Digital Ship Oslo, 12th of March 2024:

Maritime cybersecurity threat modelling: Attacker-centric and system-centric threats

Per Håkon Meland, Senior Researcher, SINTEF Digital

Technology for a better society

How?

Principle: The outcomes of threat modeling are meaningful when they are of value to stakeholders

*"there is **no single best or correct way** of performing threat modeling, it is a question of trade-offs and what we want to achieve by doing it"*

Source: A. Shostack, *"Experiences Threat Modeling at Microsoft,"* 2008.

Anti-pattern: Perfect representation

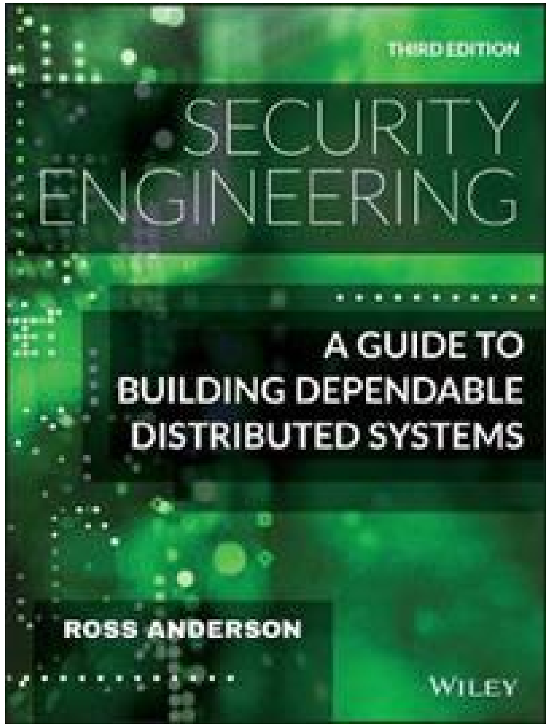
It is better to create multiple threat modeling representations because there is no single ideal view, and additional representations may illuminate different problems.

Threat modelling manifesto (2020)

Attacker-centric threat models

"One of the first things the security engineer needs to do when tackling a new problem is to identify the likely opponents"

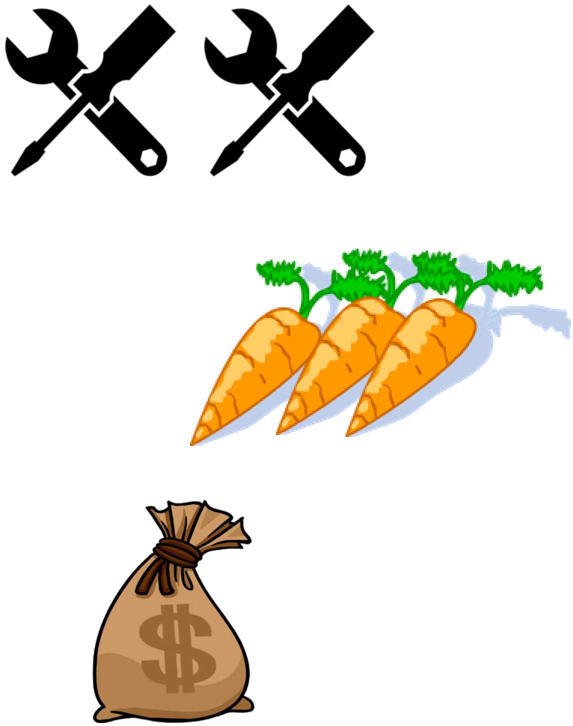
"...what sort of capabilities will the adversaries have, and what motivation?"

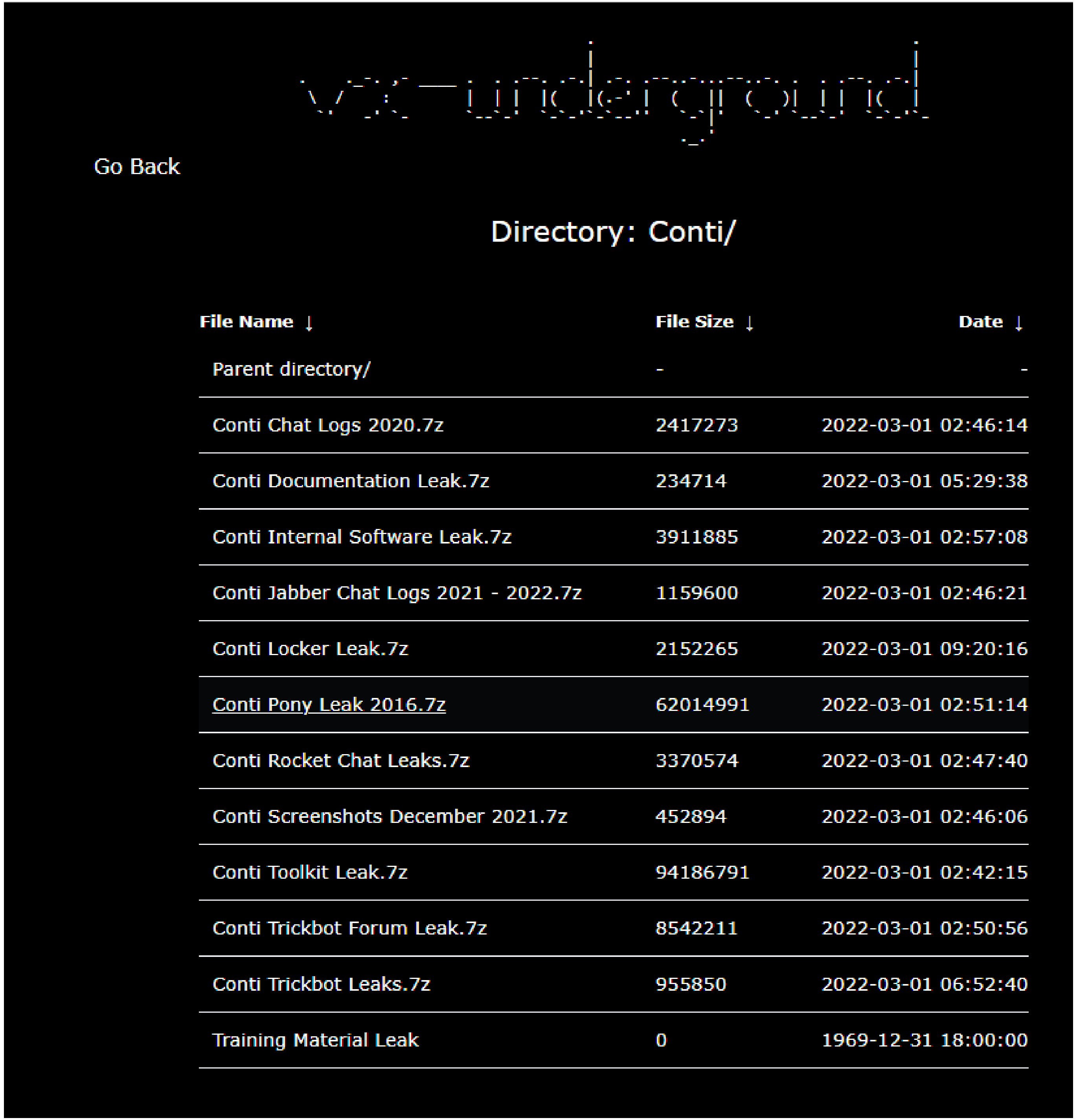


Attributes of threat agents

- Skillset
- Motivation
- Resources

Threat agent: The Crooks

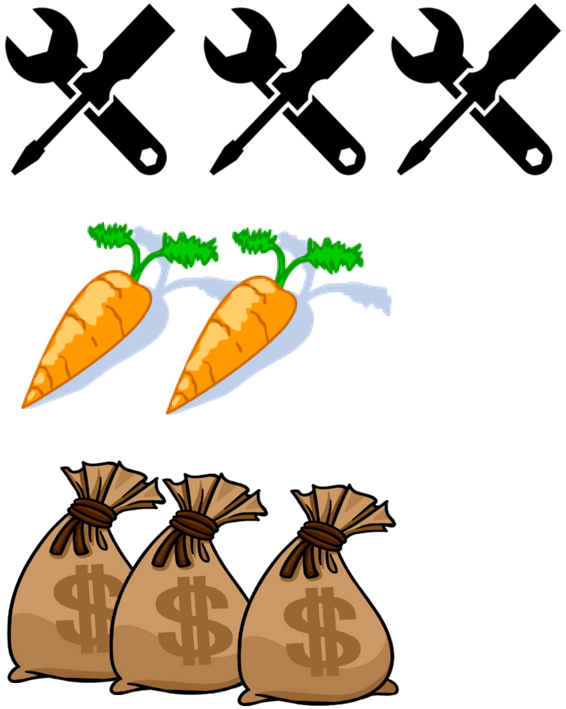




Directory: Conti/

File Name ↓	File Size ↓	Date ↓
Parent directory/	-	-
Conti Chat Logs 2020.7z	2417273	2022-03-01 02:46:14
Conti Documentation Leak.7z	234714	2022-03-01 05:29:38
Conti Internal Software Leak.7z	3911885	2022-03-01 02:57:08
Conti Jabber Chat Logs 2021 - 2022.7z	1159600	2022-03-01 02:46:21
Conti Locker Leak.7z	2152265	2022-03-01 09:20:16
Conti Pony Leak 2016.7z	62014991	2022-03-01 02:51:14
Conti Rocket Chat Leaks.7z	3370574	2022-03-01 02:47:40
Conti Screenshots December 2021.7z	452894	2022-03-01 02:46:06
Conti Toolkit Leak.7z	94186791	2022-03-01 02:42:15
Conti Trickbot Forum Leak.7z	8542211	2022-03-01 02:50:56
Conti Trickbot Leaks.7z	955850	2022-03-01 06:52:40
Training Material Leak	0	1969-12-31 18:00:00

Threat agent: Goverment cyber warriors



Nation State Actor

Volt Typhoon

Microsoft Security actively investigates and tracks threat actors in order to help protect customers, our platform and services from adversaries.

The actor that Microsoft tracks as Volt Typhoon is a nation-state activity group based out of China. Volt Typhoon is known to primarily target the United States and the manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors. Volt Typhoon focuses on espionage, data theft, and credential access.

Learn more

Also known as:

- VANGUARD PANDA, BRONZE SILHOUETTE

Country of origin:

China

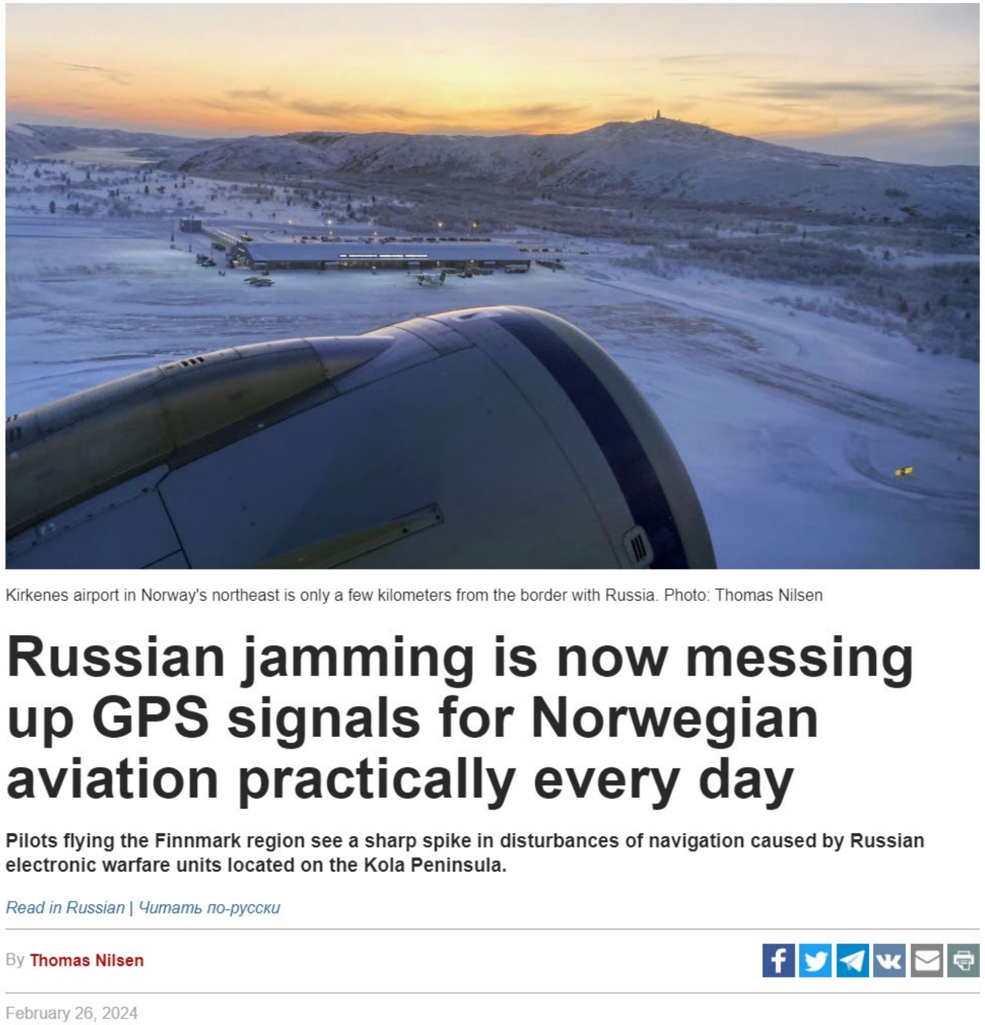
Countries targeted:

United States and Guam

Industries targeted:

- Communications Infrastructure
- Manufacturing
- Media
- Defense
- Education
- Utilities
- Software and Technology
- Transportation
- Construction
- Government

Microsoft Security



Kirkenes airport in Norway's northeast is only a few kilometers from the border with Russia. Photo: Thomas Nilsen

Russian jamming is now messing up GPS signals for Norwegian aviation practically every day

Pilots flying the Finnmark region see a sharp spike in disturbances of navigation caused by Russian electronic warfare units located on the Kola Peninsula.

Read in Russian | Читать по-русски

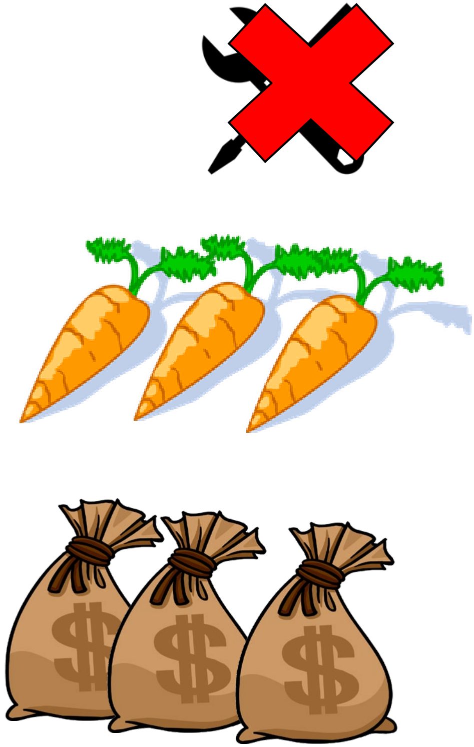
By **Thomas Nilsen**

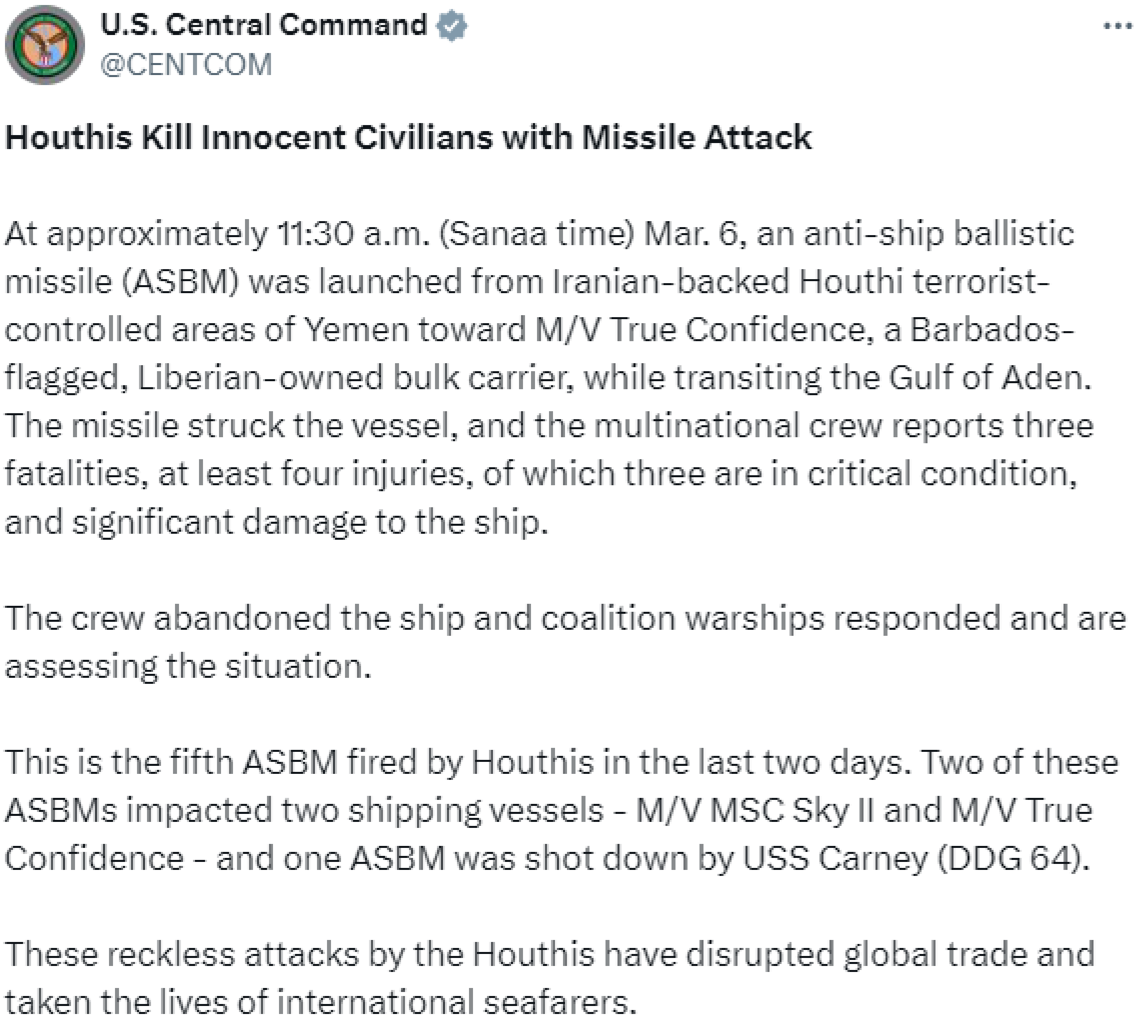
February 26, 2024

"... Moscow's parallel cyber and influence operations have largely failed"

Source: Microsoft Threat Intelligence 2023

Threat agent: The Terrorists





U.S. Central Command
@CENTCOM

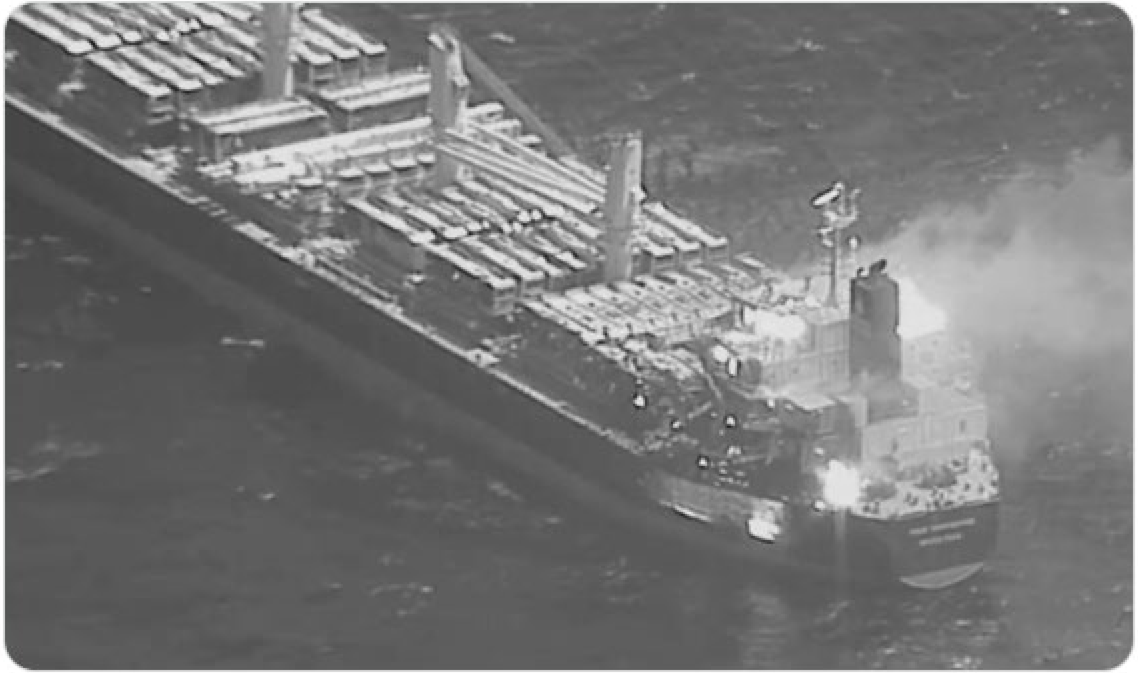
Houthis Kill Innocent Civilians with Missile Attack

At approximately 11:30 a.m. (Sanaa time) Mar. 6, an anti-ship ballistic missile (ASBM) was launched from Iranian-backed Houthi terrorist-controlled areas of Yemen toward M/V True Confidence, a Barbados-flagged, Liberian-owned bulk carrier, while transiting the Gulf of Aden. The missile struck the vessel, and the multinational crew reports three fatalities, at least four injuries, of which three are in critical condition, and significant damage to the ship.

The crew abandoned the ship and coalition warships responded and are assessing the situation.

This is the fifth ASBM fired by Houthis in the last two days. Two of these ASBMs impacted two shipping vessels - M/V MSC Sky II and M/V True Confidence - and one ASBM was shot down by USS Carney (DDG 64).

These reckless attacks by the Houthis have disrupted global trade and taken the lives of international seafarers.



Threat agent: The Swamp

International Chamber of Shipping

Shaping the Future of Shipping

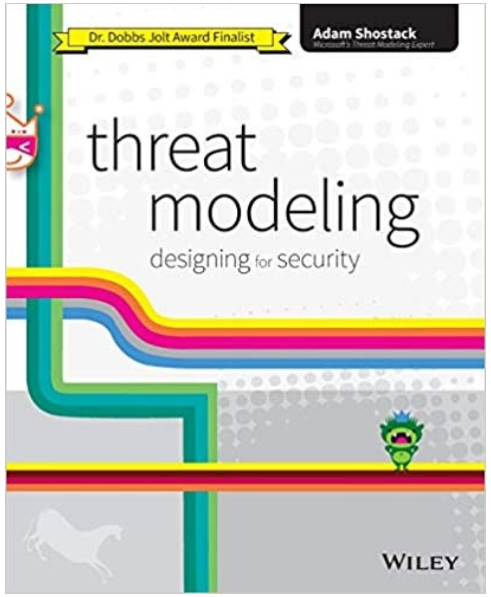
Industry Principles for Establishing Effective Measures to Combat and Eliminate Harassment and Bullying in the Maritime Sector

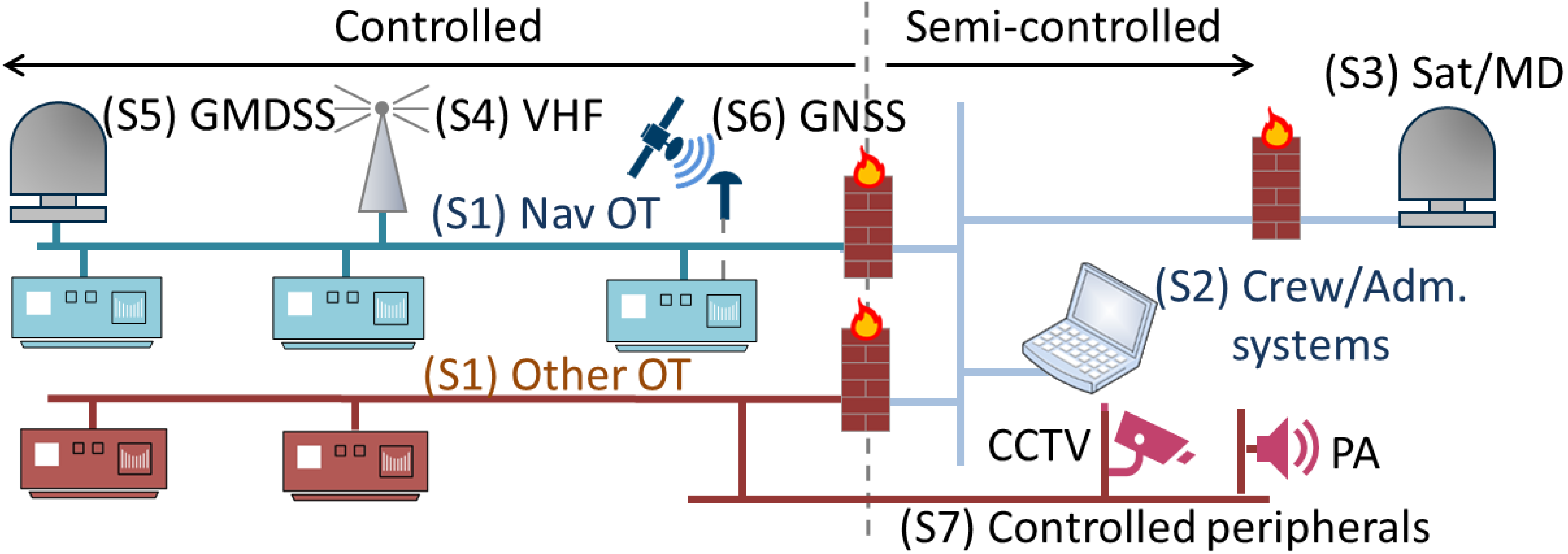
February 2024

Threat agent: The Insiders

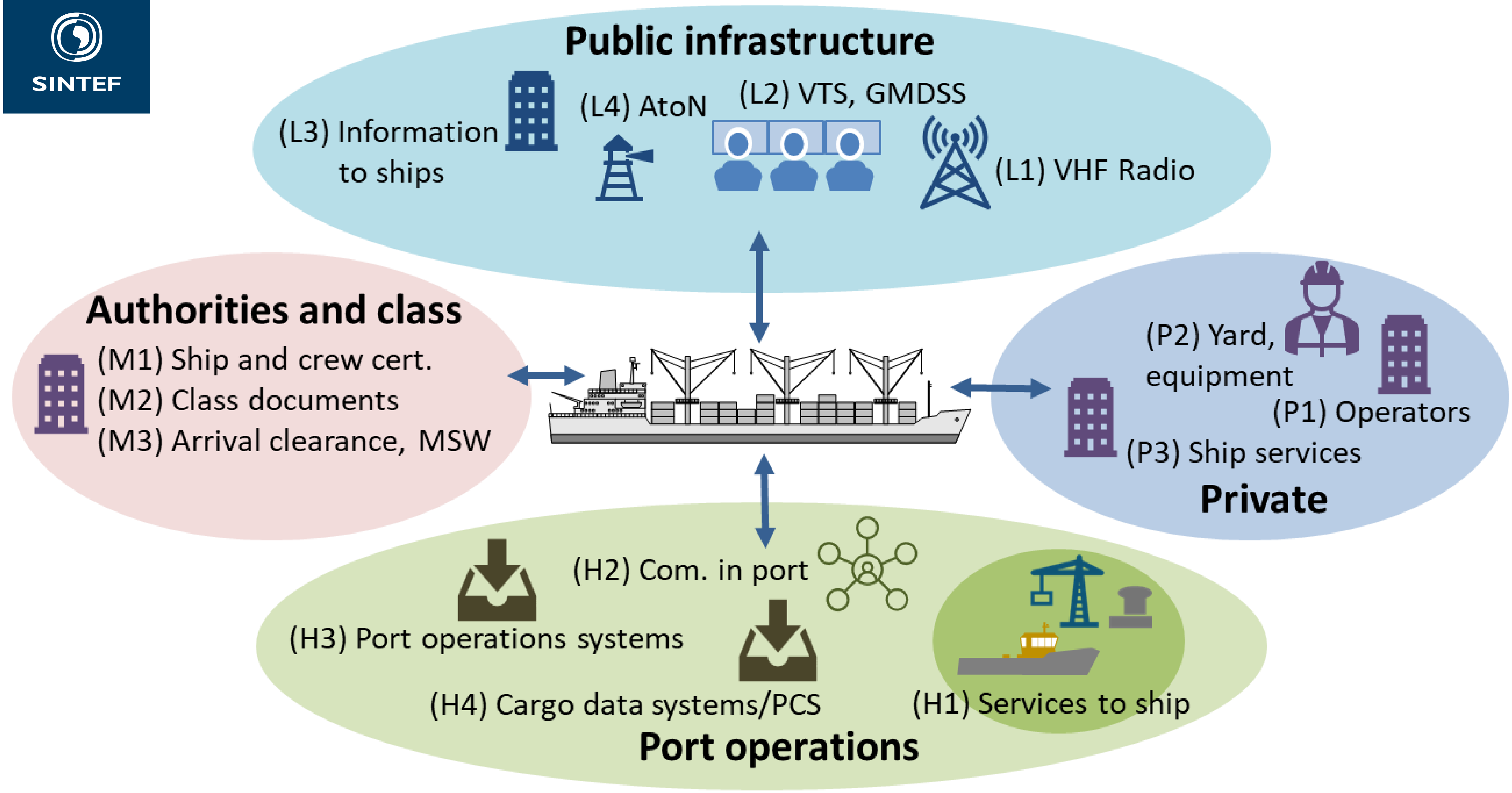
System-centric threat models

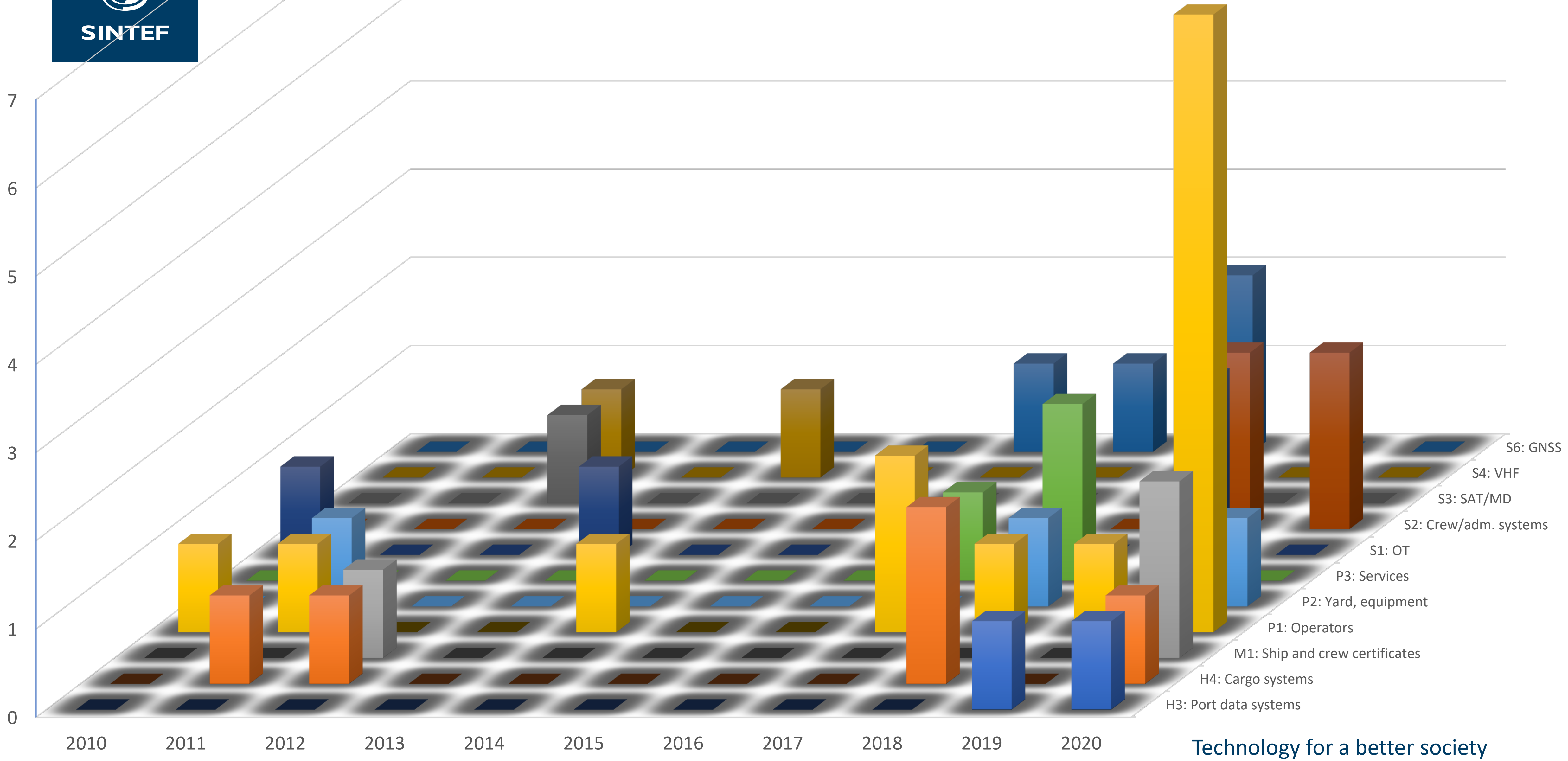
models that focus on the systems being built or a system being deployed





A Retrospective Analysis of Maritime Cyber Security Incidents (2021). Meland et al.


Public infrastructure
(L3) Information to ships
(L4) AtoN
(L2) VTS, GMDSS
(L1) VHF Radio
Authorities and class
(M1) Ship and crew cert.
(M2) Class documents
(M3) Arrival clearance, MSW
(P2) Yard, equipment
(P1) Operators
(P3) Ship services
Private
(H2) Com. in port
(H3) Port operations systems
(H4) Cargo data systems/PCS
(H1) Services to ship
Port operations

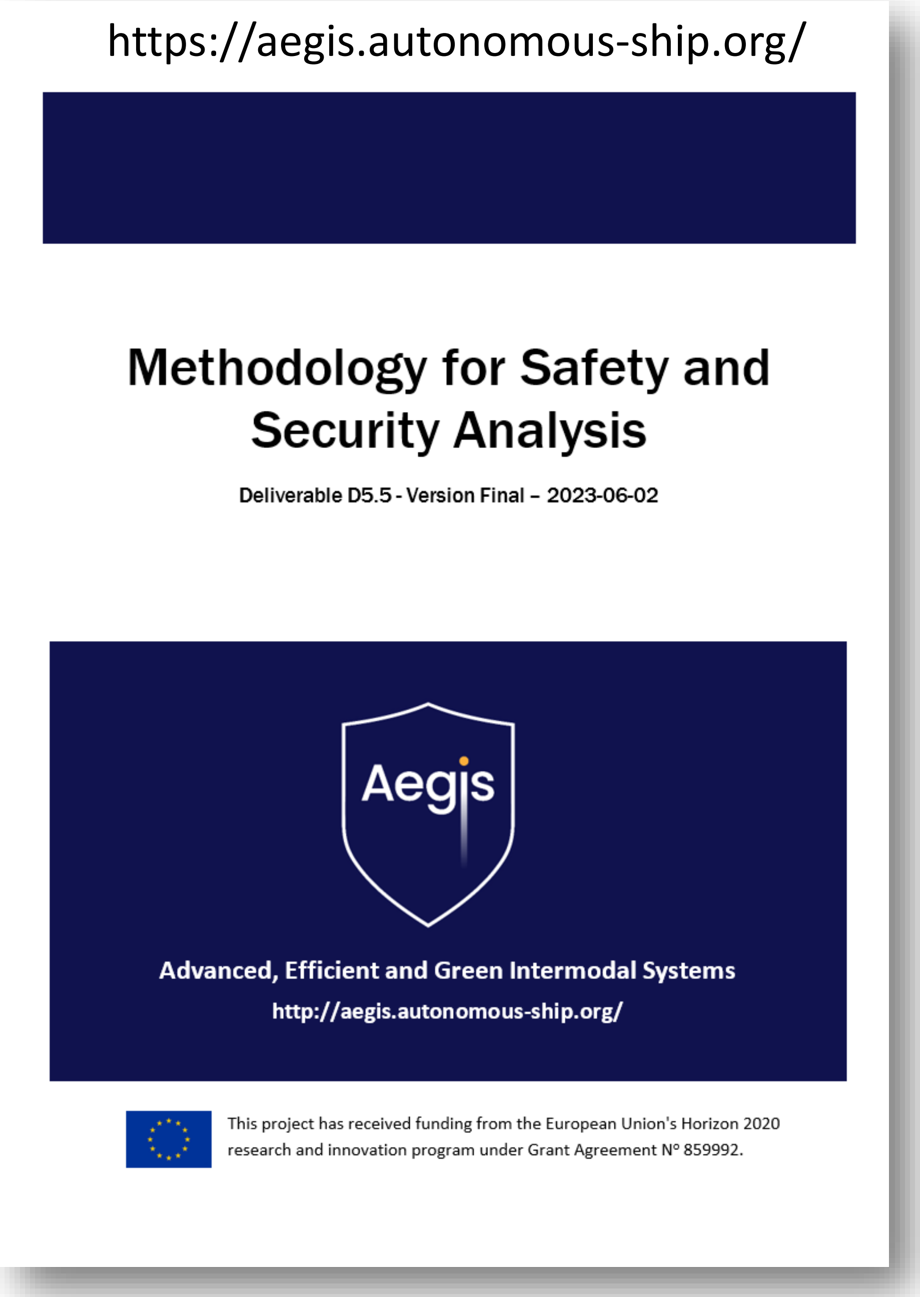


Technology for a better society

Attacker-centric

+

System-centric



https://aegis.autonomous-ship.org/

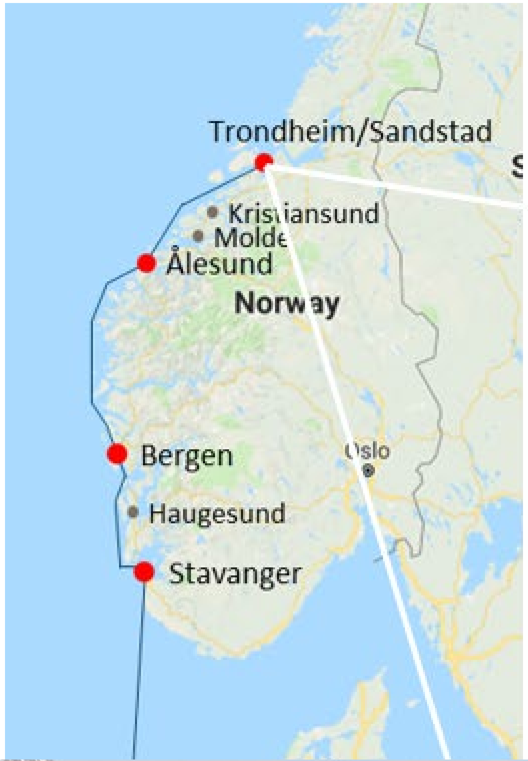
Methodology for Safety and Security Analysis

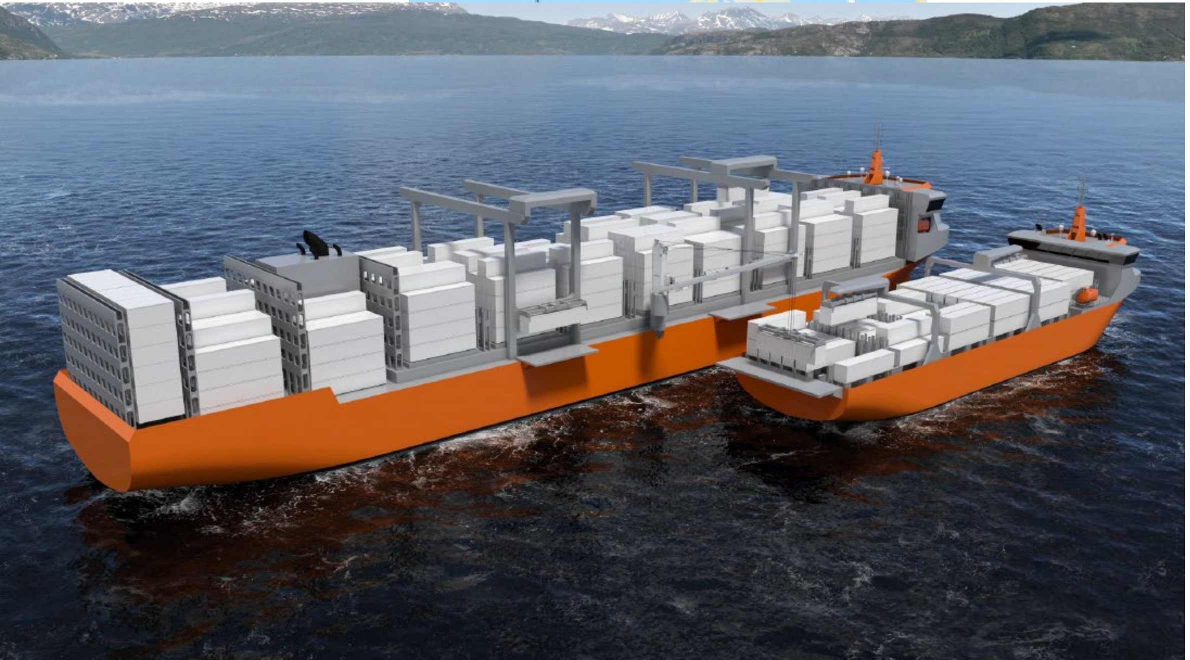
Deliverable D5.5 - Version Final – 2023-06-02

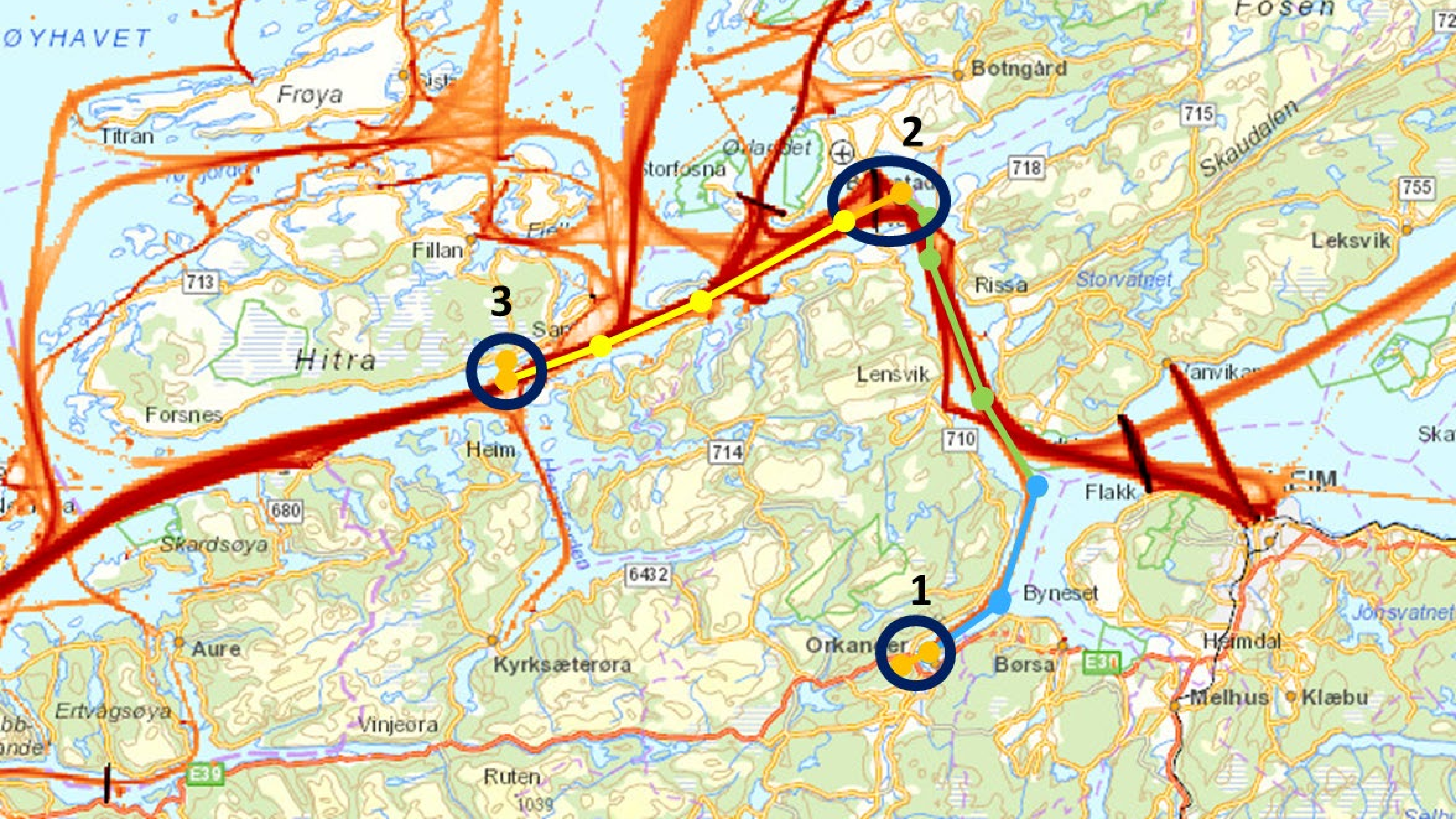
Advanced, Efficient and Green Intermodal Systems

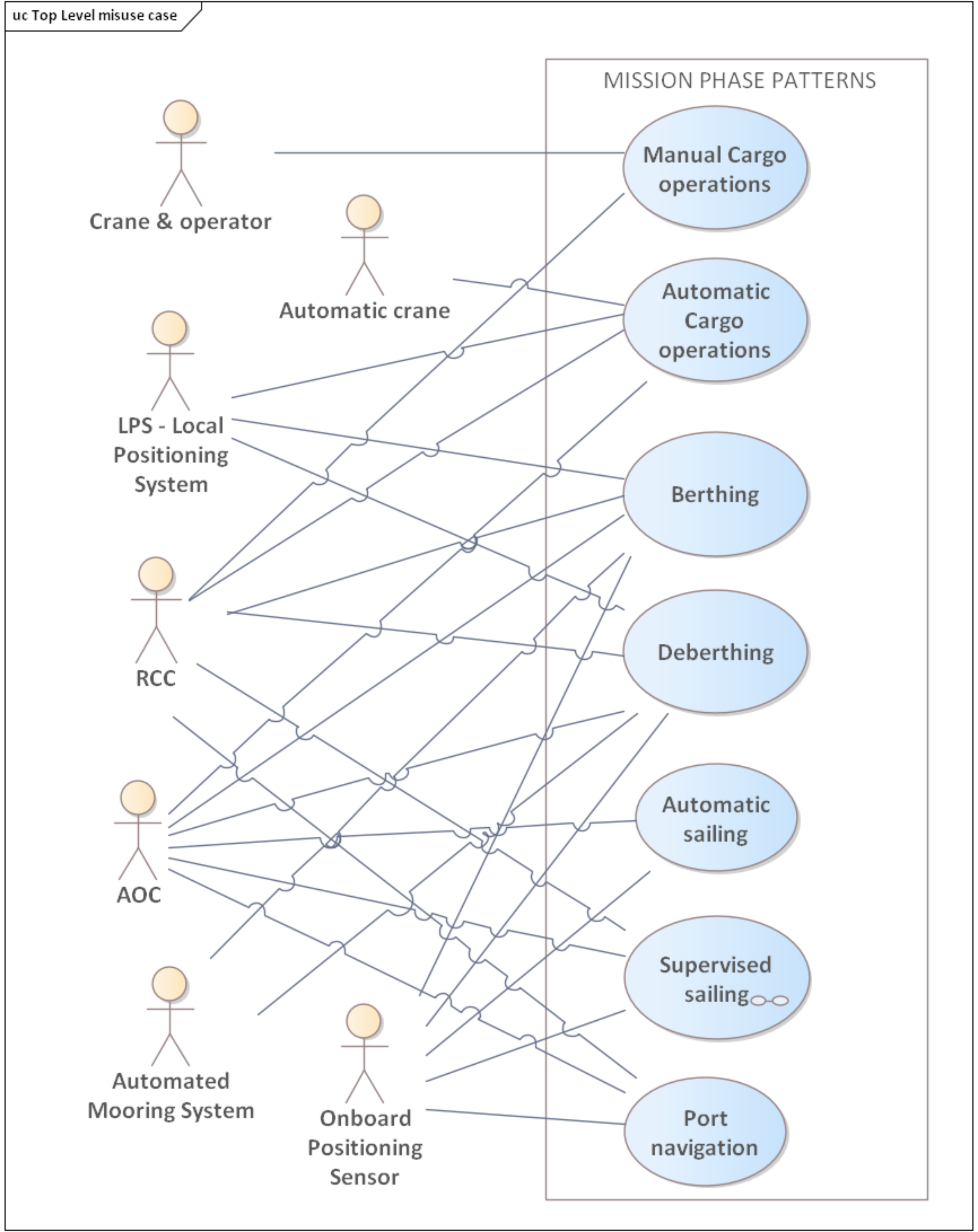
http://aegis.autonomous-ship.org/

This project has received funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement N° 859992.

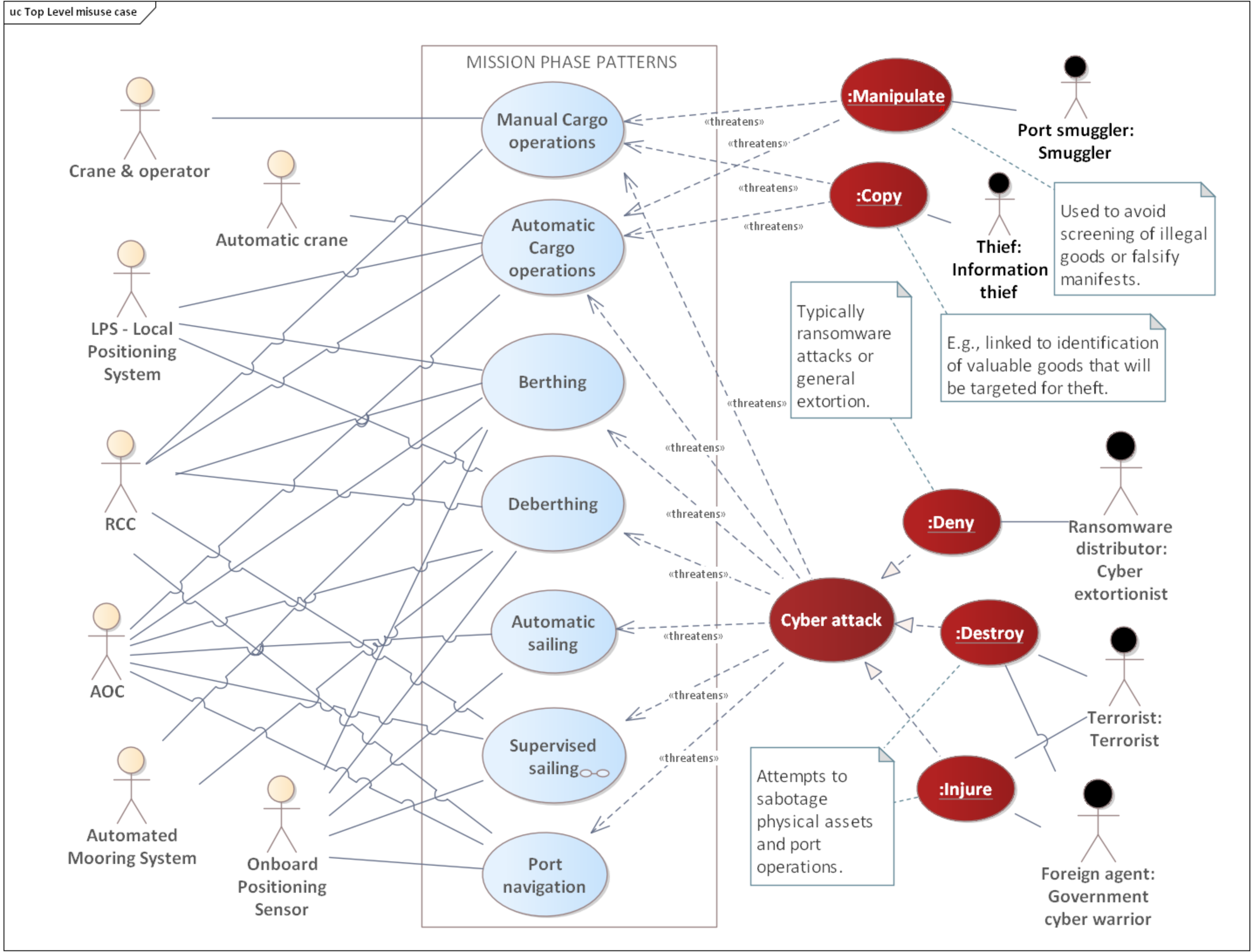

Trondheim/Sandstad
Kristiansund
Molde
Ålesund
Norway
Bergen
Oslo
Haugesund
Stavanger




1
2
3
ØYHAVET
Fosen
Frøya
Titran
Botngård
715
Skaudalen
Ørlandet
Storfosna
718
755
Leksvik
Fillan
713
Rissa
Storvatnet
Hitra
Lensvik
Forsnes
Heim
714
710
Flakk
EIM
680
Skardsøya
6432
Byneset
Jonsvatnet
Aure
Kyrksæterøra
Orkanger
Børsa
E39
Heimdal
Melhus
Klæbu
Ertvågsøya
Vinjeøra
Ruten
1039



Technology for a better society



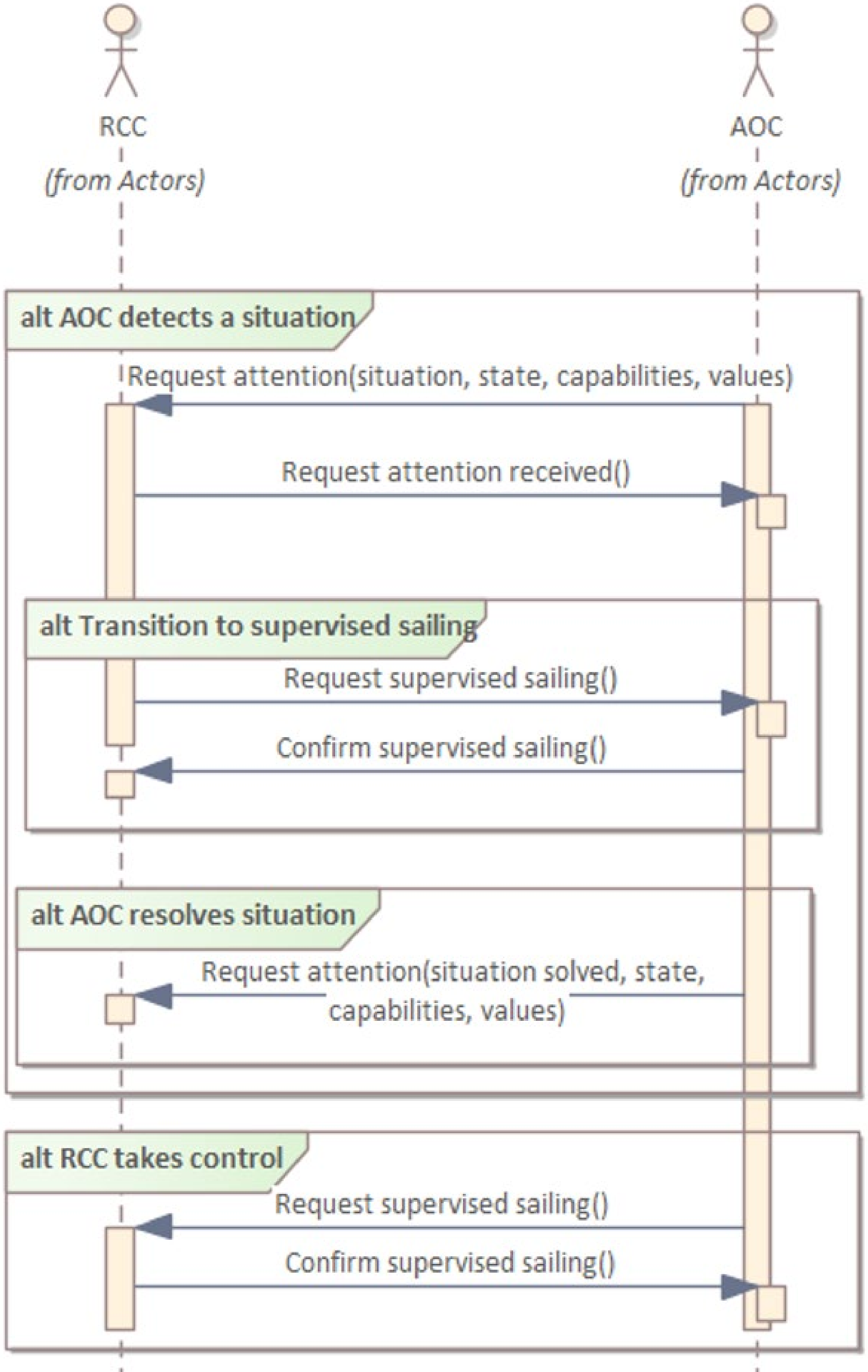
Used to avoid screening of illegal goods or falsify manifests.

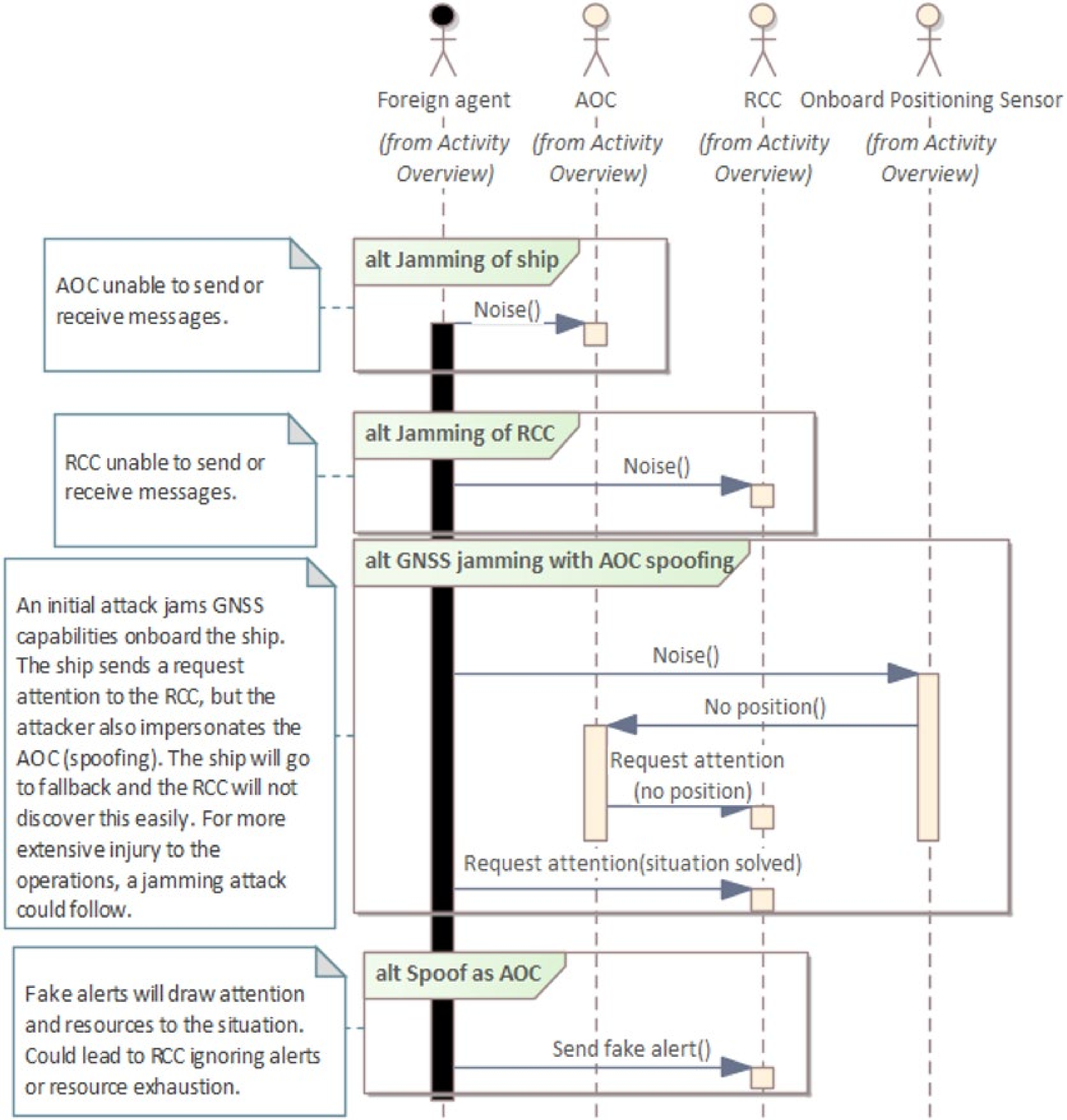
Typically ransomware attacks or general extortion.

E.g., linked to identification of valuable goods that will be targeted for theft.

Attempts to sabotage physical assets and port operations.

society


RCC
(from Actors)
AOC
(from Actors)
alt AOC detects a situation
Request attention(situation, state, capabilities, values)
Request attention received()
alt Transition to supervised sailing
Request supervised sailing()
Confirm supervised sailing()
alt AOC resolves situation
Request attention(situation solved, state, capabilities, values)
alt RCC takes control
Request supervised sailing()
Confirm supervised sailing()



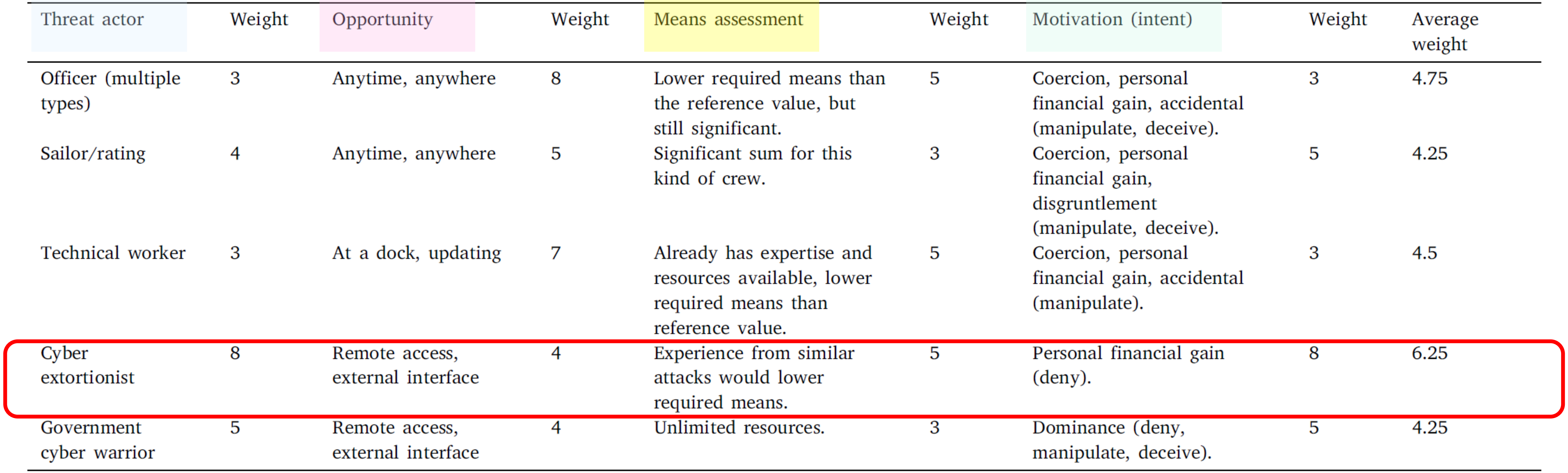
AOC unable to send or receive messages.

RCC unable to send or receive messages.

An initial attack jams GNSS capabilities onboard the ship. The ship sends a request attention to the RCC, but the attacker also impersonates the AOC (spoofing). The ship will go to fallback and the RCC will not discover this easily. For more extensive injury to the operations, a jamming attack could follow.

Fake alerts will draw attention and resources to the situation. Could lead to RCC ignoring alerts or resource exhaustion.

Summary of threats



Threat actor	Weight	Opportunity	Weight	Means assessment	Weight	Motivation (intent)	Weight	Average weight
Officer (multiple types)	3	Anytime, anywhere	8	Lower required means than the reference value, but still significant.	5	Coercion, personal financial gain, accidental (manipulate, deceive).	3	4.75
Sailor/rating	4	Anytime, anywhere	5	Significant sum for this kind of crew.	3	Coercion, personal financial gain, disgruntlement (manipulate, deceive).	5	4.25
Technical worker	3	At a dock, updating	7	Already has expertise and resources available, lower required means than reference value.	5	Coercion, personal financial gain, accidental (manipulate).	3	4.5
Cyber extortionist	8	Remote access, external interface	4	Experience from similar attacks would lower required means.	5	Personal financial gain (deny).	8	6.25
Government cyber warrior	5	Remote access, external interface	4	Unlimited resources.	3	Dominance (deny, manipulate, deceive).	5	4.25

Threat modeling essentials

- What are you building?
- What can go wrong?
- What should you do about those things that can go wrong?
- Did you do a decent job of analysis?

Threat modeling manifesto (2020)

SINTEF

Technology for a better society

CyberSecPro

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them. Project Agreement no. 101083594