MITIGATE

NEWSLETTER 02

November 2016

Multidimensional, integrated, risk assessment framework and dynamic, collaborative Risk Management tools for critical information infrastructure

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

MITIGATE DEVELOPMENT REPORT

MILESTONE REACHED

In November 2016, the MITIGATE project is entering the second half of its project duration of 30 months in total. This is a good time to look back, see what has been achieved and look into the future to plan what still has to be done.

Two of eight work packages are already completed: First of all, the requirements and technical specifications of the MITIGATE software are defined. Stakeholder and operational requirements are investigated. The software's mathematical basis, the risk assessment methodology, is developed and the software architecture is designed.

SUCCESS IN SOFTWARE DEVELOPMENT

During the last project steering committee meeting, the MITIGATE software was demonstrated. The European Commission stated in their official project review, that the "project has fully achieved its objectives and milestones for the period."

Current goals encompass the selection of evaluation criteria and the development of the evaluation approach for the software. Pilot user events for software testing and, of course, further development of the MITIGATE software rank high on the agenda.

MITIGATE presented at Posidonia 2016 in Athens (left) and SMM 2016 in Hamburg (right).

MITIGATE events REVIEW

During the first year of work in the MITIGATE project, the project consortium has already had a whole variety of opportunities to present and explain MITIGATE due to the importance of cyber security. Visitors originated from academia and research as well as from administration and maritime industry.

The partners introduced the project to academics at workshops of other EU-funded projects, such as HyRim and MEDUSA. Partners took the possibility to speak in fora like the NMIOTC Cyber Security Conference in September and at several international maritime conferences such as Digital Ship, TOC, SMM and Posidonia. MITIGATE was illustrated not only in the exhibition, but also in a separate workshop.

For the next possibilities to meet MITIGATE project partners have a look at the last page!

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

THE MITIGATE METHODOLOGY FOR RISK ASSESSMENT

A RADICAL SHIFT IN THE MARITIME SECTOR

The IT infrastructure of the maritime supply chain, and especially ports, is particularly vulnerable, because it is located at the intersection of information flows from many different users and countries, which on account of the continuously increasing digitization of business processes have to offer access and exchange capabilities for digital information. In order to ensure that these processes do not allow malware to shut down operations or allow manipulation of data for illegal purposes, a solution for identifying threats along the maritime supply chain is urgently needed.

The main goal of MITIGATE is the development of a cloud-based platform for the discovery of security gaps in the employed hardware and software. This software is based on a thorough analysis of user requirements, actual real-time threats and potential countermeasures. The open simulation environment enables the participating companies to collaborate on spotting and analyzing risk scenarios. This enables the parties to predict and avoid security risks in the most cost-effective manner.

SIX COMPONENTS OF RISK ASSESMENT

MITIGATE will comprise simulation models, which will enable the production of timely, accurate, objective, reliable, relevant and high quality evidence, information, indicators and factors. The latter will empower a first-of-a-kind analysis and assessment of multi-dimensional risks, which is not possible nowadays.

The risk assessment itself follows a methodology that consists of six components:

In the **Boundary Setting**, scope and objectives of the supply chain risk assessment are defined. Therefore, single supply chain services with the adjoining processes and business partners have to be described.

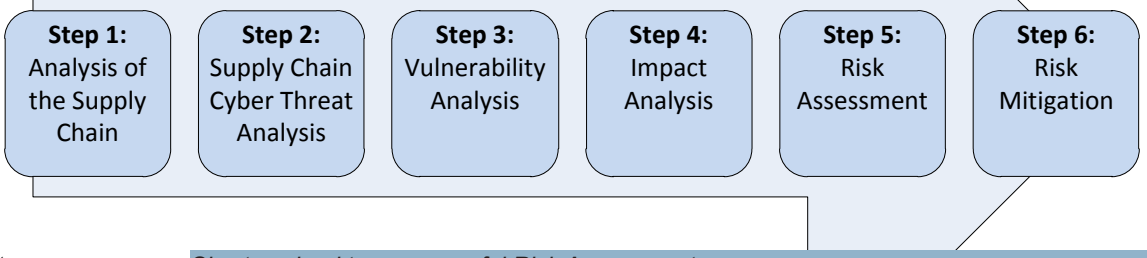
The **Threat Analysis** illustrates the overall threat scenario and conducts a first threat assessment by identifying individual cyber threats.

The **Vulnerability Analysis** describes all relevant kinds of vulnerabilities of the chosen supply chain service and assesses individual as well as cumulative vulnerabilities.

Individual and cumulative impact on the defined assets are estimated in the **Impact Analysis**. A possible diffusion of the impact along the supply chain and through the partnering networks is considered.

The **Risk Estimation** does the same with a view to the specific assets and shows how possible attacks may influence and cause malfunction of single assets and their possible infection amongst each other.

The **Mitigation Strategy** ends the analysis of the risk assessment with providing a risk mitigation strategy. This result shall ensure that of all relevant risks in a specific supply chain service is taken appropriate care of to avoid damage to own and partner's assets and the undisturbed function of the maritime supply chain.



Six steps lead to a successful Risk Assessment.

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

GAME THEORY IN THE MITIGATE SYSTEM

Number and type of potential cyber-attacks are almost infinite. Even a dynamically designed protection system and a continuous risk assessment can not satisfactorily repel all attacks. However, to achieve a high level of protection, developers are working on risk assessment systems under consideration of relevant threats and gateways for the system.

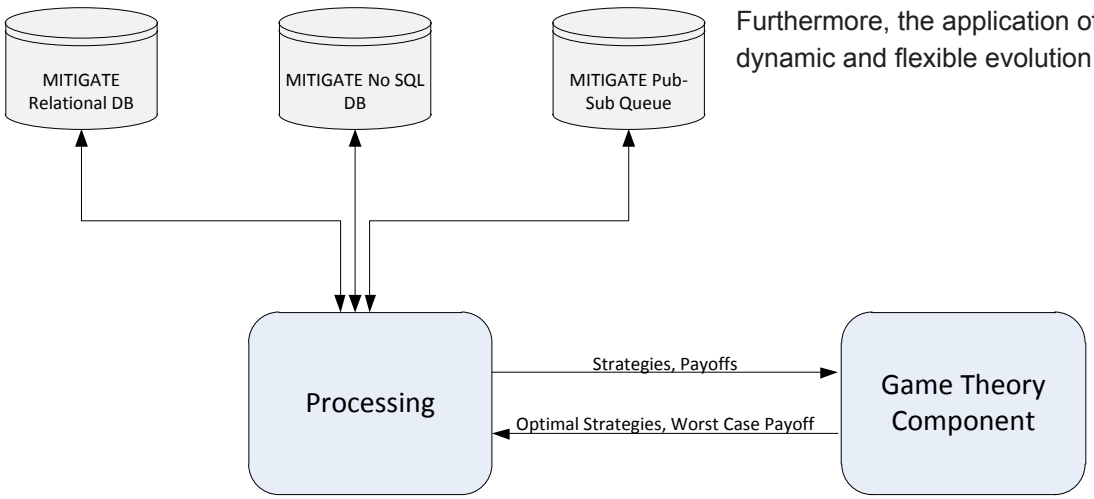
With the observation of comparable systems, but also the behavior of users and attackers, weaknesses can be eliminated accurately and comprehensively. Thus, game theoretic concepts and algorithms are examined for their suitability in the MITIGATE project.

The main idea is to model an attack on a company's ICT infrastructure as a game between the attacker and the system administrator. In this context, the attacker has a number of strategies at hand to infiltrate the infrastructure. Similarly, the system administrator has a number of defensive actions to counter these attacks. By evaluating the expected damage caused from an attack, game theory provides the system administrator with an optimal defense strategy.

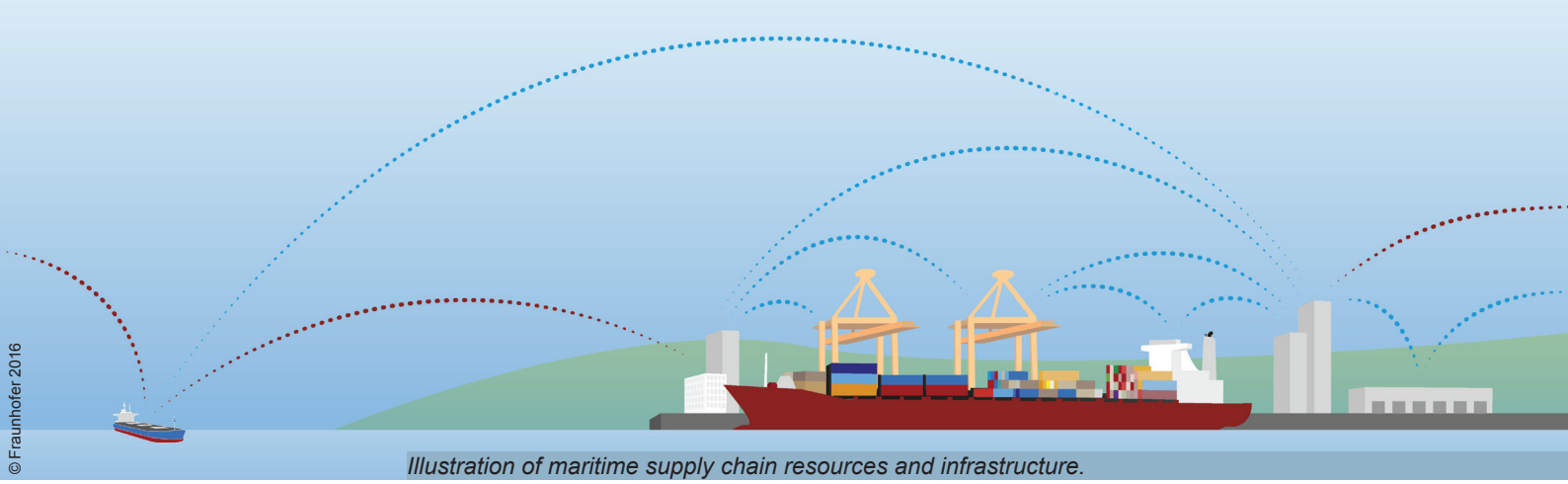
To this end, the expected damage needs to be estimated. Such an estimation can be gained by collecting expert opinions and further be supported by technical analysis of the system. In contrast to classical game theory, the MITIGATE method does not condense the collected data, as it is done, e.g., by using the maximum principle, but rather works with all available information.

Game theoretical methods can be generalized to yield an optimal defense strategy, even in the situation of multiple security objectives. An equilibrium can be computed which is optimal under all security objectives. Further, it is possible to prioritize different objectives by assigning weights.

Overall, the game theoretic approach offers completely new ways to protect critical information infrastructures since it provably provides optimal outcomes and is also efficient. Furthermore, the application of this approach supports the dynamic and flexible evolution of the MITIGATE software.



The use of Game Theory components in the MITIGATE system ensures the thorough selection of strategies.



© Fraunhofer 2016

Illustration of maritime supply chain resources and infrastructure.

PROTECTING MARITIME SUPPLY CHAIN IT INFRASTRUCTURE

PARTNERS

Fraunhofer CML

University of Piraeus Research Center

Singular Logic – Innovation at your doorstep

University of Brighton

AIT Austrian Institute of Technology

dbh Logistics IT AG

Autorità portuale Livorno

Gruppo Maggioli

FEPORTS – Instituto Portuario de Estudios y Cooperación de la Comunitat Valenciana

IMSSEA

OAΠ Piraeus Port Authority S.A.

Port of Ravenna Authority

Fundación Valenciaport

Hansestadt Bremisches Hafenamt

KEY FIGURES

- Thirteen partners from research, software development, logistics and ports
- Partners' countries: Austria, United Kingdom, Germany, Greece, Italy, Romania and Spain
- Project duration: from September 2015 till February 2018
- Budget 3.5 m€, funded within the EU Horizon 2020 programme with 3.1 m€

This project has received funding from The European Union´s Horizon 2020 research and innovation programme under grant agreement No 653212.

DATES / MEET MITIGATE

LNG Europe Conference, November 23+24, 2016 Valencia/ Spain

ITA-SEC, January 17-20, 2017 Venice/ Italy

11th ICGS3, January 18-20, 2017 Greenwich/ UK

MARENER, January 24+25, 2017 Malmö/ Sweden

PROJECT COORDINATION

Fraunhofer Center for Maritime Logistics and Services CML
Dipl.-Logist. Reiner Buhl

TECHNICAL MANAGEMENT

University of Piraeus
Associate Professor Nineta Polemi

CONTACT

info@mitigateproject.eu

MITIGATE

www.mitigateproject.eu

LinkedIn

www.linkedin.com/grps/MITIGATE-8472607

twitter.com/MITIGATE_EU