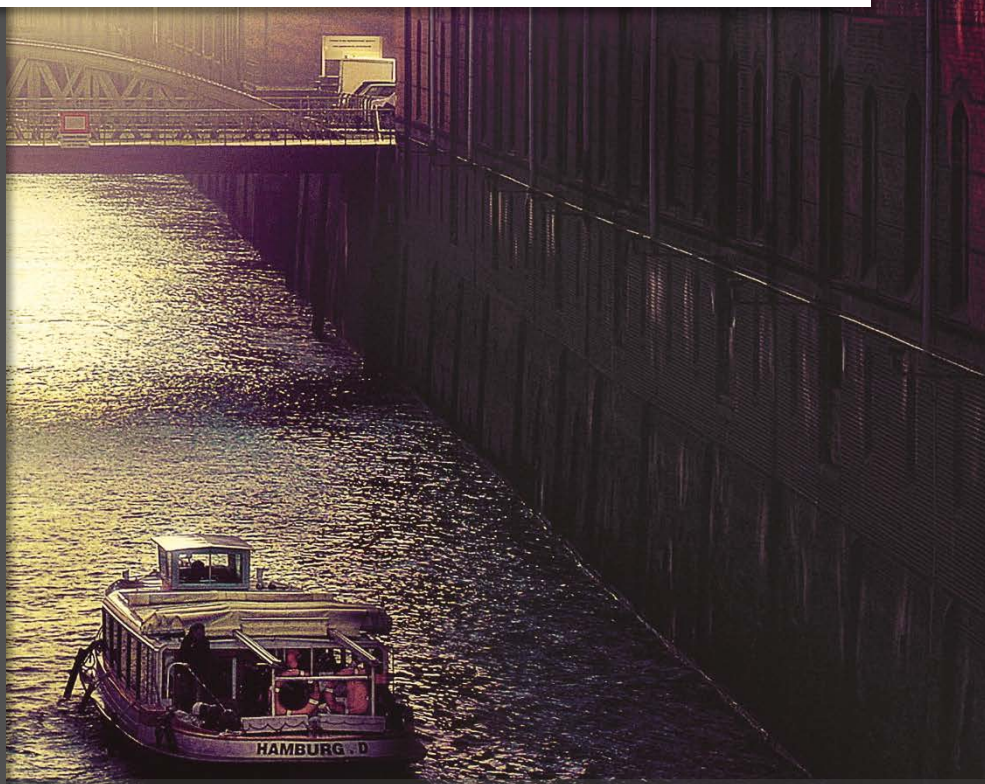
Proceedings of the Hamburg International Conference of Logistics (HICL) – 23

Stefan Schauer, Martin Stamer, Claudia Bosse, Michalis Pavlidis, Haralambos Mouratidis, Sandra König, Spyros Papastergiou

An Adaptive Supply Chain Cyber Risk Management Methodology

HICL



Published in: Digitalization in Supply Chain Management and Logistics
Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.)
ISBN 9783745043280, Oktober 2017, epubli

An Adaptive Supply Chain Cyber Risk Management Methodology

Stefan Schauer[1], Martin Stamer[2], Claudia Bosse[2], Michalis Pavlidis[3], Haralambos Mouratidis[3], Sandra König[1], Spyros Papastergiou[4]

1 – AIT Austrian Institute of Technology

2 – Fraunhofer CML

3 – University of Brighton

4 – University of Piraeus Research Center

Maritime information infrastructures have developed to highly interrelated cyber ecosystems, where ports as well as their partners are connected in dynamic Information and Communication Technology (ICT)-based maritime supply chains. This makes them open and vulnerable to the rapidly changing ICT threat landscape. Hence, attacks on a seemingly isolated system of one business partner may propagate through the whole supply chain, causing cascading effects and resulting in large-scale impacts. In this article, we want to present a novel risk management methodology to assess the risk level of an entire maritime supply chain. This methodology builds upon publicly available information, well-defined mathematical approaches and best practices to automatically identify and assess vulnerabilities and potential threats of the involved cyber assets. This leads to a constantly updated risk evaluation of each business partner's cyber assets together with their cyber interconnections with other business partners. The presented risk management methodology is based on qualitative risk scales, which makes the assessment as well as the results more intuitive. Furthermore, it enables a holistic view on all of the integrated ICT-systems as well as their interdependencies and thus can increase the security level of both a whole supply chain and every participating business partner.

Keywords: IT security; cyber risk management; cyber risk assessment; maritime supply chains

1 Introduction

For an organization, participating in a maritime supply chain implies not only the need to cooperate with other stakeholders at business level, but due to the ongoing digitalization also to set up interfaces in their information and communication technology (ICT) infrastructure for the ICT systems of their business partners. Hence, these supply chains have become highly interrelated cyber ecosystem, where the complexity and degree of networking of connected digital assets beyond company borders increases. Nevertheless, every data interface also represents a potential threat in form of a possible entry point for unplanned access to the networks and the systems located behind it.

A global study among risk managers and risk experts rated cyber incidents as the third highest business risk worldwide for all sectors and are expected to become the highest business risk in the future. In Europe, cyber risks are rated already as the second highest and in Germany as the highest business risk (Allianz Global Corporate & Specialty SE, 2017).

So far, the number of disclosed cyber incidents in the transportation sector is not very high and thus can be considered to be even smaller in maritime supply chains (Verizon, 2017). However, companies might not report every attack due to fears of reputational damage or - even worse - the attacks weren't noticed due to a lack of awareness and knowledge (Wingrove, 2017; Kotchetkova, 2015). Considering the damage potential, vessels and ports might become an appealing target for attackers in the future. The following incidents from the past illustrate the bandwidth of possibilities: (a) Drugs were hidden in containers and these containers were misled without early recognition (Bateman, 2013); (b) Customs systems were shut down, stopping operations for hours, probably to extort ransom (Port of Rotterdam, 2016); (c) Disruption of the GPS-signal stopped operations of vessels as well as of terminal cranes that store and locate containers basing on GPS for the same reason (Wagstaff, 2014; Scott, 2015; Hayes, 2016); (d) Piracy attacks use AIS-signals to identify vessels and hack into the shipping companies systems to identify their loaded goods (Allianz Global Corporate & Specialty SE, 2016); (e) Global ransomware campaign known as "WannaCry" and detected on May 12, 2017, affected various organizations with tens of thousands of infections in over 150 countries (US-CERT, 2017a).

Just a couple of weeks after the "WannaCry" attack, on June 27, 2017, another major global cyberattack (at some point linked to the existing ransomware "Petya", but later on due to its additional features also referred to as "NotPetya") was

launched, using among other attack vectors the same exploit as ”WannaCry” (US-CERT, 2017b; Fox-Brewster, 2017). It exploited a vulnerability in a Ukrainian tax preparation software update mechanism to propagate and attack entire networks (e.g. Cimpanu, 2017). Besides several Ukrainian ministries, banks and metro systems, large companies became also victim of the attack. Among many others, Beiersdorf AG, A. P. Moller-Maersk Group, Merck Sharp & Dohme (e.g. Holland, 2017) and India's largest container terminal JNPT (e.g. PTI, 2017) were affected and, as a consequence, had to deal with business interruptions. The malware's attack path leading from a Ukrainian software update to several international company networks shows how malware can propagate among the connected ICT systems in supply chains.

Due to these incidents, the general awareness for the need of cyber security and cyber risk management increases and will rise further with every new mayor security incident. Nevertheless, state-of-the-art risk management methodologies for maritime environments pay limited attention to cyber-security and do not adequately address security processes for international supply chains. Motivated by these limitations, we introduce the MITIGATE methodology, a novel risk management approach, which will empower stakeholders' collaboration for the identification, assessment and mitigation of risks associated with cyber-security assets and supply chain processes. This collaborative system will boost transparency in risk handling, while enabling the generation of unique evidence about risk assessment and mitigation.

The paper is structured as follows: Section 2 presents general regulations and standards for port security. Section 3 provides a short overview on the MITIGATE project while one of the project's main outputs, the MITIGATE risk management methodology, is described in Section 4. The key concepts of the MITIGATE methodology are sketched in Section 5 followed by a discussion, while section 7 concludes the paper.

2 Regulations and Standards for Port Security

ICT systems of ports are classified as “Critical Information Infrastructures” (CII), because ports are of crucial importance for the unrestricted supply, trade and economy of a country. The EU adopted in July 2016 the Network and Information System (NIS) Directive (EU, 2016). The directive aims to reach a common level of security for NIS in the EU. This process will be supported by the European Union

Agency for Network and Information Security (ENISA) and protected by Computer Security Incident Response Teams (CSIRT) all over Europe.

There are already several security guidelines in place, e.g., from the Baltic and International Maritime Council BIMCO (BIMCO, 2017). They provide effective advice, and awareness-rising posters for the use on board showing the need for security measures. Further, they indicate how to avoid the biggest part of incidents by giving striking rules for the use of passwords and private communication devices. The International Maritime Organization (IMO) issued the "Interim Guidelines on Maritime Cyber Risk Management" in 2016 (IMO, 2016) and the U.S. promotes "Information Sharing and Analysis Organizations" (ISAO), e.g., the "Maritime & Port Security Information Sharing and Analysis Organization" (MPS-ISAO, 2017). Finally, the International Association of Classification Societies (IACS) in shipping reacts to cyber threats with a "Cyber Systems Panel" that was installed in 2016 (IACS, 2015). The focus of this panel lies on the early development of cyber resilient onboard systems.

Beside these guidelines, there are also several standards and regulative which address security and cyber security issues in maritime supply chains. Among them, the most important is the International Ship and Port Facilities Security (ISPS) Code (International Maritime Organization, 2003). The ISPS Code is a comprehensive set of measures to enhance the security of ships and port facilities, focusing mainly on topics from the field of physical security and object protection. Hence, a major drawback is the lack of specific tools, distinct measures or general role descriptions tailored to the ICT security for port infrastructures. The main objectives of the ISPS-Code with regards to ICT infrastructures are to ensure that security communication is easily available and to prevent unauthorized deletion, destruction or amendment of the security plans. Security plans may be saved in an electronical format and therefore need to be protected.

An international standard specifically tailored to the field of ICT security is the ISO/IEC 27001:2013 (International Standardization Organization, 2013). The ISO/IEC 27001 is a commercial standard, representing a collection of best practices and guidelines, describing how to establish, implement, maintain, monitor and improve an Information Security Management System (ISMS). The standard is generic in a way that the specified ISMS is applicable to organizations of various types, sizes as well as different industries and markets. It should be noted that ISO/IEC 27001 is actually not a risk management methodology, but rather a compliance standard, reporting a list of controls for good security practices and the

requisites that an existing method should have to be standard-compliant. Specifically, it provides generic requirements that the risk analysis and management needs to fulfill and references the ISO/IEC 27005 (International Standardization Organization, 2011) (and further the ISO 31000 (International Standardization Organization, 2009)) as a possible risk management methodology.

Although the ISO/IEC 27001 is applicable to several domains, the transportation and logistics industry has introduced a common security management standard, the ISO 28001:2007 (International Standardization Organization, 2007). Whereas the ISO/IEC 27001 or the ISPS are focused on a single organization, the security of the overall supply chain is the main objective of the ISO 28001. Therefore, the standard includes the specific requirements to improve the security of all aspects of the supply chain, including financing, manufacturing, information management and the facilities for packing, storing and transferring goods between modes of transport and locations. As a specialty of the ISO 28001, all partners involved in the supply chain need to sign a security declaration specifying their currently implemented security measures to ensure a common security level over the whole supply chain.

3 MITIGATE Project

As described in the previous Section, there are several standards and guidelines at hand to prepare for cyber attacks and incidents. Nevertheless, a framework dedicated to the assessment and management of cyber risks of maritime supply chains has not been developed, yet. The ICT infrastructure of ports is particularly vulnerable, due to comprising hard- and software assets of the companies engaged in transport and goods handling in the maritime supply chain. Ports are located at the interface of information flows from many different users and countries, which have to offer access and exchange capabilities for digital information. However, all these interfaces also represent possible entry points for attackers. The ongoing digitalization will result in even more complex and a higher degree of networked ICT systems and so will the number of electronic interfaces to business partner systems in supply chains increase, which cannot be supervised and controlled by the single company.

In order to ensure that these processes and interconnections don‘t allow malware to shut down operations or allow manipulation of data for illegal purposes, a

solution to identify threats along the supply chain and beyond company boundaries is urgently needed. The H2020 project MITIGATE (MITIGATE, 2016) is looking in particular into security issues within the supply chain and aims at providing tailored solutions for these problems. MITIGATE will introduce, integrate, validate, evaluate and commercialize a risk management system for port infrastructures, which will be able to deal with port CIIs and ICT systems, as well as their impact on dynamic maritime supply chains. MITIGATE will emphasize the collaboration of various stakeholders in the identification, assessment and mitigation of risks associated with cyber-security assets and international supply chain processes. This collaborative approach will boost transparency in risk handling by the various stakeholders, while it will also generate unique evidence about risk assessment and mitigation.

The collaborative approach of the project will be empowered by the MITIGATE Open Simulation Environment enabling the participants to model, design, execute and analyze attack-oriented simulation experiments using novel simulation processes. Particular emphasis will be laid on the estimation of the cascading effects, as well as on the prediction of future risks (based upon common metrics across sectors). Relying on evidence–based simulations, port operators, decision makers and other stakeholders will be able to select cost effective countermeasures and compile holistic port security policies going beyond the ports' CII isolated domain to ensure the ports' supply chain security.

Furthermore, the tools will be equipped with real-time decision support systems, which will aim at automating the process of estimating risk and enacting risk mitigation measures. MITIGAGE will integrate open source intelligence data (including data from social networks and crowd-sourcing) towards enhancing its threat assessment and prediction functionalities. At the heart of the MITIGATE system will be a range of mathematical instruments, which will be used for threat and vulnerability analysis, as well as for the assessment of contingency plans and their cost-effectiveness.

4 Risk Management Methodology

As a core result of the MITIGATE project, the MITIGATE Risk Management Methodology has been developed. It aims at estimating the cyber risks for all assets of all business partners involved in a maritime supply chain service (SCS) and represent the basis for the MITIGATE system. The MITIGATE methodology is compliant with

SCS Analysis	Cyber Threat Analysis	Vulnerability Analysis	Impact Analysis	Risk Assessment	Risk Mitigation
S1.1:Goals & Objectives	**S2.1**: SCS Cyber Threat Identification	**S3.1**: Identification of Confirmed Vulnerabilities	**S4.1**: Individual Asset Impact Assessment	**S5.1**: Individual Asset Risk Assessment	**S6**: Risk Mitigation
S1.2: Business Partners	**S2.2**: SCS Cyber Threat Assessment	**S3.2**: Identification of Unknown Vulnerabilities	**S4.2**: Cumulative Impact Assessment	**S5.2**: Cumulative Risk Assessment	
S1.3: Modelling		**S3.3**: Individual Vulnerability Assessment	**S4.3**: Propagated Impact Assessment	**S5.3**: Propagated Risk Assessment	
		S3.4: Cumulative Vulnerability Assessment			
		S3.5: Propagated Vulnerability Assessment			

Figure 1: Overview of the different steps of the MITIGATE methodology

the main standards for port security, the ISPS Code (IT Section), ISO 27001 and ISO 28001, which have been briefly described in the previous Section 2. Accordingly, the six steps of the methodology (cf. Figure 1) represent the main steps also described in these standards. In the following, we will present a high-level overview on the different steps of the methodology going into detail on the central features later on in Section 5.

4.1 SCS Analysis

In this first step, the scope of the risk assessment is defined. Therefore, the business partners involved in the SCS under examination are identified. All the business partners agree on the goals and the desired outcome of the risk assessment. Further, the SCS under examination is decomposed and inspected in detail by the business partner's risk assessors who initiated the risk assessment. They identify the participants of the SCS involved from their perspective, i.e., within their organizations.

For each participant of the risk assessment, the main cyber and/or physical processes (i.e., controlled/monitored by a cyber system) that comprise the examined

SCS are collected. The MITIGATE methodology is focusing in particular on the interdependencies among these cyber assets. Therefore, these interdependencies are further classified based on different types (e.g., whether they are installed on the same system, communicating of network interfaces, etc.) describing the relationship between the cyber assets in more detail.

The SCS analysis results in a list of all business partners together with their cyber assets relevant for the SCS. Further, a graph of all cyber assets connected based on their interdependencies is created.

4.2 SCS Cyber Threat Analysis

Based on the list of cyber assets created in the first step, all potential threats related to these cyber assets are identified in the second step of the MITIGATE methodology. Due to today's rapidly changing threat landscape, the list of threats needs to be as exhaustive and up-to-date as possible. To achieve that, the MITIGATE methodology foresees the integration of multiple source of information, i.e., online threat repositories like the National Vulnerability Database (NVD)(NIST, 2017), crowd sourcing and social media as well as the business partners' experts. This makes the methodology highly adaptive to novel attack strategies and attacker behavior. The multitude of different data sources helps to increase the quality of the whole risk assessment.

When the list of relevant threats is established, the likelihood of occurrence is estimated for each of them. Also for this step, various sources of information are combined: information from online repositories and social media is taken into consideration as well as historical data and expert opinions. Instead of just use one of these sources (e.g., relying only on historical data or expert opinions), this approach offers the advantage of integrating a more diverse and complete overview on the topic. Thus, the assessor obtains a more realistic estimation of the threat likelihood. The resulting likelihoods are expressed using a semi-quantitative, five-tier scale and all the gathered information is integrated. Finally, a Threat Level (TL) based on this likelihood is assigned to each threat.

4.3 Vulnerability Analysis

Similar to the identification of threats in the previous step, in this step a list of vulnerabilities of the cyber assets of the SCS under examination is compiled. In the context of the MITIGATE methodology, a vulnerability is understood as a defective state of a cyber assets due to a poor configuration, the lack of security patching, etc. A threat can manifest in the SCS by exploiting a vulnerability of one of the involved cyber assets.

The MITIGATE methodology differences between two main types of vulnerabilities: confirmed vulnerabilities and potentially unknown or undisclosed vulnerabilities. In more detail, vulnerabilities which are already know in the community and are listed in online repositories or by specific Computer Emergency Response Teams (CERTs) are understood as confirmed vulnerabilities. On the other hand, there are vulnerabilities in software systems which are not publicly known, yet. Such unknown or undisclosed vulnerabilities are more dangerous since security experts are not aware of them but they can be (easily) exploited by adversaries.

A core feature of the MITIGATE methodology is to take these unknown and/or undisclosed vulnerabilities into account. In this context, the data coming from various information sources (online repositories, social media, expert knowledge, etc.) is collected and processed to estimate the existence of unknown vulnerabilities. In more detail, the analysis is carried out over all time scales in the available dataset (e.g., by empirically characterizing the distribution of a vulnerability's lifespan) or determining the number of vulnerabilities publicly announced for a specific period of time (e.g., using the rate of vulnerability announcements in the NVD).

To characterize both confirmed and unknown/undisclosed vulnerabilities within one methodology and make them comparable, the Common Vulnerability Scoring System (CVSS) (Mell and Scarfone, 2007) is applied. For each vulnerability, the Individual Vulnerability Level (IVL) is specified by assessing the Access Vector, Access Complexity and Authentication. The scores for these three values are coming from the online database NVD and are mapped onto a qualitative, five-tier scale for further processing. The details on this mapping are given in section 5.1.

Additionally, the MITIGATE methodology is not only looking at the immediate effects of an attack exploiting a specific vulnerability but is also taking the respective cascading effects into account. Therefore, the concepts of a Cumulative Vulnerability Level (CVL) and a Propagated Vulnerability Level (PVL) are introduced. They

are described in detail in the following Section 5.2. Accordingly, the vulnerability analysis results in a list of all vulnerabilities together with their respective IVL, CVL and PVL.

4.4 Impact Analysis

After the vulnerability analysis done in the previous step, the MITIGATE methodology is also looking at the potential impact an exploitation of these vulnerabilities might have. To stay consistent with the vulnerability analysis, the CVSS (more specifically, the three security criteria Confidentiality, Integrity and Availability) is applied for assessing the impact. Accordingly, the scores for the security criteria are also mapped onto the same qualitative, five-tier scale as the vulnerabilities (cf. Section 5.1).

Furthermore, the notion of cascading effects is carried on for the impact analysis, resulting in the concepts of Individual Impact Level (IIL), Cumulative Impact Level (CIL) and Propagated Impact Level (PIL). Details on these impact levels are also discussed in further detail in Section 5.2.

4.5 Risk Assessment

The risk assessment in the MITIGATE methodology is loosely based on the general approach risk = likelihood $\times$ impact (Oppliger, 2015). Hence, in our context the threat level (as described in Step 2, Section 4.2), vulnerability level (as described in Step 3, Section 4.3) and impact level (as described in Step 4, Section 4.4) contribute to the risk level. Further carrying on the notion of cascading effects, the MITIGATE methodology describes three risk levels: Individual Risk Level (IRL), Cumulative Risk Level (CRL) and Propagated Risk Level (PRL). This leads to the following formula

$$IRL = TL \times IVL \times IIL$$

for the Individual Risk Level; the other two risk levels (CRL and PRL) are computed accordingly. The overall result is then again mapped onto a qualitative, five-tier scale.

4.6 Risk Mitigation

In the final step of the MITIGATE methodology, the main results of the risk assessment are compared against specific thresholds, which have been set and agreed by all business partners. If some of the results exceed these predefined thresholds, additional security controls need to be implemented by the business partners and by the SCS (as a whole) to lower the respective risk levels. To identify the best choice of mitigation actions out of a set of possible controls, a game-theoretic approach is applied. This represents a mathematically sound method to find a way to minimize the expected damage caused by an attack that exploits multiple vulnerabilities.

To formalize the game, the possible actions taken by the adversary (i.e., a malicious party performing an attack) and the defender (i.e., all business partners in the supply chain) need to be identified. Any combination of these attack and defense strategies yields a particular damage (i.e., the risk level), which is interpreted as the respective payoff for this combination. Minimizing over all these damages (i.e., the game's payoff matrix) leads to the three main outcomes of this step: an optimal attack strategy, an optimal defense strategy and the maximum risk level for the case the attacker and defender both follow their optimal strategies.

The optimal defense strategy indicates which mitigation actions should be chosen by all the business partners to minimize the damage to the entire SCS. Due to the mathematical basis of game theory, it can be shown that even if the adversary deviates from the optimal attack strategy, the business partners don't have to change their defensive strategy; a deviation by the adversary only manifests in a lower maximum risk level as long as the defender plays his optimal strategy. We describe this approach in more detail in section 5.3.

5 MITIGATE Key Concepts

The MITIGATE methodology builds on three major concepts for the assessment of the cyber risks within the SCS, which also represent the main research results of the MITIGATE project. Further, the combination of these concepts also represents the main difference and advantage of the MITIGATE methodology over existing solutions. In the following, we will describe these three concepts in more detail.

AV	Local			Adjacent			Network		
Auth / AC	High	Medium	Low	High	Medium	Low	High	Medium	Low
Multiple	VL	VL	L	L	L	M	M	M	H
Single	VL	L	M	L	M	H	M	H	VH
None	L	M	M	M	H	H	H	VH	VH

Figure 2: Mapping of the CVSS metric ”Exploitability” onto the IVL

5.1 Semi-Automated Vulnerability Analysis

As already pointed out in previous sections, threats and attacks on cyber systems have evolved drastically over the last years. An increasing number of more and more complex attacks have been carried out and large companies as well as critical infrastructures have fallen victim to those attacks. One major reason for that is the large number of vulnerabilities in software systems, which can be exploited by malicious parties to circumvent security systems and infiltrate an organization’s infrastructure. As mentioned in Section 4.3, unknown vulnerabilities are the most critical ones in this context, because neither the users nor the creators of a software system are aware of their existence.

Most of today’s risk assessment methodologies and frameworks are not able to keep up this speed of evolving attacks and are not aware of the vulnerabilities within examined systems. The MITIGATE methodology is able to adapt to this fact and to build the risk assessment on top of a constantly updated vulnerability database, i.e., the NVD. It is maintained by the National Institute of Standards and Technology (NIST) (NIST, 2017) and updated frequently with the most current information on numerous software systems. Further, the NVD applies the CVSS to assess each vulnerability, providing an estimation of a specific vulnerability’s relative importance, which further allows setting up a prioritization later on.

As described in Section 4.2 above, all the assets relevant for a specific SCS are collected during Step 2 of the MITIAGTE methodology. In addition, information on existing vulnerabilities is imported from the NVD on a daily basis and checked against the identified assets. This results in a list of assets together with the latest version of their vulnerabilities. Furthermore, the CVSS scoring given in the NVD is mapped onto a five-tier scale, ranging from ”Very Low” to ”Very High”. The resulting score represents the above mentioned Individual Vulnerability Level (IVL) and is automatically assigned to every vulnerability of every asset in the SCS (cf. Figure 2).

C	None			Partial			Complete		
I / A	None	Partial	Complete	None	Partial	Complete	None	Partial	Complete
None	VL	VL	L	L	L	M	M	M	H
Partial	VL	L	M	L	M	H	M	H	VH
Complete	L	M	M	M	H	H	H	VH	VH

Figure 3: Mapping of the CVSS metric ”Impact” onto the IIL

Since the CVSS also estimates the consequences exploiting a specific vulnerability may have on the Confidentiality (C), Integrity (I) and Availability (A) of the underlying asset, this information is integrated into the Individual Impact Level (IIL) by applying a similar mapping (cf. Figure 3).

Furthermore, also currently unknown vulnerabilities can be defined in the MITIGATE methodology for each asset. As already mentioned in Section 4.3 above, this information is usually found by involving expert knowledge or interpreting contributions in news feeds or social media. The MITIGATE methodology supports this activity by an automated search of the respective online sources and highlighting potential relevant topics. Nevertheless, the assessment has to be carried out by an expert but can be done using the CVSS metrics (or the five-tier scale) as for to the known vulnerabilities. In this way, information coming from different sources can be easily integrated into the same assessment process.

5.2 Cumulative and Propagated Risks

When looking at the vulnerabilities identified in the beginning of Step 3 (cf. Section 4.3), we have to be aware that the exploitation of one vulnerability may just be the entry point of an adversary into a business partner’s infrastructure. For example, using the enhanced access rights gained by the exploiting a specific vulnerability, an adversary might be able to further navigate through the organization’s asset network towards another (and maybe more profitable) target. In particular, this is the case for Advanced Persistent Threats (APT)s. Therefore, the following two views also need to be considered in the analysis of a specific vulnerability: on the one hand, what are the possible ways (paths in the asset network) to reach that vulnerability instead of attacking it directly (if that is possible at all). On the other hand, after exploiting one vulnerability, what are the other possible vulnerabilities

an adversary is able to reach (e.g., due to additional privileges or access to other assets).

The MITIGATE methodology accounts for both ideas by introducing the concepts of Cumulative Vulnerability Level (CVL) and Propagated Vulnerability Level (PVL). The goal of the CVL is to accurately reflect the exploitation level of the vulnerabilities by taking into consideration the IVL and the context within which these vulnerabilities appear (i.e., the assets' interdependencies). In other words, the CVL measures the likelihood that an attacker can successfully reach and exploit a vulnerability, given a specific path in the asset network. Such a path describes the list of sequential vulnerabilities on different assets that arise from consequential multi-steps attacks.

Whereas the CVL focuses on all possible attack chains concluding into the same target point, the PVL inspects the likelihood that an attacker can penetrate a network up to some specific depth. In other words, the PVL takes all possible paths of sequential vulnerabilities of a specific length into account, starting from one particular vulnerability.

Analogously to the CVL and PVL, the Cumulative Impact Level (CIL) and Propagated Impact Level (PIL) are defined. As indicated by the naming, the only difference is that in this case the potential impact of exploiting a specific vulnerability is assessed. Carrying on as already mentioned in Step 5 of the MITIGATE methodology (cf. Section 4.5), both concepts of vulnerability and impact are combined to result in the respective notions of risk. Hence, the MITIGATE methodology outputs a Cumulative Risk Level (CRL) and a Propagated Risk Level (PRL) together with the IRL already mentioned in Section 4.5.

5.3 Attack Paths Discovery

Essential element of risk management, and of the MITIGATE methodology, is the mitigation of risks through the identification of appropriate security controls. To this end, attack paths are a valuable tool to business partners, illustrating paths an attacker can use to reach a particular cyber asset. It can support the analysis of risks to a specific cyber asset that may not be the entry point of an attack and support the examination of possible consequences of a successful attack. Moreover, the attack paths support the identification of appropriate security controls by providing knowledge about attributes that make an attack possible. The generated attack paths can answer 'what-if' questions regarding the security

implications of configuration changes to assets, such as patching a specific asset. Furthermore, they can reveal which attacks can be performed by highly skilled attackers and well-funded attackers and which attacks can be performed by low skilled attackers.

The MITIGATE methodology includes an algorithm to discover attack paths. In particular, it examines how an attacker can exploit identified cyber asset vulnerabilities in order to perform undesired actions. For every attack, a set of related weaknesses (CWE) and vulnerability types are defined. It is assumed that to perform this kind of attack the attacker must have access to an asset that has one or more vulnerabilities that are compatible with either the weaknesses or the type defined. Attack paths are then modelled by employing attack graphs. Each node in the graph represents a combination of asset and vulnerabilities that an attacker can exploit. Each edge represents the transition of an attacker from one asset to another.

The algorithm requires as input a physical network topology, an asset configuration, a set of entry points and target points, and an attacker's profile. In particular, the network topology includes a list of cyber assets and their relationships. For example, an asset may be installed on another asset or it just communicates with another asset. The asset configuration includes information about a particular asset. For example, the name of the asset, an id, the business partner to which this asset belongs, its vulnerabilities, and attributes from the CVE repository, such as access complexity and access vector. The entry point and the target points are specific cyber assets on which a business partner wants to focus on. The attacker's profile includes information about the assumed attacker, such as the attacker capability, which is the counterpart to a vulnerability's access complexity and the attacker location, which is the counterpart to a vulnerability's access location. The attackers profile is used to induce whether a particular attack can exploit an asset's vulnerability.

The output of the algorithm is a list of attacks paths. Each attack path contains an ordered list of cyber assets that an attacker with a particular attacker's profile can successfully compromise by exploiting their vulnerabilities. Each cyber asset in the attack path can be used as a stepping stone to an attack to the next cyber asset. A business partner must be able to locate all potential attack paths into the network and prevent attackers from using it. Business partners can hypothesize new 'zero-day" vulnerabilities of cyber assets, evaluate the impact of changing configuration settings, and determining the security effectiveness of adding new

security controls. The identification of an optimal set of security controls, which receives as input the generated attack paths, is described in the next section.

5.4 Game-Theoretic Risk Minimization

Besides identifying and assessing the vulnerabilities of assets and thus obtaining a risk estimation based on latest threat information, mitigating these risks is an essential part of the MITIGATE methodology. Whereas other approaches only offer guidance on which mitigation actions to choose, the MITIGATE methodology applies a game-theoretic framework to identify the optimal set of mitigation actions.

The game is setup as a two-player zero-sum game, applying a minimax-approach (Maschler, Solan and Zamir, 2013). To be more specific, the game describes the combating situation between two players (in our case an adversary and the defender, i.e., security officer) where each player tries to optimize his payoff. In a zero-sum game, the gain of one player represents, at the same time, the loss of the other player, which describes the real-life situation between an adversary and the defender quite well. Both players have a set of strategies they can follow and each strategy results in a specific profit for each player. These profits are collected in the payoff matrix and the goal is to minimize the maximum profit (i.e., minimax-approach) of the adversary. Thus, the strategies for both the adversary and the defender are the central parts in the MITIGATE methodology. The adversary's strategies are defined by the paths through the asset network, which the adversary is able to take to reach a specific vulnerability. These paths have been defined in Step 3 (Section 4.3). The defender's strategies are given by the respective security measures a business partner is able to implement. These countermeasures may come from the business partner's experience or can be deduced from the information stored in the NVD. Such a defense strategy could be to do spot checking or patching of a specific asset (i.e., closing a specific vulnerability).

Each combination of an attack and a defense strategy defines a scenario with a specific payoff for both the adversary and the defender. In our context, this payoff is the potential damage caused by the attack (represented by the IIL, CIL and PIL). The adversary wants to maximize this damage; the defender wants to minimize it. Since both the CIL and PIL representing the damage are based on the potential paths an adversary can take in the asset network, the effect of a defense strategy

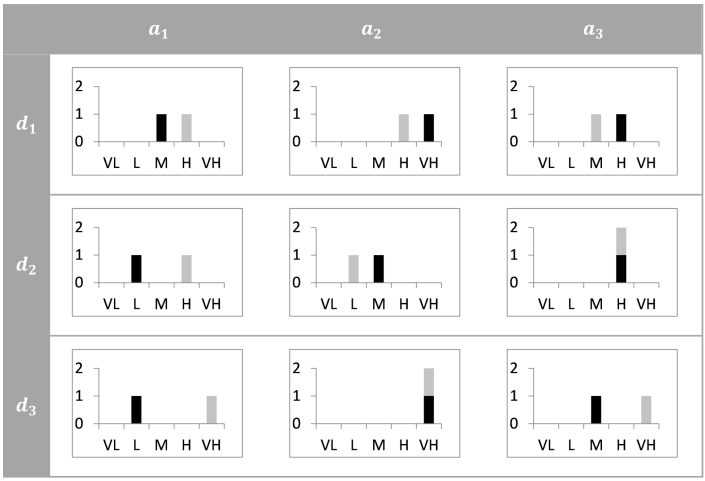


Figure 4: Example of a payoff matrix for the game with attack strategies a_1 to a_3 and defense strategies d_1 to d_3 (cf. Schauer et al., 2016).

is modeled by closing some vulnerabilities and thus eliminating some of these paths. In general, every scenario will consist of multiple paths, each one causing a specific damage. The best way to represent the collection of all these damages without losing any information is to use a histogram (Rass, König and Schauer, 2015).

The payoffs for all scenarios are collected in the payoff matrix, which is used to evaluate the game (cf. Figure 4 for an example). Since we are using histograms as payoffs, we are going beyond standard game theory and have to apply a novel framework (Rass, 2015; Rass, König and Schauer, 2015) to solve the game. The game yields the three main outputs of the risk minimization step: the first is an optimal attack strategy, i.e., a selection of the identified attack strategies, together with a probability for each strategy to be played. Following these strategies causes the maximum amount of damage to the infrastructure (worst case). The second result is an optimal defense strategy, i.e., a subset of all possible security measures together with a probability for each strategy. Implementing this strategy protects

the infrastructure against the optimal attack strategy. The third result is maximum damage (characterized by the maximum risk level) an adversary can cause, if the optimal attack strategy and the optimal defense strategy are implemented.

6 Discussion

The MITIGATE risk management methodology, as presented in the previous sections, provides a structured approach for maritime information infrastructures to be prepared for today's rapidly changing threat landscape and the associated challenges. Due to the automated integration of publicly accessible information on threats and vulnerabilities, the estimation of potential risks within the infrastructure is updated on a daily basis. Hence, the methodology is able to adapt quickly to novel threats or incidents and deliver an accurate risk assessment.

The collection and processing of alternative information sources (e.g., social media), as sketched in Section 4.3, allows to include also possible future (i.e., currently unknown) vulnerabilities into the risk assessment. Although this is an integrated feature of the MITIGATE methodology, the expert knowledge of a risk officer is still required to evaluate the gathered data. Nevertheless, this marks an additional step towards an adaptive risk management framework suitable for todays' complex and highly dynamic threats.

The application of a game-theoretic approach to identify the optimal mitigation actions represents an additional benefit of the MITIGATE methodology over other methodologies and frameworks in this field. Whereas generally the question which mitigation actions to implement in the end is often left to the risk office, our methodology outputs an optimal set of security measures to be implemented. Moreover, the methodology indicates, how often (i.e., at which frequency) the respective actions have to be carried out.

Nevertheless, the MITIGATE methodology strongly relies on existing information about the infrastructure of an organization. In particular, the information about the setup of the supply chain service and about the involved assets gathered in the first two steps (cf. Section 4.1 and Section 4.2) needs to be as exhaustive and as complete as possible. This information can be taken from network scanning tools, existing documentation or expert knowledge, but is created outside of the methodology. Additionally, the set of available mitigation actions also needs to be as accurate and complete as possible. Only in that case, all scenarios possible

in real life are evaluated in the game and the resulting defense strategy will reflect a realistic setting. In general, the quality of the results heavily depends on the quality of this information serving as input to the methodology.

Over all, the MITIGATE methodology has the ability to increase the security and risk awareness not only within ports or other maritime information infrastructures but also among the various business partners involved in maritime supply chains. In the end, this is a first - and maybe the most important - step to effectively and persistently raise the security level in these organizations.

7 Conclusion

Risk management is a core duty of maritime information infrastructures, in particular when considering the rising number of security incidents all over the world. The MITIGATE methodology represents a supply chain risk management framework going beyond state-of-the-art standards and guidelines. To this end, it integrates an effective, collaborative, standards-based risk management approach, which considers up-to-date information on all threats and vulnerability arising from the supply chain, including threats associated with ports' interdependencies and their potential cascading effects.

Although the MITIGATE methodology integrates several open intelligence sources and thus can quickly adapt to upcoming threats, the results are only as good as the input data. Especially when it comes to the interdependencies between the cyber assets within and among business partner's organizations, expert knowledge is required to model these relations correctly. Additionally, the experts need to identify a level of abstraction when analyzing the cyber assets within their organization since not all cyber assets within the organization will be relevant for the SCS and thus not all of them need to go into the analysis.

The MITIGATE methodology is currently being implemented in a collaborative system (http://mitigate.euprojects.net/) to enable all business partners within a SCS to perform their cyber risk assessment in context of the entire supply chain. By the end of the MITIGATE project, a large number of port operators, maritime stakeholders and security experts will have been engaged in the process of evaluating the capacity of the MITIGATE methodology and system.

Based on this evaluation, future research in this field will examine the question, how collaborative aspects of the methodology can be facilitated and strengthened

as well as how small companies without specific IT related knowledge can be further supported in the security management of their cyber assets.

Acknowledgements

We would like to thank our partners in the MITIGATE project, who also contributed to the development of the MITIGATE methodology, in particular Nineta Polemi,Thanos Karantzias, Christos Douligeris and Evangelos Rekleitis.

Financial Disclosure

This work is supported by the European Commission's Project No. 653212, MITIGATE (Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs) under the Horizon 2020 Framework Programme (H2020-DS-2014-1).

References

Allianz Global Corporate & Specialty SE (2016). *Safety and Shipping Review 2016.*

Allianz Global Corporate & Specialty SE (2017). *Allianz Global Risk Barometer Top Business Risks 2017.*

Baltic, T. and I. M. C. (BIMCO) (2017). *The guidelines on cyber security onboard ships. Version 2.0.*

Bateman, T. (2013). *Police warning after drug traffickers' cyber-attack.*

Cimpanu, C. (2017). *Petya Ransomware Outbreak Originated in Ukraine via Tainted Accounting Software.*

Classification Societies (IACS), I. A. of (2015). *IACS Council 72 Press Release 14 Dec 2015 - IACS.*

(EU), E. U. (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.*

Fox-Brewster, T. (2017). *Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry.*

Hayes, G. (2016). *GPS can be jammed and 'spoofed'–just how vulnerable is it?*

Holland, M. (2017). *Rückkehr von Petya – Kryptotrojaner legt weltweit Firmen und Behörden lahm.*

(IMO), I. M. O. (2016). *Interim guidelines on maritime cyber risk management.*

International Maritime Organization, ed. (2003). *ISPS Code: International Ship and Port Facility Security Code and SOLAS amendments adopted 12 December 2002*. 2003 ed. OCLC: ocm51823054. London: International Maritime Organization.

International Standardization Organization (2007). *ISO 28001: Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance*. English Version. Geneva, Switzerland.
International Standardization Organization (2009). *ISO 31000: Risk Management – Principles and Guidelines*. English Version. Geneva, Switzerland.
International Standardization Organization (2011). *ISO/IEC 27005: Information technology - Security techniques - Information security risk management*. English Version. Geneva, Switzerland.
International Standardization Organization (2013). *ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements*. English Version. Geneva, Switzerland.
Kotchetkova, K. (2015). *Maritime industry is easy meat for cyber criminals.*
Maschler, M., E. Solan, and S. Zamir (2013). *Game Theory*. Cambridge University Press.
Mell, P. and K. Scarfone (2007). *A Complete Guide to the Common Vulnerability Scoring System*.
MPS-ISAO (2017). *Maritime & Port Security ISAO | Operationalizing Cyber Resilience*. 2016.
Oppliger, R. (2015). "Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale". In: *IEEE Security Privacy* 13.6, pp. 18–21.
Port of Rotterdam (2016). *How the Port of Rotterdam is investing in cybersecurity.*
PTI (2017). *New malware hits JNPT operations as APM Terminals hacked globally | The Indian Express*.
Rass, S. (2015). "On Game-Theoretic Risk Management (Part One) – Towards a Theory of Games with Payoffs that are Probability-Distributions". In: *ArXiv e-prints*.
Rass, S., S. König, and S. Schauer (2015). "Uncertainty in Games: Using Probability-Distributions as Payoffs". In: *Decision and Game Theory for Security*. Lecture Notes inComputer Science 9406. London, UK: Springer, pp. 346–357.
Schauer, S., S. König, S. Rass, and M. Latzenhofer (2016). "Spieltheoretische Risikominimierung in IKT Infrastrukturen". In: *DACH Security 2016*. Klagenfurt, Austria: syssec, pp. 174–187.
Scott, L. (2015). *Protecting Position in Critical Operations*.
Standards, N. I. of and T. (NIST) (2017). *National Vulnerability Database (NVD)*.
(US-CERT), U. S. C. E. R. T. (2017a). *Alert (TA17-132A) Indicators Associated With WannaCry Ransomware*.
(US-CERT), U. S. C. E. R. T. (2017b). *Alert (TA17-181A) Petya Ransomware*.
Verizon (2017). *2017 Data Breach Investigations Report.*
Wagstaff, J. (2014). *All at sea: global shipping fleet exposed to hacking threat.*
Wingrove, M. (2017). *Ships are already under cyber attack.*