Kaptein:
«Hei! Jeg fikk en melding her i stad med en faktura. Forsøkte å åpne vedlegget, men kom ingenting. Mulig noe vi bør sjekke opp?»

IT-ansvarlig:
«OK, når fikk du den? Trykket du på noe?»

Kaptein:
«Nja, var vel en 3-4 timer siden. Var sikkert ikke noe.»

Det var jo sikkert ikke noe…

Det er jo ikke noe interessant hos oss.

Hvem skulle ta seg bryet med å angripe oss?

Hvem er egentlig interessant?

https://e24.no › naeringsliv › kjoettindustrigigant-utsatt-...

Kjøttindustrigigant utsatt for dataangrep i USA - E24

NorSIS
Norsk senter for informasjonssikring

Meny

– Dørlåsene fungerte jo ikke i begynnelsen, og vi visste ikke om dørene var oppe eller igjen. I tillegg var alle fagsystemene borte, og vi måtte ha manuell kontroll på skoler og sykehjem, forteller kommunedirektør Ole Magnus Stensrud i Østre Toten til Digi.no.

Hjem - Dataangrepet i Østre Tot

Dataangrepet i Østre Toten kommune: Minst 9000 dokumenter og store e-postmengder stjålet

NASJONAL SIKKERHETSMYNDIGHET

RISIKO 2021
– helhetlig sikring mot sammensatte trusler

https://www.[illegible]artikler › nesten-90-prosent-av-ty

Nesten 90 prosent av tyske selskaper utsatt for dataangrep

5. aug. 2021 — Nesten alle tyske selskaper har vært
månedene, melder informasjons- og telekomforening

https://www.vl.no › nyheter › 2021/03/10 › stortinget-uts

Stortinget utsatt for nok et dataangrep

10. mar. 2021 — Stortinget utsatt for nok et dataangre
omfanget av angrepet, men bekrefter at data er hentet

https://www.dagsavisen.no › innenriks › 2021/03/22 › os

Oslo rådhus utsatt for dataangrep - Da

22. mar. 2021 — Oslo rådhus ble utsatt for et dataang
andre virksomheter i starten av mars

https://www.smp.no › ntb › innenriks › 2021/06/23 › B...

Biblioteker over hele landet utsatt for d

23. jun. 2021 — Datasystemene til biblioteker over hele
kveld etter et dataangrep. Hackere krever løsepenger

https://www.aftenposten.no › norge › et-titall-norske-bedr...

Et titall norske bedrifter er rammet av dataangrep - Aftenposten

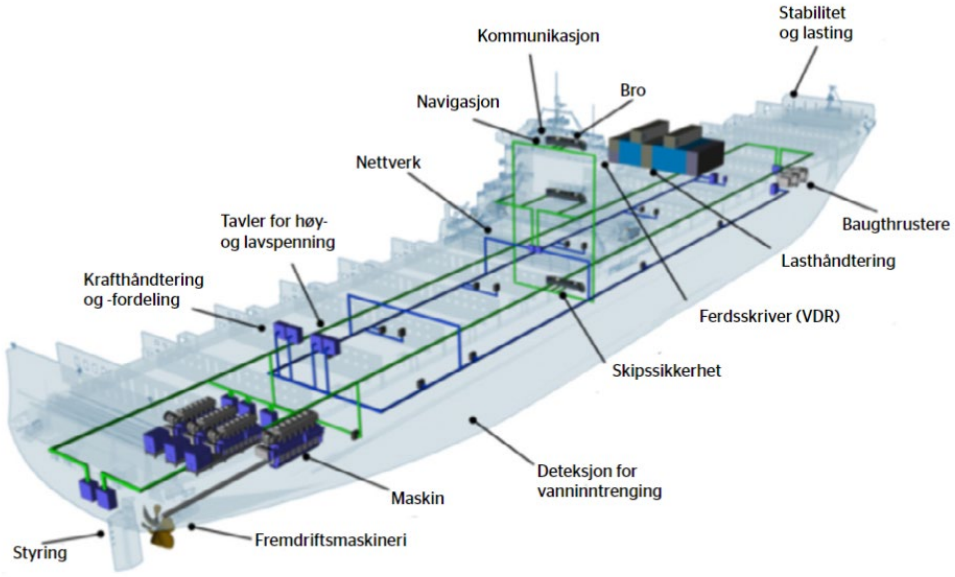
11. mar. 2021 — mars er det minst 142 servere som fortsatt ikke er oppdatert. - Disse er spesielt utsatt for kryptovirus, fordi flere aktører og kanskje mindre ...

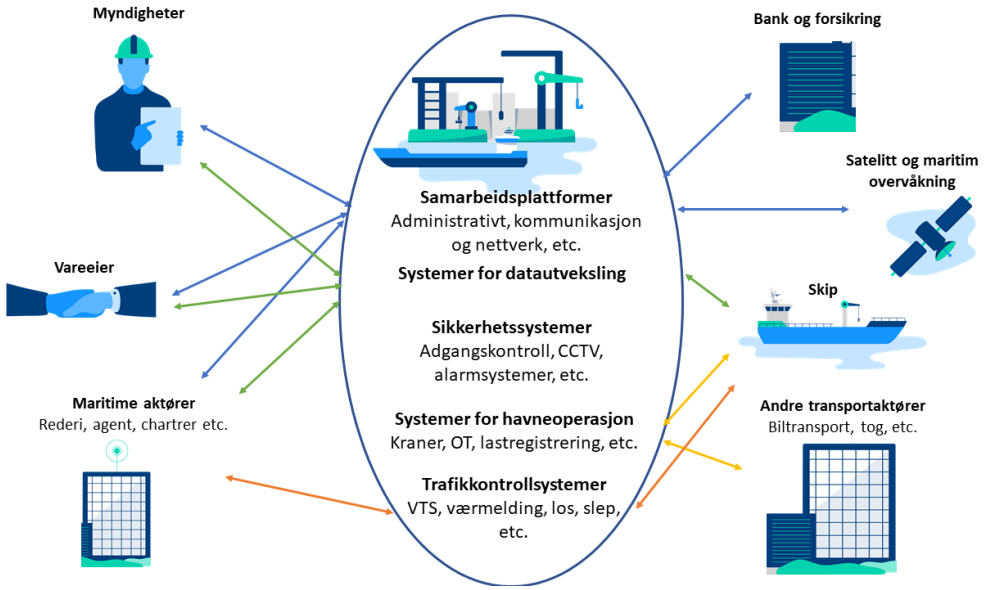
virksomheter. NSM vurderer fortsatt at virksomheter innen offentlig forvaltning, forsvars-, petroleums-, ekom[4]- og kraftsektoren er risikoutsatt. Det samme gjelder for romvirksomhet og maritim produksjon og teknologi. Det siste året

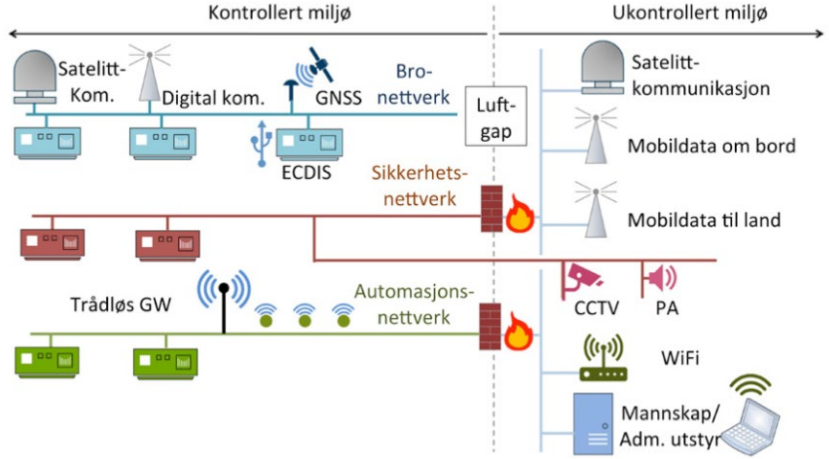
Sjøfartsdirektoratet
Norwegian Maritime Authority

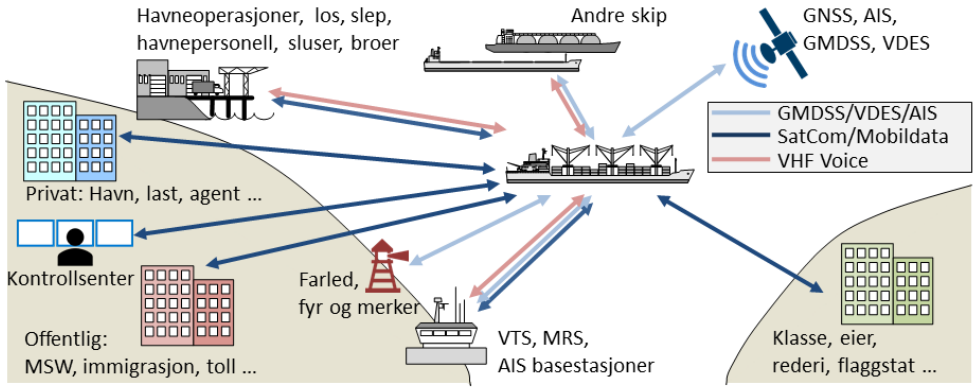
Den foretrukne maritime administrasjonen

Id	År	Angreps-punkt	Beskrivelse	Tiltak i etterkant
A3	2011 - 2013	H4	Ved Antwerpen havn ble lastesporingssystemet infisert for å smugle containere med narkotika og våpen (skjult som bananer fra Sør-Amerika). Dette pågikk i to år før det ble oppdaget. Også i 2018 ble samme havn utsatt for samme type angrep. Kilder: Walker og Spencer [24], Lysneutvalget [6], Kapalidis [18], KNect365 [19].	Første tiltak var å installere en brannmur for å beskytte havna sine IT-systemer, men angriperne gjorde senere et fysisk innbrudd og installerte en trådløs bro slik at de kunne angripe systemet igjen.
A4	2011 - 2013	P2	Et angrep døpt "Icefog" av Kaspersky [25] rammet Japanske og Koreanske forretninger blant annet knyttet til skipsverft og maritime operasjoner. Dette var et målrettet angrep knyttet til industrispionasje, og benyttet teknikker som spear-phishing og utnyttelse av kjente sårbarheter. Kilde: Kaspersky [25].	For dette spesifikke angrepet ble det gjort tilgjengelig maskinlesbare angrepsindikatorer for OpenIOC-rammeverket.
A5	2011	P1	I et cyberangrep mot det statseide shipping-selskapet IRISL (Islamic Republic of Iran Shipping lines) ble all data knyttet til tariffer, last- og forsendelsesdata ødelagt, og lastedata stjålet. Det interne kommunikasjonsnettet ble også ødelagt. Hendelsen førte store økonomiske tap og tap av last. Kilder: Reuters [26], CyberKeel [21].	Etter flere cyberangrep mot kritisk infrastruktur i Iran har landet investert tungt i cyberforsvar [27]. Veldig få maritime cyberhendelser har blitt annonsert etter 2012 [20].
A6	2012	S3	Iran melder om angrep på deres kommunikasjonsnett på offshore-installasjoner i den persiske gulf. Kilde: Singh [20]	
A7	2012	H4	Fraktsystemet brukt av for toll- og grensekontroll i Australia ble infisert slik at angriperne kunne sjekke om deres containere var flagget som mistenkelige. I disse tilfellene ble smuglergodset aldri hentet. Kilde: CyberKeel [21].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.
A8	2012	M1	Kinesiske hackere blir anklaget for å ha stått bak et målrettet angrepet mot den Danske Søfartsstyrelsen (Danish Maritime Authority). Det ble stjålet dokumenter og informasjon om nettverksstrukturen for videre angrep. Infeksjonen kom fra en epost med et PDF-vedlegg. Kilde: Shippingwatch [28], CyberKeel [21].	Hendelsen ble avdekket, men det er ikke dokumentert spesifikke tiltak i etterkant.


Kommunikasjon
Stabilitet og lasting
Navigasjon
Bro
Nettverk
Tavler for høy- og lavspenning
Baugthrustere
Krafthåndtering og -fordeling
Lasthåndtering
Ferdsskriver (VDR)
Skipssikkerhet
Deteksjon for vanninntrenging
Maskin
Styring
Fremdriftsmaskineri


Myndigheter
Bank og forsikring
Samarbeidsplattformer
Administrativt, kommunikasjon og nettverk, etc.
Satelitt og maritim overvåkning
Systemer for datautveksling
Vareeier
Skip
Sikkerhetssystemer
Adgangskontroll, CCTV, alarmsystemer, etc.
Maritime aktører
Rederi, agent, chartrer etc.
Systemer for havneoperasjon
Kraner, OT, lastregistrering, etc.
Andre transportaktører
Biltransport, tog, etc.
Trafikkontrollsystemer
VTS, værmelding, los, slep, etc.


Kontrollert miljø
Ukontrollert miljø
Satelitt-Kom.
Digital kom.
GNSS
Bro-nettverk
Luft-gap
Satelitt-kommunikasjon
ECDIS
Mobildata om bord
Sikkerhets-nettverk
Mobildata til land
Trådløs GW
Automasjons-nettverk
CCTV
PA
WiFi
Mannskap/ Adm. utstyr


Havneoperasjoner, los, slep, havnepersonell, sluser, broer
Andre skip
GNSS, AIS, GMDSS, VDES
GMDSS/VDES/AIS
SatCom/Mobildata
VHF Voice
Privat: Havn, last, agent ...
Kontrollsenter
Farled, fyr og merker
Offentlig: MSW, immigrasjon, toll ...
VTS, MRS, AIS basestasjoner
Klasse, eier, rederi, flaggstat ...

Sentrale rammer / føringer

- ISM
- Lov om skipssikkerhet (skipssikkerhetsloven)
- Forskrift om melde- og rapporteringsplikt ved sjøulykker og andre hendelser til sjøs
- NIS direktivet
- Nasjonal strategi for digital sikkerhet
- NSM Rammeverk for håndtering av IKT hendelser
- Instruks for departementenes arbeid med samfunnssikkerhet
- Havne- og farvannsloven

Title	RESOLUTIONs / MSC Resolutions / 98th Session / Res.MSC.428(98)

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)
MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

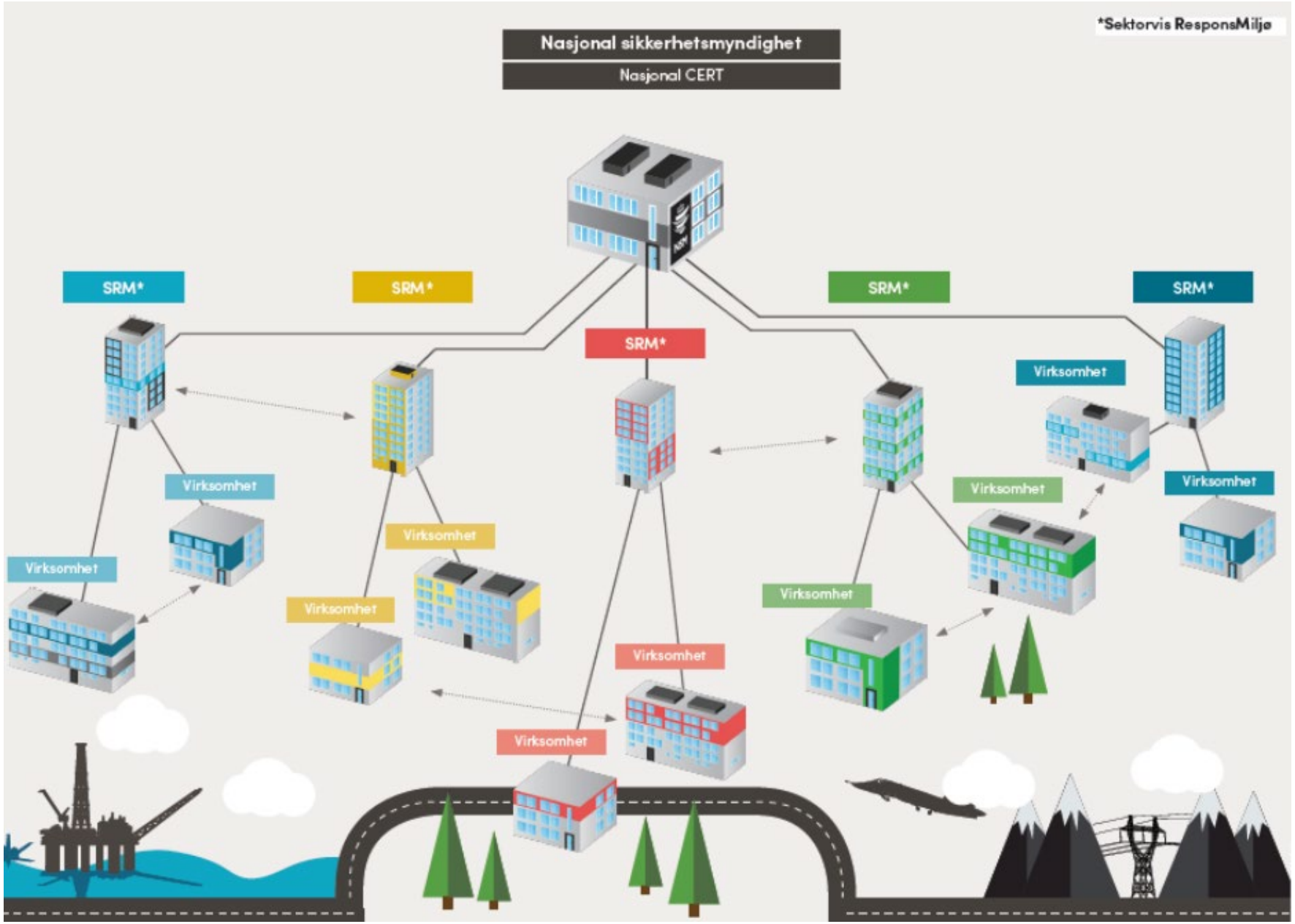
4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

Utkast til strategi for maritim digital sikkerhet

- Autonomi
- Digital sikkerhet i ytelseskrav
- Digital sikkerhet i maritim kommunikasjon
- Overvåke signalene fra satellittnavigasjonssystemene
- Digitalisering av kommunikasjon
- AIS integritet
- Kritisk maritim infrastruktur
- NIS-direktivet

- Responsmiljø for maritim sektor
- Totalforsvaret
- Virksomheters verdier og avhengigheter
- Sårbarhetskartlegging
- Digital sikkerhetskompetanse
- Sikkerhetskompetanse i internasjonalt regelverk
- Opplæringstiltak
- Sikkerhetskompetanse i havner


*Sektorvis ResponsMiljø
Nasjonal sikkerhetsmyndighet
Nasjonal CERT
SRM*
SRM*
SRM*
SRM*
SRM*
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet
Virksomhet

Takk for meg!