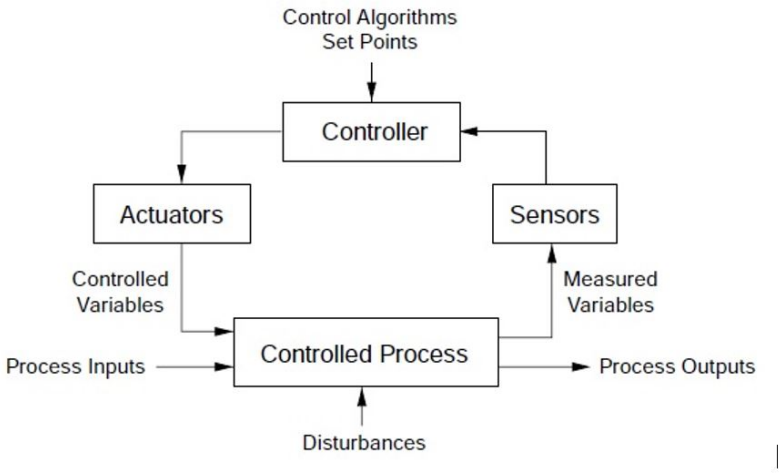

Figure 7: Basic control system

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 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 STAMP methodology framework (Estefan, 2007; Leveson, 2011; Salmon et al., 2012; Altabbakh et al., 2013), with examples of application in different industries, such as medical (Antoine,2013), environmental (Hardy et al., 2011), robotics (Mitka et al., 2015), power production (Karami et

al., 2015), software development (Wang et al., 2016), and defense (Chiesi, 2016). However, no application has been documented for CyberShip systems.

The systems theoretic process analysis (STPA) application is outlined in figure 8.

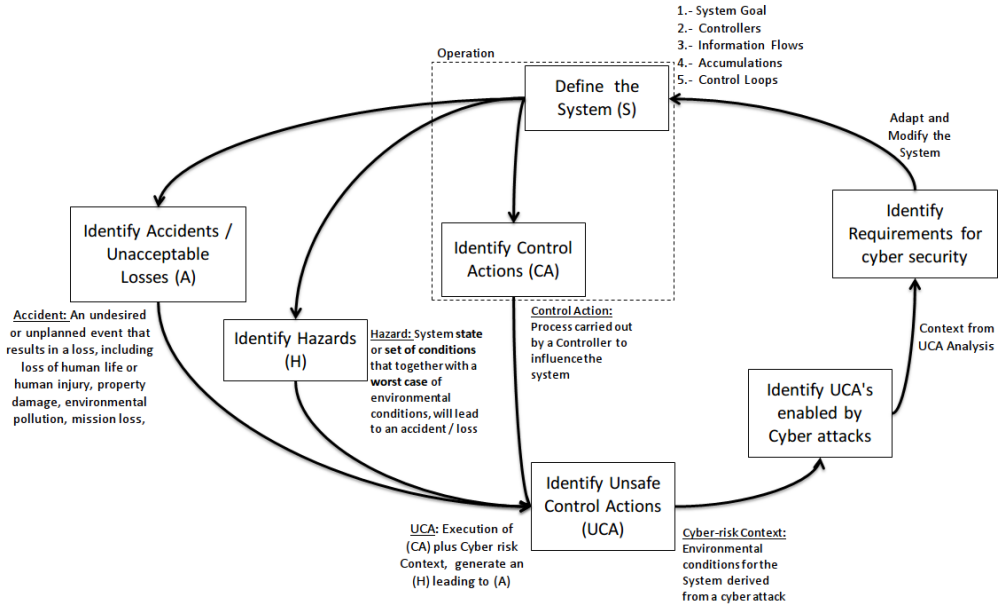

Figure 8: Systems theoretic process analysis sequence

The proposed analysis is an adaptation of the analysis proposed by Leveson [28], 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 unplanned 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 [28] 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 9 shows the representation of a CyberShip STPA analysis.

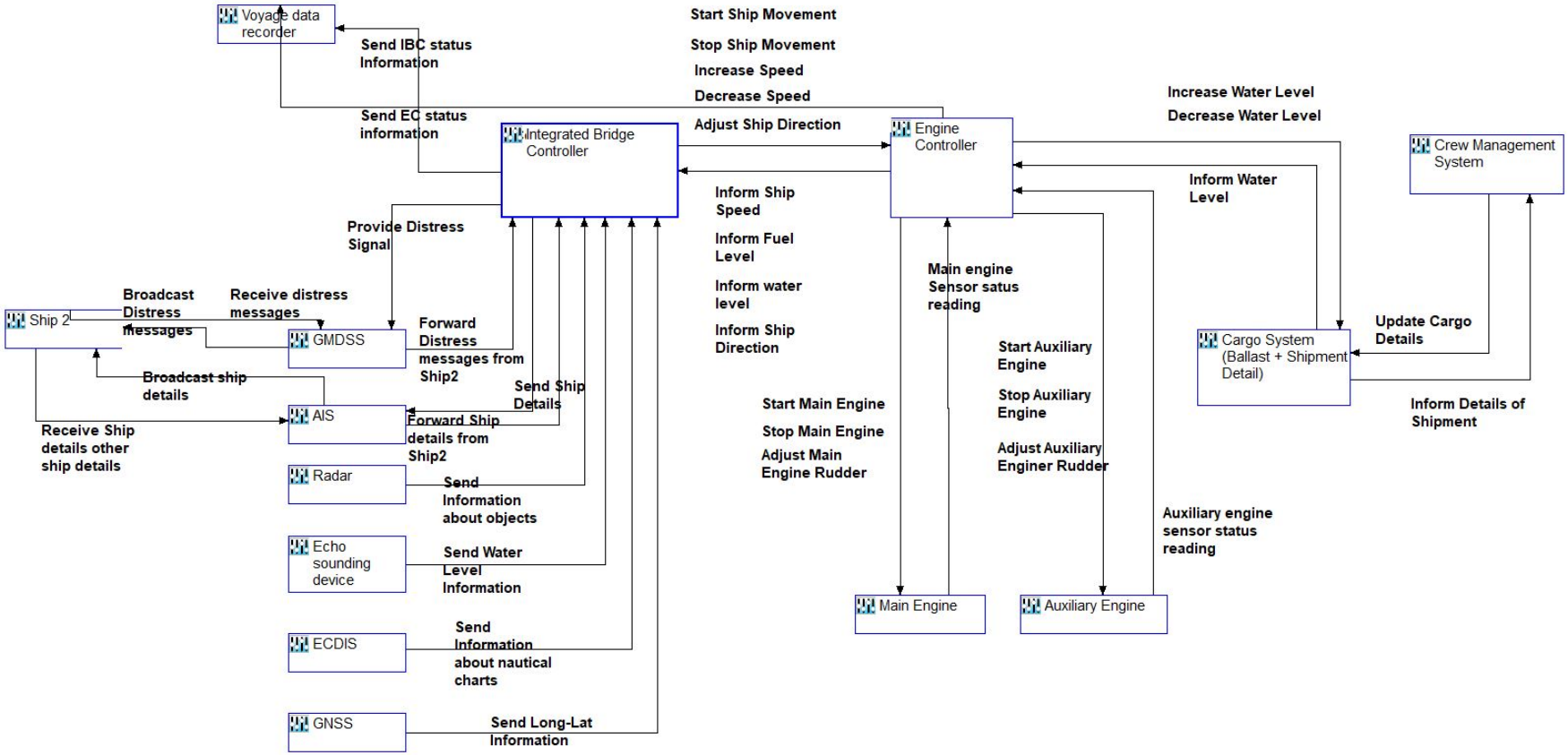

Figure 9: STPA representation of a CyberShip system

4 The reaction to cyber-attacks in the CyberShip Model

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. 10, while the details are given below:

4.1 Components of the Framework

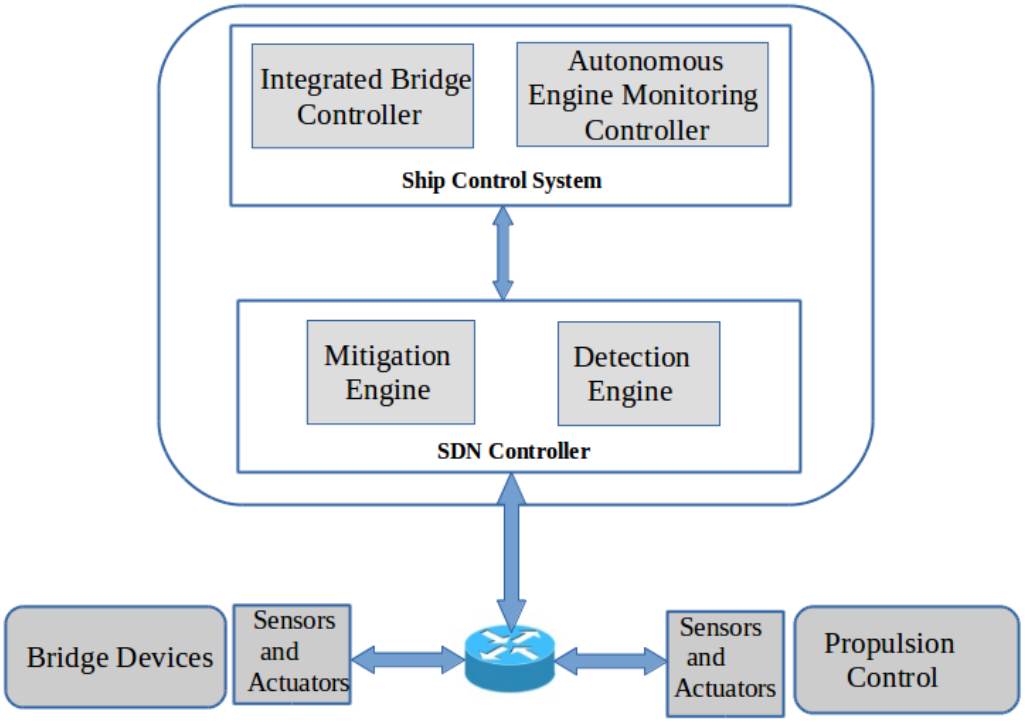

Figure 10: CyberShip Framework

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 [31]. 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 [5]. 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 [9]. 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.

4.2 Use Case

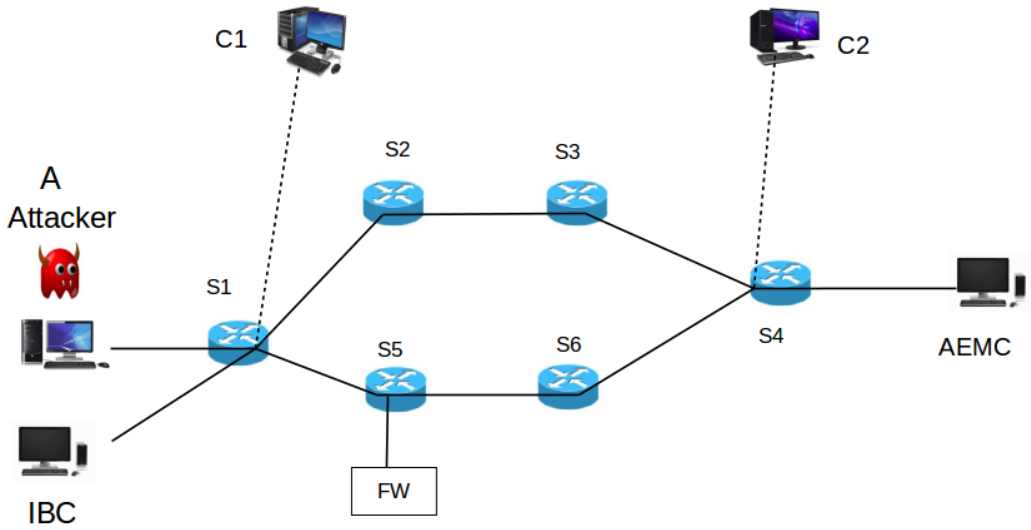

Figure 11: Application of the framework Framework

This section presents a use case exemplifying how the framework enables us to achieve the resiliency by mitigating the attack traffic.

We focus on a scenario of mitigating the impact of the DDoS attack targeting the *AEMC* and congesting the network.

The scenario consists of an attacker denoted as *A*, *IBC* and *AEMC* as shown in Fig. 11.

Moreover, *Mitigation* and *Detection* engine are deployed on a separate controller denoted as C_1 and C_2 respectively.

Controller C_1 is connected through the switch S_1 and manages all the switches in the network except the switch S_4.

Controller C_2 and *AEMC* are connected through the switch S_4. In the scenario, *Detection Engine* is deployed close to the *AEMC*, as the detection can be performed effectively close to the system under protection.

In this use case, we assume that the detection is performed based on the threshold set for packet arrival rate, average of bytes per flow, average of duration per flow.

IBC sends the messages to the *AEMC* either to increase or decrease the speed or to reroute the ship through different waypoints.

Attacker (A) shown in the scenario which is a compromised machine in the ship communication network, launch the UDP flood traffic towards

the *AEMC* to flood the system and network with bogus packets, so that the *AEMC* can not receive the messages from the *IBC*.

A firewall (FW) is deployed at the switch S_5 to process the suspicious and malicious traffic.

Upon detecting an attack, *Detection engine* sends an alert message to the *Mitigation engine* deployed at the controller C_1.

It sends an alert in the IDMEF [22] format for processing the UDP flood traffic. After receiving the alert, *Mitigation engine* extracts the information from the alert message.

Extracted alert information are: source IP of attacker (10.0.0.1), destination IP of *AEMC* (10.0.0.3), event type (UDP Flood), flow class which is ”malicious”.

Depending on the event type (UDP Flood) and conditions: flow class (malicious) it gets the high-level action as a ”Redirect_Firewall” from its policy in the mitigation engine.

Mitigation engine also maintains the information about the different paths along with the middlebox deployment location in the network to divert the flow. The high-level action "Redirect_Firewall" along with flow information are used by the mitigation engine to configure the rules in the switch S_1 to redirect the flow towards the firewall.

To configure the rule, *Mitigation engine* modifies the output port information for the concerned flow in the switch S_1. After redirection of the attack traffic from machine ’A’, IBC gets the fair share of the bandwidth in the path containing switches S_2 and S_3.

5 Discussion

The design description and use case presented in section 4 demonstrates that this architecture enables a dynamic and automated mitigation of attacks in the ship's communication network. Multi-path routing approach in the framework provides failover in case of link failure or congestion. Thanks to the global visibility of the network achieved through the SDN controller, flow details and low-level actions can be quickly modified for the concerned flow.

The high-level policy language and translation mechanism in the framework reduces the burden on the crew member to enforce the low-level rules manually. Moreover, it is not required to learn the device specific syntax to express the policies, since our high-level policy language offers to express the policies in human understandable language.

Furthermore, the framework promotes the collaboration between the controllers managing different network devices and the critical components of the ship. For instance, in case of a fault in the engine system, *AEMC* can request mitigation engine to divert the traffic through different path to reach the secondary engine. Moreover, the *Detection engine* in the framework is responsible to detect cyber attacks at the network layer. This reduces the burden on the controllers managing the ship system as they are responsible to manage and control only bridge and engine system.

6 Conclusion and Future Work

This report lays out the measures and tools proposed through this research project to prevent and recover from cyber events, for the case of a CyberShip system.

The next step in the process is to apply these tools to cases from the shipping industry, as considered in the Work Package#5 of the CyberShip project.

7 References

[1] Code of Practice Cyber Security for Ships. Technical report, IET Standards.

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

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

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

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

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

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

[8] Guidelines on Maritime Cyber Risk Management. Technical report, IMO, 2017. 2

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

[10] K. Ahmed, J. O. Blech, M. A. Gregory, and H. Schmidt. 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, Dec 2015.

[11] Izzat Alsmadi and Dianxiang Xu. Security of software defined networks: Asurvey. *Computers & Security*, 53:79 – 108, 2015.

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

[13] G. L. Babineau, R. A. Jones, and B. Horowitz. 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, Nov 2012. 2

[14] M.B. Barfod, H. Psaraftis, C.D. Jensen, D.A. Sepúlveda Estay, and R. Sahay. Cyber resilience for the shipping industry (cybership), 2018. 1

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

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

[17] E. Germano da Silva, L. A. Dias Knob, J. A. Wickboldt, L. P. Gaspary, L. Z. Granville, and A. Schaeffer-Filho. 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, May 2015.

[18] Nicodemos Damianou, Naranker Dulay, Emil Lupu, and Morris Sloman. 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, 2001. Springer-Verlag.

[19] Xinshu Dong, Hui Lin, Rui Tan, Ravishankar K. Iyer, and Zbigniew Kalbarczyk. 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, 2015.

[20] Christian F. Durach, Joakim Kembro, and Andreas Wieland. A new paradigm for systematic literature reviews in supply chain management. *Journal of Supply Chain Management*, 53(4):67–85, Mar 2017. 3.1, 8.1.2

[21] Seyed K. Fayaz, Yoshiaki Tobioka, Vyas Sekar, and Michael Bailey. Bohatei: Flexible and elastic ddos defense. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 817–832, Washington, D.C., 2015. USENIX Association.

[22] Benjamin Feinstein, David Curry, and Herve Debar. The Intrusion Detection Message Exchange Format (IDMEF). RFC 4765, October 2015. 4.2

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

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

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

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

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

[28] Nancy Leveson. *Engineering a safer world: Systems thinking applied to safety*. MIT press, 2011. 3.2, 3.2.1, 3

[29] Jun Li, Skyler Berg, Mingwei Zhang, Peter Reiher, and Tao Wei. Drawbridge: Software-defined ddos-resistant traffic engineering. *SIGCOMM Comput. Commun. Rev.*, 44(4):591–592, August 2014.

[30] Qi Liang and Yu Menghong. Research on ship cpp networked control system based on svm, gpc and qs. In Liangzhong Jiang, 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, 2012. Springer Berlin Heidelberg.

[31] Ajay Mahimkar, Jasraj Dange, Vitaly Shmatikov, Harrick Vin, and Yin Zhang. dfence: Transparent network-based denial of service mitigation. In *4th USENIX Symposium on Networked Systems Design & Implementation (NSDI 07)*, Cambridge, MA, 2007. USENIX Association. 3

[32] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. Openflow: Enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74, March 2008.

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

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

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

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

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

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

[39] Seungwon Shin, Phillip A. Porras, Vinod Yegneswaran, Martin W. Fong, Guofei Gu, and Mabry Tyson. FRESCO: Modular Composable Security Services for Software-Defined Networks. In *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*, 2013.

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

[41] H. Yelan and C. Hui. 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, Nov 2014.

[42] Chen Yuanbao, Huang Shuang, and Lv Yunfei. Intrusion tolerant control for warship systems. In *4th International Conference on Computer, Mechatronics, Control and Electronic Engineering (ICCMCEE 2015)*, pages 165–170, 2015. 2

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

[44] Jianchao Zhang, Boon-Chong Seet, Tek-Tjing Lie, and Chuan Heng Foh. Opportunities for software-defined networking in smart grid. In *2013 9th International Conference on Information, Communications Signal Processing*, pages 1–5, Dec 2013.

8 Appendix

8.1 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.

8.1.1 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.

8.1.2 Methodology for the SLR

Durach et al. [20] 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 research question is defined as "How should the risks derived from the use of IT systems be managed along the supply chain?". After the inclusion and exclusion criteria are determined, a baseline sample is retrieved by using different search queries that contain combinations of the keywords supply chain, information technology, cyber, security, risk, management and resilience. Those search queries are used in the databases Scopus and DTU Findit, publications that meet the inclusion and exclusion criteria. The results shown in this study are drawn from 123 of those publications.