MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology

S. Schauer, N. Polemi, H. Mouratidis

Abstract. Modern port infrastructures have become highly dependent on the operation of complex, dynamic ICT-based maritime supply chains. This makes them open and vulnerable to the rapidly changing ICT threat landscape and many ports are not yet fully prepared for that. Furthermore, these supply chains represent highly interrelated cyber ecosystem, in which a plethora of distributed ICT systems of various business partners interact with each other. Due to these interrelations, isolated threats and vulnerabilities within a system of a single business partner may propagate and have cascading effects on multiple other systems, thus resulting in a large-scale impact on the whole supply chain. In this context, this article proposes a novel evidence-driven risk assessment methodology, i.e., the MITIGATE methodology, to analyze the risk level of the whole 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. As a major benefit, the methodology provides a constantly updated risk evaluation not only of all cyber assets within each business partner in the supply chain but also of the cyber interconnections among those business partners. Additionally, the whole process is based on qualitative risk scales, which makes the assessment as well as the results more intuitive. The main goal of the MITIGATE methodology is to support the port authorities as well as the risk officers of all involved business partners.

Keywords: Risk Assessment, Supply Chain Services, Critical Information Infrastructures (CIIs)

1 Introduction

Over the last decades, logistics and supply chain services (SCS) have become globally distributed and interconnected. In particular in the maritime sector, there are multiple interdependencies between Critical Information Infrastructures (CIIs) (e.g., transport, energy and telecommunication networks), organizations (e.g., authorities, ministries and companies) as well as people, processes and services. Due to the ongoing digitalization, the business partners involved in these supply chains are depending on a plethora of distributed information and communication technology (ICT) systems. With the goal to increase flexibility and efficiency in the supply chain, these ICT systems have evolved into a highly interrelated cyber ecosystem, where the complexity and degree of networking of connected digital assets is going beyond company borders. Nevertheless, precisely these interconnection points between the ICT

adfa, p. 1, 2011.

systems also represent potential threats since they are possible entry points for unplanned access to a business partner's network and the systems located behind it. Hence, isolated vulnerabilities and related cyber incidents within one business partner may propagate in the overall network of interconnected ICT assets, putting the entire supply chain at risk.

In the last years, the number of cyber incidents has increased, making cyber risks the second highest business risk in Europe [1]. Further, CIIs have moved into the center of cyber terrorists' and activists' attention, who want to deliberately compromise the operation of CIIs and thus destroy their supply chains (at least for a certain amount of time) [6, 12]. Arguably, the number of disclosed cyber incidents in the transportation sector is not very high, yet, and can be considered to be even smaller in maritime supply chains [33]. Nevertheless, there have been several incidents within ports as the center of maritime supply chains [3], but also terminal cranes [31], customs [29], and supporting technology like the GPS systems [10, 34]. Most recent malware attacks like WannCry [4] and (Not)Petya [5, 7] also showed that no business partner involved in a maritime supply chain is immune to being attacked and hacked by malicious third parties. After all, a general awareness for the need of cyber security and cyber risk management has established in the course of these events. Nevertheless, state-of-the-art security frameworks for maritime environments (like [13] or [14]) pay limited attention to cyber-security and do not adequately address security and risk management processes for international maritime supply chains [26].

As the above-mentioned incidents show, attacks are not limited to a single organization any longer due to the highly interconnected and automated nature of modern supply chains. Looking at recent incidents in connection with WannaCry or (Not)Petya, these pieces of malware propagated over the ICT networks of several organizations only due to the high interconnection between these networks [4, 7]. Moreover, although the consequences within an organization might be limited, cascading effects and their impact on connected business partners in the supply chain as well as on society as a whole have become highly relevant. Hence, the processes comprising a supply chain need to be protected from disclosure and exploitation. Unfortunately, the lack of visibility and traceability in the often opaque processes and practices used to develop and acquire ICT related products and services from each actor make this difficult. Consequently, intentional and unintentional compromise may be introduced through a variety of means, including counterfeit materials and malicious software, and might not be detect and remediate appropriately. Hence, there is a clear need for targeting sophisticated global risk assessment frameworks to deal with the threats, vulnerabilities and risks as well as their cascading effects associated with the ICT-based logistics and related supply chains.

In this context, the present article introduces a rigorous, rational approach to risk management, which will produce high quality scientific and experimental based proofs and findings, including simulation results, indicators and recommendations in order to assist supply chain operators to evaluate and mitigate the risks they are faced with. The paper presents a novel integrated collaborative supply chain risk assessment methodology, which enables the involved supply chain business partners to collabo-

rate in the identification and classification of the various risks, while at the same time facilitating them in risk resolution and the creation of related supply chain plans.

The remainder of this article is structured as follows: in Section 2 we give an overview on supply chain risk management together with relevant standards and research work done on this topic. Section 3 presents the MITIGATE Methodology in detail, whereas the respective subsections describe each step of the methodology individually. A discussion on the strengths and weaknesses of the methodology as well as it applicability is provided in Section **Error! Reference source not found.**; Section 4 concludes the work.

2 Supply Chain Risk Management

2.1 Standards and Guidelines

A structured and integrated risk management process has become a central part of the daily business of organizations in various sectors. Hence, several standards, and frameworks have been formulated, for example, ISO 31000 [17], ISO/IEC 27005 [20], NIST SP800-30 [32], Cobit 5 for Risk [21] or others (cf. [8] for an extensive overview of risk management approaches). They provide methodologies and guidelines for businesses to implement such a risk management process. The traditional goal is to protect the business assets of an organization and minimize costs in case of failures and thus it represents a core duty of successful company management. As a major drawback, all the above mentioned standards and frameworks are designed to work *within* organizations, i.e., looking at their individual risk and how to tackle them.

However, risk management is also essential in the provision of logistics and supply chain services. Instead of the individual risks, the connections and interdependencies between the various business partners are of central importance when assessing risks and their impacts. In this context, a plethora of assets from various organizations interact and need to be protected from threats which might have an impact on the whole supply chain. To generate a supply chain security policy ensuring the secure operation of any logistic network or the secure provision of any supply chain service, the estimation of risks and the development of appropriate protective measures for all (cross-partner) assets involved in the supply chain are required.

Among international standards, the ISO 28000 [15] and ISO 28001 [16] deal with the specification and guidelines for a supply chain risk management. In further detail, the ISO 28000 specifies a management system, which has been developed and introduced in response to a demand from the transportation and logistics industry. The goal is a common security management standard, with the ultimate objective of improving the overall security of supply chains. The ISO 28001 focuses more on the practical implementation of such management system. The main goal is to assist organizations in establishing reasonable levels of security and make better risk-based decisions for protection of the supply chain. Both the ISO 28000 and ISO 28001 are

kept quite generic with the intention to be applicable to various sectors. Hence, they have to be tailored to fit to the context of maritime supply chains.

Since both standards do not particularly consider ICT and information security, they are not very practical as a standalone framework for supply chains heavily based on the interaction of ICT systems (as, for example, in the maritime sector). For this purpose the ISO/IEC 27001 [18] and ISO/IEC 270002 [19] have been established. They are specifying the requirements for an information security management system (ISMS), i.e., in the ISO/IEC 27001, as well as a code of practice (in the ISO/IEC 27002) providing details on how to implement such an ISMS within an organization. Risk management aspects in the context of information (and ICT) security are not covered by these two standards but rather by the additional ISO/IEC 27005 [20]. Hence, an organization within a maritime supply chain would have to implement aspects from both standards, ISO 28001 and ISO/IEC 27005, to come up with an appropriate supply chain risk management method.

Besides the international standards, other methodologies have been developed, which are inspecting the high interdependencies between critical infrastructures in general. A first analysis approach for the interdependencies between critical infrastructures is given in [30], describing several classes of interdependencies. Building on this classification, other approaches looked in further detail into the analysis of the interdependencies [2, 9, 28]. When it comes to analyzing the risk within the whole network of critical infrastructures, the cascading effects stemming directly from these interdependencies are an important factor. Identifying and assessing them is crucial and several methodologies have been presented in the past years [35, 11, 24, 22, 23]. These methodologies are applicable also for the analysis of cascading effects in maritime supply chains, since the interdependencies are the same as in the context of general critical infrastructures.

It has to be noted that the objectives of the above mentioned standards are not intended to constitute a risk management method. Rather, these standards aim to establish a comprehensive framework and to describe requirements for the risk assessment process, for the identification of the threats and vulnerabilities allowing to estimate the risks in advance, their level and finally to define an effective treatment plan. Further, the generic nature of these standards does not include the ability for the individual users (or business partners) to collaborate in the risk management process.

2.2 Research Projects

Although efforts have been made to standardize supply chain security risk assessment as mentioned above, there is a lack of targeted methodologies. The already completed project S-PORT[1] took a first step towards a collaborative system for risk assessment and security management for maritime environments. However, the S-PORT methodology [26] focused on the internal security processes of a port, ignoring dimensions

[1] http://s-port.unipi.gr/

relating to the supply chain and the business partners therein. The main idea of the S-PORT project has been extended in the project CYSM[2], which implemented risk management methodology that relies on collaborative modeling and group decision making techniques using the collective knowledge of all users [25]. This methodology integrates aspects of the International Ship and Port Facility Security (ISPS) Code [13] as well as the ISO 27001 [18] and thus allows estimating physical and cyber risks across diverse target types, attack modes, and geographic levels.

Recently, the MEDUSA project[3] developed a novel supply chain risk assessment methodology compliant with ISO28001 [16], ISO27001 [18] and the ISPS Code [13]. The MEDUSA methodology [27] concentrates on the business needs and requirements of the maritime supply chains and can be applied to assess the risks of a specific SCS. The derived overall risk values are used to generate a baseline supply chain security policy, identifying the least necessary security controls for each participant in the supply chain. In addition, the MEDUSA methodology assesses the risk of cascading threat scenarios within a supply chain. This enables the business partners in the supply chain to adapt their security policies according to their business role as well as their dependencies. Furthermore, a practical MEDUSA tool[4] has been developed that implements the methodology enabling port operators and supply chain business partners to conduct risk assessments of the SC services that are involved in each of their domain.

The current CORE project[5] aims to develop an innovative approach to design global supply chains, which are resilient (in real-time) to major disturbances caused by high impact events. The main idea behind the CORE project is to discover gaps and practical problems in the global supply chain and to develop capabilities and solutions to identify these problems. The focus lies on the interoperability between the business partners involved in the supply chain to counter incidents with the potential to disrupt the supply chain in real-time. However, CORE does not plan to provide a concrete risk assessment methodology for the global supply chain.

Finally, the ongoing project MITIGATE[6] aims to realize a radical shift in supply chain risk management methodologies towards a collaborative, evidence-driven approach, i.e., the MITIGATE methodology presented here, that alleviates the limitations of state-of-the-art risk management frameworks. In the course of the project, a collaborative risk management system[7] is integrated and validated in maritime use case scenarios. The system is parametrized for ports' SCS and the individual business partners will be able to analyze all threats arising from their supply chain cyber assets, including threats associated with port CIIs interdependencies and associated cascading effects.

---

[2] http://www.cysm.eu
[3] http://medusa.cs.unipi.gr
[4] http://medusascsra.cs.unipi.gr
[5] http://www.coreproject.eu
[6] http://www.mitigateproject.eu
[7] http://mitigate.euprojects.net

3 MITIGATE SCRA Methodology

A core result of the MITIGATE project is the MITIGATE supply chain risk assessment (SCRA) methodology. The methodology is compliant with ISO 28001 [16], ISO 27005 [20] as well as ISO 31000 [17] and aims at estimating the cyber risks for all assets of all business partners involved in a maritime SCS. Further, a special focus is laid on the cascading effects in multi-sector environments and in the provision of support for security processes associated with the dynamic, ICT-based supply chains. Therefore, the MITIGATE methodology includes technical, policy-compliant, techno-economic and usability perspectives into the risk assessment process thus taking the viewpoints of a variety of stakeholders into account.

In more detail, information on the interaction between various cyber assets (i.e., the cross-partner's cyber assets) from the different business partners is required and stored in a graph representation. Using specific propagation rules depending on the characteristics of each asset, attack paths are identified within the graph. During the analysis of these paths, three novel concepts are defined in the MITIGATE methodology: the concepts of individual, cumulative and propagated vulnerabilities, impacts and risks. Based on these concepts, the cascading effects within the overall graph of assets can be estimated by looking at the possible paths in the graph an adversary can take to reach a specific asset, thus representing the cumulative aspects, and the possible paths the adversary can take starting from a specific asset, thus representing the propagated aspects (cf. Sections 3.3, 3.4 and 3.5 for details). Based on the results of these analyses, a set of optimal mitigation actions is identified using a game-theoretic approach.

Overall, the main outputs of the MITIGATE SCRA methodology are:

- a list of all cyber assets within a SCS together with a corresponding graphical representation
- a list of all potential attack paths based on specific propagation rules considering various attackers' profiles
- an estimation on the existence of zero-day exploitable vulnerabilities
- an evaluation of the individual, cumulative and propagated vulnerabilities, impacts as well as risks of all assets
- an optimal mitigation strategy based on the given set of possible defensive measures

The MITIGATE SCRA methodology can be triggered by any partner within the SCS and consists of six main steps (cf. FIG), which represent the recurring main steps given in the standard risk management frameworks mentioned above. The realization of each block contains several sub-steps (Si.j) as presented in Fig . In the following sections, the main steps of the methodology are described in further detail.

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 six steps of the MITIGATE methodology

3.1 Step 1: SCS Analysis

In this first step, the SCS under examination is decomposed. The actors of this step are the risk assessors that initiate the assessment in consensus with the business partners (based upon the SLA and the signed ESD). They define the scope of the risk assessment in consensus with the other business partners, fixing also the goals and the desired outcome of the risk assessment. Further, the business partners involved in the SCS under examination are identified, who themselves identify the participants of the SCS involved from their perspective, and so forth.

After all participants of the risk assessment are identified, the main cyber and/or physical processes (i.e., controlled/monitored by a cyber system) that comprise the examined SCS have to be collected. To achieve that, all cyber assets required for the provision of the examined SCS and its respective business process are reported. The interdependencies between these cyber assets are of particular interest for the risk assessment and thus the interdependencies are characterized using several types (e.g. hosting, exchanging data/information, storing, controlling, processing, accessing, installing).

3.2 Step 2: SCS Cyber Threat Analysis

All threats related to the SCS cyber assets reported in the previous step are identified and evaluated in terms of their likelihood of occurrence. In more detail, all individual cyber threats against all of the SCS cyber assets are collected and stored. To compile an exhaustive threat list, the MITIGATE methodology foresees the integration of multiple source of information, i.e., online threat repositories like the National Vulnerability Database (NVD), crowd sourcing and social media as well as the business partners' experts. By taking all these data sources into account, this approach helps to increase the quality of the whole risk assessment supports.

After the threats are identified, the likelihood of occurrence is estimated for each of them. Also for this step, several different sources of information are used: information from online repositories and social media is taken into consideration as well as historical data and expert opinions. Again, this helps to obtain a more realistic estimation of the likelihood compared to taking only one of these sources. This likelihood is 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.

3.3 Step 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 this context, vulnerabilities can be induced through poor configuration, lack of security patching, etc. The MITIGATE methodology differences between two main types of vulnerabilities: confirmed vulnerabilities and potentially unknown (zero-day) 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, vulnerabilities which exist in software systems but are not publicly known are referred to as zero-day vulnerabilities.

Such zero-day vulnerabilities are more dangerous since security experts are not aware of them but they can be (easily) exploited by adversaries. Hence, it is important to model such unknown and/or undisclosed vulnerabilities in order to gain a pragmatic view of the SC's risk exposure. To estimate the existence of zero-day vulnerabilities, crowd sourcing and publicly available information on the security of a particular system is used. In this way, the estimation can be done 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).

Confirmed and zero-day vulnerabilities are characterized using specific data coming from the Common Vulnerability Scoring System (CVSS), e.g., Access Vector, Access Complexity, Authentication, Threat & Vulnerability Categories, Exploitability, etc. This data is used to compute the Individual, Cumulative and Propagated Vulnerability Level as described in the following three sub-sections.

Individual Vulnerability Level.

This step aims at estimating the severity of all (confirmed and zero-day) vulnerabilities. In this way, we estimate the likelihood of successfully exploiting each vulnerability when all the prerequisite conditions required are met. In the MITIGATE methodology, we rely on qualitative values for representing the Individual Vulnerability Level (IVL) and use a five-tier scale ranging from "Very Low" (VL) to "Very High" (VH).

To calculate the Individual Vulnerability Level (IVL) of a specific vulnerability, we use parts of the CVSS metrics (i.e., the Access Vector (AV), the Access Complexity (AC) and the Authentication (Auth)) retrieved from the online databases. The detailed mapping from the CVSS metrics onto one category of the five-tier scale is presented in the following Table 1.

Table 1. Mapping of the CVSS metrics on the Individual Vulnerability Level (IVL)

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

Cumulative Vulnerability Level

The key limitation of the Individual Vulnerabilities Level produced in the previous step is that the IVL represents the likelihood that the corresponding vulnerability is successfully exploited when exposed to an attacker without considering the individual actions that the attacker has to perform to satisfy the preconditions required for their exploitation [20], [21].

Thus, the goal of the Cumulative Vulnerability Level (CVL) is to accurately reflect the exploitation level of the vulnerabilities by taking into consideration the IVL, the context within which these vulnerabilities appear (e.g. the assets interdependencies/interconnections) and the attacker's profiles.

Thus, the CVL measures the likelihood that an attacker can successfully reach and exploit a vulnerability, given a specific vulnerability chain. Such a chain describes the list of sequential vulnerabilities on different assets that arise from consequential multi-steps attacks). Each vulnerability chain has one entry point, i.e., a certain vulnerability of a specific asset an adversary uses to break into the system, and one target point, i.e., a specific vulnerability on (another) asset an adversary finally wants to exploit. In general, several other vulnerabilities on other assets can exist between the entry point and the target point, connecting the entry point and the target point based on the interdependencies between them.

Starting from the entry point, an adversary has to exploit one vulnerability after the other to reach the target point. His success is determined by his relationship to the organization (insider or outsider), his skills (ICT skilled or pre-mature) and his target. These attributes of the adversary have to be estimated by the risk assessor beforehand. To identify how the vulnerabilities are connected and whether an adversary can hop from one vulnerability to another, we use a set of rules to decide whether an asset can be compromised to be used as an intermediate step to induce further attacks. In detail, in order to deduce:

- the accessibility of a vulnerability, we use two metric: (a) the Vulnerability Access vector's attribute that shows how a vulnerability can be exploited, and (b) the Dependency Access vector's attribute that shows how the assets are connected;
- the complexity degree of a vulnerability, we consider the attackers' profiles i.e., the skills and characteristics the user grants the attacker and the Vulnerability Access complexity attribute;
- whether an asset can be used as a stepping stone to launch further attacks on other assets, we take into account the technical effects and impact of the vulnerability;
- the exploitability of a vulnerability, we take into consideration whether there is an known exploitation technique for the vulnerability.

From the resulting vulnerability chains not all are equally probable and some can be excluded from the calculation of the CVL by the business partners. For each of the remaining chains, the Individual Chain Vulnerability Level (ICVL) can be computed, indicating the vulnerability level of this chain. First, this computation is based on the IVL of a vulnerability and the adversary's capabilities (also measured on a five-tier scale). For each vulnerability involved, these two categories are combined as described in the mapping given in Table 2.

Table 2. Mapping of the Attacker's Capability and the IVL onto the likelihood of exploitation

Capability / IVL	**Very Low**	**Low**	**Moderate**	**High**	**Very High**
Very Low	VL	VL	L	L	M
Low	VL	L	M	M	H
Moderate	L	M	M	M	H
High	L	M	M	H	VH
Very High	M	H	H	VH	VH

For the non-trivial case that the vulnerability chain is of length 2 or higher, the computation of the ICVL has to take all the IVLs (adapted according to the attacker's capability) into account. Therefore, the IVLs have to be "multiplied" or "concatenated" in a specific way such that in the end, the result is again a vulnera-bility level between VL and VH. Therefore, we define a "multiplication" operation "×" to describe how two vulnerability levels are mapped onto a new level (cf. Table 3). Using this operation, the overall vulnerability of the attack chain can be computed from the different IVLs along the chain by pairwise multiplying the IVLs, starting from the entry point.

Table 3. Description of the "multiplication" operation × for two vulnerability levels

×	**Very Low**	**Low**	**Moderate**	**High**	**Very High**

Very Low	VL	VL	L	L	M
Low	VL	L	M	M	H
Moderate	L	M	M	M	H
High	L	M	M	H	VH
Very High	M	H	H	VH	VH

The CVL has to take the ICVLs for all possible chains leading from the entry point to the target point into account. To prevent losing some of the information, the ICVLs are not aggregated into one value (as it is done in many other methodologies using, for example, the maximum approach). In fact, the CVL consists of all the information coming from the ICVLs, which are integrated into a histogram. In this way, the CVL can be easily represented and also be easily processed in the next steps of the methodology.

Propagated Vulnerability Level.

Whereas the CVL focuses on all possible attack chains concluding into the same target point, the Propagated Vulnerability Level (PVL) inspects the likelihood that an attacker can penetrate a network up to some specific depth. In other words, the PVL takes all possible vulnerability chains of a specific length into account, starting from one particular entry point. Similarly to the CVL, the individual vulnerability chains are used for the computation of the PVL. However, the main difference is that the length of each chain is limited to a maximum value l, predefined by the business partners.

To compute the PVL for a specific entry point, all possible vulnerability chains up to length l are identified and their respective ICVL is computed. Therefore, we follow the same approach as already described for the CVL above. In detail, we use the mapping in Table 2 to adapt the IVLs of the identified chains according to the adversary's capabilities and then use the mapping in Table 3 to get to the ICVL of the respective vulnerability chain. Similar to the CVL, the PVL consists of the ICVLs of all the vulnerability chains and is represented by a histogram. This histogram can then be used in the next steps of the methodology.

3.4 Step 4: Impact Analysis

Individual Impact Level

Based on the vulnerability analysis done in the previous step, we are also looking at the potential impact exploiting these vulnerabilities might have. To stay consistent with the vulnerability analysis, for categorizing the impact we also rely on qualitative values ranging from "Very Low" (VL) to "Very High" (VH) to describe the Individual Impact Level (IIL). To calculate the IIL cause by a specific vulnerability, we also use information coming from the CVSS metrics (i.e., the three security criteria Confidentiality (C), Integrity (I) and Availability (A)) retrieved from the online databases.

The detailed mapping from the CVSS metrics onto one category of the five-tier scale is presented in Table 4 and provides a single estimation for the overall impact of a specific asset/vulnerability combination.

Table 4. Mapping of the CVSS metrics on the Individual Impact Level (IIL)

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

Cumulative Impact Level.

Accordingly to the definition of the CVL, the Cumulative Impact Level (CIL) is defined as the impact that occurs after a specific asset-/vulnerability-combination has been exploited by an attacker using any possible entry point (cf. the Cumulative Vulnerability Level in Step 3.4). IN other words, the CIL reflects upon the effects of the successful exploitation of a vulnerability at the target point. Similarly to the CVL, also the CIL depends on all vulnerability chains originated from all possible entry points and leading to the target point. To assess the impact level of a specific vulnerability chain, i.e., the Individual Chain Impact Level (ICIL), the ICVL together with the IIL is used. As specified above, the ICVL indicates the likelihood that an adversary (with some predefined capabilities) is able to exploit a specific vulnerability chain and the IIL indicates the impact (or damage) the adversary can cause by doing that. Table 5 shows how the ICVL and the IIL are combined to map onto the ICIL.

Table 5. Mapping of the Impact level and the ICVL onto the Individual Chain Impact Level

Impact Level / ICVL	Very Low	Low	Moderate	High	Very High
Very Low	VL	VL	L	L	M
Low	VL	L	M	M	H
Moderate	L	M	M	M	H
High	L	M	M	H	VH
Very High	M	H	H	VH	VH

Analogously to the CVL, the CIL consists of the ICILs for all possible paths from the entry point to the target point compiled into a single histogram.

Propagated Impact Level

The Propagated Impact Level (PIL) is defined as the overall impact that occurs when an adversary exploits a specific asset/vulnerability combination and further penetrates the network up to a specific depth starting from this entry point (similarly to the PVL defined in step XXX above). In other words, this relates to the damage an attack can cause at any asset/vulnerability combination on his way through the network. The computation of the PIL runs accordingly to the computation of the PVL, i.e., ICILs of a predefined length l are used (described by the mapping of ICVL and IIL given in Table 5) and then compiled into a histogram to preserve all the collected information. Note that the PIL includes the impact of each vulnerability that lies on any possible path the adversary can take in the network. Hence, not only the ICVLs of length l, but also shorter ICVLs have to be taken into account.

3.5 Step 5: Risk Assessment

To estimate the risk level, the vulnerability level as well as the impact level has to be taken into account. Additionally, the risk level is specified for individually for each threat, hence also the threat level needs to be included in the estimation. In the following, we will describe how this is done for each of the three risk levels (Individual, Cumulative and Propagated).

Individual Risk Level.

The computation of the Individual Risk Level (IRL) is rather straight forward, taking the IVL and the IIL already defined in Sections 3.3 and 3.4 above and combining it with the Threat Level (TL). This combination can be done using the "multiplication" operation "×" given in Table 3. Therefore, we end up with the simple formula

$$IRL = TL \times IVL \times IIL \tag{1}$$

As a result, we obtain a risk level according to the five-tier scale (i.e., running from VL to VH) for each asset/vulnerability combination.

Cumulative Risk Level.

Looking at the Cumulative Risk Level (CRL), the computation becomes a little more complex. As a basic principle, we can use the approach from the IRL above and combine the TL, the CVL and the CIL to obtain the CRL. However, we have to take into account that the CIL already consists of a combination of the ICVL and the IIL (cf. Section 3.4 above). Hence, it is fully sufficient to combine only the TL and the CIL to obtain the CRL

$$CRL = TL \times CIL = TL \times \bigcup ICIL = \bigcup TL \times ICIL \tag{2}$$

Note that the CIL is a collection of all the ICILs represented as a histogram. Hence, the above formula means that the TL has to be "multiplied" with each ICIL, separately. Accordingly, the CRL is again represented as a histogram.

Propagated Risk Level

For the computation of the Propagated Risk Level (PRL) we also have to be aware that the PIL is already based on the ICVL and thus the PVL does not need to be included. Hence, only the TL and the PIL are included in the computation and we have the formula

$$PRL = TL \times PIL = TL \times \bigcup ICIL = \bigcup TL \times ICIL \quad (3)$$

Also with regards to the PRL we have to note that the PIL is a collection of multiple ICILs and thus in the above formula each of these ICILs has to be "multiplied" with the TL. Consequently, the PRL can also be represented as a histogram.

3.6 Step 6: Risk Mitigation

In this step, the risk assessment values are compared against specific criteria (set and agreed by all business partners), in order to select additional security controls required by the business partners and by the SCS (as a whole) meeting these thresholds. For the selection of the optimal security controls a game theoretic approach is applied, based on a mathematically sound method to find a way to minimize the expected damage due to an attack that exploits multiple vulnerabilities.

We set up a game to optimize the actions of a business partner to minimize the expected damage. In order to do this formally, we need to describe the actions of both the attacker and the defender as well as to assign payoffs for each combination of strategies (as described in more detail below). Playing the game then yields an optimal solution in the sense that it indicates which countermeasures should be chosen to minimize the damage.

Attack and Defense Strategies

The strategies of the adversary are directly linked to the assets he wants to infiltrate and accordingly to the vulnerabilities he has to exploit to achieve that. To model the attack strategies, we are relying on the information already collected and computed in the previous steps. In more detail, the strategies of an adversary are characterized by the vulnerability chains he is able to use (i.e., the paths through the network he is able to take) to attack a specific vulnerability, i.e., the target node (these chains have been identified in Section 3.3 above).

The strategies of the defender are the available actions and measures he can take in order to protect his assets. Besides the potential countermeasures a business partner knows from past experiences, vulnerability analysis tools may provide further strategies to mitigate vulnerabilities. For example, a defense strategy could be to do spot checking or patching of a specific asset (i.e., closing a specific vulnerability).

Payoff Estimation for each Scenario

Each combination of an attack and a defense strategy defines a scenario. In order to find an optimal solution, it must be possible to compare the impacts (payoffs) for different scenarios. In our context, these payoffs are described by the damage that

occurs to the business partner and are represented by the IIL, CIL or PIL, respectively (cf. Section 3.4 above).

When modelling one strategy of the attacker, i.e., by choosing a target node and the respective vulnerability chains leading to this target, the payoff is the amount of damage he can cause at that particular node. This damage is described by the impact of exploiting a specific vulnerability at a particular asset. Since we want to capture all possible ways the adversary could exploit that vulnerability, this directly links to the CIL. If we were focusing on the total damage an attacker causes inside the network, this would correspond to different attack strategies and, accordingly, to the PIL.

The strategies of the defender are described as changes to the overall structure of the network. In detail, a security strategy is able to close a vulnerability, hence eliminating specific vulnerability chains, or to improve the security of some assets, hence lowering the likelihood of a successful exploitation be the attacker. To model the effect of a defense strategy against a specific attack strategy, the CIL needs to be reevaluated based on the new setting.

Outcome of the Game-Theoretic Approach

Once all attack and defense strategies are identified and the corresponding payoffs for each combination are determined, they are filled into the game matrix. This matrix represents the main input to the game-theoretic algorithm, which yields an optimal way of choosing the actions of both attacker and defender based on the payoffs given in this matrix. This equilibrium yields two piece of information:

1. An optimal attack strategy. This is a selection of the identified attack strategies, together with a probability for each strategy, which an adversary would follow to cause maximum damage to the infrastructure. This represents the worst case scenario for the defender.
2. An optimal defense strategy. This is a selection of the available defense strategies (counter measures), together with a probability for each strategy, which a security officer should implement to have the best protection against the worst case attack strategy.
3. A maximum risk level, i.e., the maximum damage that can be caused by an adversary following the optimal attack strategy and a defender following the optimal security strategy.

The security measures defined in item 2 are the optimal mitigation actions the security office can take to be prepared for the worst case scenario. If the security officer does not implement these actions accordingly, the adversary will be able to cause more damage than given in item 3. Correspondingly, if the adversary deviates from the optimal attack strategy given in item 1, he will cause less damage to the infrastructure and thus end up in a worse situation for him.

3.7 Operational Context and Assumptions

Since the scope of the MITIGATE methodology covers different areas within various SCS providers, several assumptions have to be made. These assumptions are in place to support the development of a methodology that can be used in real life (rather than a purely theoretical methodology). In particular, the MITIGATE SCRA methodology is designed to operate on asset level, which means that the specific assets and implemented controls of each business partner involved in the SCS are necessary inputs to the methodology. To ensure the privacy and protection of this data, the partners are asked to provide an Enhanced Security Declaration (ESD), which is a confidential, legally binding document included in the SCS SLA. The ESD reveals the commitment of the partners to identify all of their organizations' cyber assets which are relevant for the implementation of the SCS together with the controls already in place. The ESD is based on the Security Declaration given in the ISO 28001 and, since the MITIGATE methodology is compliant with the ISO 28001, it can be understood as a basic requirement for the methodology.

On the other hand, we advocate that the interconnection between the cross-partner's cyber assets can be represented by directed linear paths. In this context, the interdependencies are acyclic to omit circular attack paths during the analysis. Second, we postulate that the cross-partners' cyber assets are used only for the provision or delivery of the SCS and are isolated from the partners' individual ICT infrastructure. Third, it is also assumed that every SCS is accompanied by a Service Level Agreement (SLA) which includes the standard aspects of the SCS (scope, quality, responsibilities between the service providers and the service users). It is also worth mentioning that MITIGATE SCRA only considers cyber threats and we only consider independent attacks and not cyclic attacks (since the SCSs under consideration are represented by one way directed graphs). In that context, we assume the three main threat categories (loss of confidentiality/integrity/availability) map to specific vulnerability categories and we consider that security controls are either implemented or not (we omit levels of implementation). For operational purposes, we make use of the open NIST national vulnerability repository, although one may use any other repository.

It is worth noting that we consider some of the above operational assumptions foundational for the correct operation of the MITIGATE methodology (e.g. ESD), while others as important for the current version of the methodology with a view to further extend in the near future (e.g. levels of implementation).

4 Conclusion

Although there is a plethora of cyber security and supply chain security standards and conventions (e.g., ISO27001, ISO27005, NIST Framework, ISO28000, ISO28001, ISPS) the literature does not provide clear evidence of practical Supply Chain Risk Assessment methodologies that business partners in a logistic chain can comprehensively apply manage its risks and their cascading effects.

In this paper we have presented an overview of the MITIGATE methodology, which aims to contribute to the effective protection of the ICT-based supply chain. Curently, we are implementing the MITIGATE methodology to a collaborative tool that will automate its stages and will enable all business partners within a SCS to perform their SCRA. It will be localized in the maritime sector so maritime stakeholders can test its functionality and performance.

Acknowledgement

This work has received funding from The European Union's Horizon 2020 research and innovation program under grant agreement No 653212.

References

1. Allianz Global Corporate & Specialty SE: Allianz Global Risk Barometer Top Business Risks 2017., http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2017_EN.pdf , (2017).
2. Aung, Z.Z., Watanabe, K.: A Framework for Modeling Interdependencies in Japan's Critical Infrastructures. In: Critical Infrastructure Protection III. pp. 243–257 Springer, Berlin, Heidelberg (2009).
3. Bateman, T.: Police warning after drug traffickers' cyber-attack., www.bbc.com/news/world-europe-24539417.
4. Bill, B.: WannaCry: the ransomware worm that didn't arrive on a phishing hook. Sophos Ltd (2017).
5. Cimpanu, C.: Petya Ransomware Outbreak Originated in Ukraine via Tainted Accounting Software, https://www.bleepingcomputer.com/news/security/petya-ransomware-outbreak-originated-in-ukraine-via-tainted-accounting-software/.
6. E-ISAC: Analysis of the Cyber Attack on the Ukrainian Power Grid. , Washington, USA (2016).
7. Fox-Brewster, T.: Petya Or NotPetya: Why The Latest Ransomware Is Deadlier Than WannaCry, http://www.forbes.com/sites/thomasbrewster/2017/06/27/petya-notpetya-ransomware-is-more-powerful-than-wannacry/.
8. Giannopoulos, G. et al.: Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art. Publications Office of the European Union, Luxembourg, Luxembourg (2012).
9. Haimes, Y. et al.: Risk Analysis in Interdependent Infrastructures. In: Critical Infrastructure Protection. pp. 297–310 Springer, Boston, MA (2007).
10. Hayes, G.: GPS can be jammed and 'spoofed'--just how vulnerable is it?, https://www.marineelectronicsjournal.com/content/newsm/news.asp?show=view&ac=1&a=128.
11. Hokstad, P. et al. eds: Risk and Interdependencies in Critical Infrastructures. Springer London, London (2012).

12. ICS-CERT: Cyber-Attack Against Ukrainian Critical Infrastructure, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.
13. International Maritime Organization ed: ISPS Code: International Ship and Port Facility Security Code and SOLAS amendments adopted 12 December 2002. International Maritime Organization, London (2003).
14. International Standardization Organization: ISO 20858: Ships and marine technology - Maritime port facility security assessments and security plan development. , Geneva, Switzerland (2007).
15. International Standardization Organization: ISO 28000: Security management systems for the supply chain. , Geneva, Switzerland (2007).
16. International Standardization Organization: ISO 28001: Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance. , Geneva, Switzerland (2007).
17. International Standardization Organization: ISO 31000: Risk Management – Principles and Guidelines. , Geneva, Switzerland (2009).
18. International Standardization Organization: ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements. , Geneva, Switzerland (2013).
19. International Standardization Organization: ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security controls. , Geneva, Switzerland (2013).
20. International Standardization Organization: ISO/IEC 27005: Information technology - Security techniques - Information security risk management. , Geneva, Switzerland (2011).
21. ISACA: COBIT 5 for Risk. , Rolling Meadows, USA (2013).
22. König, S. et al.: A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks. In: Brumley, B. and Röning, J. (eds.) Secure IT Systems. 21st Nordic Conference, NordSec 2016, Oulu, Finland, November 2-4, 2016. Proceedings. pp. 67–81 Springer International Publishing, Cham (2016).
23. König, S. et al.: Risk Propagation Analysis and Visualization using Percolation Theory. Int. J. Adv. Comput. Sci. Appl. 7, 1, 694–701 (2016).
24. Kotzanikolaou, P. et al.: Assessing n-order dependencies between critical infrastructures. Int. J. Crit. Infrastruct. 9, 1–2, 93–110 (2013).
25. Papastergiou, S. et al.: CYSM: An Innovative Physical/Cyber Security Management System for Ports. In: Human Aspects of Information Security, Privacy, and Trust. pp. 219–230 Springer, Cham (2015).
26. Polemi, D. et al.: S-Port: Collaborative security management of Port Information systems. In: IISA 2013. pp. 1–6 (2013).
27. Polemi, N., Kotzanikolaou, P.: Medusa: A Supply Chain Risk Assessment Methodology. In: Cyber Security and Privacy. pp. 79–90 Springer, Cham (2015).
28. Porcellinis, S.D. et al.: A Holistic-Reductionistic Approach for Modeling Interdependencies. In: Critical Infrastructure Protection III. pp. 215–227 Springer, Berlin, Heidelberg (2009).

29. Port of Rotterdam: How the Port of Rotterdam is investing in cybersecurity., https://www.portofrotterdam.com/en/news-and-press-releases/how-the-port-of-rotterdam-is-investing-in-cybersecurity.
30. Rinaldi, S.M. et al.: Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. 21, 6, 11–25 (2001).
31. Scott, L.: Protecting Position in Critical Operations, http://gpsworld.com/protecting-position-in-critical-operations/.
32. Stoneburner, G. et al.: NIST SP800-30 Risk Management Guide for Information Technology Systems. , Gaithersburg, USA (2002).
33. Verizon: 2017 Data Breach Investigations Report., http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf, (2017).
34. Wagstaff, J.: All at sea: global shipping fleet exposed to hacking threat., http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424.
35. Zio, E., Sansavini, G.: Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins. IEEE Trans. Reliab. 60, 1, 94–101 (2011).