EUROPEAN
COAST GUARD
FUNCTIONS
FORUM

Maritime Cybersecurity

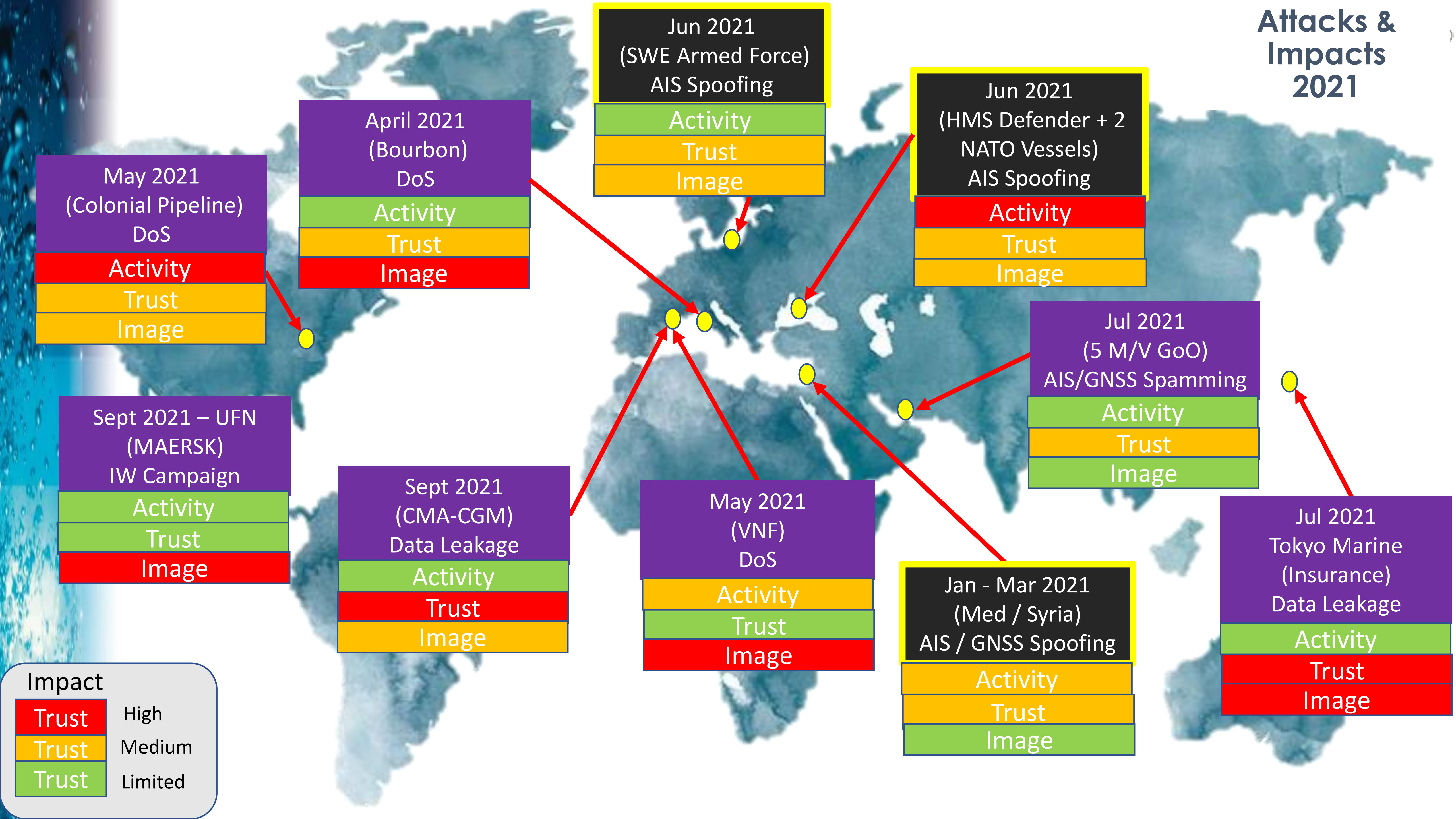
ECGFF Cybersecurity Working group – 2021

Webinar Cyber-Security challenges and future perspectives

18th January 2022

The ECGFF Cybersecurity Working Group

Attacks & Impacts 2021



May 2021
(Colonial Pipeline)
DoS
- 🟥 Activity
- 🟧 Trust
- 🟧 Image

April 2021
(Bourbon)
DoS
- 🟩 Activity
- 🟧 Trust
- 🟥 Image

Jun 2021
(SWE Armed Force)
AIS Spoofing
- 🟩 Activity
- 🟧 Trust
- 🟧 Image

Jun 2021
(HMS Defender + 2 NATO Vessels)
AIS Spoofing
- 🟥 Activity
- 🟧 Trust
- 🟧 Image

Jul 2021
(5 M/V GoO)
AIS/GNSS Spamming
- 🟩 Activity
- 🟧 Trust
- 🟩 Image

Sept 2021 – UFN
(MAERSK)
IW Campaign
- 🟩 Activity
- 🟩 Trust
- 🟥 Image

Sept 2021
(CMA-CGM)
Data Leakage
- 🟩 Activity
- 🟥 Trust
- 🟧 Image

May 2021
(VNF)
DoS
- 🟧 Activity
- 🟩 Trust
- 🟥 Image

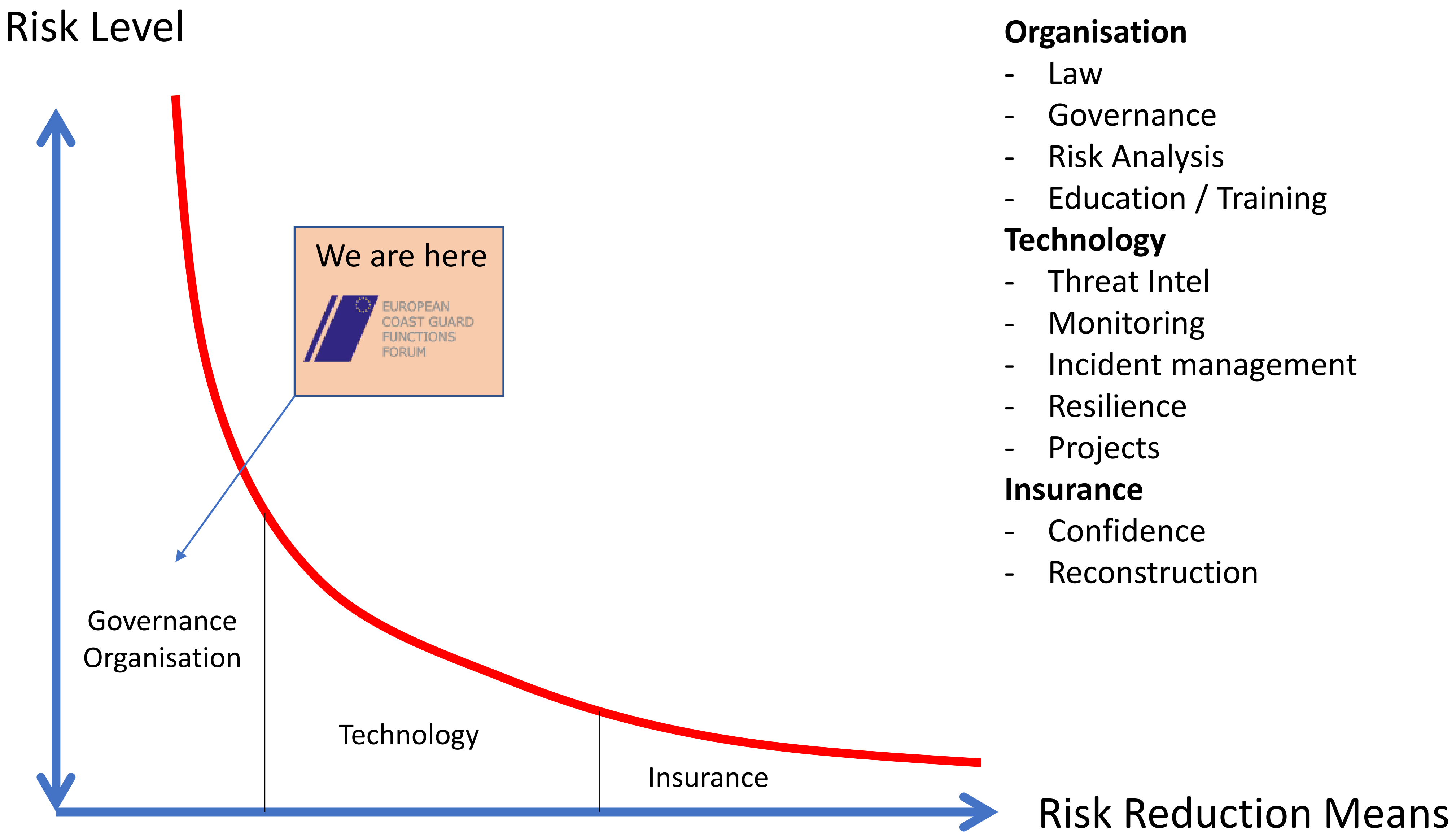
Jan - Mar 2021
(Med / Syria)
AIS / GNSS Spoofing
- 🟧 Activity
- 🟧 Trust
- 🟩 Image

Jul 2021
Tokyo Marine
(Insurance)
Data Leakage
- 🟩 Activity
- 🟥 Trust
- 🟥 Image

Impact

🟥 Trust	High
🟧 Trust	Medium
🟩 Trust	Limited

The Cybersecurity Risk reduction



Organisation
- Law
- Governance
- Risk Analysis
- Education / Training

Technology
- Threat Intel
- Monitoring
- Incident management
- Resilience
- Projects

Insurance
- Confidence
- Reconstruction

EU Coastguard Cybersecurity Working Group”

Achievements - The continuation of the current efforts

Build on the initiative of the ECGFF workshops on "Cyber Attack Prevention in the Maritime Domain" initiated by the German presidency, and implementing a "EU Coastguard Cybersecurity Working Group".

Need to furthermore develop common approach of cyber-security for the coastguard community. For that, the legal, organizational and technical understanding shall be further developed together improving the cross-sectoral and cross-border cooperation, elaborating guidelines and best management practice to this end.

Animation of the coastguard cybersecurity community and implementation of an information sharing platform dedicated to cybersecurity and hosted by EMSA.

Consensual validation of the "EU Coastguard Cybersecurity Working Group" terms of reference addressed to the EU Commission.

Support for further improvements on information-sharing processes for timely information exchange on cyber-attacks and incidents targeting the maritime community.

Continuation during the Croatian Chairmanship of the ECGFF (2019-2020).

ECGFF Achievements - Action Plan

Action 1: Certification /classification:

Action 2: Information sharing & risk analysis : ☑

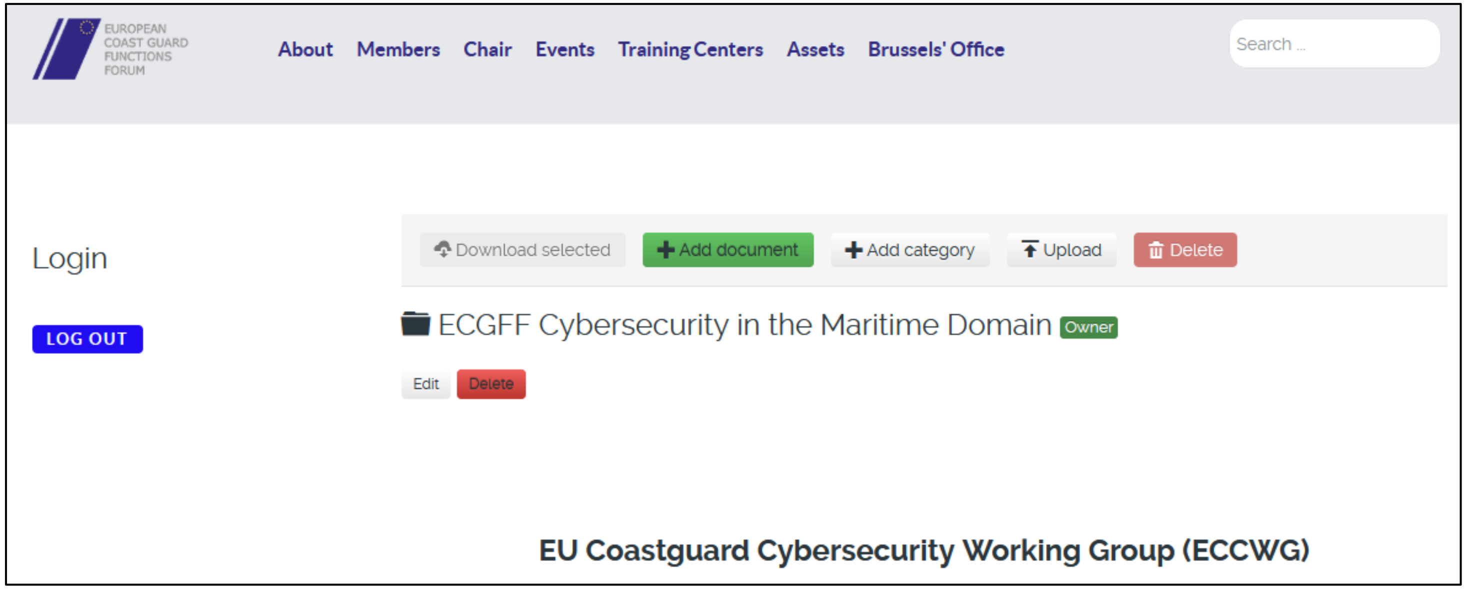
Action 3: Terms of Reference and Information sharing portal : ☑

Action 4: Development of Spoofing / jamming detection ☑

Action 5: IT Security Concept

Action 6: Criminal aspects on Cyber Security for Coast Guards

https://ecgff.emsa.europa.eu/cyprev



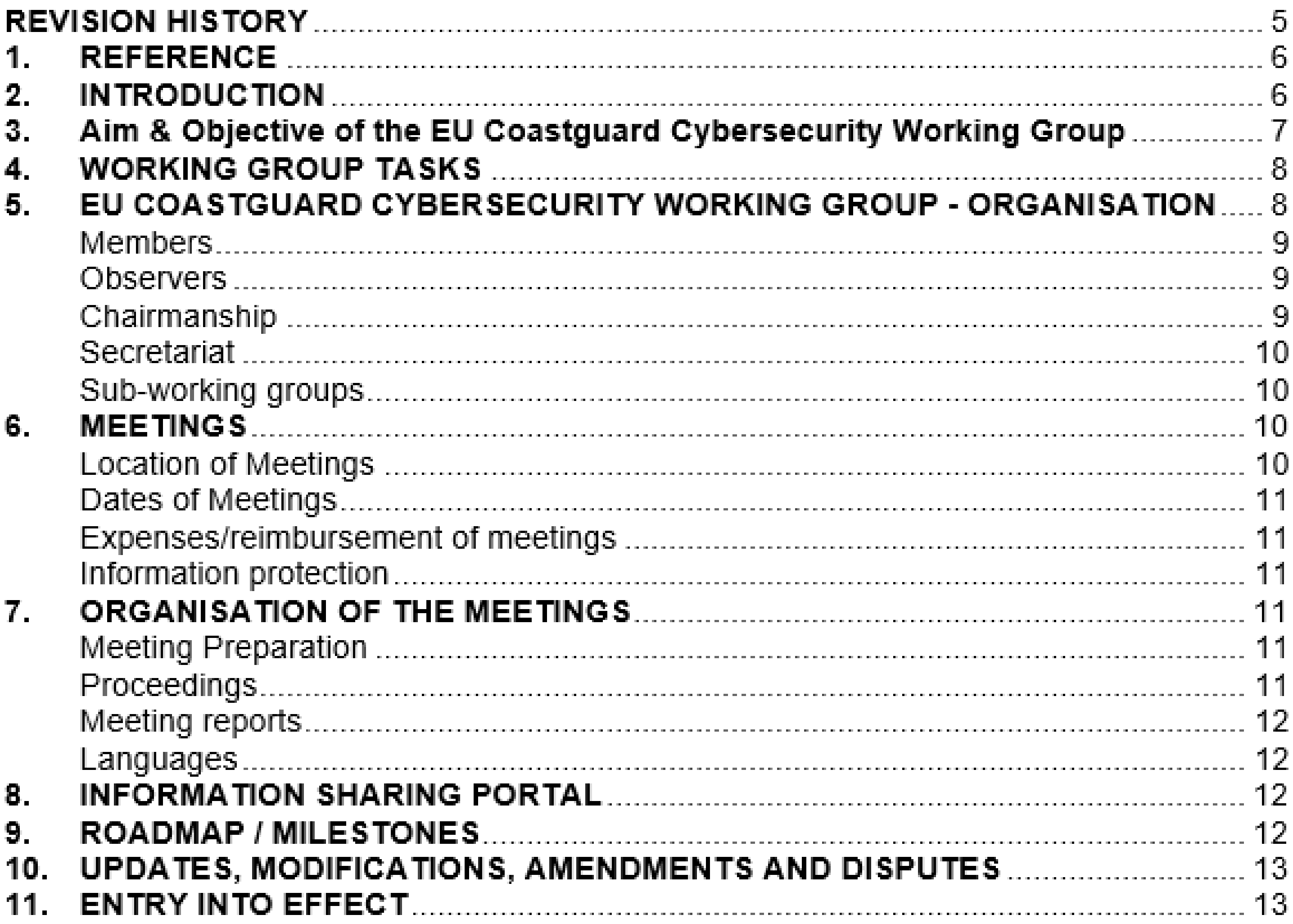
ECGFF Cybersecurity in the Maritime Domain

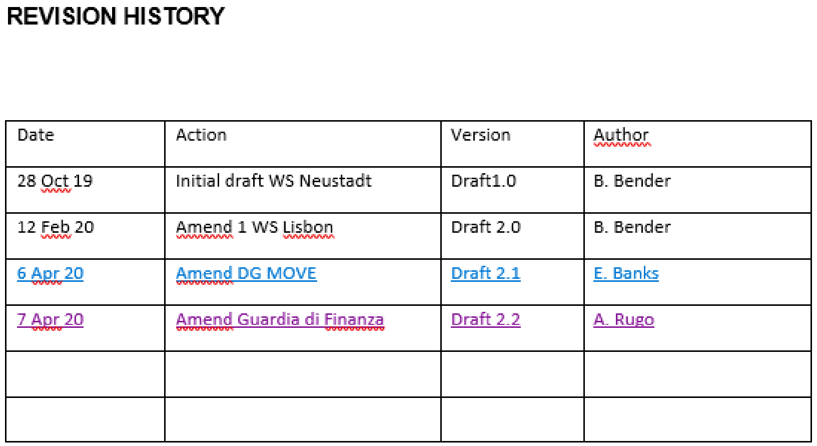
EU Coastguard Cybersecurity Working Group (ECCWG)

TERMS OF REFERENCE

ECGFF Working group

EUROPEAN COAST GUARD FUNCTIONS FORUM



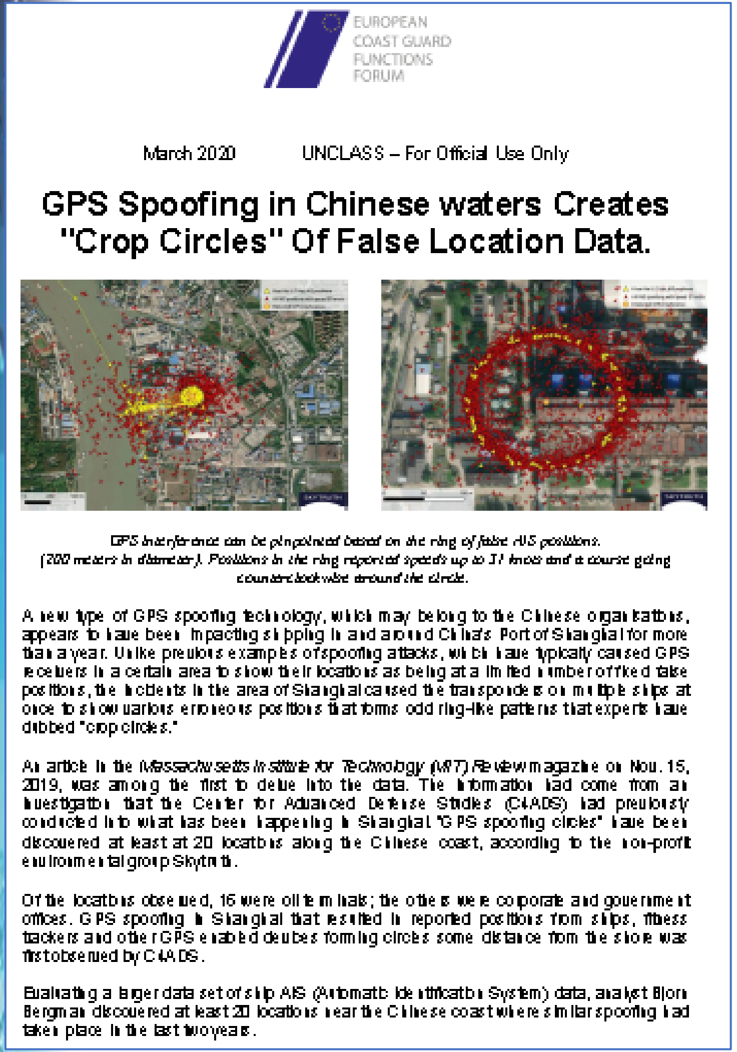


REVISION HISTORY

Date	Action	Version	Author
28 Oct 19	Initial draft WS Neustadt	Draft1.0	B. Bender
12 Feb 20	Amend 1 WS Lisbon	Draft 2.0	B. Bender
6 Apr 20	Amend DG MOVE	Draft 2.1	E. Banks
7 Apr 20	Amend Guardia di Finanza	Draft 2.2	A. Rugo

Actions conducted: Cybersecurity information letter

EUROPEAN COAST GUARD FUNCTIONS FORUM



EUROPEAN COAST GUARD FUNCTIONS FORUM

March 2020 UNCLASS – For Official Use Only

GPS Spoofing in Chinese waters Creates "Crop Circles" Of False Location Data.

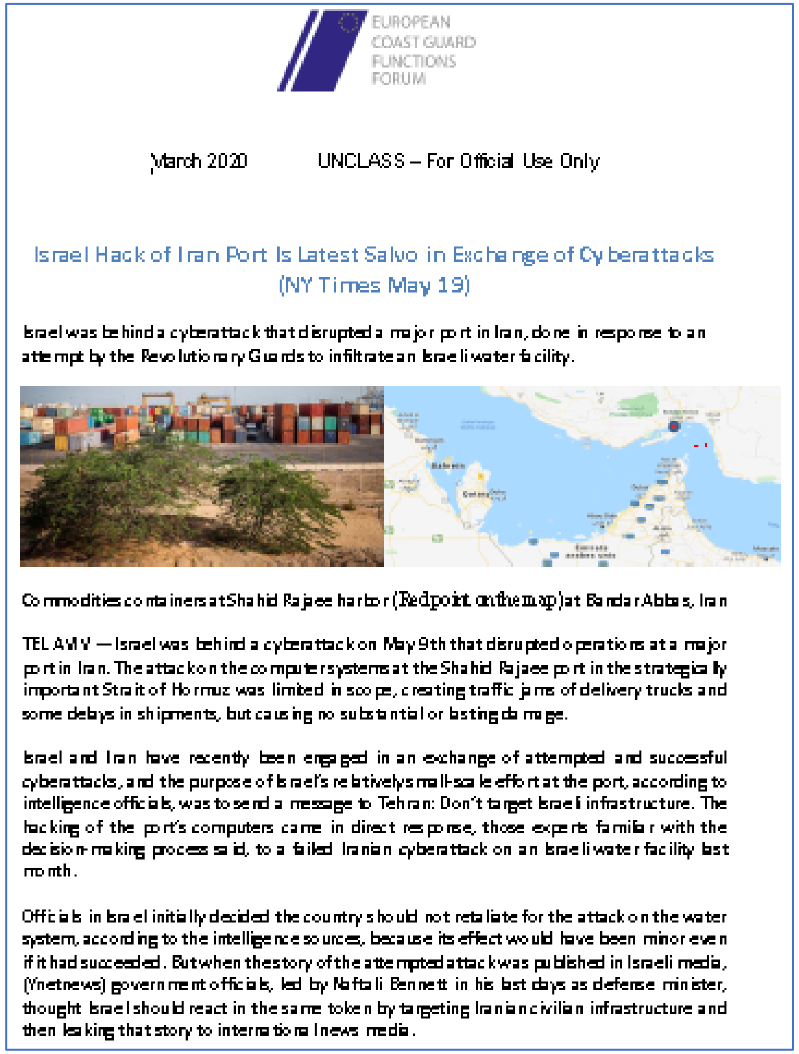
GPS interference can be pinpointed based on the ring of false AIS positions. (200 meters in diameter). Positions in the ring reported speeds up to 31 knots and a course going counterclockwise around the circle.

A new type of GPS spoofing technology, which may belong to the Chinese organizations, appears to have been impacting shipping in and around China's Port of Shanghai for more than a year. Unlike previous examples of spoofing attacks, which have typically caused GPS receivers in a certain area to show their locations as being at a limited number of fixed false positions, the incidents in the area of Shanghai caused the transponders on multiple ships at once to show various erroneous positions that forms odd ring-like patterns that experts have dubbed "crop circles."

An article in the *Massachusetts Institute for Technology (MIT) Review* magazine on Nov. 15, 2019, was among the first to delve into the data. The information had come from an investigation that the Center for Advanced Defense Studies (C4ADS) had previously conducted into what has been happening in Shanghai. "GPS spoofing circles" have been discovered at least at 20 locations along the Chinese coast, according to the non-profit environmental group Skytruth.

Of the locations observed, 16 were oil terminals; the others were corporate and government offices. GPS spoofing in Shanghai that resulted in reported positions from ships, fitness trackers and other GPS enabled devices forming circles some distance from the shore was first observed by C4ADS.

Evaluating a larger data set of ship AIS (Automatic Identification System) data, analyst Bjorn Bergman discovered at least 20 locations near the Chinese coast where similar spoofing had taken place in the last two years.



EUROPEAN COAST GUARD FUNCTIONS FORUM

March 2020 UNCLASS – For Official Use Only

Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks (NY Times May 19)

Israel was behind a cyberattack that disrupted a major port in Iran, done in response to an attempt by the Revolutionary Guards to infiltrate an Israeli water facility.

Commodities containers at Shahid Rajaee harbor (Red point on the map) at Bandar Abbas, Iran

TEL AVIV — Israel was behind a cyberattack on May 9th that disrupted operations at a major port in Iran. The attack on the computer systems at the Shahid Rajaee port in the strategically important Strait of Hormuz was limited in scope, creating traffic jams of delivery trucks and some delays in shipments, but causing no substantial or lasting damage.

Israel and Iran have recently been engaged in an exchange of attempted and successful cyberattacks, and the purpose of Israel's relatively small-scale effort at the port, according to intelligence officials, was to send a message to Tehran: Don't target Israeli infrastructure. The hacking of the port's computers came in direct response, those experts familiar with the decision-making process said, to a failed Iranian cyberattack on an Israeli water facility last month.

Officials in Israel initially decided the country should not retaliate for the attack on the water system, according to the intelligence sources, because its effect would have been minor even if it had succeeded. But when the story of the attempted attack was published in Israeli media, (Ynetnews) government officials, led by Naftali Bennett in his last days as defense minister, thought Israel should react in the same token by targeting Iranian civilian infrastructure and then leaking that story to international news media.

EUROPEAN COAST GUARD FUNCTIONS FORUM

UNCLASS - For Official Use Only

CYBERSECURITY Information letter for the maritime

Nmr 1 / 2021 – March 2021

The end of 2020 raised major cyber attacks that no longer spare the major cybersecurity communities. The maritime domain has also seen a significant increase in the number of attacks. A large-scale communications operation in the field was launched by an Israeli operator in the first half of the year, which would tend to confirm the particularly appropriate cybersecurity adage that "noise does not do good and good does not make noise".

The new EU cybersecurity strategy issued by the Commission last week marks the absolute need for all sectors and member States to coordinate their action for greater efficiency.

Maritime news

GEFCO logistic operator suffers major Cyber-attack.

On September 22, 2020, GEFCO was the target of an external cyber-attack. According to its president the attack could have endangered its global activity. Operations in the warehouses, sites and transportation services were disconnected from their systems and the operator's internal network were out of order. The implementation of alternative processes to ensure the continuity of its activities was necessary. Crisis communication in relation to customers during this attack was developed by the company. Several days of work with IT providers and public actors were needed to rebuild the commercial applications affected by the attack.

CMA CGM group victim of Ragnar-Locker ransomware

After MAERSK in 2017, and MSC in April 2020, September the 28th, 2020, CMA CGM reported on the social network Twitter that it was the victim of a major cyberattack on its operational CRM (Customer Relationship Management) System. The technical teams of the French company were mobilized in connection with several public and private actors, speclists of cybersecurity, in order to prevent any lateralization of the attack. CMA-CGM was significantly impacted for activity with its customers for several days without ever severing the relationship with them.
The ransomware source of the attack was known. It was "Ragnar Locker", known for compromising "Carlson Wagon lit Travel" two months earlier. The modus-operandi was also identified as an increasing risk for operators by the French Cybersecurity agency (ANSSI), which has put online a special guide dedicated to the ransomware threat.
Guide on the specific Ransomware threat: https://www.ssi.gouv.fr/tag/ransomware/
(In French)

International Maritime Organization targeted by cyberattack

The UN International Maritime Organization (IMO) has admitted to having suffered a "sophisticated cyberattack" on its information systems during the CoVid Pandemy. The incident was discovered on Thursday 1st of October 2020 and had an impact on the organization's public website and other online services, the UN agency said in a statement. The systems involved were disconnected and restored the next day. The type of attack is still officially unknown and IMO is reportedly investigating the source.
The unavailability of its services is the result of a large scale cyberattack and comes at a time when IMO is under pressure, trying to draw attention to the global Covid crew crisis and calling on member countries to enforce "IMO 2021," a resolution requiring shipowners to invest in cybersecurity measures.

Sources:

- EU CERT
- Member States

Letter Nmr 1 / 2021

Focus on AIS theats

Ship spoofing – AIS message is broadcast giving details of a non-existent ship. Scenarios where this could be used include spoofing a ship of one nation into the territorial waters of a hostile nation, leading that nation to take countermeasures. Alternatively, multiple versions of the details of a real ship can be broadcast, placing it in many different locations simultaneously to obscure its true location (e.g. illegal fishing).

Aid-to-navigation spoofing – Fake aid-to-navigation, such as a buoy warning of hidden shoals, are broadcast in order to force a ship to change its course. This might be done to force a vessel into a region where it can be hijacked.

Collision spoofing – Collision avoidance is one of the primary uses of AIS. By providing spoofed details of a vessel on a collision course, an attacker can force a ship to change course to avoid the anticipated collision. This could, for example, be used to steer the ship into a real collision

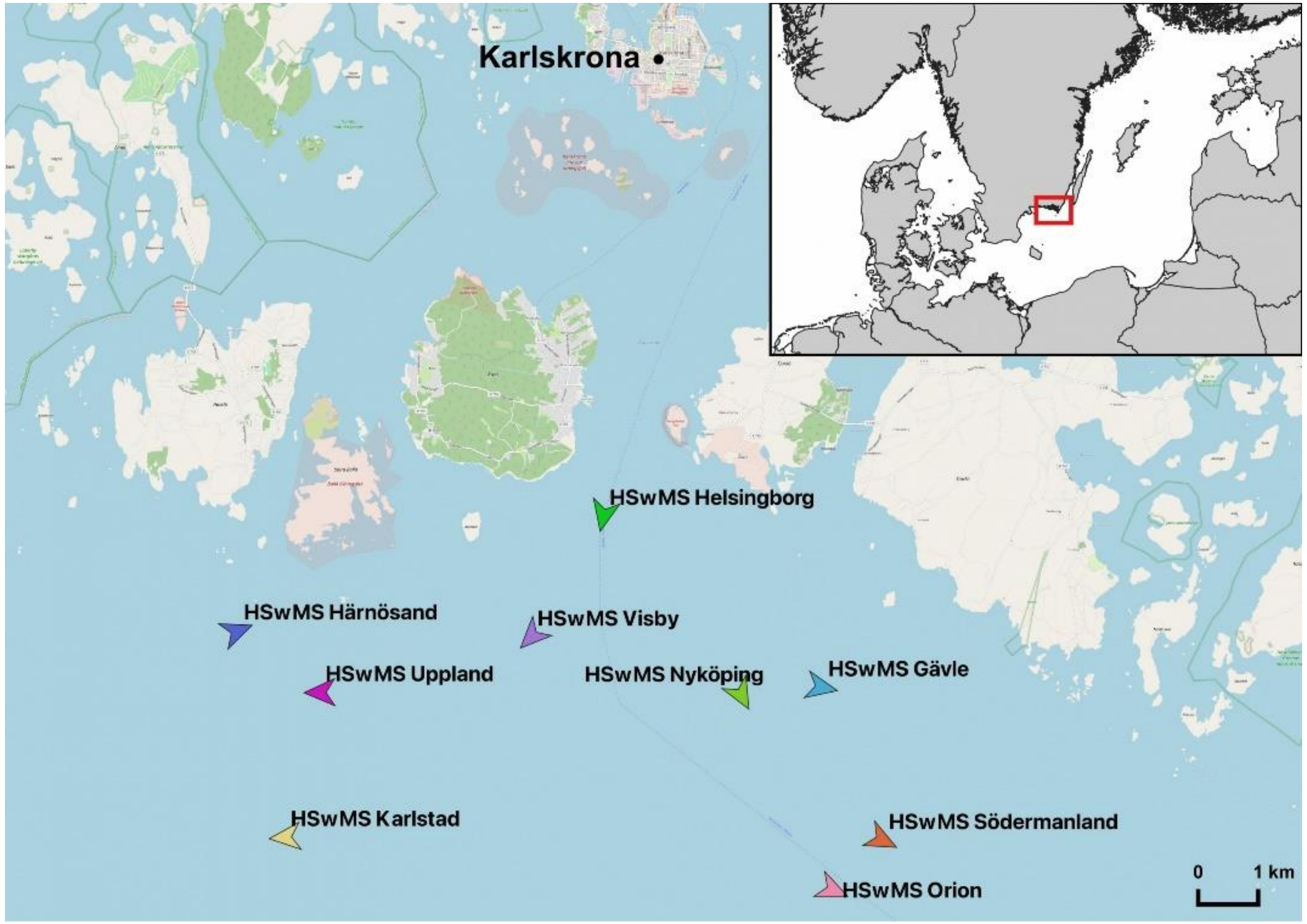
AIS-SART spoofing – Search & rescue is another of the primary uses of AIS. This attack generates a spoofed SAR-T transponder signal, which gives details of a distress. As ships are legally obliged to assist, SART spoofing can be used as a decoy to lure vessels to a location where they can be attacked.

Weather forecast spoofing – AIS can be used to relay information about prevailing weather conditions between marine craft. A fake forecast, particularly one that predicts fine conditions when a storm is incoming, could be used to lead vessels into difficulties.

AIS hijacking – It is also possible to override signals being sent by vessels, by broadcasting a higher-power signal at the same time and frequency. The attacker can then change some details of the original message, for example to suggest that the vessel has a nuclear cargo in an area where such cargoes are illegal.

AIS SPOOFING – Feb 2021

Swedish AIS Spoofing in the Baltic (Feb 21)



Modified AIS tracks appearing south of Karlskrona. Initially, these false positions seemed indistinguishable from legitimate AIS tracks and followed the AIS system's broadcast protocols.

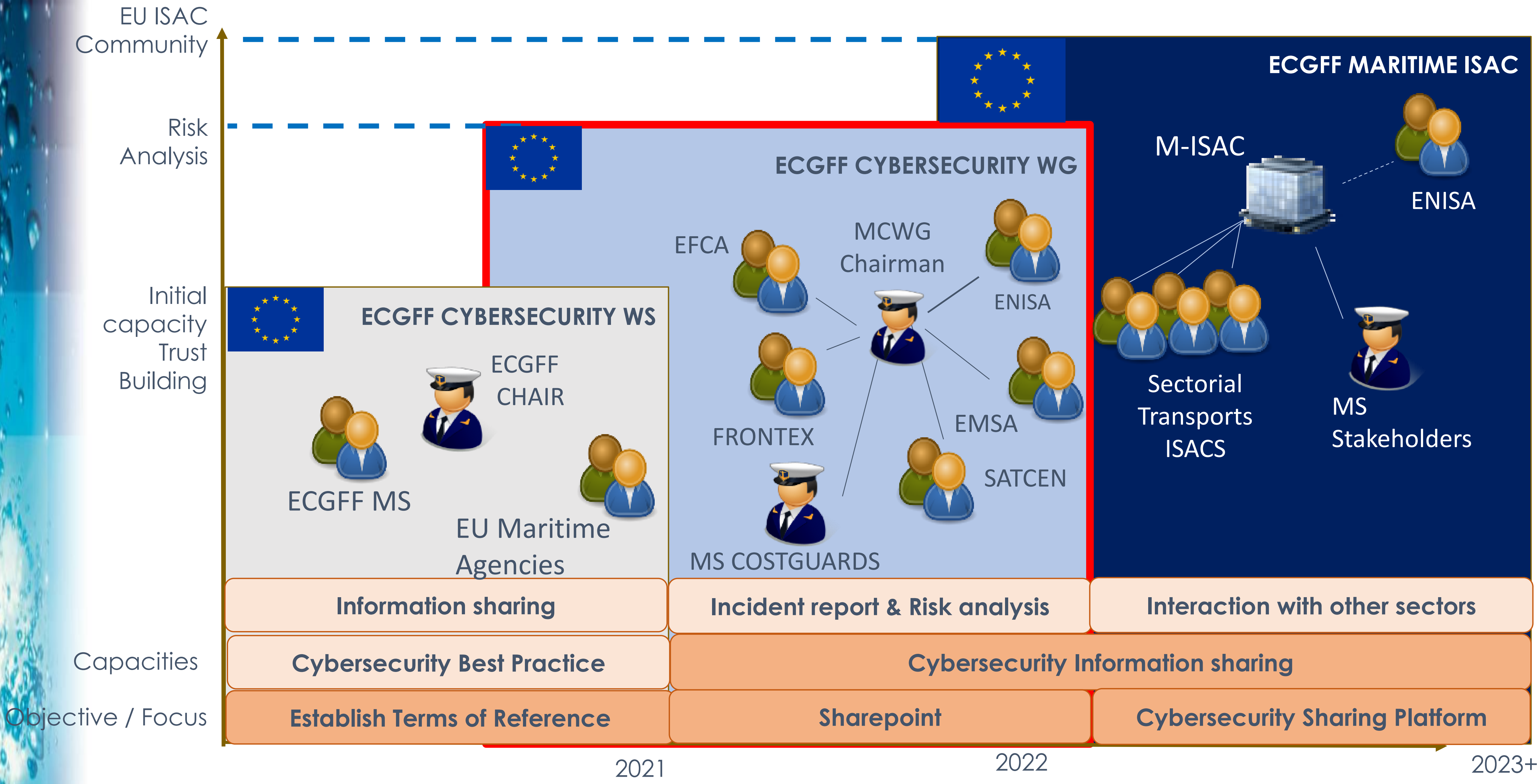
A pattern specific to simulated false AIS positions was able to be established from automated computer requests to identify other vessels with this same AIS broadcast model.

Almost a hundred warships had same message segments than the ones observed next to Karlskrona. Using additional sources of information, the locations and identities of the vessels have be confirmed.

False AIS positions for 15 naval vessels from seven countries have been identified in addition to the 9 Swedish ships.

sources	US Naval Institute: https://www.usni.org/ US Coastguards NAVIGATION CENTER: https://navcen.uscg.gov/?Do=GPSReportStatus; https://navcen.uscg.gov/?Do=AISReportStatus OS1: https://twitter.com/SCS_PI Skytruth: https://skytruth.org/ Global Fishing watch: https://globalfishingwatch.org/ Athanor-Engineering: https://athanor-engineering.com/en/solutions-for-maritime-security-en/ Marine Traffic: https://www.marinetraffic.com/ warshipcam (http://Warshipcam.com)

Way Ahead



EU ISAC Community

Risk Analysis

Initial capacity Trust Building

Capacities

Objective / Focus

ECGFF CYBERSECURITY WS

ECGFF CHAIR

ECGFF MS

EU Maritime Agencies

ECGFF CYBERSECURITY WG

EFCA

MCWG Chairman

ENISA

FRONTEX

EMSA

SATCEN

MS COSTGUARDS

ECGFF MARITIME ISAC

M-ISAC

ENISA

Sectorial Transports ISACS

MS Stakeholders

Information sharing

Incident report & Risk analysis

Interaction with other sectors

Cybersecurity Best Practice

Cybersecurity Information sharing

Establish Terms of Reference

Sharepoint

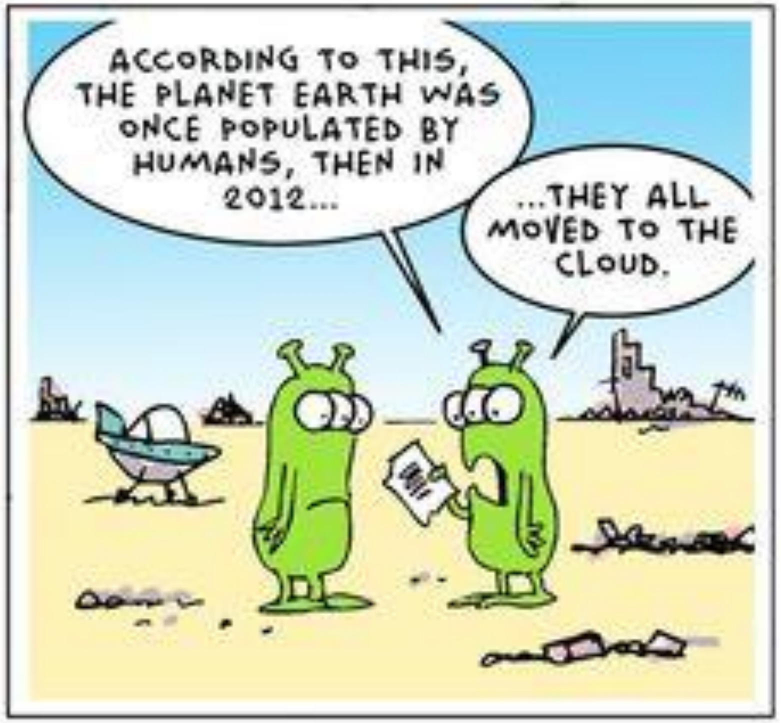
Cybersecurity Sharing Platform

2021

2022

2023+

Questions


ACCORDING TO THIS, THE PLANET EARTH WAS ONCE POPULATED BY HUMANS, THEN IN 2012...
...THEY ALL MOVED TO THE CLOUD.