

GraMSec 2017, Santa Barbara, CA:

VISUALIZING CYBER SECURITY RISKS WITH BOW-TIE DIAGRAMS

SINTEF Digital: Karin Bernsmed, Christian Frøystad, **Per Håkon Meland**

SINTEF OCEAN: Dag Atle Nesheim, Ørnulf Jan Rødseth



Image Courtesy: Port of Los Angeles

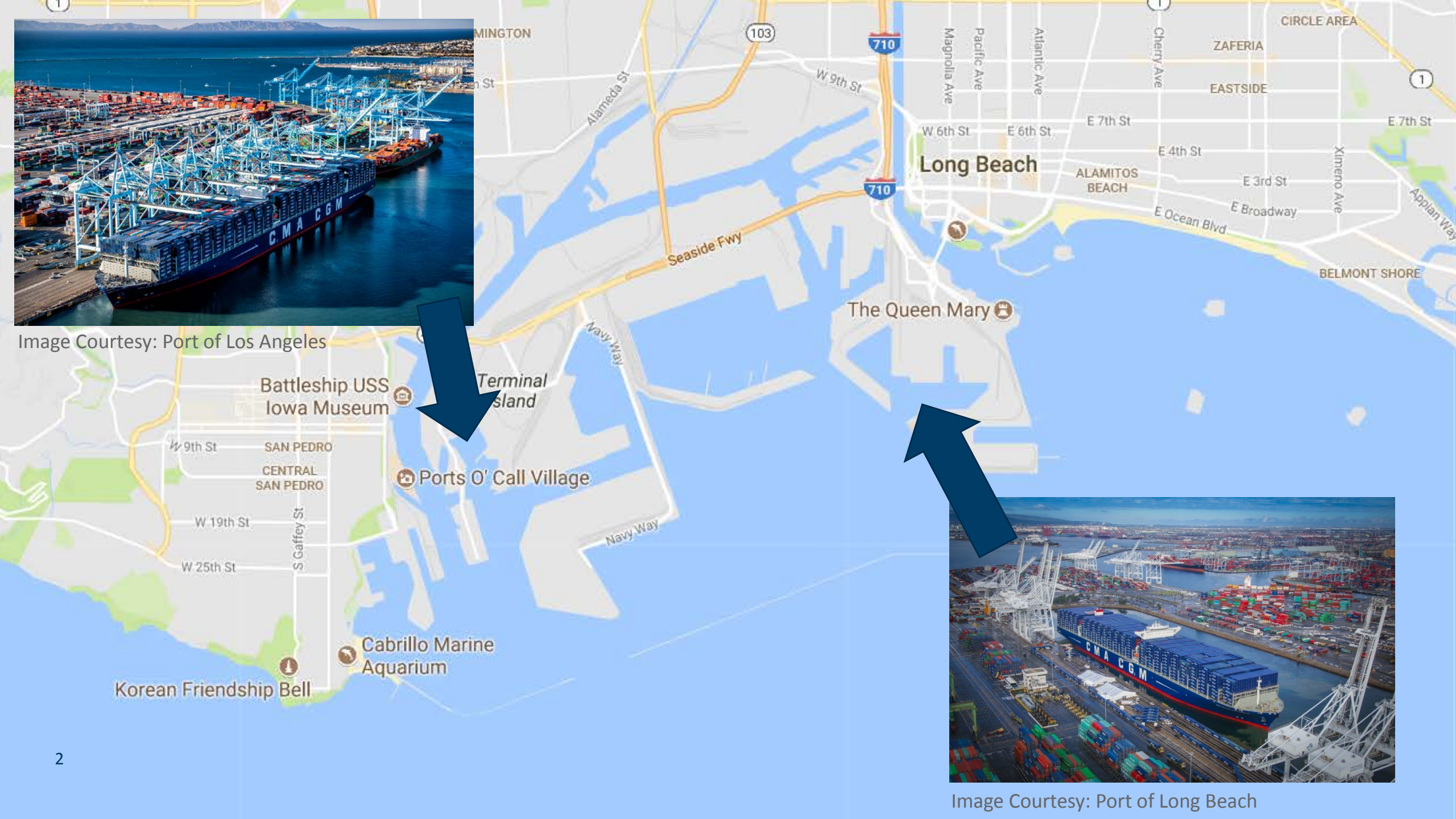
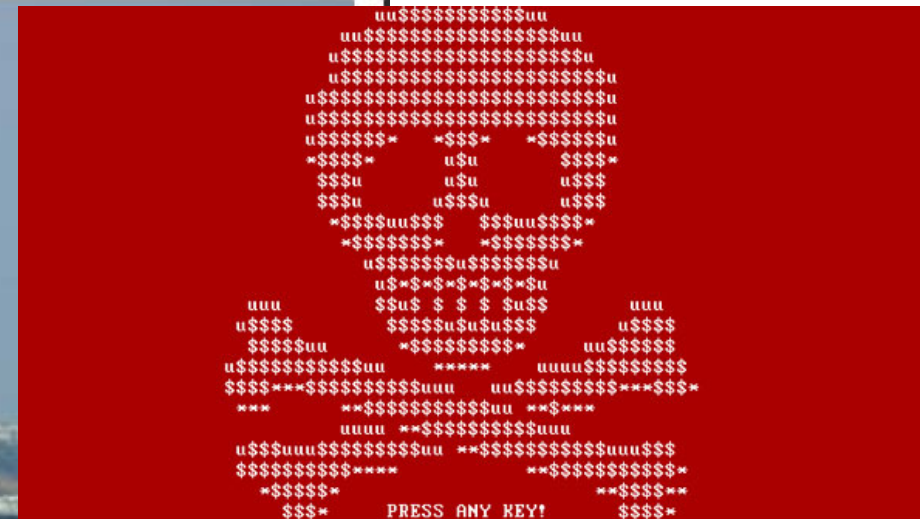


Image Courtesy: Port of Long Beach





[Home](#) / [Region](#) / [Europe](#)

Maersk hit by giant cyber attack

 JUNE 28TH, 2017

 SAM CHAMBERS

 EUROPE, TECH

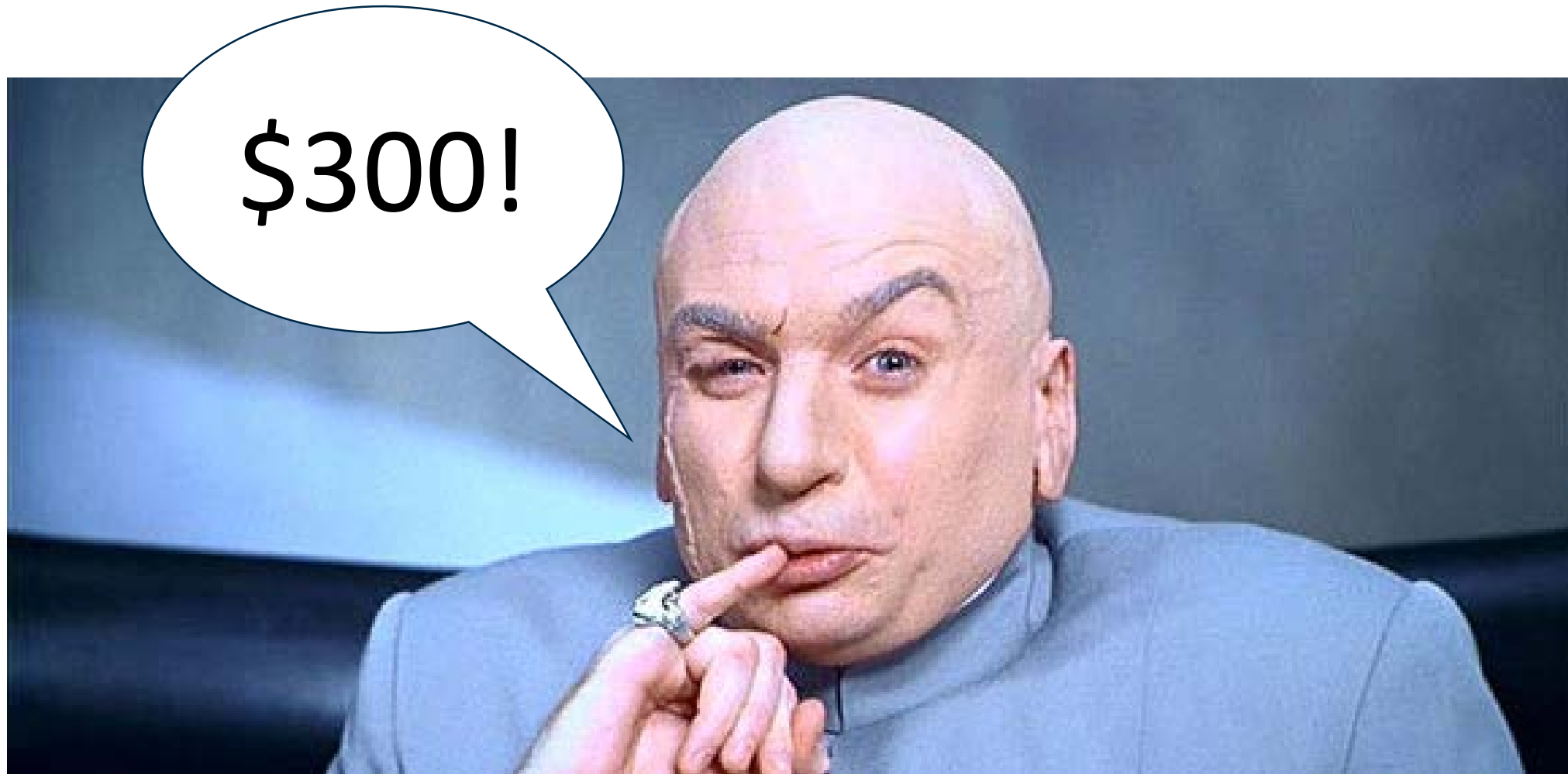
 0 COMMENTS

Tuesday's massive ransomware attack which spread across the world claimed a big shipping scalp in the form of Danish shipping giant AP Moller-Maersk. The cyber attack caused outages of Maersk's computer systems across the world.

"We can confirm that Maersk IT systems are down across multiple sites and business units due to a cyber attack," Maersk said on Twitter.

The breakdown affected all business units at Maersk, including container shipping, port and tug boat operations, oil and gas production, drilling services, and tankers.

It marks the most high profile victim yet of a cyber attack in shipping.





Home / Sector / Containers

Maersk still not back to normal three weeks on from Petya attack

 JULY 18TH, 2017



SAM CHAMBERS

 CONTAINERS, EUROPE, PORTS AND LOGISTICS, TECH

 0 COMMENTS

Three weeks on from the day Maersk was [hit hard by the Petya ransomware](#) and business is still not 100% back to normal.



"awareness on cyber security needs and challenges in the maritime sector is currently low to non-existent"

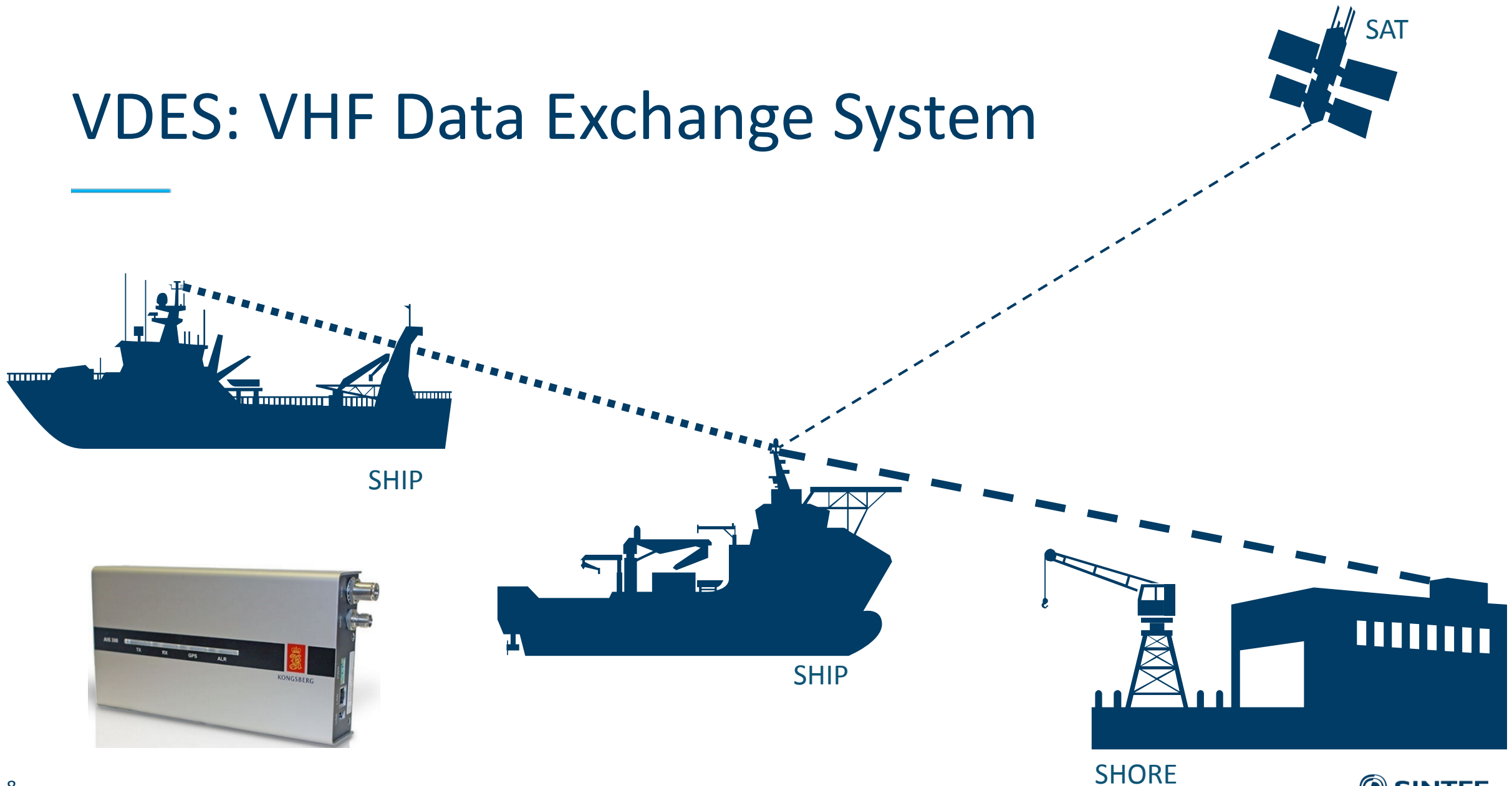


"Maritime is way behind the curve in standards on cyber security"

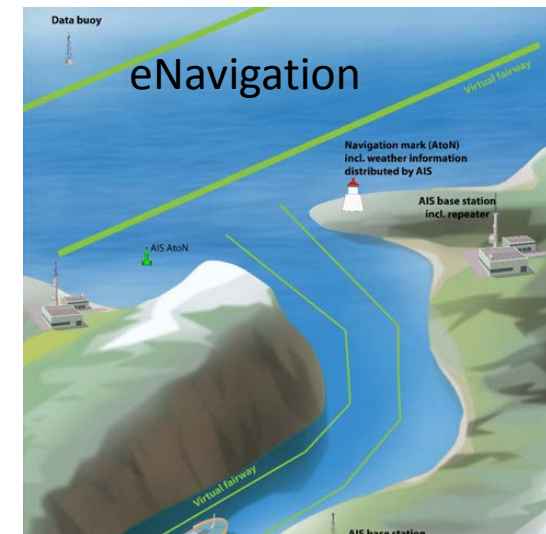


"the soft underbelly of the maritime industry is its reliance on Information and Communication Technology"

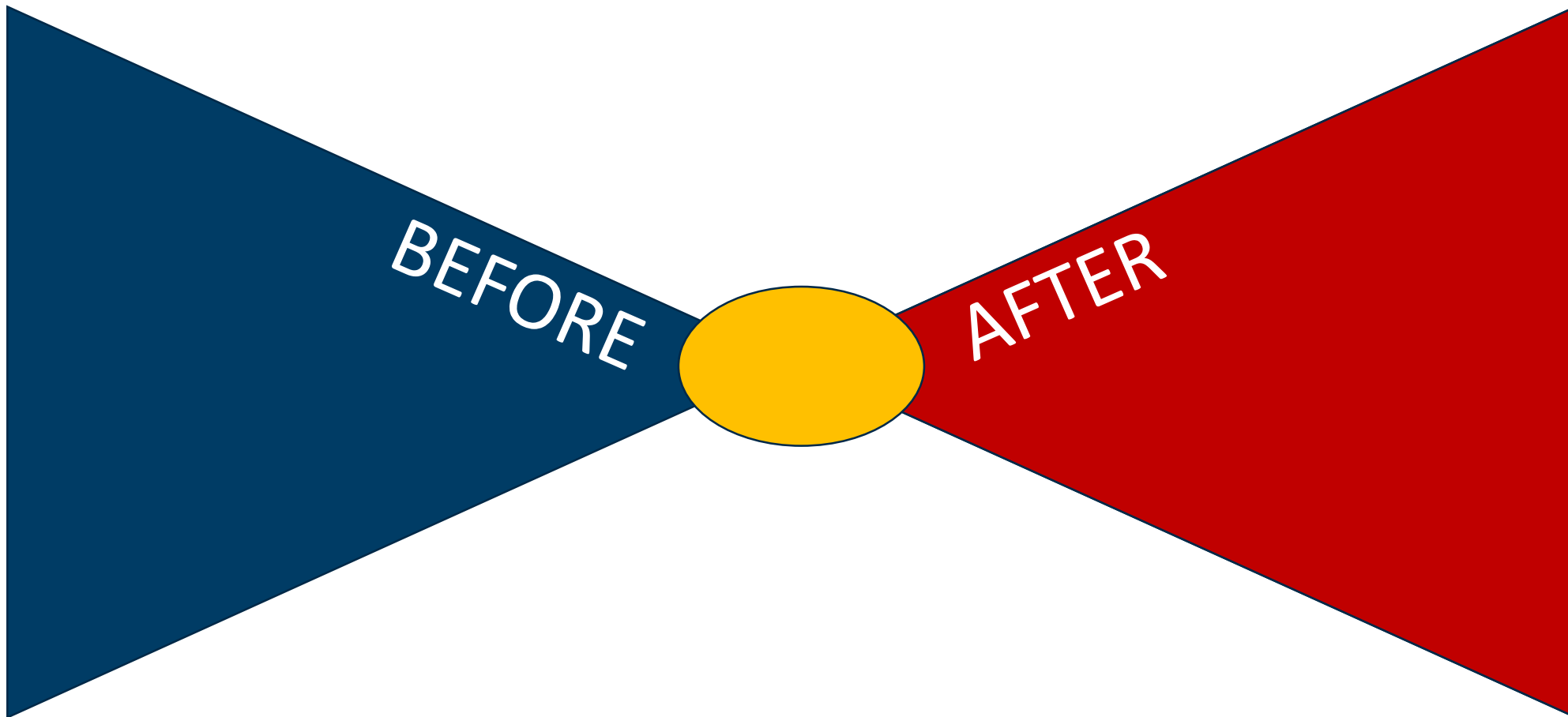
VDES: VHF Data Exchange System



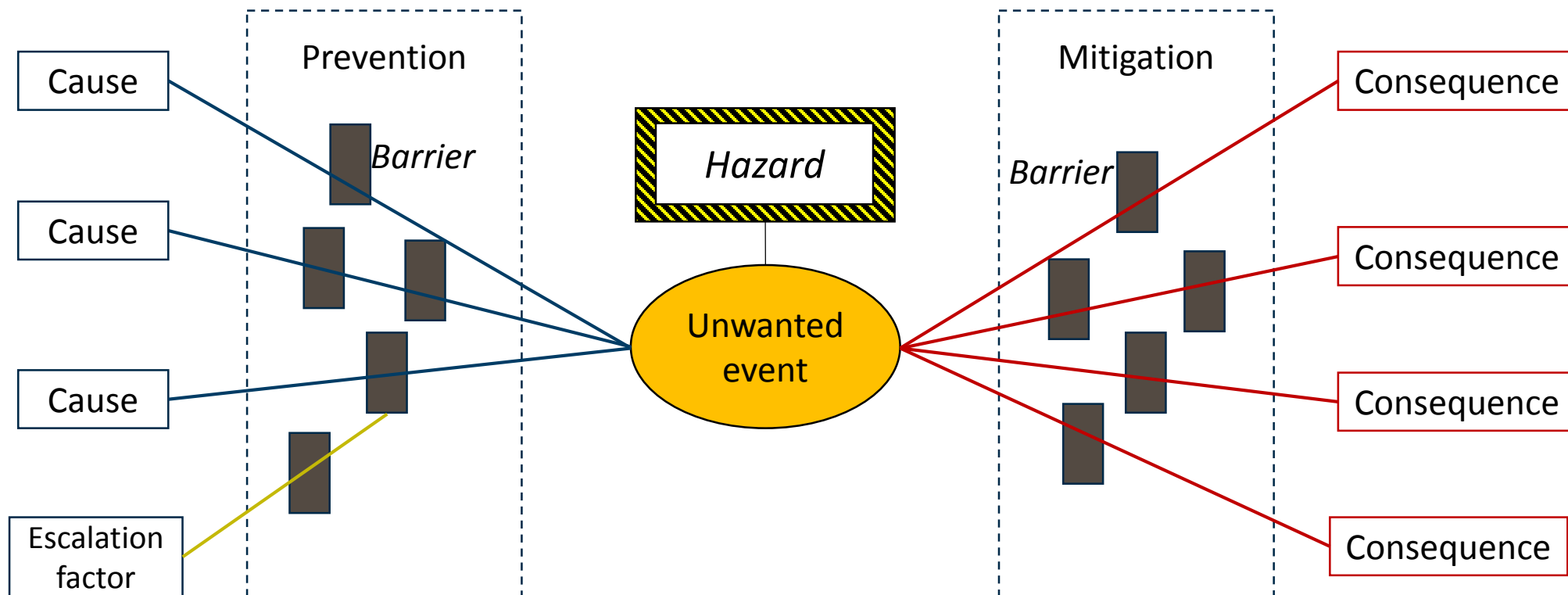
Why do we need VDES?

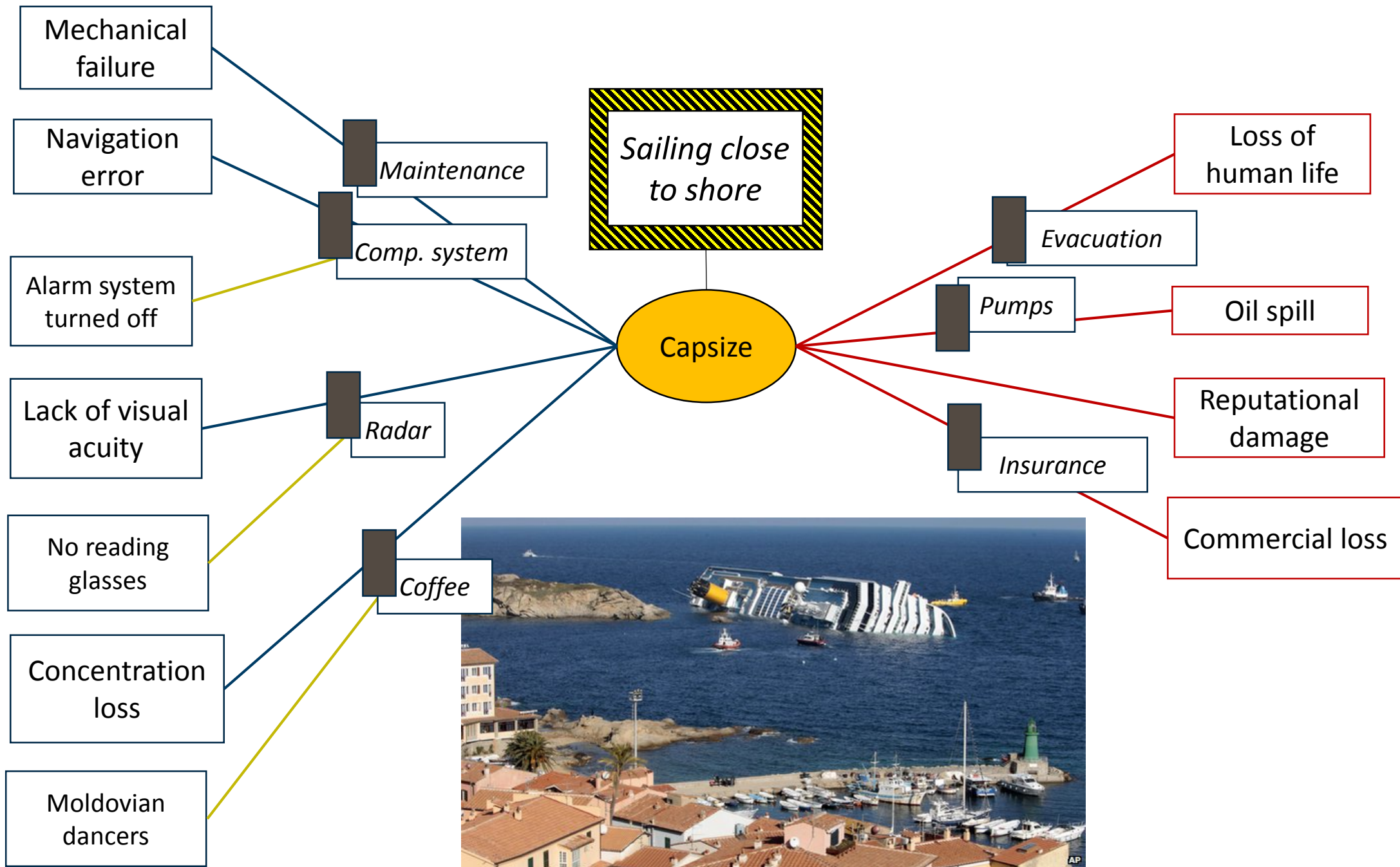


Bow-tie diagram

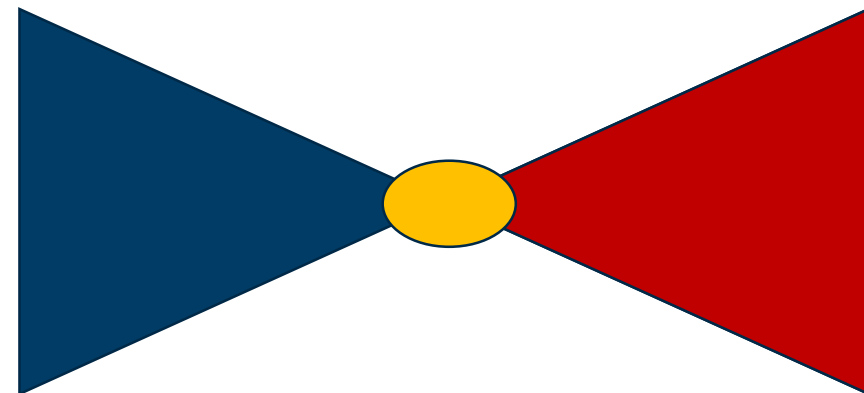


Bow-tie diagram






Research Questions

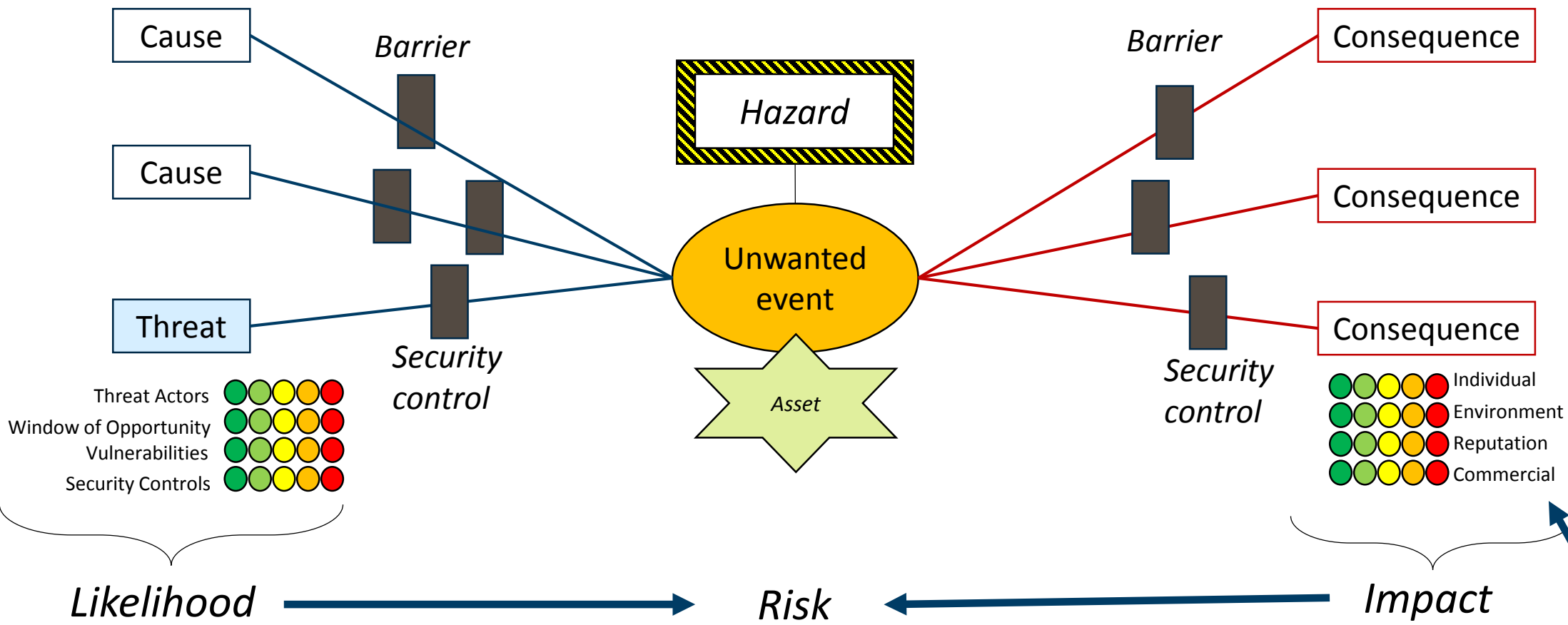


1. How can bow-tie diagrams be extended to include security considerations in addition to safety considerations?
2. How can the likelihood of cause and severity of cyber attacks be visualized in bow-tie diagrams?



			Likelihood				
	Qualitative descriptors		Never	Extremely rare	Rare	Frequent	Always
		Quantitative scales	0.0001	0.001	0.01	0.1	1
Consequence	Catastrophic	\$50 000 k					
	Critical	\$ 5 000 k					
	Moderate	\$ 500k					
	Negligible	\$ 5 k					
	None	\$ 1					

Extensions



$$R(U) \approx p(U) \times L_C \times p(C)$$

		Likelihood				
Consequence	Qualitative descriptors	Never	Extremely rare	Rare	Frequent	Always
	Quantitative scales	0.0001	0.001	0.01	0.1	1
	Catastrophic \$50,000k					
	Critical \$5,000k					
	Moderate \$500k					
	Negligible \$5k					
	None \$1					

Threat actors

Dangerousness	Description	Color coding
<i>Severe</i>	There are threat actors highly capable of pursuing this threat	
<i>High</i>	There are threat actors capable of pursuing this threat	
<i>Moderate</i>	There are threat actors somewhat capable of pursuing this threat	
<i>Low</i>	There are threat actors interested in pursuing this threat, but their capability is limited	
<i>None</i>	There are threat actors interested in pursuing this threat, but they are not capable of acting on this interest	

Window of opportunity

Window	Description	Color coding
<i>Always</i>	This threat is always possible.	
<i>Frequent</i>	This threat is frequently possible (there will be an opportunity about once every week).	
<i>Rare</i>	This threat is rarely possible (there will be an opportunity about once every year).	
<i>Extremely rare</i>	This threat is extremely rarely possible (there will be an opportunity about once every 10th year).	
<i>Never</i>	This threat is never possible.	

Vulnerabilities

Vulnerability	Description	Color coding
<i>Known easy</i>	One or more known vulnerabilities exist, which are easy to exploit.	
<i>Known-difficult</i>	One or more known vulnerabilities exist, but they are either not publicly known, or they are difficult to exploit.	
<i>Unknown</i>	No known vulnerabilities exist, however, vulnerabilities are expected to appear in the near future.	
<i>Very unlikely</i>	It is very unlikely that the system has, or will have, any vulnerabilities in the near future.	
<i>Formally proven absence</i>	Formal methods, or the like, have been applied to demonstrate that no vulnerabilities exist. It is extremely unlikely that vulnerabilities will appear in the near future.	

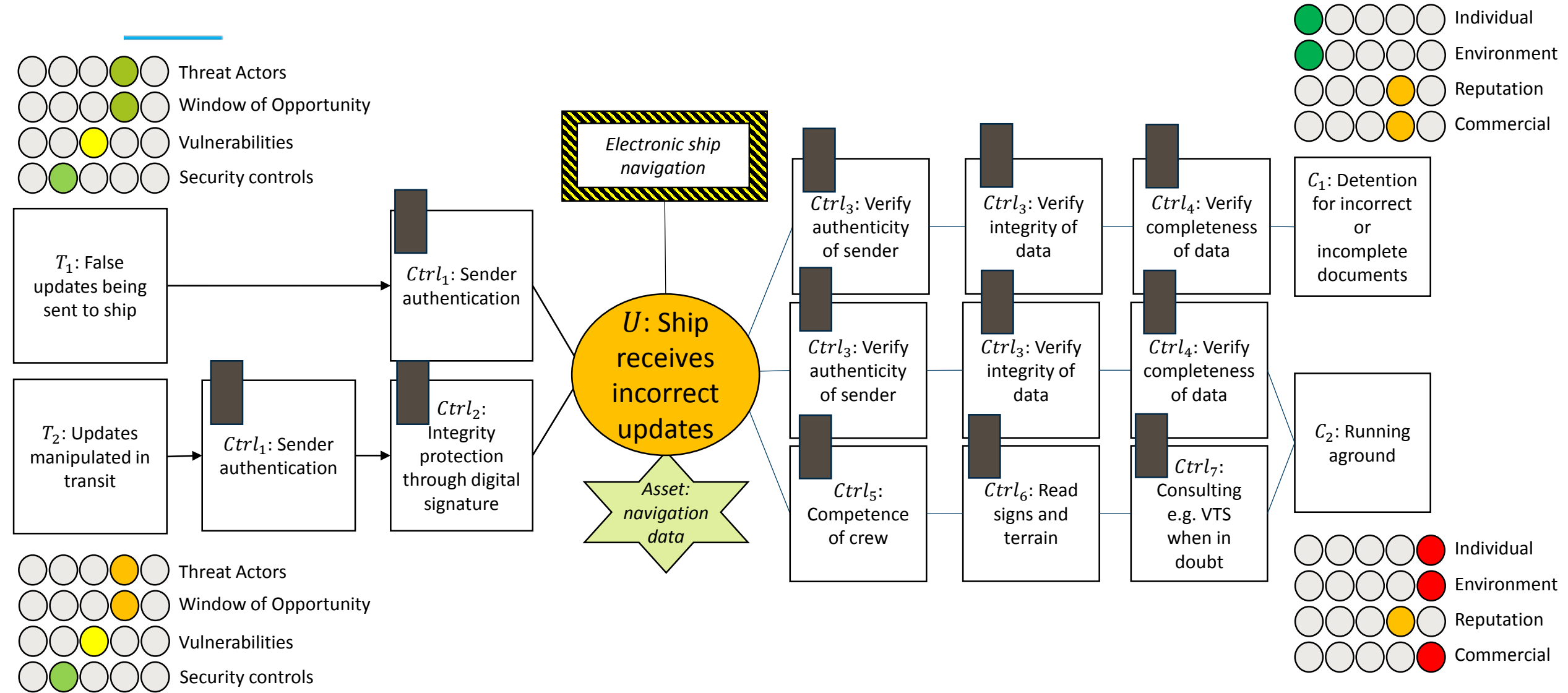
Security controls

Control	Description	Color coding
<i>Known to be ineffective</i>	No security countermeasure exists, or, one or more security countermeasures exists but they are known to be ineffective.	
<i>Probably not effective</i>	One or more security countermeasures exists but they can be circumvented.	
<i>Effective</i>	One or more security countermeasures exists, which are believed to be effective.	
<i>Very effective</i>	One or more security countermeasures exists, which are very effective.	
<i>Formally proven effective</i>	Formal methods, or the like, have been applied to demonstrate that existing security mechanisms are sufficient and work as intended.	

Consequences

Level	Individual	Environment	Reputation	Commercial	Color coding
<i>Catastrophic</i>	Multiple deaths	Uncontained release with potential for very large environmental impact	International coverage, unrecoverable damage	\$ 50 000 k	
<i>Critical</i>	One death	Uncontained release with potential for major environmental impact	National and some international coverage, impact lasting more than a year	\$ 5 000 k	
<i>Moderate</i>	Multiple severe injuries	Uncontained release with potential for moderate environmental impact	National media coverage, impact lasting more than 3 months	\$ 500 k	
<i>Negligible</i>	One minor injury	On site release contained without external assistance	Local complaint/ recognition, impact less than one month	\$ 5 k	
<i>None</i>	No injuries	No effect	No damage	\$ 1 k or less	

Use case example



Final remarks

- Scenario based analysis proves that:
 - security concepts can be contained within bow-ties (RQ1)
 - RMA-inspired indicators work well to visualize likelihood (RQ2)
- High level overview of causes, consequences, barriers
 - more suitable to put details in other types of diagrams

