UBITECH ubiquitous solutions

GRUPPO Maggioli

Demo Webinar

July 12, 2023

CYSMET

Integrated, Dynamic & Collaborative Risk Management System
for Maritime Transport & Supply Chains

Project code: T2EDK-03488

Risk Management Methodology

Ευρωπαϊκή Ένωση
Ευρωπαϊκά Διαρθρωτικά
και Επενδυτικά Ταμεία

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΕΠΕΝΔΥΣΕΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΠΡΟΓΡΑΜΜΑΤΩΝ ΕΤΠΑ & ΤΣ
ΕΥΔ ΠΡΟΓΡΑΜΜΑΤΟΣ «ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ»

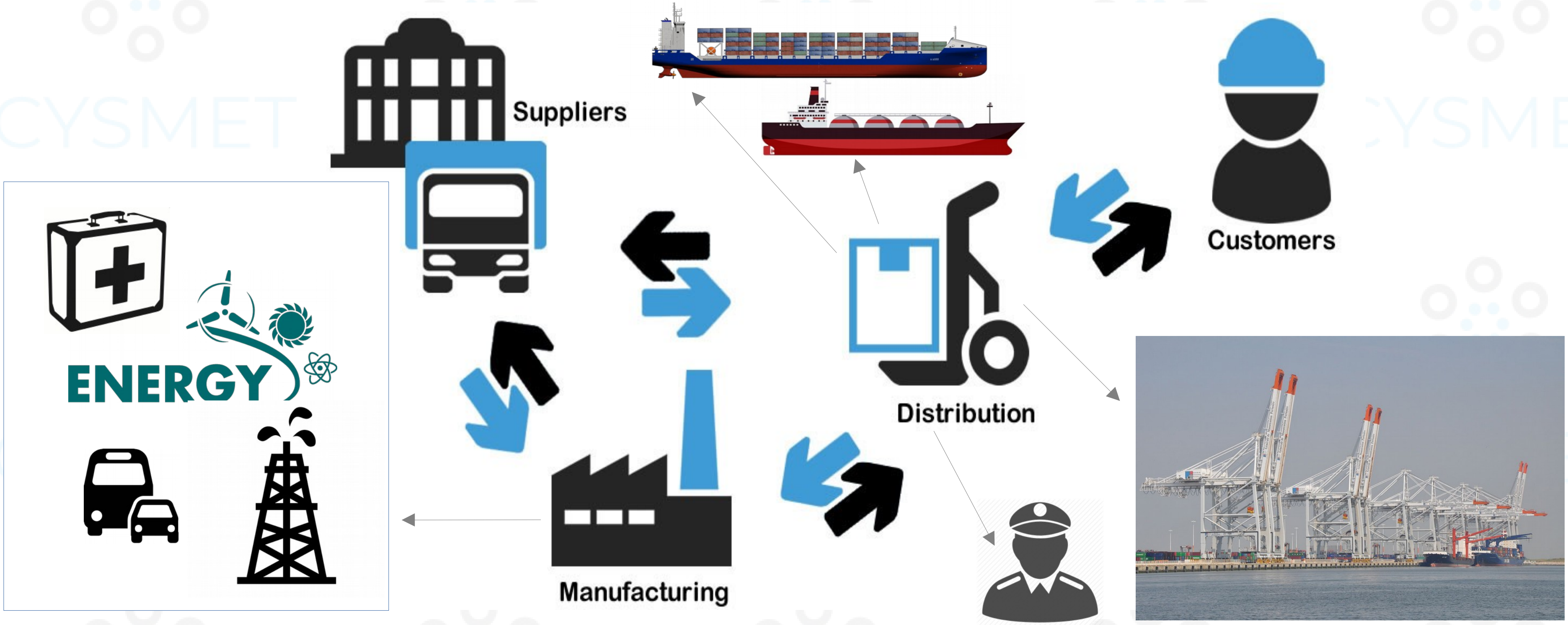
ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ
2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Introduction

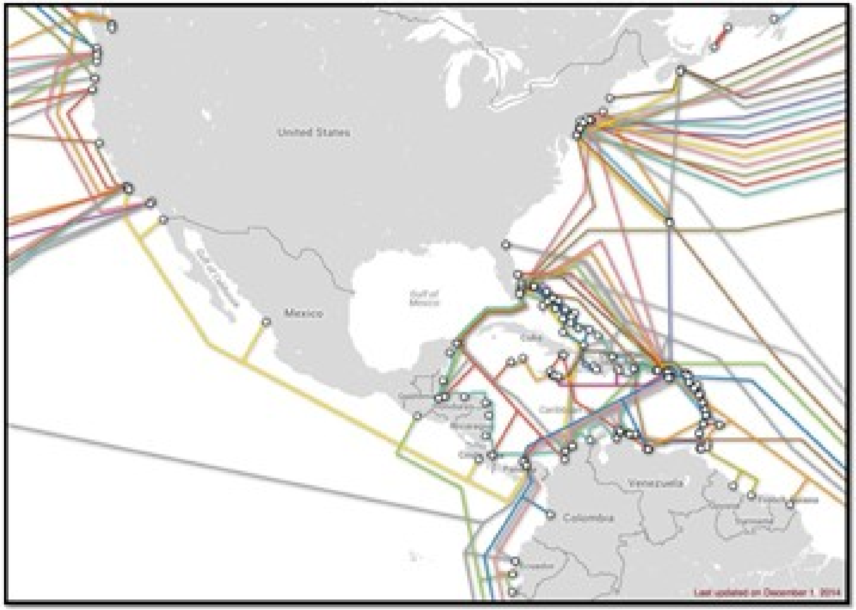
Maritime Supply Chain Service (SCS) – dynamic system of interconnected organizations (e.g. port authorities, customs services, marine insurance companies), critical infrastructure (e.g. energy, transportation, telecommunications), people and other elements aimed at providing a product/service to end users.



Graph: http://wifimurahlaju.blogspot.com/2017/08/supply-chain-service-output.html

Introduction

- **SCS cybersecurity incidents** increased by 51% during the second half of 2021 due to the pandemic [1]
- **IoT malware** increased by almost 100% in the first half of 2022, after the drop of COVID-19 – volume of attacks higher than the last 4 years [2]
- **Such events** also affect the SCSs, whose cybersecurity incidents have also found fertile ground in the conflict between Russia and Ukraine [3]



- **Maritime SCSs & ports** significantly increased its reliance on Information and Communications Technology (ICT) [4],[5]
- **Small & Medium Sized Ports (SMP)**
  – are the mainstay of a variety of activities in remote areas
  – use similar systems as the larger ones but on a smaller scale – lack of resources

[1] NCC Group research. https://campaign.cyber.nccgroup.com/insight-space-issue-6
[2] European Union Agency for Cybersecurity (ENISA) (2022). ENISA Threat Landscape 2022. Available online at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[3] National Maritime Foundation (2022). Available online at: https://maritimeindia.org/cyber-operations-associated-with-the-ukraine-russia-conflict-an-open-source-assessment/
[4] ENISA, "Cyber security aspects in the maritime sector", December 19, 2011. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
[5] ENISA, "Port Cybersecurity- Good practices for cybersecurity in the maritime sector", November 26, 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
[Picture] Journal of Business and Management Sciences, "How Digitalization and IoT Can Improve the Operations of Panama Canal", 2019. http://pubs.sciepub.com/jbms/7/3/5/

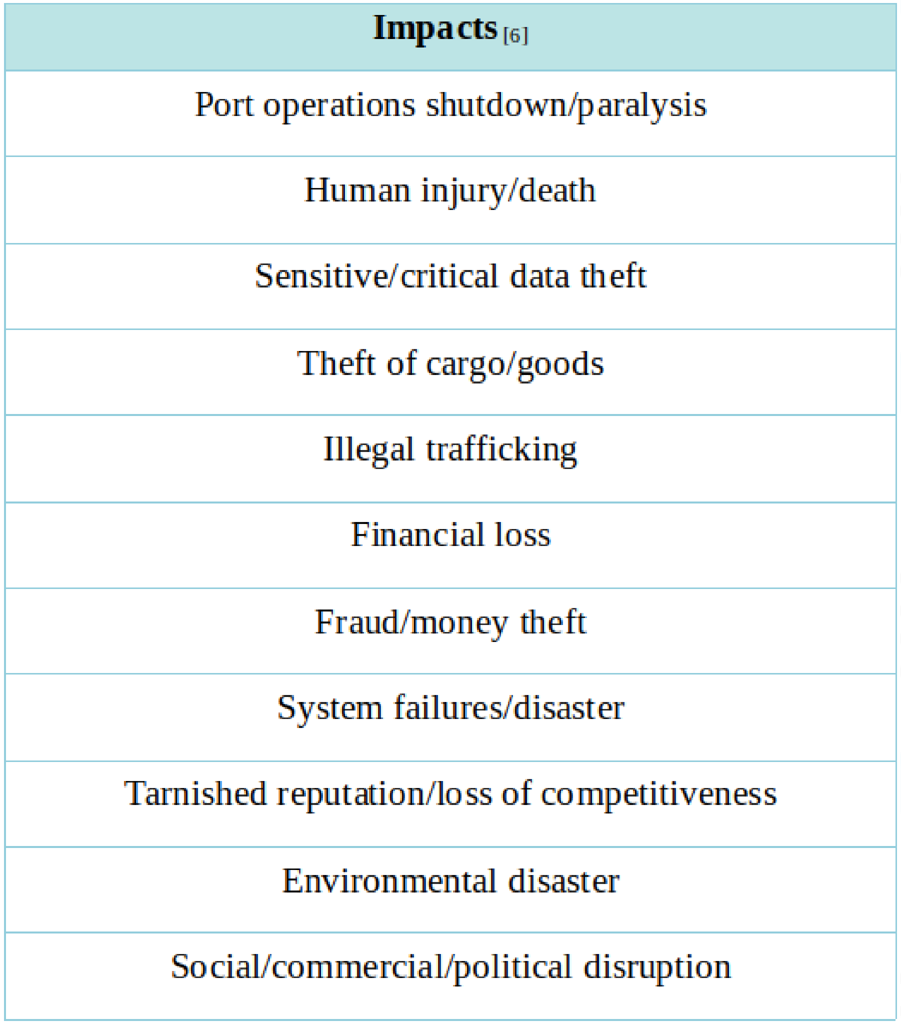
Potential Threats & Attacks

Physical Threats [6]	Cyber Threats [6]
- fraud - sabotage for military, political or ideological reasons - vandalism - theft of property - unauthorized access to premises, vehicles and equipment / unauthorized entry via vehicles - terrorism for political, ideological or religious reasons - hacktivism - coercion, extortion or corruption - piracy - any sort of illegal action or other crime - environmental or natural disasters	- espionage - interception or causing functional problems in systems through various cyber attacks - entry of malware - social engineering, phishing - leakage or deletion of information by employees - system errors / failures or malfunctions - power or network outages - staff shortages

Attacks
- Cyber (e.g. DDOS, XSS) - Physical (e.g. burglary, explosion) - Cyber-physical (combined)

[6] ENISA, "Port Cybersecurity - Good practices for cybersecurity in the maritime sector", November 26, 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

Impacts



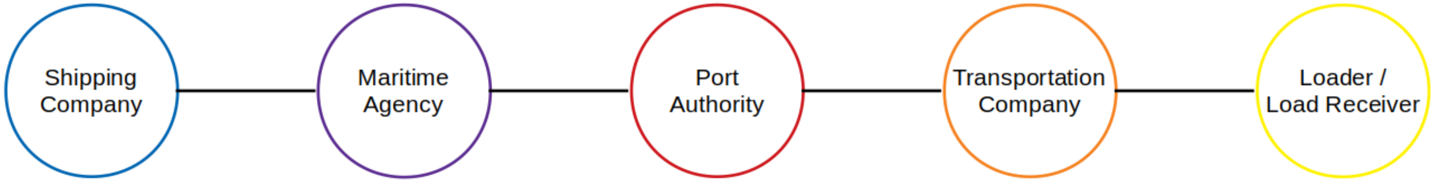
Impacts [6]
Port operations shutdown/paralysis
Human injury/death
Sensitive/critical data theft
Theft of cargo/goods
Illegal trafficking
Financial loss
Fraud/money theft
System failures/disaster
Tarnished reputation/loss of competitiveness
Environmental disaster
Social/commercial/political disruption

The impact of cyber attacks can extend to a SCS, even on a physical level, which, depending on the type of good (e.g. classes of dangerous goods, according to the IMO [7]) being transported, can be more or less devastating.

[6] ENISA, “Port Cybersecurity - Good practices for cybersecurity in the maritime sector”, November 26, 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
[7] IMO, “International Maritime Dangerous Goods (IMDG) Code”, 2020, Corrigenda May 2022. https://wwwcdn.imo.org/localresources/en/publications/Documents/Supplements/English/QM200E_180522.pdf

Attack Scenario

SCS: Supply of local industry with raw materials in containers

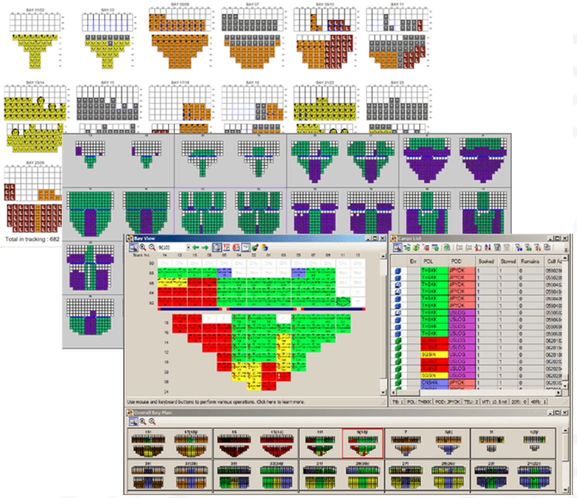


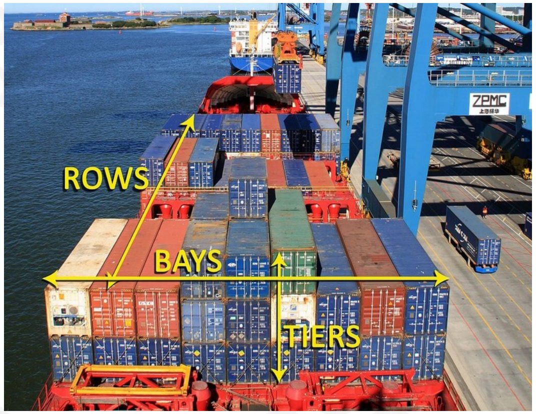
Assets

Cyber	- Stacking plan design software - Data exchanged via BAPLIE EDIFACT messages	- Stacking plan design software - Data exchanged via BAPLIE EDIFACT messages			
Physical	- Carrier ship - Containers - Staff	- Staff	- Port facilities - Staff	- Transport trucks - Staff	- Load

Attack Scenario

Attack on shipping company's container stacking planning system

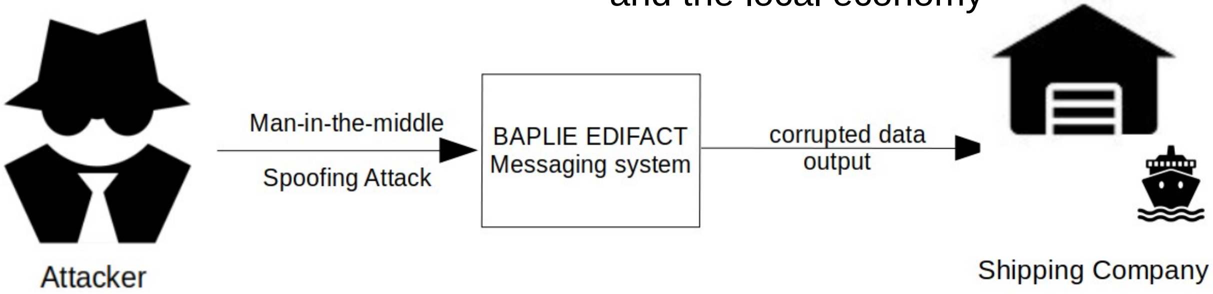




Impacts:

- injuries / loss of human life
- environmental disaster
- difficulty in recovering and returning to the normal operation of the port
- strong blow to the shipping company's reputation
- serious financial consequences for all the SCS BPs, the local industry, and the local economy

```
UNB+UNOA:2+SENDER-ID+RECEIVER-ID+090211:0811+0001+++++GEKU'
UNH+0001+BAPLIE:D:95B:UN:SMDG20'
BGM++0001+9'
DTM+137:0902110811:201'
TDT+20+00018NB+++GEK:172:ZZZ+++47AVS:103:ZZZ:SALERNO PRIDE:IT'
LOC+5+ITCAG:139:6'
LOC+61+ITSAL:139:6'
DTM+132:090211:101'
DTM+178:0902111230:201'
DTM+136:0902112330:201'
RFF+VON:GKS01A'
LOC+147+0010112::5'
MEA+WT++KGM:22500'
LOC+9+ITCAG:139:6'
LOC+11+ITSAL:139:6'
RFF+BM:1'
EQD+CN+GEKS1504090+22G1+++5'
NAD+CA+GEK:172:ZZZ'
UNT+18+0001'
UNZ+1+0001'
```



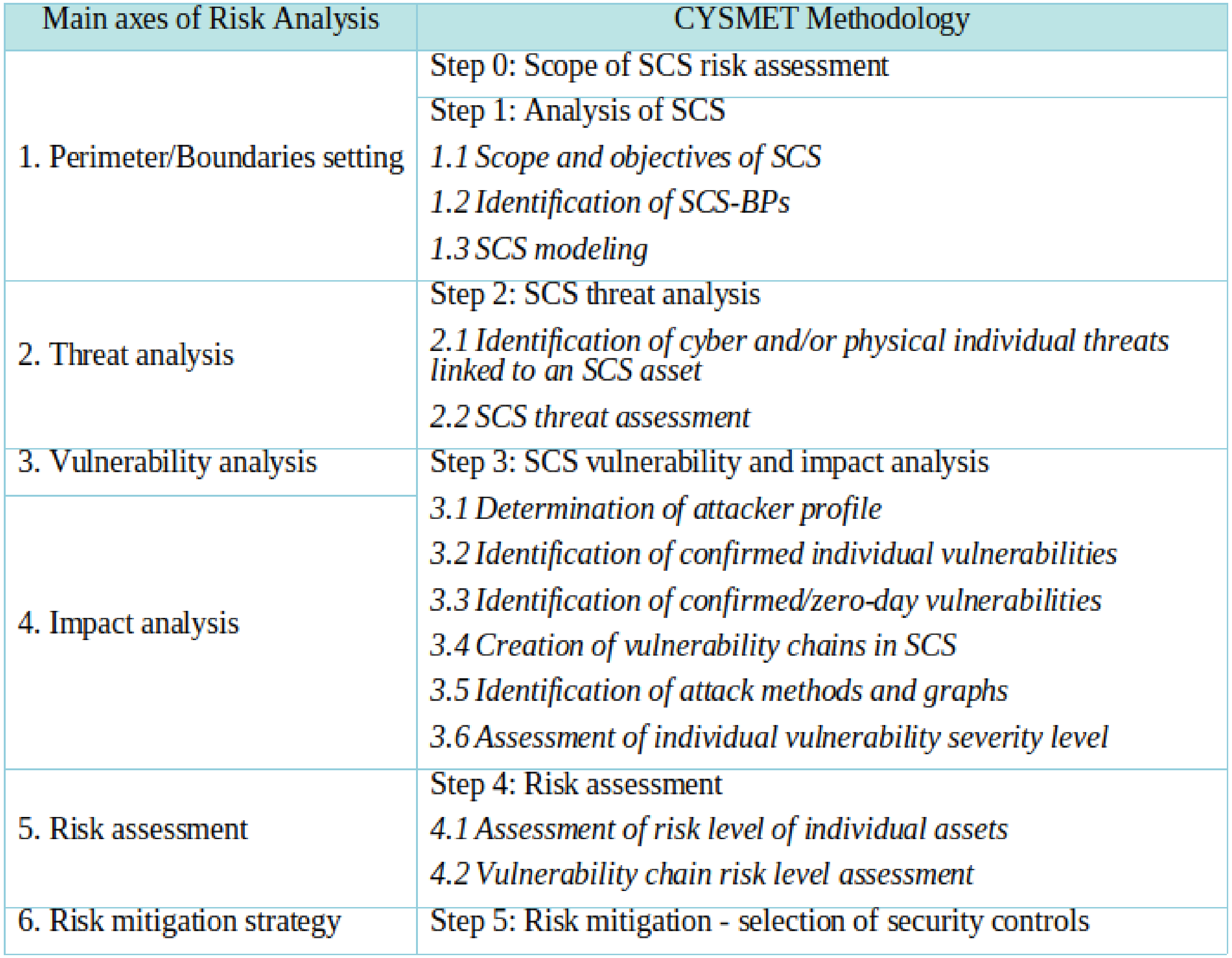
CYSMET

- Risk Management Methodology [8]
- Complies with all relevant standards and frameworks [9]
- Enhances the existing methodologies (e.g., CYSM [10], MEDUSA [11], MITIGATE [12], eBIOS [13]) by:

  – including additional to ICT assets in the perimeter of the assessment (OT, IoT);
  – using additional vulnerability DB records related to OT and IoT;
  – calculating risk and attack paths originated by both cyber and cyber-physical threats;
  – applying the updated v3.1 of the CVSS;
  – utilizing all CVSS v3.1 metric fields: Base, Temporal and Environmental Scores to increase accuracy of the measurements;
  – using the vulnerability and impact assessments as a combined process (the CVSS v3.1 takes into account the impact that a vulnerability exploitation could have on the environment under consideration).

[8] Kyranoudi, P., Polemi, N. (2023). Securing small and medium ports and their supply chain services. Frontiers Computer Science Journal, Section Computer Security, Research Topic: The Impacts of Cyber Threat in the Maritime Ecosystem, Volume 5. doi: https://doi.org/10.3389/fcomp.2023.1156726
[9] Kyranoudi, P., Kalogeraki, E., Michota, A., Polemi, N. (2021). Cybersecurity Certification Requirements for Supply Chain Services. IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, pp. 1-7. doi: 10.1109/ISCC53001.2021.9631467
[10] ENISA, “Cyber security aspects in the maritime sector”, December 19, 2011. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
[11] ENISA, “Port Cybersecurity- Good practices for
[12] Journal of Business and Management Sciences, “How Digitalization and IoT
[13] Can Improve the Operations of Panama Canal”, 2019. http://pubs.sciepub.com/jbms/7/3/5/

CYSMET at a glance



Main axes of Risk Analysis	CYSMET Methodology
1. Perimeter/Boundaries setting	Step 0: Scope of SCS risk assessment
	Step 1: Analysis of SCS *1.1 Scope and objectives of SCS* *1.2 Identification of SCS-BPs* *1.3 SCS modeling*
2. Threat analysis	Step 2: SCS threat analysis *2.1 Identification of cyber and/or physical individual threats linked to an SCS asset* *2.2 SCS threat assessment*
3. Vulnerability analysis	Step 3: SCS vulnerability and impact analysis *3.1 Determination of attacker profile* *3.2 Identification of confirmed individual vulnerabilities* *3.3 Identification of confirmed/zero-day vulnerabilities* *3.4 Creation of vulnerability chains in SCS* *3.5 Identification of attack methods and graphs* *3.6 Assessment of individual vulnerability severity level*
4. Impact analysis	
5. Risk assessment	Step 4: Risk assessment *4.1 Assessment of risk level of individual assets* *4.2 Vulnerability chain risk level assessment*
6. Risk mitigation strategy	Step 5: Risk mitigation - selection of security controls

Step 0

Scope of SCS risk assessment

- The assessor selects the SCS for which the risk assessment will be carried out, as well as its limits
  i.e., the scope, the objective and the expected result

- A Service Level Agreement (SLA) is created and signed by the SCS Provider and all Business Partners (BPs)

Step 1

Analysis of SCS

Step 1.1 Scope and objectives of SCS

The assessor defines the under consideration SCS scope and provides its objective and expected outcome.

Step 1.2 Identification of SCS-BPs

The assessor identifies the SCS-BPs, in agreement with them. Each of them declares all participants from their organization for the current risk assessment.

Step 1.3 SCS modeling

The main objective is to identify and model the main processes involved in the SCS under consideration.

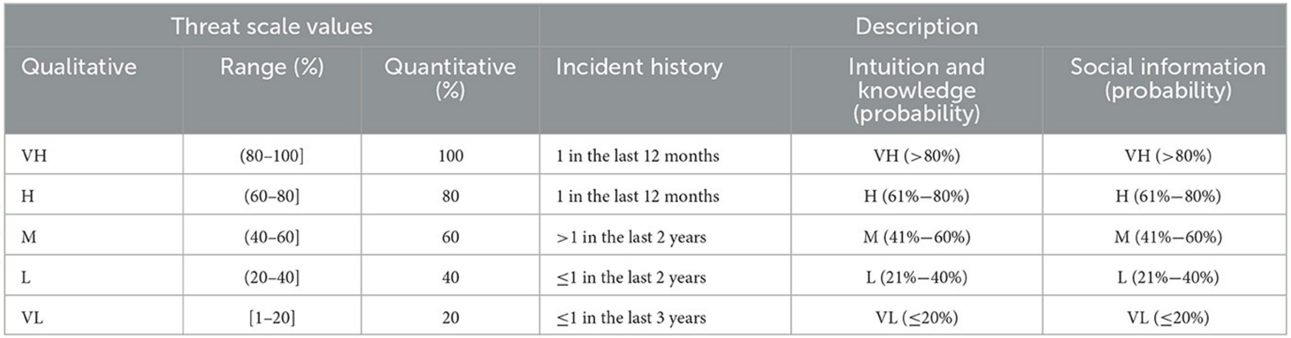
Step 2

SCS threat analysis

Step 2.1 Identification of cyber and/or physical individual threats linked to an SCS asset

All cyber and/or physical individual threats for a specific SCS asset will be identified using online repositories, social media, crowd sourcing, threat data recorded by BPs, etc.

Step 2.2 SCS threat assessment

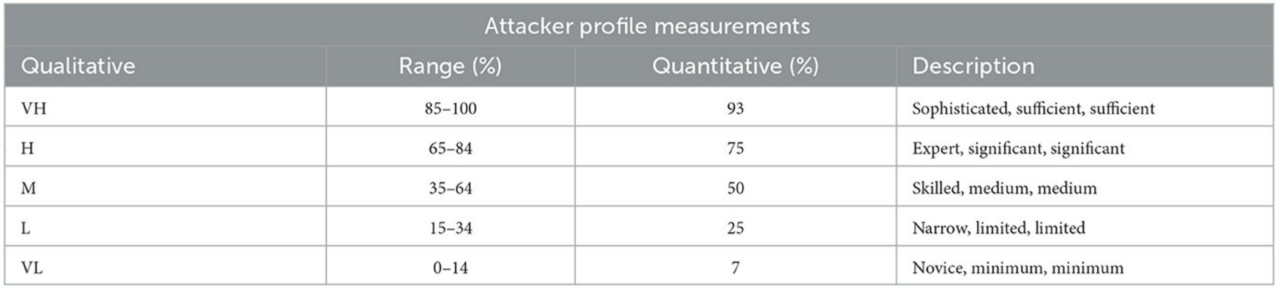


Threat scale values			Description		
Qualitative	Range (%)	Quantitative (%)	Incident history	Intuition and knowledge (probability)	Social information (probability)
VH	(80–100]	100	1 in the last 12 months	VH (>80%)	VH (>80%)
H	(60–80]	80	1 in the last 12 months	H (61%–80%)	H (61%–80%)
M	(40–60]	60	>1 in the last 2 years	M (41%–60%)	M (41%–60%)
L	(20–40]	40	≤1 in the last 2 years	L (21%–40%)	L (21%–40%)
VL	[1–20]	20	≤1 in the last 3 years	VL (≤20%)	VL (≤20%)

Step 3

SCS vulnerability and impact analysis

Step 3.1 Determination of attacker profile



Attacker profile measurements

Qualitative	Range (%)	Quantitative (%)	Description
VH	85–100	93	Sophisticated, sufficient, sufficient
H	65–84	75	Expert, significant, significant
M	35–64	50	Skilled, medium, medium
L	15–34	25	Narrow, limited, limited
VL	0–14	7	Novice, minimum, minimum

Step 3.2 Identification of confirmed individual vulnerabilities

Online and various DBs are searched to find confirmed vulnerabilities, i.e.: NVD, CVE Details, other online DBs, commercial or open-source vulnerability scanners (e.g., OpenVas), etc.

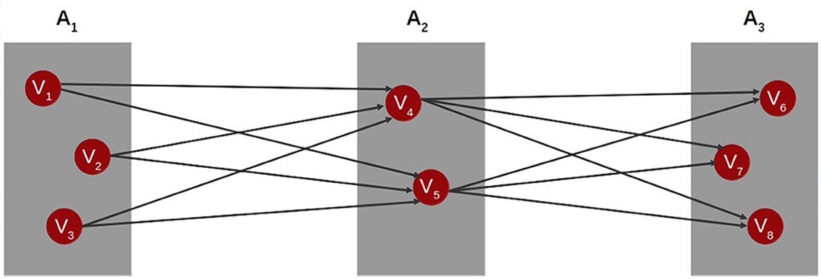
Step 3.3 Identification of confirmed/zero-day vulnerabilities

Defined either empirically or by determining the number of publicly announced vulnerabilities for a specific time period.

Step 3

SCS vulnerability and impact analysis

Step 3.4 Creation of vulnerability chains in SCS



Step 3.5 Identification of attack methods and graphs

e.g.: $V_1,A_1 \to V_5,A_2 \to V_7,A_3$

Step 3.6 Assessment of individual vulnerability severity level

The individual vulnerability severity level (IVSL) of each vulnerability found in the previous sub-steps is assessed, using all metrics of the CVSS v3.1 (Base, Temporal, and Environmental Scores)

Step 4

Risk
assessment

Step 4.1: Assessment of risk level of individual assets

$$\begin{aligned} Individual\ Risk\ Level &= (Threat\ Level^{*} Vulnerability\ Level^{*} Impact\ Level) \\ &\ {}^{*} Attacker\ Profile, where Vulnerability\ Level^{*} Impact Level \\ &= IVSL \end{aligned}$$

Step 4.2: Vulnerability chain risk level assessment

$$\begin{aligned} Risk(Vulnerability\ Chain) &= Risk(Node1) * Risk(Node2) * Risk(Node3) \\ &\ {}^{*}...^{*} Risk(NodeN) \end{aligned}$$

Step 5

Risk mitigation – selection of security controls

- As CYSMET is an ISO/IEC 27002 compliant risk management methodology, they can use this standard, among others, for guidance.

Conclusions

SMPs:

- are main economic and strategic regional drivers
- act as hubs of an SCS like major ports
- have similar needs/work under the same laws and regulations as major ports
- can be exposed to similar threats and attacks
- face financial resources limitation and security management is expensive
- can use CYSMET methodology to assess and manage their risks

Conclusions

CYSMET Risk Management Methodology:

- collaborative
- complies with all relevant standards and frameworks
- enhances the existing methodologies (i.e., IT/OT/IoT, CVSS v3.1, etc)
- allows self-assessment (easy to use, low cost)
- provision of the corresponding tool

Thank you!

CYSMET

https://cysmet.ubitech.eu/

Acknowledgment:
This research has been co-financed by the European Regional Development Fund of the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH – CREATE -INNOVATE
(project code:T2EDK-03488)

Ευρωπαϊκή Ένωση
Ευρωπαϊκά Διαρθρωτικά και Επενδυτικά Ταμεία

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ
ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΕΠΕΝΔΥΣΕΩΝ
ΕΙΔΙΚΗ ΓΡΑΜΜΑΤΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΠΡΟΓΡΑΜΜΑΤΩΝ ΕΤΠΑ & ΤΣ
ΕΥΔ ΠΡΟΓΡΑΜΜΑΤΟΣ «ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ»

ΕΠΑνΕΚ 2014-2020
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ
ΚΑΙΝΟΤΟΜΙΑ

ΕΣΠΑ
2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

UBITECH ubiquitous solutions

GRUPPO Maggioli