

Åpning Nasjonal sikkerhetsmåned med Øvelse Digital 25



NSM



DSB



NorSIS

IKT-sikkerhetshendelse desember 2024



GRAN KOMMUNE



Ellen Sagengen

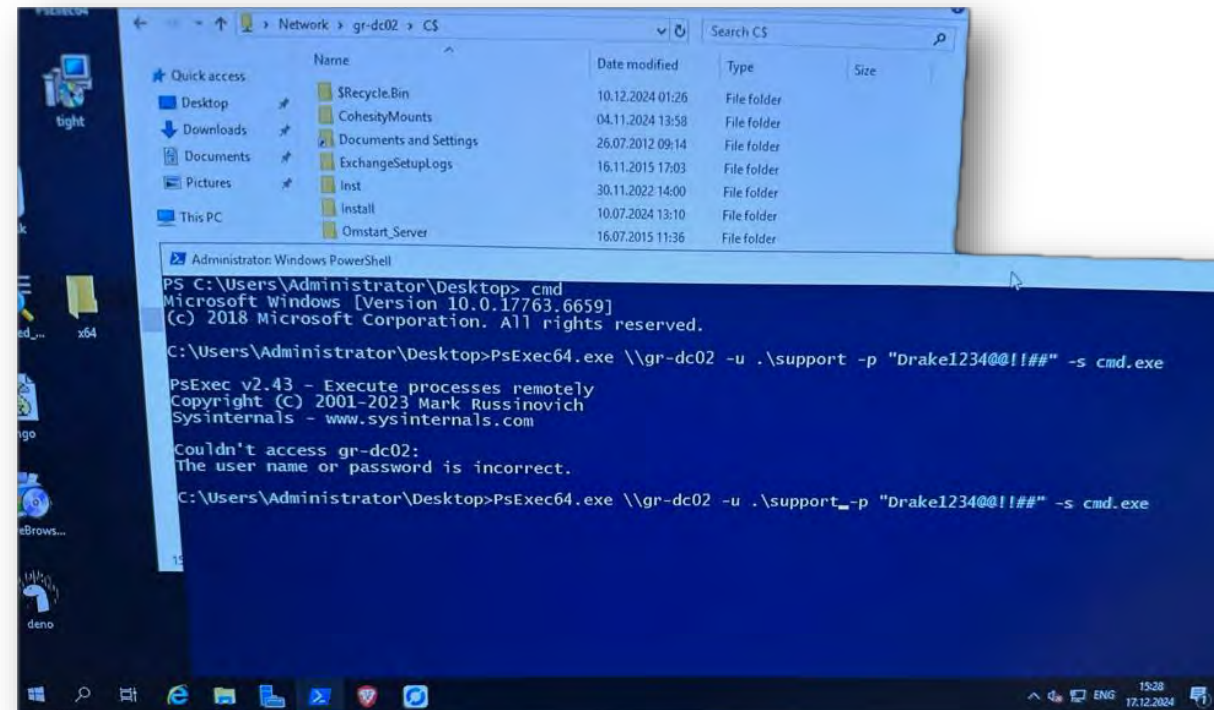
Kommunalsjef Stab og støtte

ellen.sagengen@gran.kommune.no



IKT-sikkerhetshendelse

- Oppdaget 17. desember klokka 15.30
- En IKT-medarbeider logget seg på en server med Remote desktop verktøy via konsoll
- Så aktiviteten til angriper og slo alarm
- IKT-drift kontaktet Helse- og KommuneCERT, for analyse og vurdering
- Anbefalte å kontakte «Incident response team» godkjent av NSM
- Defendable ble koblet på samme kveld gjennom avrop på rammeavtale for Digi Innlandet





GRAN KOMMUNE

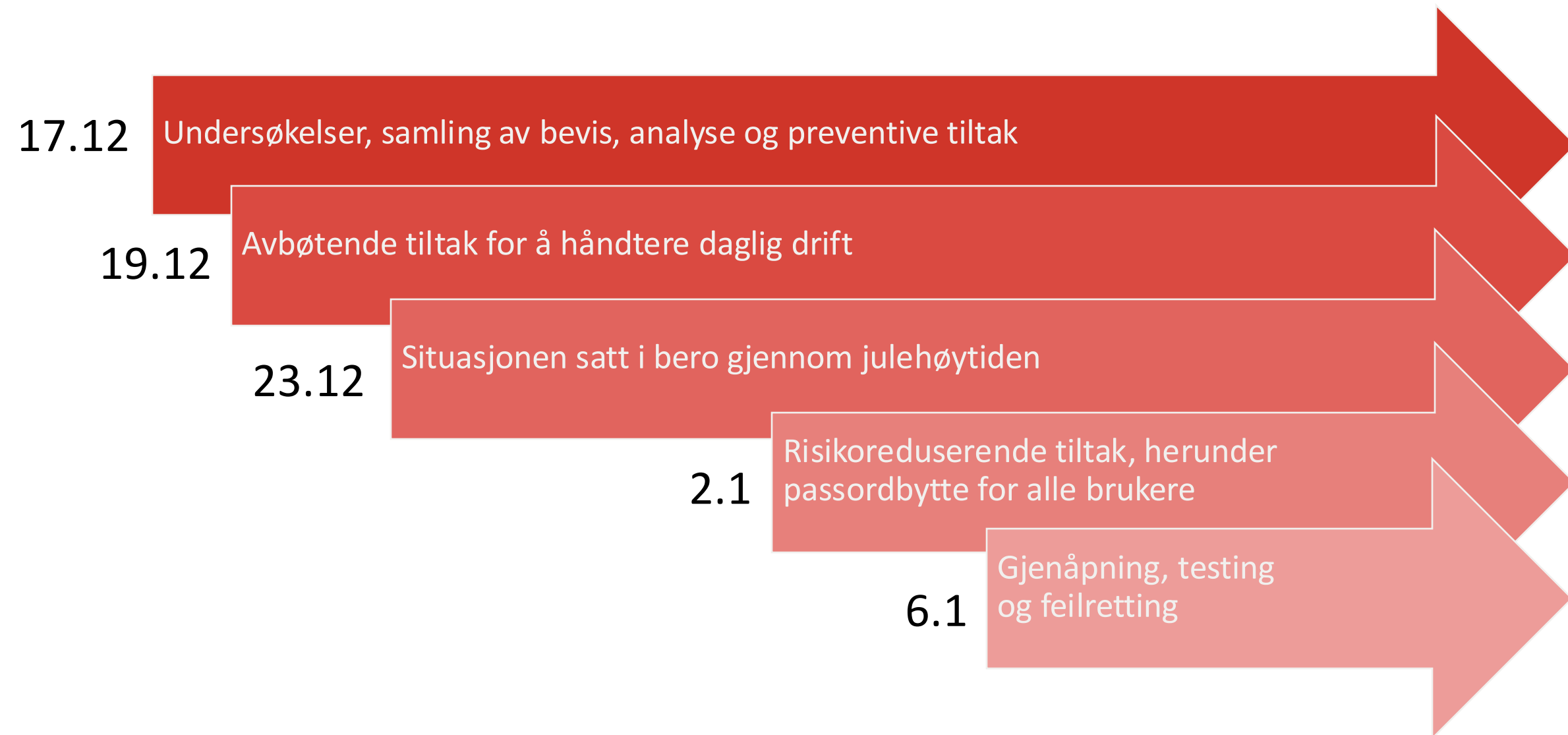
17. Desember 2024





GRAN KOMMUNE

17. desember 2024 – 7. januar 2025





Avrop på rammeavtale med Digi Innlandet



Hendelseshåndtering

- preventive tiltak
- analyse, undersøkelser og avklaringer
- fysisk tilstedeværelse i Gran rådhus og fjernarbeid
- prosjektledelse og rådgivning

Nød-MDR

- 24/7 vakt
- alarmer og avdekke sårbarheter
- undersøkelser og avklaringer



GRAN KOMMUNE

- cybersikkerhetssenter for både helse- og kommunesektoren i Norge
- øke motstandsdyktigheten gjennom en rekke tjenester i Nasjonalt beskyttelsesprogram (NBP)
- forebygge, oppdage og håndtere uønskede IKT-sikkerhetshendelser
- spisskomptanse innen operativ cybersikkerhet
- helse- og kommunesektorens felles kontaktpunkt ved cyberhendelser - vil koordinere henvendelser mot andre responsmiljøer



Norsk helsenett

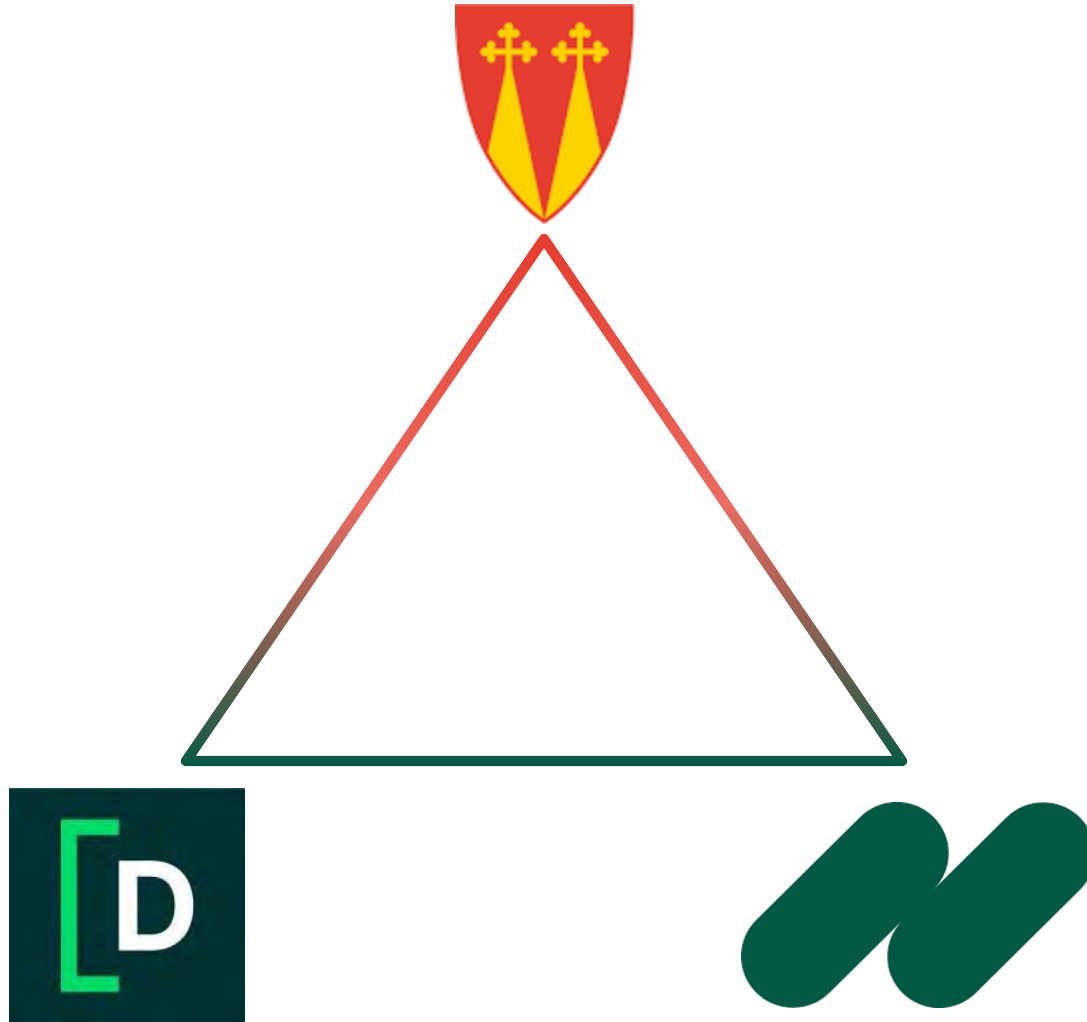
Helse- og KommuneCERT

Tjenester i NBP:

- + Anbefalte sikkerhetstiltak
- + Blokkeringslister
- + Brukernavn og passord på avveie
- + Hendelseshåndtering
- + Hurtigtest
- + Informasjonsdeling og forebygging
- + Sikkerhetsskanning
- + Situasjonsbilde
- + Tilbakeblikk
- + Webinarer



GRAN KOMMUNE

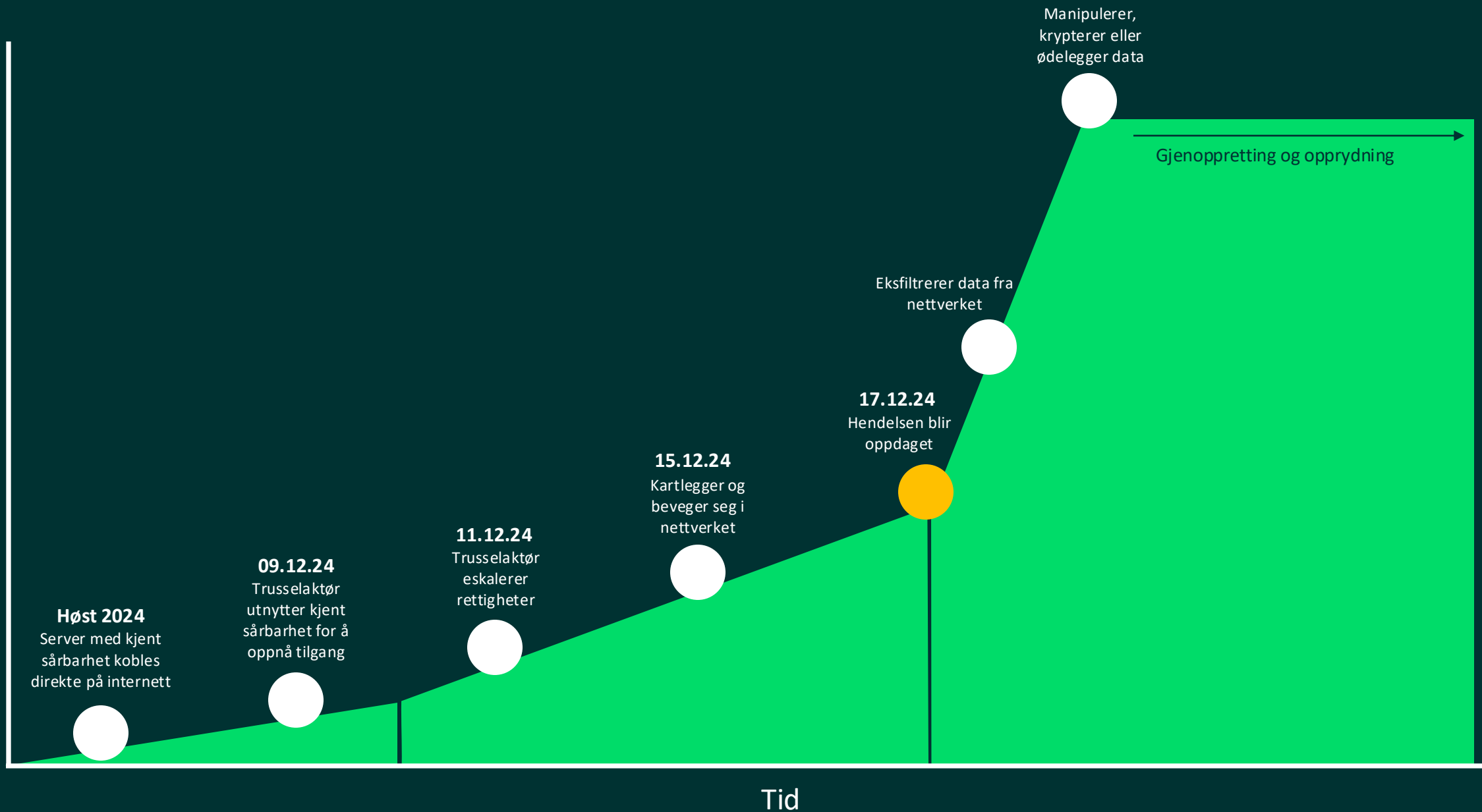


Hendelseshåndtering

Koordinering, dialog og samarbeid mellom IKT-drift, Helse- og KommuneCERT og Defendable

- teknisk og taktisk analyse
- tiltak
- informasjonsdeling

Konsekvenser og kostnader





GRAN KOMMUNE

Kriseledelse



Ti møter i kommunal kriseledelse 17. desember 2024 – 7. januar 2025

- status for hendelses-
håndteringen fra IKT-drift,
Stab og støtte og Defendable
- status for hvert
kommunalsjefområde
 - kartlegging av
konsekvenser
 - vurdering av tiltak
- informasjon og
kommunikasjon
- oppgaver og
oppfølgingspunkter
- felles situasjonsforståelse

Foto: Anne Berit Reinsborg, avisen Hadeland



Myndighetskontakt

Vi har

- meldt hendelsen til Datatilsynet
- anmeldt angrepet til Politiet v/KRIPPOS
- rapportert til Statsforvalteren, fra kriseledelsen





Leverandørkontakt

- Systemeiere og -ansvarlige sendte ved nyttår informasjon til systemleverandører om pågående sikkerhetshendelse, status og risiko.
- Enkelte systemleverandører stilte oppfølgingsspørsmål, de fleste gjorde ingen spesielle tiltak.
- Noen få leverandører valgte å stenge oppkoblinger mot Gran kommune da datainnbruddet ble kjent i media, men åpnet igjen etter tilsendt informasjon.



Melding til våre systemleverandører 2. januar 2025

Gran kommune håndterer datainnbrudd

Gran kommune er utsatt for et datainnbrudd. Dette ble oppdaget tirsdag 17. desember. Mange av våre leverandører og samarbeids-partnere har fulgt situasjonen gjennom omtale i media og informasjon lagt ut på våre hjemmesider. Nå har vi fått såpass god oversikt over situasjonen, at vi mener det er riktig med en generell orientering til våre systemleverandører.

Oppsummering av hendelsen

Selv om det er for tidlig å se et fullstendig bilde av hva som har skjedd og hvilke konsekvenser angrepet har, er det grunn til å tro at angrepet er oppdaget på et tidlig tidspunkt. Vi ser per nå ingen skadevirkninger utover konsekvensene av en preventiv og kontrollert stenging av vår internettforbindelse. Dette gir en del uheldige konsekvenser for daglig drift, men vi er ellers skadefrie.

Vi satte kriseledelse 17. desember og orienterte overordnede myndigheter ved statsforvalter. Gran kommune får bistand fra Helse- og KommuneCERT og et hendelseshåndteringsteam fra Defendable. Saken er meldt til Datatilsynet og anmeldt til Kripos. Vi er opptatt av at våre erfaringer skal deles med alle legitime interessenter, slik at vi sammen bekjemper denne typen kriminalitet.

Det er Defendable vi først og fremst støtter oss på når det gjelder vurdering av alvorlighetsgrad og hvilke tiltak som må iverksettes. Vi innførte raskt risikoreducerende tiltak og valgte å stenge ned internettforbindelsen for å forhindre et angrep med et større skadepotensiale.

Vurdering av situasjonen

Våre digitale undersøkelser antyder at datainnbruddet ble oppdaget i en tidlig fase og før trusselaktøren klarte å gjennomføre sitt endelige mål. Det er ikke funnet noen indikasjoner på kompromittering av Gran kommune

sitt sky-miljø og det er ingenting som tyder på at det er foretatt noe eksfiltrering av data per nå.

Gran kommune har iverksatt en rekke sikkerhetstiltak for å gjennomføre en trygg gjenåpning av nettverket og kommunens tjenester. Tiltakene inkluderer, men er ikke begrenset til:

- overvåking av alle internett-eksponerte tjenester, ansattkontoer og maskinobjekter

- tekniske sikkerhetstiltak for å redusere sårbarhets- og eksponeringsflaten til kommunen

Gran kommune anser ikke lenger hendelsen som pågående og er i sluttfasen med å gjenopprette sine systemer, for å gjennomføre en trygg og kontrollert gjenåpning av de kommunale tjenestene.

Spørsmål og svar

- Er data kryptert?
Nei
- Er data eksfiltrert?
Så langt viser etterforskningen ingen indikasjoner som tilsier at data er eksfiltrert.

Hva betyr dette for Gran kommunes systemleverandører?

Alle med skyforbindelse kan trygt forholde seg til oss. Leverandører med en annen forbindelse til oss (for eksempel site-2-site VPN) må gjerne ta kontakt for dialog og tilpasninger knyttet til de tekniske koblingene.

Systemansvarlig hos Gran kommune vil være førstelinje-kontaktpunkt for det enkelte system. For ytterligere spørsmål og avklaringer, kan vår digitaliseringsrådgiver/informasjons sikkerhetsansvarlig kontaktes:

Tore Løvhaug
Tore.lovhaug@gran.kommune.no
tlf 90 59 64 33

Jaren, 2. januar 2025

Ellen Sagengen
kommunalsjef Stab og støtte



Tekniske funn og konklusjoner

- Det var sårbarhet i forbindelse mellom tredjepart og kommunens nett.
- To trusselaktører ble identifisert.
 - Aktiviteten spores tilbake til 6. desember.
 - Angripere forsøkte i liten grad å gå under radaren eller å slette spor underveis.
- Det er ikke funnet kryptering eller forsøk på kryptering, men vi har grunn til å tro at dette var hensikten til minst den ene trusselaktøren.
- Vi har ikke funnet at data er stjålet.
- Rask tilbakestilling var mulig fordi vi slapp å kjøpe nytt utstyr, i liten grad måtte reinstallere/oppgradere programvare og hente backup.
 - Sårbarheter har blitt eliminert forløpende, herunder endring av konfigureringer, sletting av tilganger og resetting passord.



Effekter på arbeidshverdag og tjenesteyting

Internettforbindelse tatt ned førte til:

- hjemmekontor (mobildata/hjemmenettverk)
- delt internett fra mobil på kontoret
- delt internett fra 4G-ruter i kommunestyremøtet
- ruteplanlegging i hjemmetjenesten
- fagsystem barnevern/PPT
- overføre data mellom lokale og eksterne systemer:
 - pasientinformasjon/elektroniske meldinger
 - apotekmeldinger
 - vedtak tildeling
 - digitalt skjemamottak
 - betalingsløsning kino
 - biblioteket (bytte av fagsystem)
 - SMS-varslng fra driftsstasjon til vakt VA
 - noen prosesser i sak- og arkivsystemet
- tilgang til lokale filservere
- utskrifter
- manuell håndtering av grunnlag for bankutbetalinger (sosialhjelp)
- fakturering (barnehage, SFO, helsetjenester, husleie, kommunalteknisk)

Noen leverandører tok ned forbindelsen til våre systemer:

- Kartverket
- Norkart
- Volue

Stengt forbindelse til NAV Hadeland:

- Ansatte i NAV pendlet mellom kontoret i Gran og rådhuset på Jaren.
- Det krevde ekstra logistikk og planlegging.

Alle involverte i krisehåndteringen la vekk alt annet arbeid:

- tapte tid til andre oppgaver

Ingen påvirkning på pedagogisk virksomhet i skole, kun administrasjon:

- Skole-IKT er i egen tenant og har egen forbindelse til internett.



GRAN KOMMUNE

Håndtering av mer enn teknologi



Ledelse og beslutninger



Koordinering
og samhandling



Psykososial ivaretagelse



Krisekommunikasjon
og mediehåndtering



GRAN KOMMUNE

Gran kommune utsatt for dataangrep - vet ikke hvilke konsekvenser det får ennå



DATAANGREP: Gran kommune
Skjervum Bjerkehagen

Dataangrepet i Gran: - Hjemmetjenesten har skrevet ut manuelle lister



Mange henvendelser til Gran kommune: - En tilleggsbelastning

KRISESTAB: Gran kommune h
onsdag formiddag. Foto: Anne



ANGREPET: Gran kommune er utsatt for et dataangrep. Omfanget og konsekvensene av det er fortsatt i det uvisse. Foto: Sissel Skjervum Bjerkehagen

Ordføreren om dataangrepet: - Klart vi er bekymret



Grunn til å tro at angrepet ble oppdaget tidlig: - Anmeldt datainnbruddet

BEKYMRET: Ordfører C
Thorbjørnsen



Vet mer om dataangrepet: Identifisert to aktører



ANGREPET: Gran kommune i
Skjervum Bjerkehagen

Erfarne medarbeidere reddet dagen under dataangrep i Gran: - Lange dager og lite søvn

BEROLIGER: Fredag kveld
Berit Reinsborg



Ellen Sagengen orienterte kommunestyret i Gran torsdag morgen. Foto: Anne Berit Johansen Reinsborg

Sadeland

Alarm fra Gran etter dataangrepet: - Får ikke tatt i mot digitale søknader



Stenger nettverket gjennom jula: Vil unngå unødvendig risiko

VIL VARE: Gran kommune
kommunikasjonssjef i Gra



Tilbake i normal drift etter dataangrepet: - Begynte å bli problematisk for flere av tjenestene våre

TRAVELT: Kommunalsjef stab



TRAVELT: Kommunalsjef stab og støtte, Ellen Sagengen har hatt en travel tid siden dataangrepet for jul. Foto: Anne Berit Reinsborg



GRAN KOMMUNE

Defendable

Kort oppsummert

- Gran kommune ble utsatt for dataangrep den 17. desember 2024. Det ble satt krisestab, ledet av rådmann og beredskapsleder. Som kommunalsjef for området for IKT og informasjonssikkerhet, hadde Ellen Sagengen en sentral rolle. Hun fikk raskt ekstern hjelp, som umiddelbart startet arbeidet med å analysere angrepet og finne bevis på at data er stjålet eller ødelagt. Kommunen ble tengt ned internettforbindelsen og informerte ansatte og innbyggere om situasjonen. Angrepet ble løst raskt, og kommunen var involvert tidlig. De har funnet spor og bevis som kan hjelpe i videre etterforskning. Kommunen innfører tiltak for å forhindre lignende angrep i fremtiden.



Foto: Anne Berit Reinsborg

Ellen (51) måtte ta avgjørelsen om å «trykke på den røde knappen»: – Det gir en veldig sterk opplevelse av alvor

Dette er cybersikkerhet

Cybersikkerhet er et sett prosesser, anbefalt praksis og teknologiske løsninger som bidrar til å beskytte de kritiske systemene og nettverkene mot digitale angrep.

Etter hvert som data har spredt seg og flere mennesker jobber der de vil, har ondsinnede aktører svart med å utvikle sofistikerte metoder for å få tilgang til ressurser og stjele data, sabotere for virksomheter eller drive med pengeutpressing.

Hvert år øker antallet angrep, og fienden utvikler nye metoder for å unngå å bli oppdaget.

Et effektivt program for cybersikkerhet omfatter mennesker, prosesser og teknologiske løsninger som samlet reduserer risikoen for forstyrrelser i virksomheten, økonomisk tap og skadet omdømme fra et angrep.

Kilde: microsoft.com

Tirsdag ettermiddag, 17. desember 2024, ca. kl. 15.30

En IKT-ansatt oppdager mistenksom aktivitet på en av kommunens servere. IKT-ansvarlig får melding om hendelsen og forlater ledermøte om informasjonssikkerhet.

17. desember 2024, ca. kl. 16

Innledende undersøkelser avklarer at det er uvedkommende inne på serveren. Akutte preventive tiltak iverksettes.

17. desember 2024, ca. kl. 16

Helse- og KommuneCERT, et cybersikkerhetssenter som jobber spesielt med helse- og kommunesektoren blir kontaktet. De analyserer situasjonen sammen med kommunens IKT-avd.

17. desember 2024, ca. kl. 17.30

Helse- og KommuneCERT mener at det er en potensielt stor hendelse og anbefaler at Gran kommune tar kontakt med et ekspertfirma som tilbyr «Incident response team» godkjent av NSM.

17. desember 2024, ca. kl. 18

Beredskapsplaner iverksettes, og arbeidet systematiseres.

17. desember 2024, ca. kl. 18

IKT-drift tar kontakt med Defendable. Den første kartleggingen av bistandsbehov gjennomføres, og administrative prosesser rundt samarbeidet starter. Analyse og preventive tiltak i samarbeid mellom IKT-drift, Defendable og Helse og kommuneCERT igangsettes.

17. desember 2024, ca. kl. 19

Kommunalsjef Ellen Sagengen forhåndsvarsler rådmann og beredskapsleder om en mulig krisehendelse.

17. desember 2024, ca. kl. 20

IKT-drift tar kontakt med hjemmetjenesten og noen andre tjenesteområder for å få hjelp til å iverksette en del manuelle rutiner, blant annet utskrift av kjørelister og minster.

17. desember 2024, ca. kl. 21.30

Kommunalsjef Ellen Sagengen «trykker på den røde knappen» og ber beredskapsleder om at det settes kriseledelse.

17. desember 2024, ca. kl. 22

Kommunalsjef Ellen Sagengen orienterer om situasjonen. Råd fra Defendable om å tette internettforbindelsen for å ha kontroll på ressen av beshåndteringen. Informasjon til organisasjonen. Andre uniktastiltak.

17. desember 2024, ca. kl. 23.30

Alle informeres om situasjonen. Deretter legges det ut informasjon på kommunens hjemmeside og det sendes ut pressemelding.

18. desember 2024

IKT-drift følger opp situasjonen gjennom hele natta for å få oversikt over situasjonen.

18. desember 2024, ca. kl. 4

Om kvelden og natta har stenging av internettforbindelsen blitt forberedt. I tillegg iverksettes tiltak i brannmuren. Forbindelsen stenges.

18. desember 2024, ca. kl. 10

Det blir et krisemøte og møte med pressen. Mye mediehåndtering fra morgen til kveld.

18. desember 2024, ca. kl. 14

Saken anmeldes i samråd med Kripos som kobles inn i saken.



GRAN KOMMUNE

NRK

Innlandet

Kontakt oss

Mobilvideo

Langlesing

TV

Radio

Klassequizen

Gran kommune jobber for å gjenåpne nettverket etter dataangrep

Gran kommune håper å være tilbake i normal drift i løpet av neste uke etter dataangrepet i desember.



DATAANGREP: 17. desember ble det oppdaget et dataangrep mot Gran kommune.

FOTO: STINE BÆKKELIEN / NRK

Publisert 2. jan. kl. 19:23
Oppdatert 2. jan. kl. 19:25





GRAN KOMMUNE

Kommunal Rapport



Gran kommune utsatt for datainnbrudd

Gran kommune har satt kriseledelse. Kommunen ble i går klar over at de er utsatt for et datainnbrudd. Det er ikke kjent hvor stort innbruddet er.

© 18.12.2024 - 08:25 📰 nyheter



Gran tror de oppdaget datainnbruddet i tide

Foreløpige undersøkelser tyder ikke på at data er på avveie.

© 19.12.2024 - 10:59 📰 nyheter



Fortsatt i nødmodus to uker etter dataangrep

Etter to uker uten internett-forbindelse begynner situasjonen i Gran kommune å bli krevende.

© 3.1.2025 - 10:59 📰 nyheter



Priser seg lykkelig over at dataangrepet ble stoppet: Pengeutpressing var trolig neste steg



Kripes tør ennå ikke si noe sikkert om hvordan de datakriminelle klarte å bryte seg inn i datasystemet til Gran kommune. Foto: Colourbox

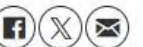
Politiet: Tror Gran var et tilfeldig offer

– De skyter med hagle, og så håper de at noe treffer, sier politiadvokat Terje Nedrebø Michelsen i Kripes etter datainnbruddet i Gran kommune.

Hanne Wien

JOURNALIST I KOMMUNAL RAPPORT

PUBLISERT 14.01.2025 - 15:32 SIST OPPDATERT 16.01.2025 - 10:06



17. desember oppdaget ansatte i Gran kommune tegn til at noen hadde brutt seg inn i kommunens datasystem. Umiddelbar stengte de ned internettforbindelsen. Først i forrige uke var kommunen tilbake i normal drift.



GRAN KOMMUNE

digi.no

Ledige stillinger

Nyhetsbrev

Nyhetsstudio

Tips oss

digi.no

[Ledige stillinger](#)

[Nyhetsbrev](#)

[Nyhetsstudio](#)

[Tips oss](#)

Ekstra +

GRAN RÅDHUS

– Vi har spøkt med han som oppdaget angrepet, at han skal få en egen statue

Tror angrepet var nødvendig:

– Angrer på at jeg ikke snakket mer med utestemme

Bamsemums og Battery

Det var en fast ansatt IT-konsulent som avverget det pågående angrepet.

Han oppdaget det han mente var mistenkelig aktivitet på en filserver og varslet raskt om hendelsen.

IT-avdelingen iverksatte straks en kontrollert nedstenging av nettet de selv drifter.

Sagengen forteller at avdelingen, som teller fire seniorer og to lærlinger, har blitt smurt opp med Bamsemums og Battery gjennom jula for å holde motivasjonen gående.

– Flere av disse skal nå få en skikkelig påskjønnelse, det skal vi få orden på, sier hun.

Avgjørende nedstengning

Allerede samme kveld angrepet ble oppdaget, hyret kommunen inn Defendable for å bistå med undersøkelser og tiltak.



Kommunalsjef Ellen Sagengen i Gran kommune forteller at de har jobbet iherdig for å åpne opp nettet igjen. Foto: Gran kommune



Økonomiske konsekvenser (foreløpige tall)

Engangskostnader til hendeshåndteringen:

- cirka 2 millioner kroner, fordelt med cirka 1 million kr merforbruk i hvert av årene 2024 og 2025

Behov for økte budsjetter til informasjonssikkerhet, generell heving av sikkerhetsnivået:

- cirka 2-3 millioner kroner årlig (for tidlig å konkludere)





GRAN KOMMUNE

Digi Innlandet

Om Digi Innlandet Kontakt oss Søk Meny

Webinar om dataangrepet i Gran kommune

Se opptak av webinarer der Digi Innlandet, Gran kommune og Defendable inviterte til erfaring om hendelsen på Gran i desember 2024.



Fra venstre nettverksleder i Digi Innlandet Hans Ivar Festad, kommunedirektør i Gran kommune Ellen Sagengen og leder for cyber defence center i Defendable Sarah Camilla Ansen

I dette webinarer får du innsikt i hva som skjedde, hvordan Gran løste situasjonen, viktigheten av å ha en sikkerhetspartner og gode tips på hva din kommune bør gjøre for å redusere risikoen for at dere er neste mål.

[Se opptak av webinarer her](#)

<https://www.digiinnlandet.no/aktuelt/webinar-om-dataangrepet-i-gran-kommune.55108.aspx>

Norsk helsenett



Angriper i sving

Gran kommune – Helse- og KommuneCERT



Helge Meland

- Fagansvarlig IKT
- Gran Kommune



Hans Kristian Strømme

- Senior sikkerhetsanalytiker
- Helse- og KommuneCERT



Norsk helsenett

Troverdighet og arbeidsro

Gran kommune – Helse- og KommuneCERT



Kine Therese Vik-Erstad

Kommunikasjonssjef,
Gran kommune



Helse- og KommuneCERT

Ellen Sagengen

Kommunalsjef Stab og støtte,
Gran kommune



<https://www.nhn.no/tjenester/helsecert/webinarer>



GRAN KOMMUNE

Vi sto han av



Sikkerhetsmåned 2025

Øystein Andreassen
Nasjonalt cyberkrimsenter
Kripos

Kripos

- Den nasjonale enheten for bekjempelse av organisert og annen alvorlig kriminalitet
- Nasjonalt kompetansesenter for norsk politi
- Nasjonalt kontaktpunkt for internasjonalt politisamarbeid



Trusselvurderinger

- Politiets årlige trusselvurdering relatert til cyberkriminalitet
- Hver rapport bygger videre på fjorårets situasjonsbilde, vurderinger og analytiske rammeverk
- Ønsker å bidra med kunnskap og innsikt for å ruste samfunnet mot lovbrudd



Vurderinger for 2025

01

Det er *sannsynlig* at uønsket påvirkning på **fysiske prosesser** vil føre til produksjonsstans og store økonomiske kostnader for **norske OT-avhengige virksomheter** i løpet av 2025, og derigjennom påvirkning på fysiske prosesser tilknyttet **kritisk infrastruktur**

02

Det er *meget sannsynlig* de fleste cyberangrep mot OT-avhengige virksomheter retter seg mot **virksomhetssystemer**.

Det er *sannsynlig* at **løsepengevirus** vil utgjøre den største andelen cyberrettede angrep mot OT-avhengige virksomheter i Norge. Det er videre *meget sannsynlig* at flesteparten av løsepengevirusangrep mot OT-avhengige virksomheter vil være **profittmotiverte**

03

Det er *meget sannsynlig* at **kulturelle og språklige barrierer** som tidligere har utgjort en del av det digitale forsvaret til norske enkeltpersoner og virksomheter, nå er i ferd med å **bytes ned** som følge av kunstig intelligens

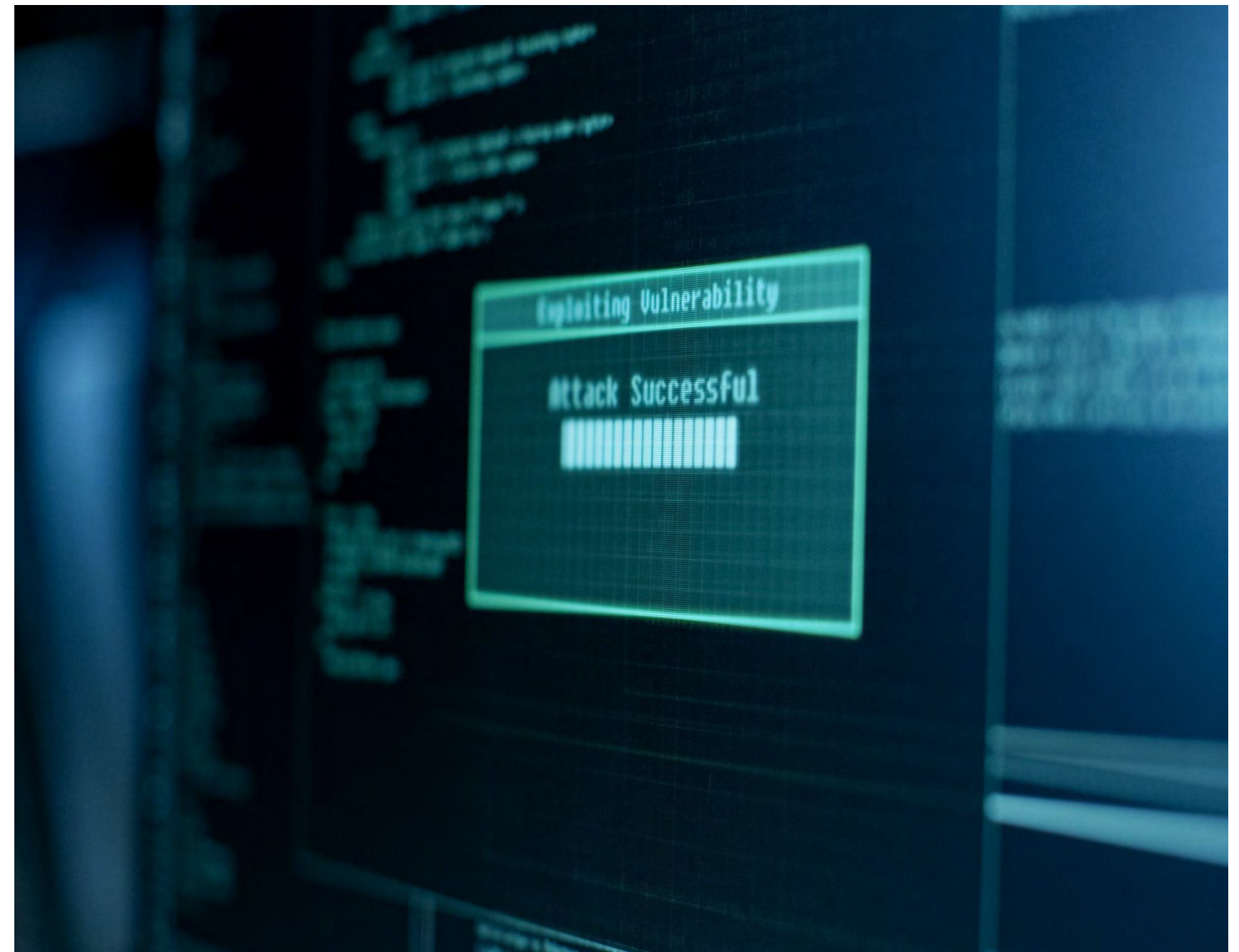
Situasjonsbildet – hvem er utsatt?

- Norske virksomheter er ikke et prioritert mål for cyberrettet kriminalitet
- SMB og kommuner er allikevel utsatt



Trussellandskapet 2024

- En moderat økning innen all cyberrettet kriminalitet
- Mengden av data som stjeles er større enn før
- Økt profesjonalisering av kriminalitet som handelsvare (KSH)
 - Vi venter et taktskifte
 - KI – en styrkemultiplikator for all krim
 - Krim som handelsvare – økt tilbud og etterspørsel



Utvikling hos løsepengevirusaktører

- Antallet løsepengevirusvarianter har økt i 2024
- Løsepengevirusgrupperinger er sammensatte og i bevegelse – samarbeid på tvers
- Lekkede kildekoder og internasjonale politiaksjoner har bidratt til at løsepengeviruslandskapet har blitt mer fragmentert
- Utviklingen peker mot nedleggelse og rask opprettelse av nye varianter

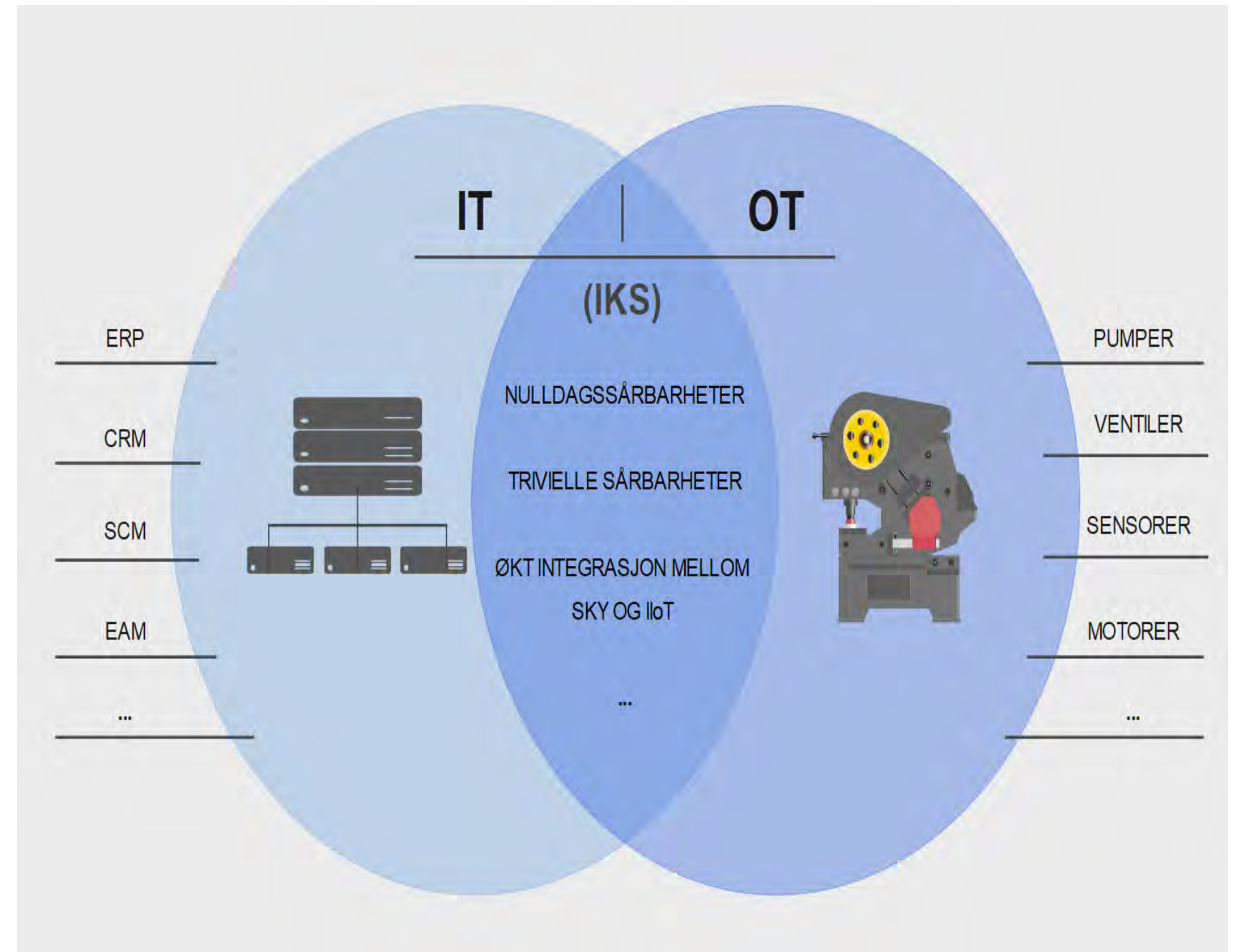
Aktivitet fra hacktivister

- Tjenestenekt mest brukt, men økt bruk av destruktive metoder
- Gråsoner mellom ytringsfrihet og ulovlig påvirkning
- Økende samarbeid i pro-russiske nettverk



Trusselen mot ot-avhengige virksomheter

- Gammelt utstyr med lav sikkerhet
- Påvirkes via internett
- Produksjon og leveranse av fysiske varer og tjenester



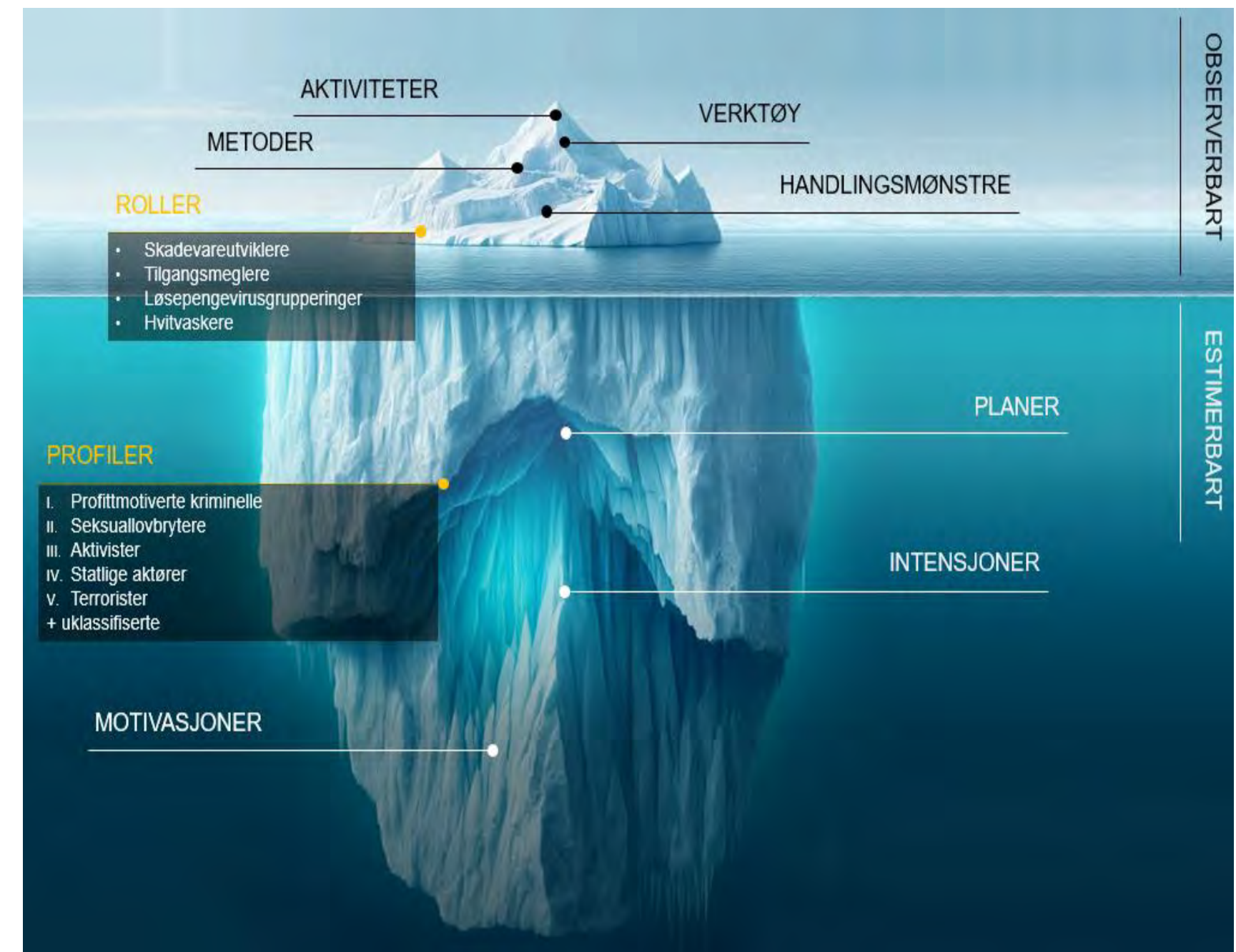
Bekjempelse av cyberkriminalitet

- Mange forskjellige aktører jobber langs flere akser for å bekjempe cyberrettet kriminalitet
- Politiet har noen særegenheter
- Vi har monopol på å benytte tvangsmidler



Hendelseshåndtering vs. etterforskning

- Fokus på hendelseshåndtering eller etterforskning?
- Se begge sporene i sin helhet
- Hendelseshåndtering og etterforskning understøtter hverandre



Gråsoner

- Det er vanskelig å vite hvem som står bak et cyberangrep
- Kjøp, salg og leie av verktøy og metoder er et viktig premiss for drift av kriminell virksomhet
- Geopolitiske spenningsforhold tåkelegger allerede uklare skillelinjer
- Kriminelle aktører løper i statlige aktørers ærend som stedfortredere innenfor flere digitale kriminalitetsområder
- Det er uklart for politiet hvem som fører hvem i denne dansen

Formål med etterforsking av cyberkriminalitet

- Identifisere gjerningsperson(er)
- Deling av informasjon med utenlandske politimyndigheter
- Avdekke andre fornærmede
- Identifisere modus til forebyggende bruk
- Understøtte hendelseshåndteringen
- Fremskaffe informasjonsgrunnlag for situasjonsforståelse



Borgerne

Teknologiprodusenter

Næringslivet

Politiet og andre sikkerhetsaktører

Takk for
oppmerksomheten



En dag uten satellitter



Først – en dag MED satellitter



En dag uten satellitter

07:00

Frokost TV - svart skjerm for de som har satellitt-TV. Du skrur på radio og hører på nyheten - at børsene i Tokyo måtte stenge. Problemer med synkronisering av tid.

NRK prøver å få link til sin korrespondent i Tokyo uten hell.



En dag uten satellitter

07:30

De siste internasjonale sportsnyhetene lar vente på seg.

Met.no sier de ikke kan gi deg noe langtidsvarsel - så du kan ikke planlegge fjellturen til helgen.



En dag uten satellitter

8:00 ute

Tap av globale kommunikasjonssatellitter setter verdensfreden i fare. I en bunker et sted i USA - mistet de kontakt med en drone med våpen som fløy over Midt-østen.

Tap av satellittkommunikasjon gjør det umulig å gi kommandoer til soldater, skip og fly og som nå er utsatt for angrep

Verdenslederne sliter med å få kontakt med hverandre mens den globale spenningen øker.



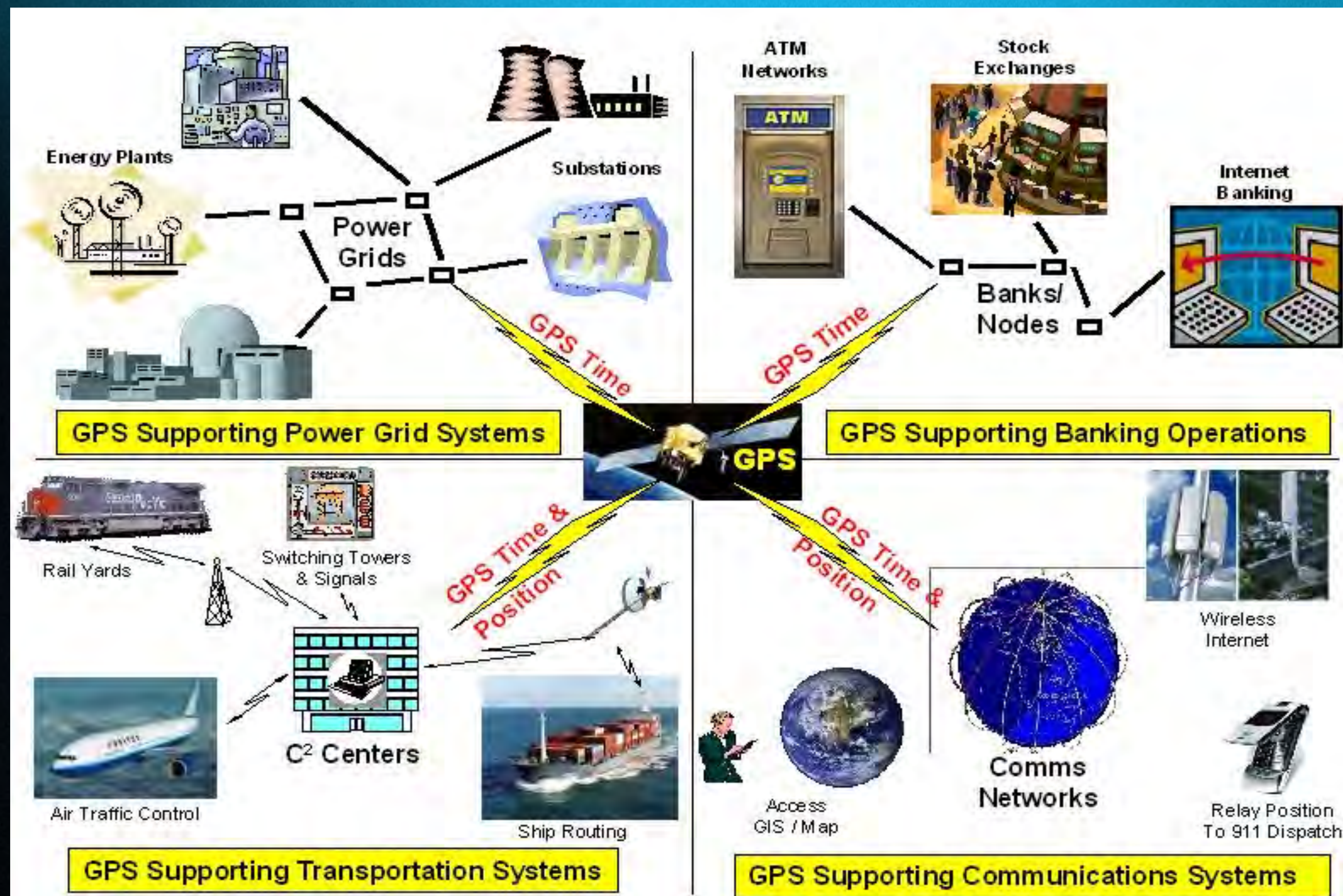
En dag uten satellitter

12:00

GPS gir oss også en nøyaktig klokke/tidsreferanse.

En rekke av de ting vi tar som gitt er helt avhengig av GPS-klokka.

Minibanker kan slutter å virke
Børsen kan måtte stenge
Strømnettet blir ustabilt.



En dag uten satellitter

13:00

Datanettverk som styres av datamaskiner er i faresonen.

Når GPS klokken forsvinner har mange systemer backup for å finne klokketider. Men raskt vil små feil på 0.1 sekund mellom systemer få konsekvenser.

«Skyen» svikter, Web-søk går tregere.

Internet går ned.



Wikipedia

En dag uten satellitter

14:00

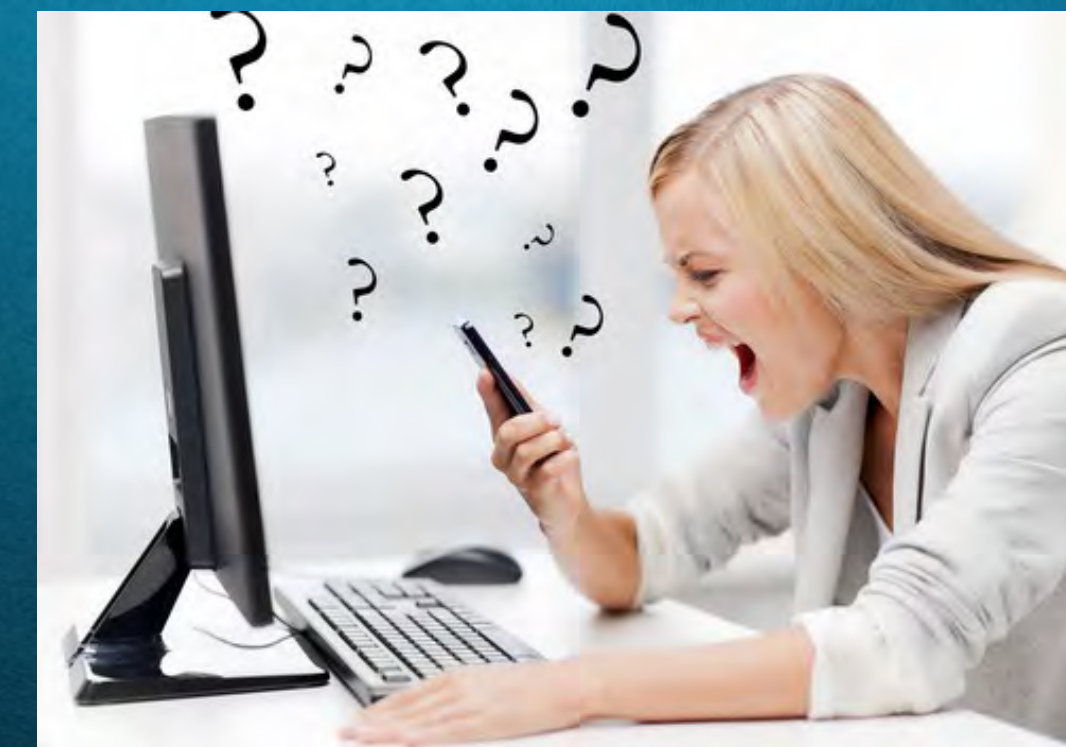
De første strømbrudd inntreffer. Nettleverandørene sliter med å balansere etterspørsel og synkronisere nettet.

Solstormen kan alt ha slått ut strømnettet på høye breddegrader.

Datastyrte renseanlegg må over på manuell drift.

I større byer begynner trafikklys og togsignaler å lyse rødt og skaper trafikkaos.

Mobilnettet som har vært ustabilt hele dagen faller ut.

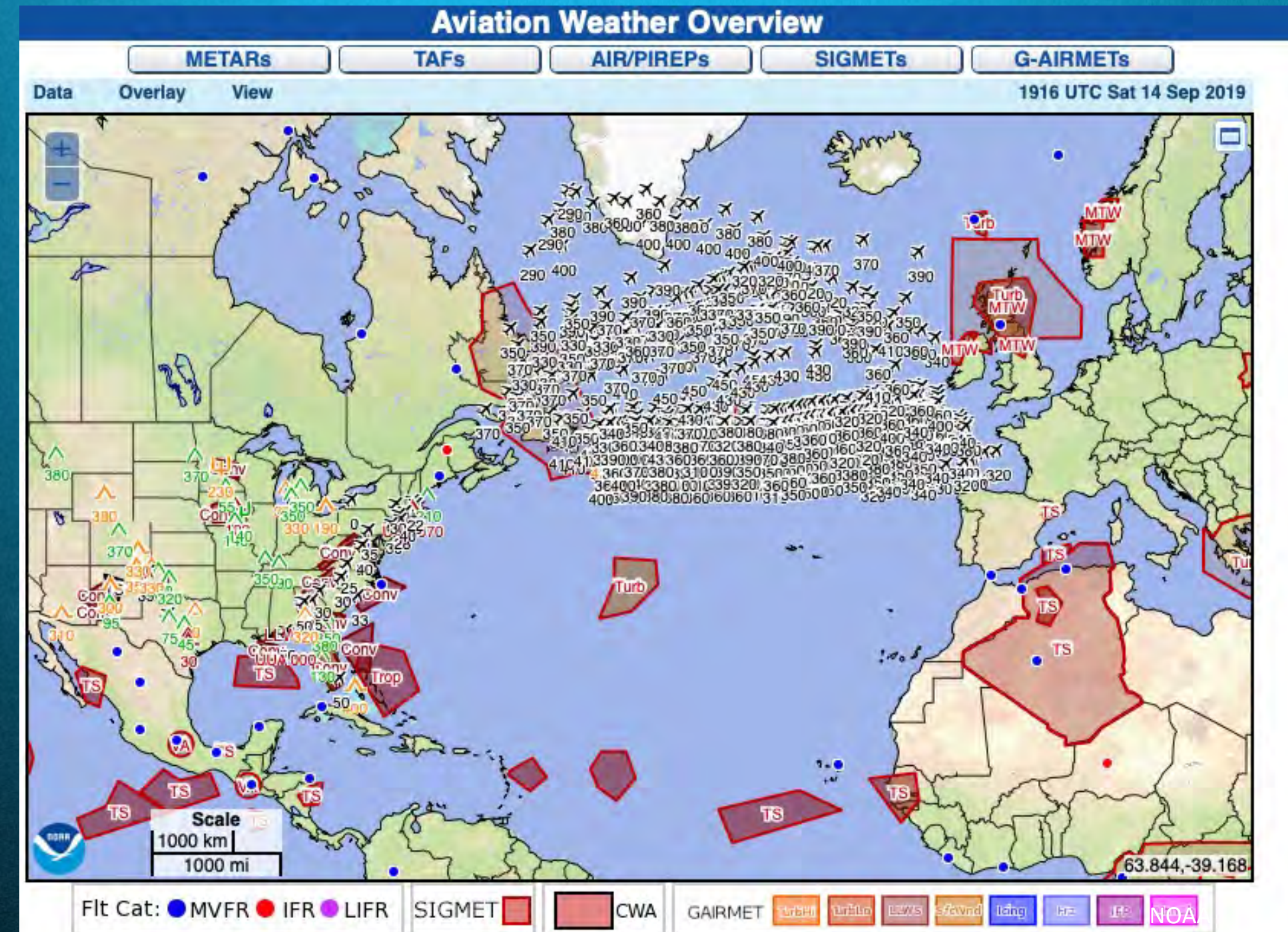


En dag uten satellitter

16:00

Mangel på oppdaterte værmeldinger gjør det uforsvarlig å fly. Særlig over hav der det er få andre observasjoner.

Større avstand mellom flykorridorer - forsinkelser

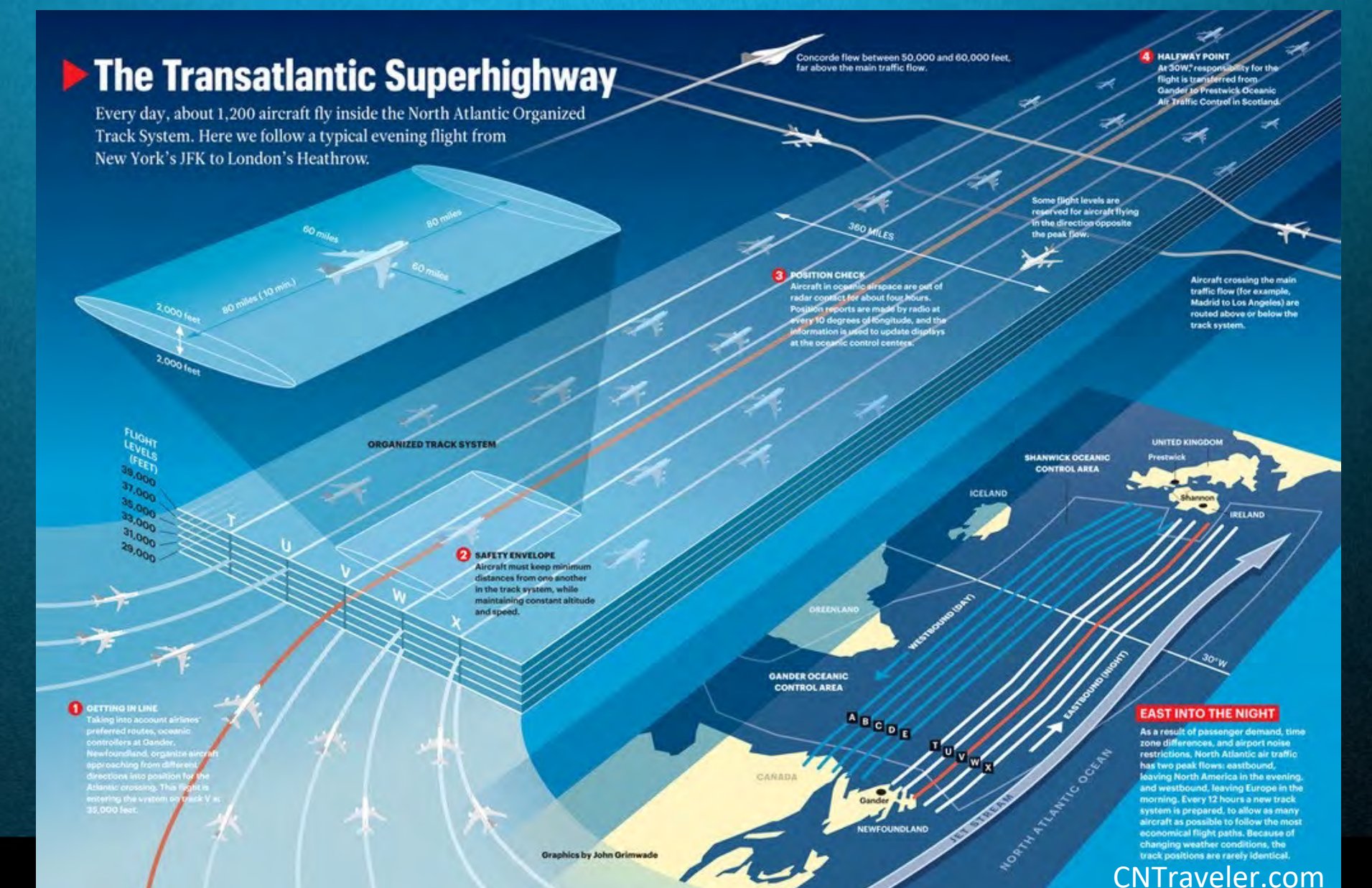
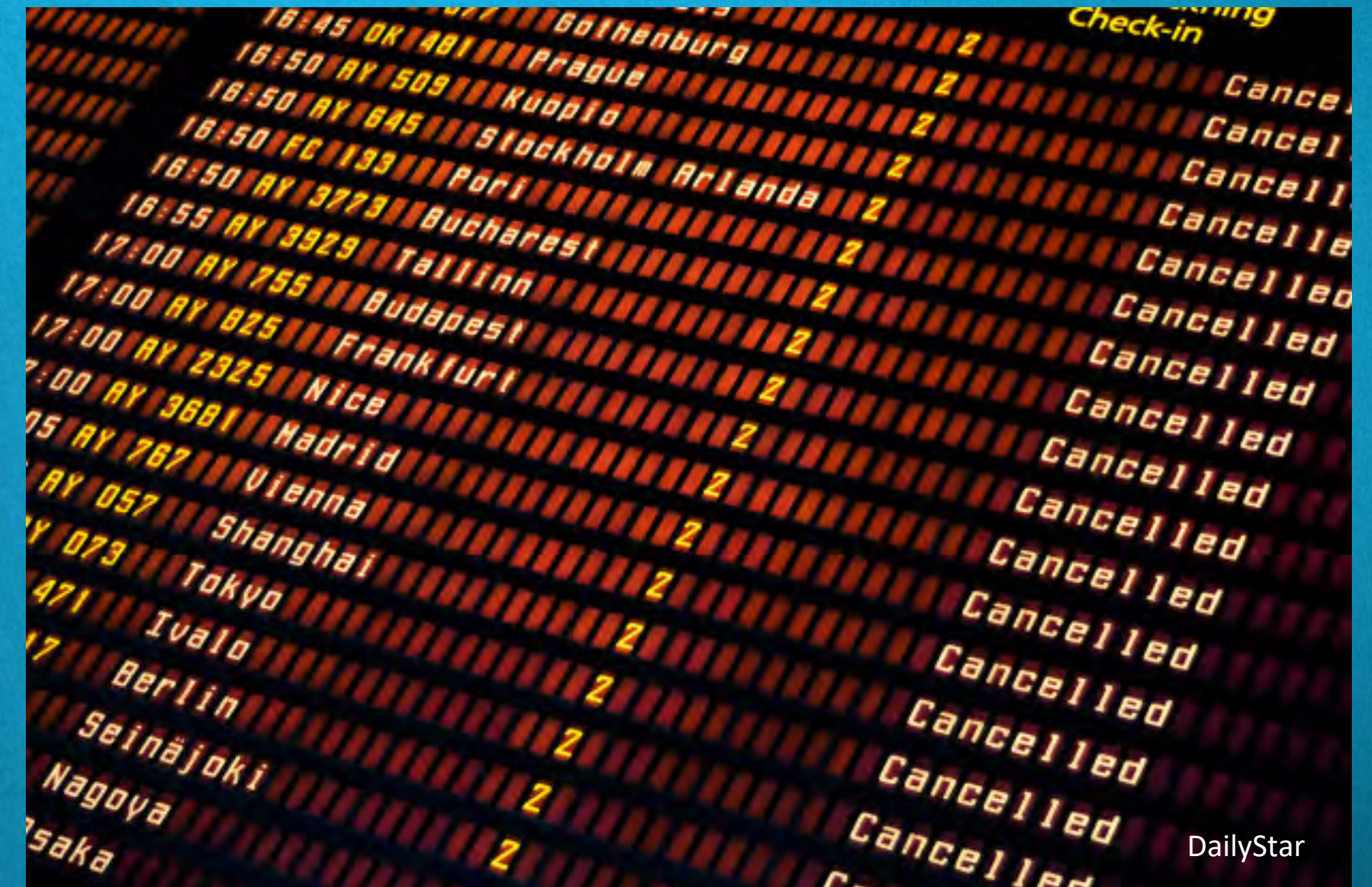


En dag uten satellitter

17:00

Tap av satellittkommunikasjon og GPS fører til mange flykanselleringer og forsinkelser.

Selv om de fleste fly bruker interne «treghets» navigasjonssystemer (gyroskoper etc.) så benyttes i dag GNSS signaler til å oppdatere de interne for å opprettholde høy nøyaktighet.



En dag uten satellitter

22:00

Nå er effekten av «en dag uten satellitter» tydelig.

Kommunikasjon, transport, strømnett og datasystemer er alvorlig svekket.

Sanntids bus/tog-info virker ikke

Global handel har stoppet

Myndigheter i alle land har store utfordringer.

Matvareforsyninger kan bryte sammen.



Flere dager uten satellitter

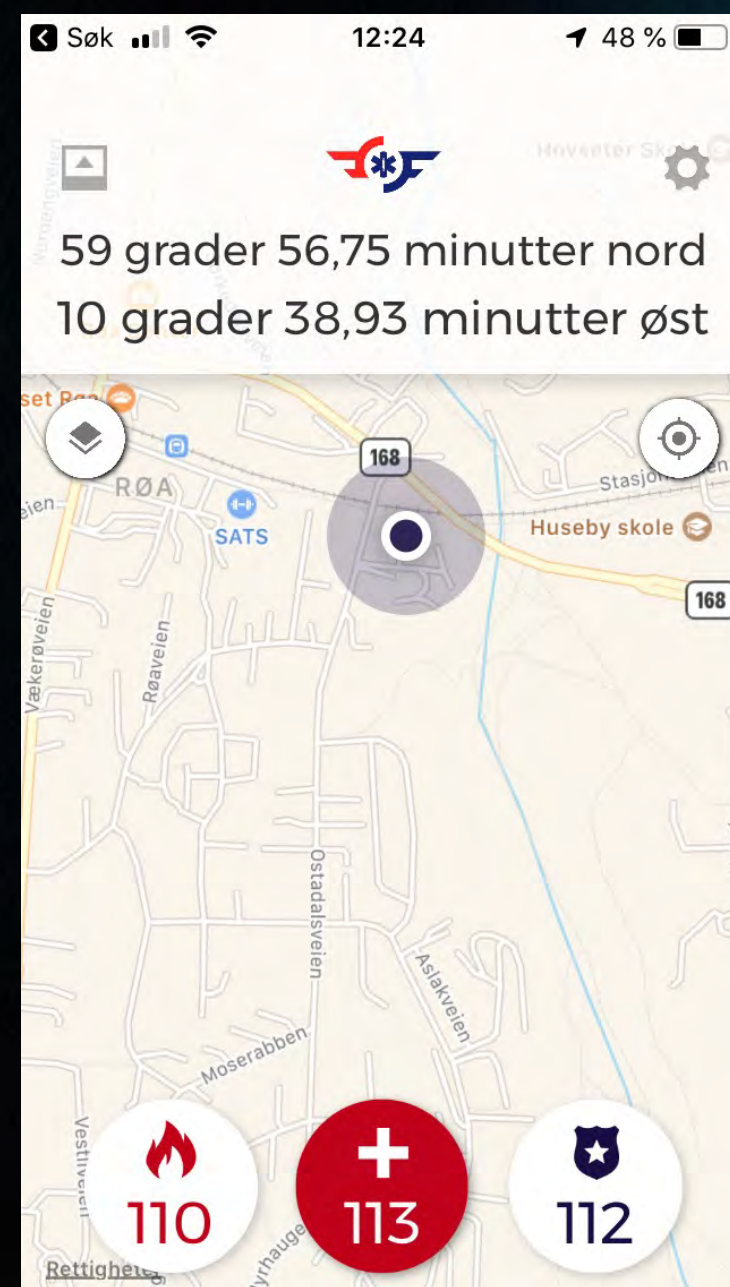
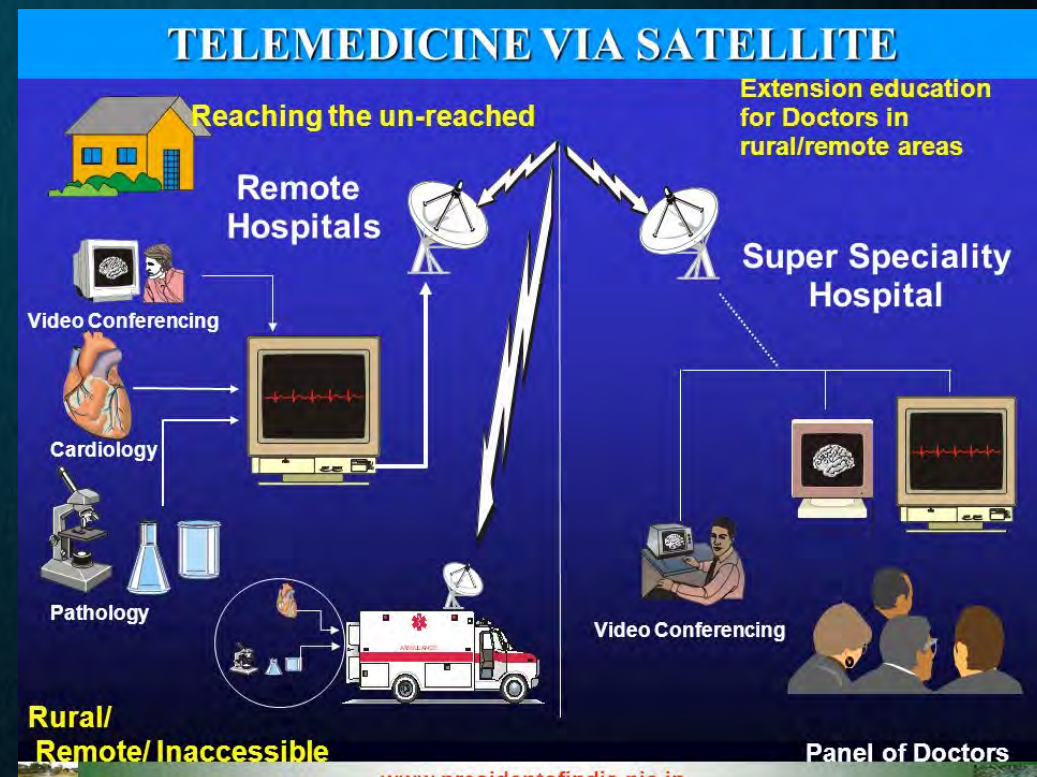
Søk og redning.

Nødpeilesendere vil ikke fungere.

Redningsaksjoner vanskeliggjort uten GPS

Telemedisin blir utilgjengelig

113-Appen vil ikke gi din posisjon

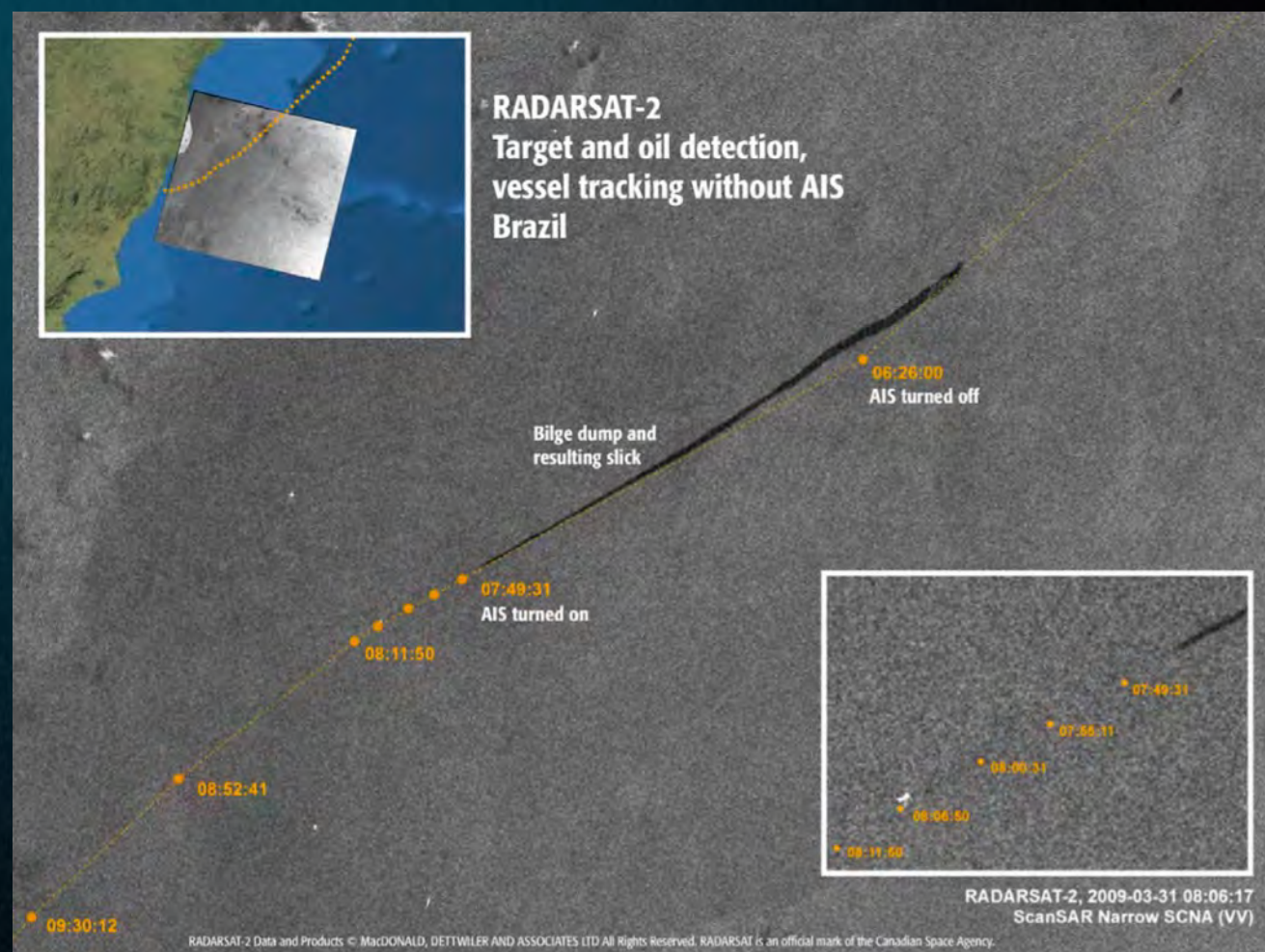


Flere dager uten satellitter

Umulig å overvåke skipstrafikk, ulovlig fiske og oljesøl

Umulig å få oversikt over katastrofeområder etter jordskjelv/flom og styre redningsarbeidet

Umulig å følge opp avskoking i Amazonas



Skip og oljesøk



Jordskjelv - før og etter



Følge med på avskoking

GPSLogic

Flere dager uten satellitter

Utfordringer for forsvaret

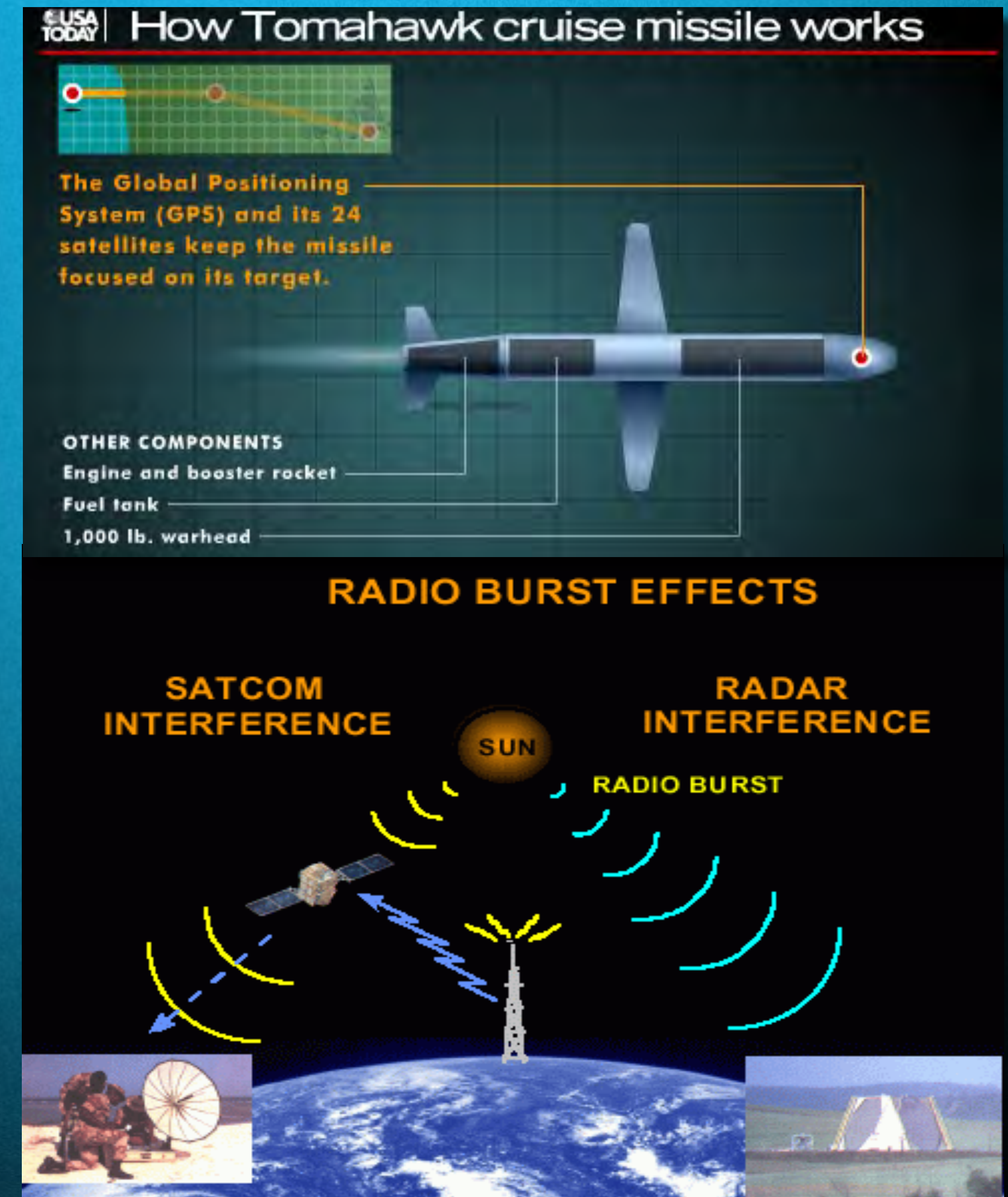
Smarte bomber og våpensystemer

Satellittkommunikasjon med tropper.

Militære satellittsystemer

Tidlig varslingsystemer

HF satellittkommunikasjon (SATCOM)

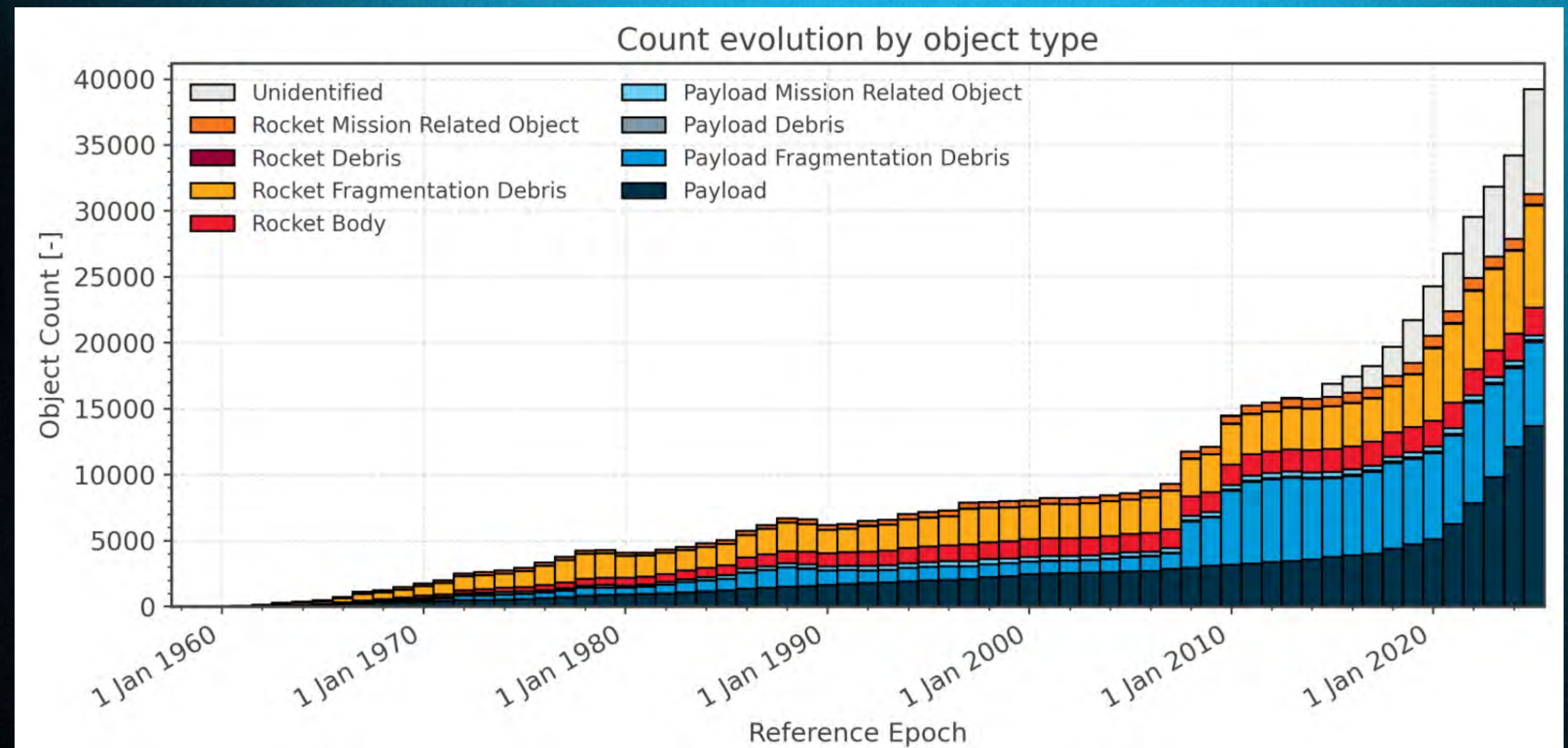


Satellitter og romsøppel

- 6840 raketter
- 20650 satellitter skutt opp
- 13660 fremdeles i bane
- 11100 operative
- 39230 objekter overvåkes
- Total masse: 13500 tonn
- 40500 objekter > 10 cm
- 1.1 million objekter 1 - 10 cm
- 130 millioner objekter 1 mm - 1 cm

2024:

- 259 oppskytinger
- 2802 satellitter ble skutt opp



US Space Surveillance Network

Hva kan slå ut kritisk rominfrastruktur

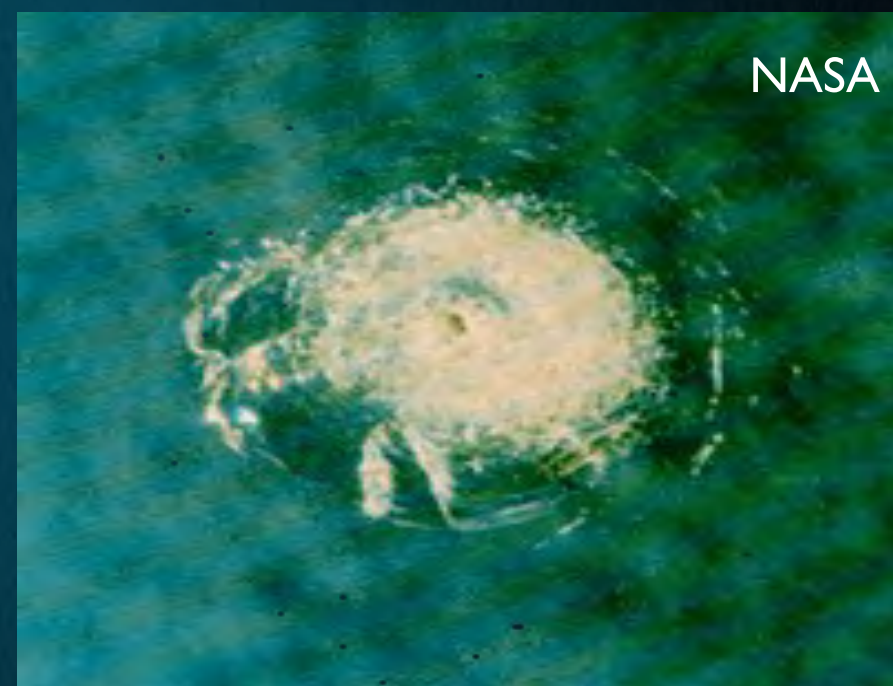
- Romsøppel
- Asteroider/meteoritter
- Jamming/Cyber-angrep
- Antisatellittvåpen – fra bakken og i rommet
- Solstormer

Slike trusler mot rominfrastrukturen er reell og myndigheter verden rundt jobber nå med å gjøre systemene mest mulig robuste.

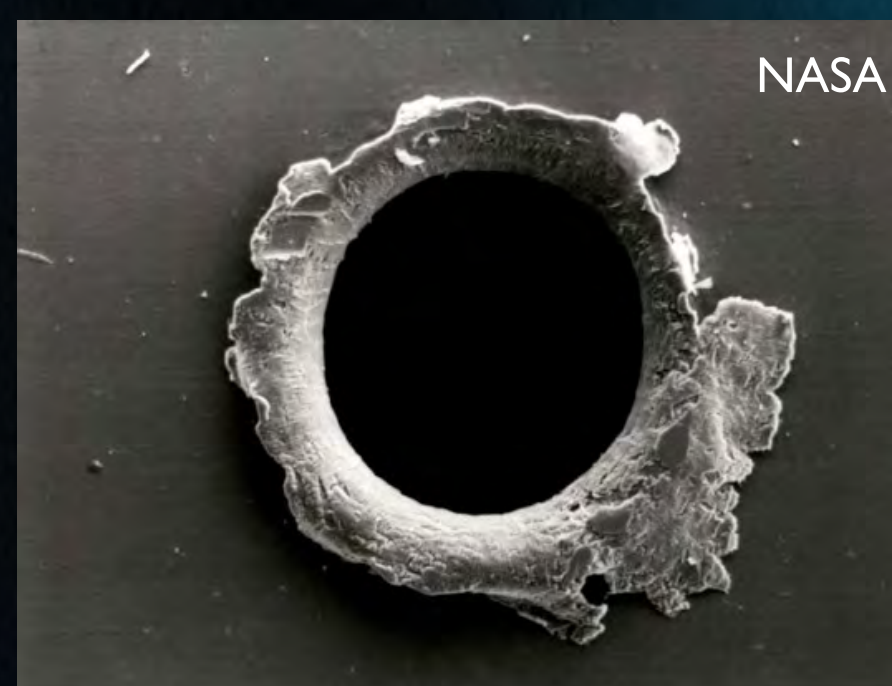


Romsøppel

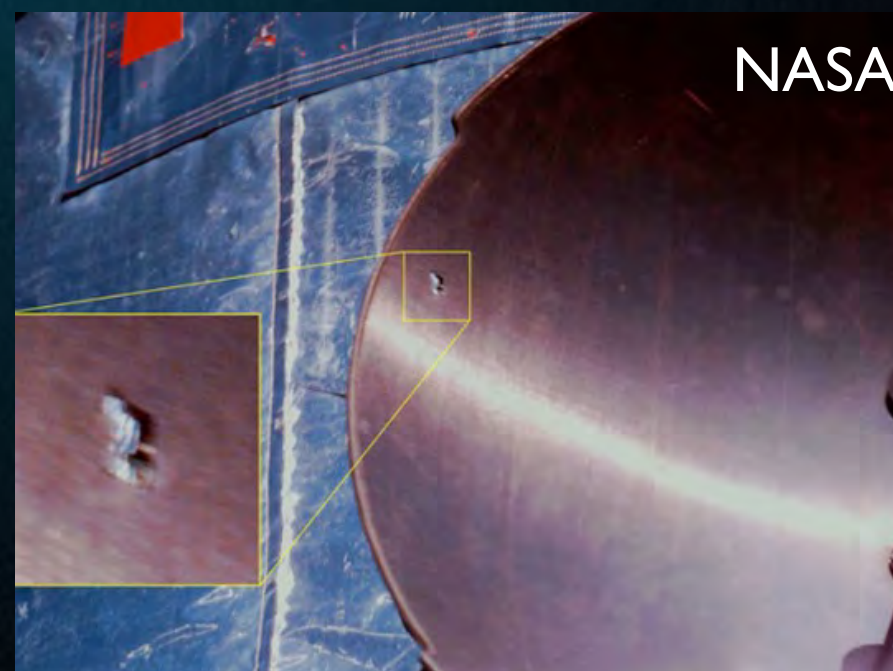
- Kollisjoner med satellitter
- Kollisjoner med fragmenter



Front window Space Shuttle



Hole in the Solar Maximum Mission



Hole in the parabola antenna Hubble



4 cm hole in the solar panel on Hubble

Interferens og tilsiktede forstyrrelser

- Radiosystemer kan utilsiktet forstyrre hverandre
- Fiendtlig forstyrrelser
 - Jamming
 - Narring

Nettavisen **Nyheter.**

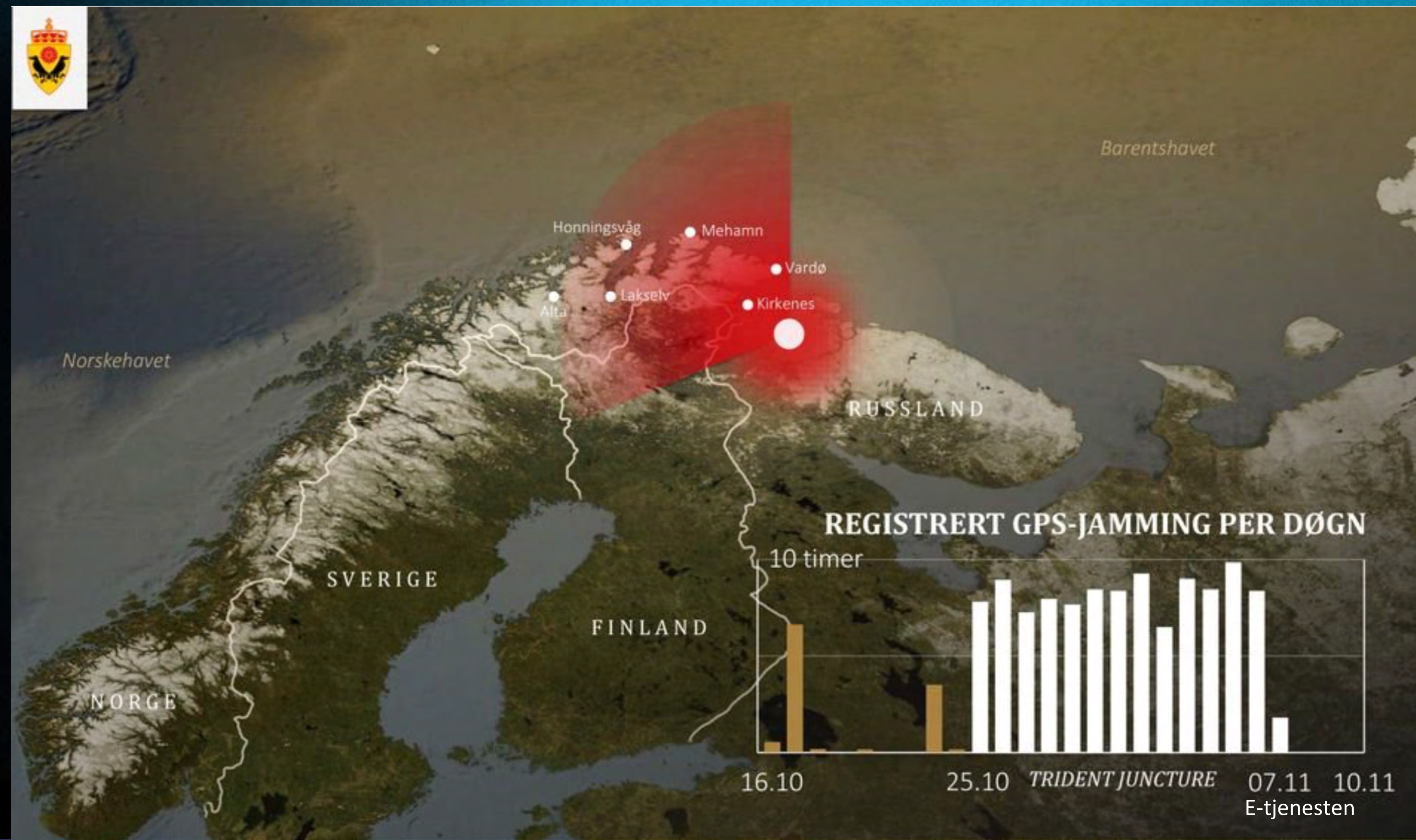
Direktesport Pluss Na Live Nyhetsbrev Sportspill Annonsering Meny

Russland

Mistenker at russisk GPS-angrep rammer 46.000 feriefly



Ryanair var blant flyselskapene som opplevde navigasjonsproblemene. Foto: Getty Images



Antisatellitsystemer

- Antisatellitsystemer på bakken eller i rommet kan slå ut satellitter vi er avhengige av.
- Antisatellitthendelser kan skape enorme mengder romsøppel og slik ende med å ta ut mye mer enn kanskje intensjonen var.



Getty images

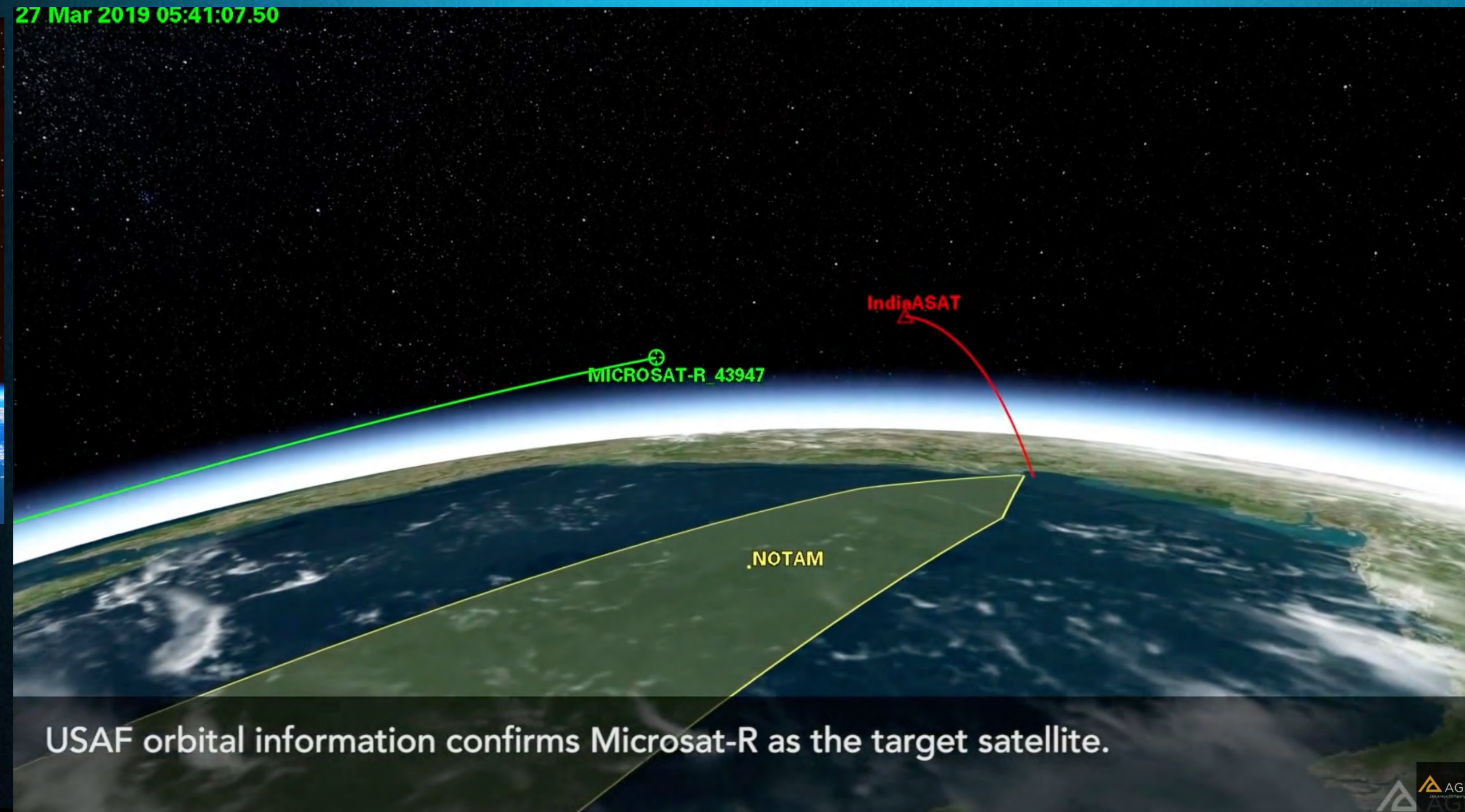


Antisatellitsystemer

- Antisatellitsystemer på bakken eller i rommet kan slå ut satellitter vi er avhengige av.
- Antisatellitthendelser kan skape enorme mengder romsøppel og slik ende med å ta ut mye mer enn kanskje intensjonen var.



Getty images



Antisatellitsystemer

- Antisatellitsystemer på bakken eller i rommet kan slå ut satellitter vi er avhengige av.
- Antisatellitthendelser kan skape enorme mengder romsøppel og slik ende med å ta ut mye mer enn kanskje intensjonen var.



Getty images

27 Mar 2019 05:15:00.00



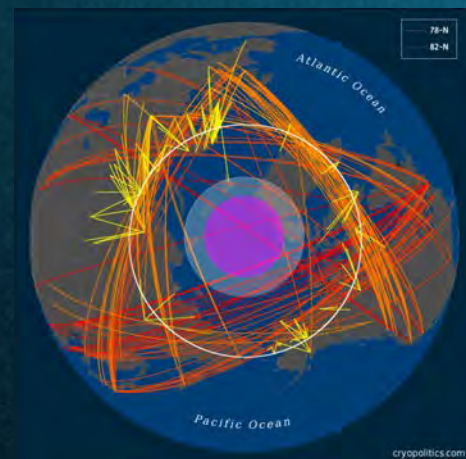
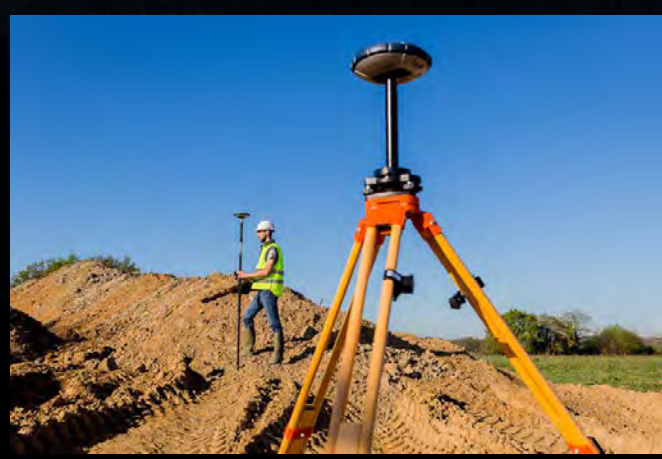
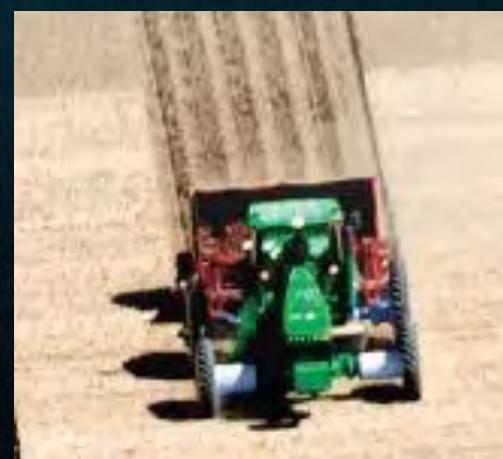
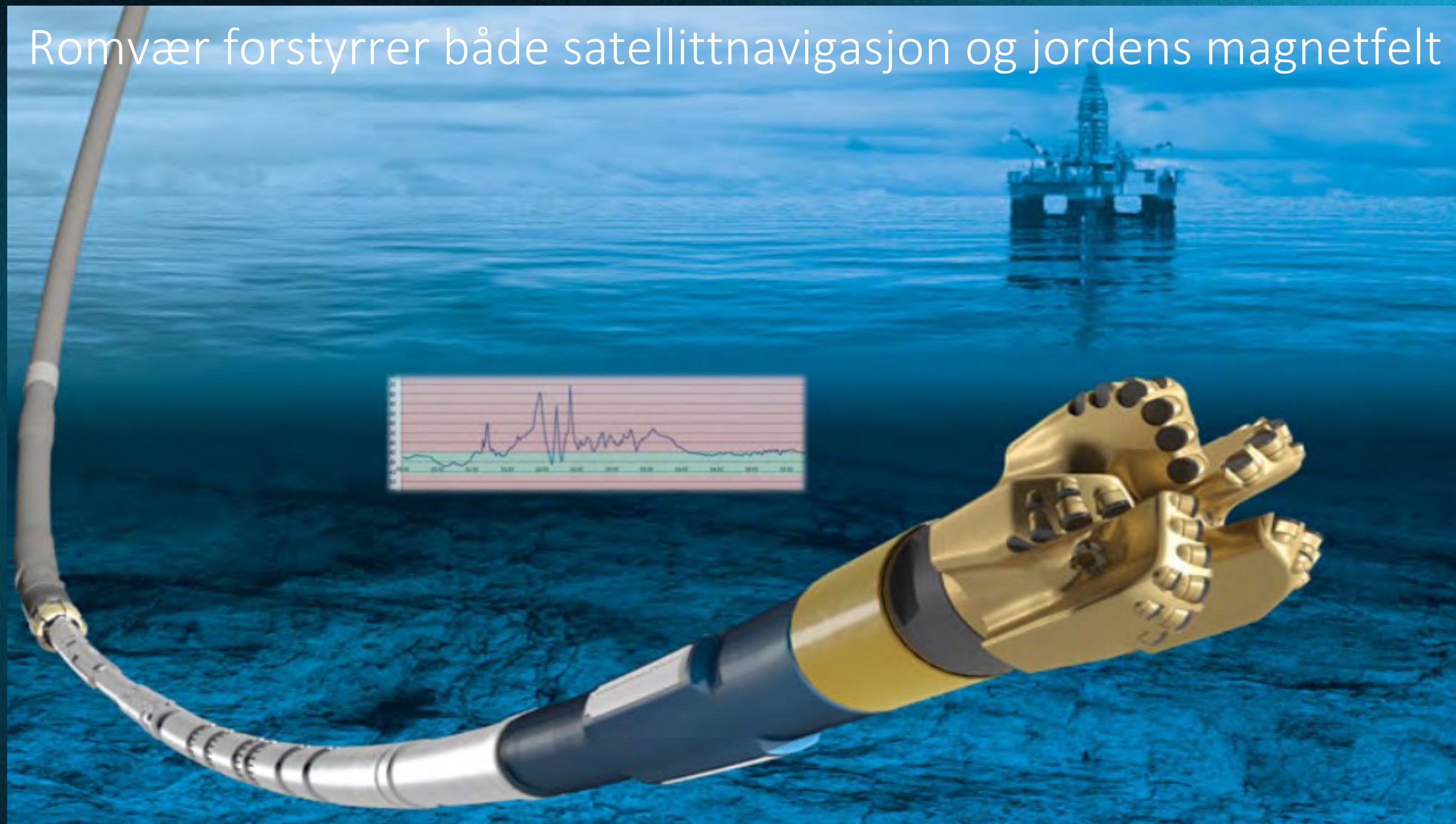
Romvær

De effektene Solen har på Jorden og dens nære verdensrom kalles romvær.



Vanlige romværsdager

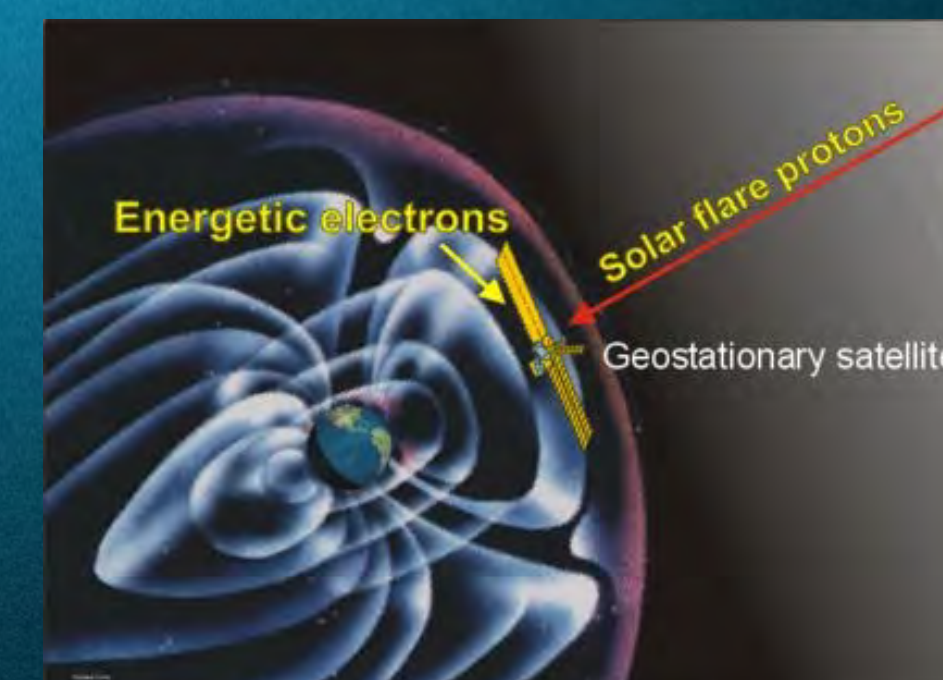
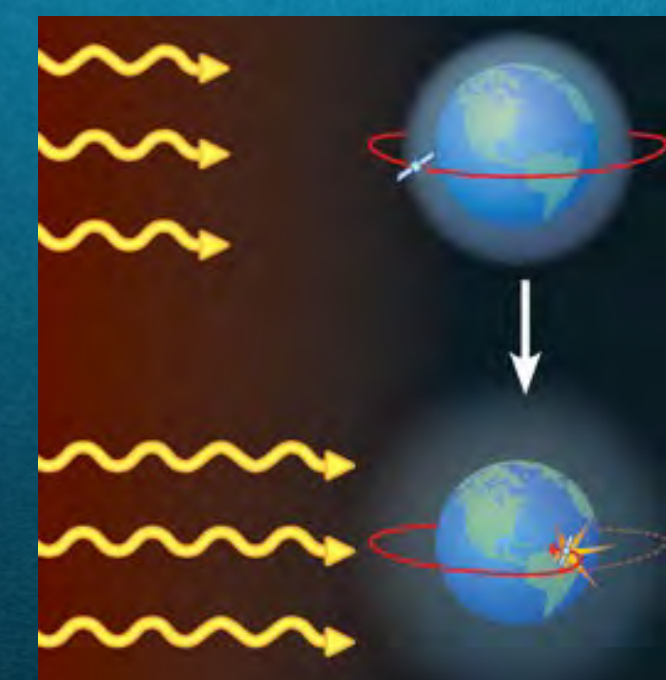
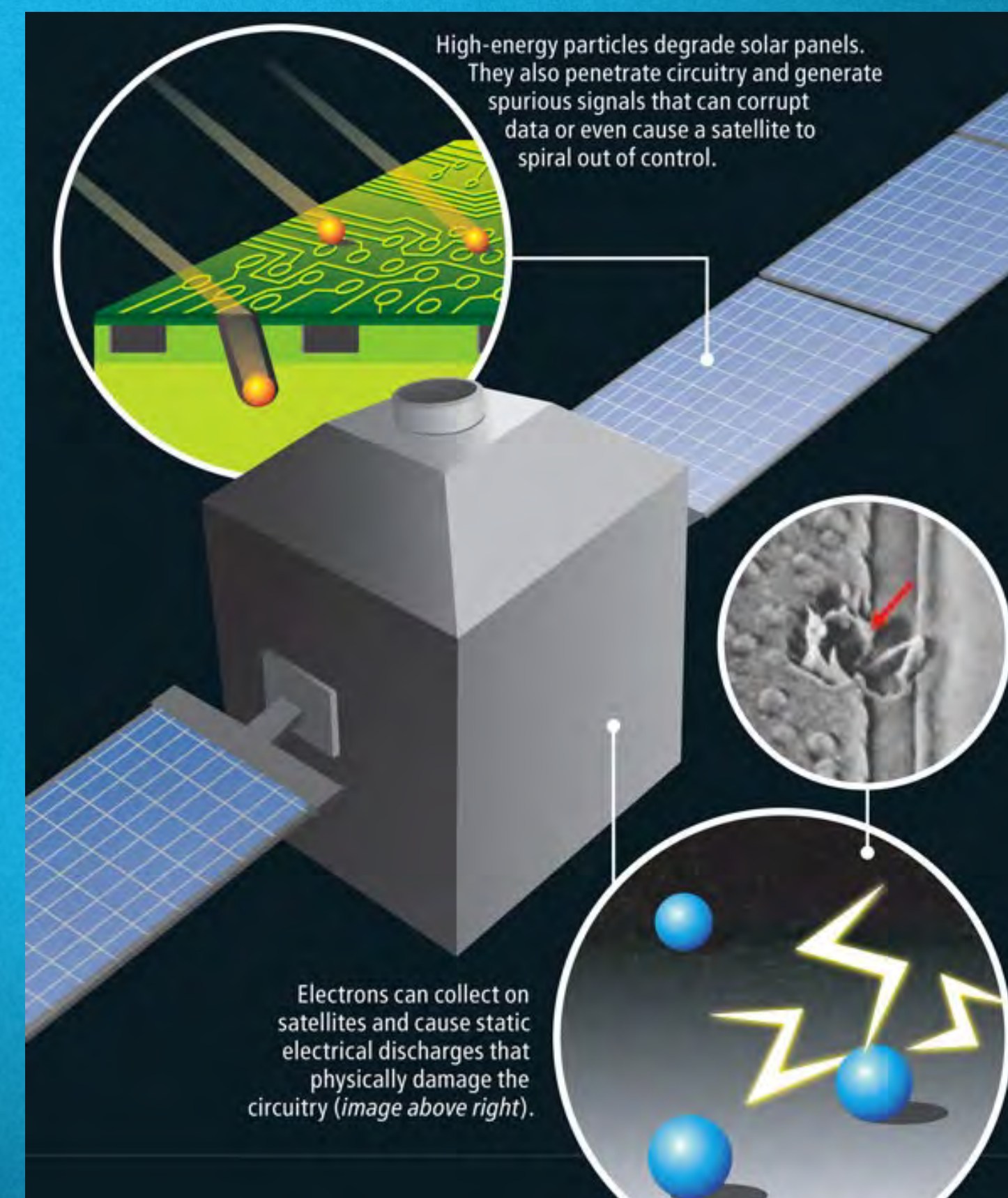
Romvær forstyrrer både satellitnavigasjon og jordens magnetfelt



NASA

Effekter på satellitter

- Statisk utladning
- Skader på elektronikk grunnet høyenergipartikler
- Degradering av materialer/solpaneler grunnet høyenergipartikler
- Støy på stjerne «trackers»/navigasjonssystemer grunnet høyenergipartikler
- Orienteringsproblemer
- Økt «luft»-motstand (friksjon/drag)
- Mikro meteoritt-skader
- Romsøppel-treff
- Signalforstyrrelser



Romvær slo ut personsøkertjenester

I 1998 ble Galaxy IV satellitten skadet av romvær. Satellitten kostet 250 millioner USD og overførte 80% av alle personsøkertjenester i USA (påvirket 40 millioner personsøkere). Den sendte og PC-Direct, NPR, CBS radio og CNNs airport TV.



Figure courtesy of The Solar Data Analysis Center

SpaceX Starlink satellitter falt ned etter solstorm

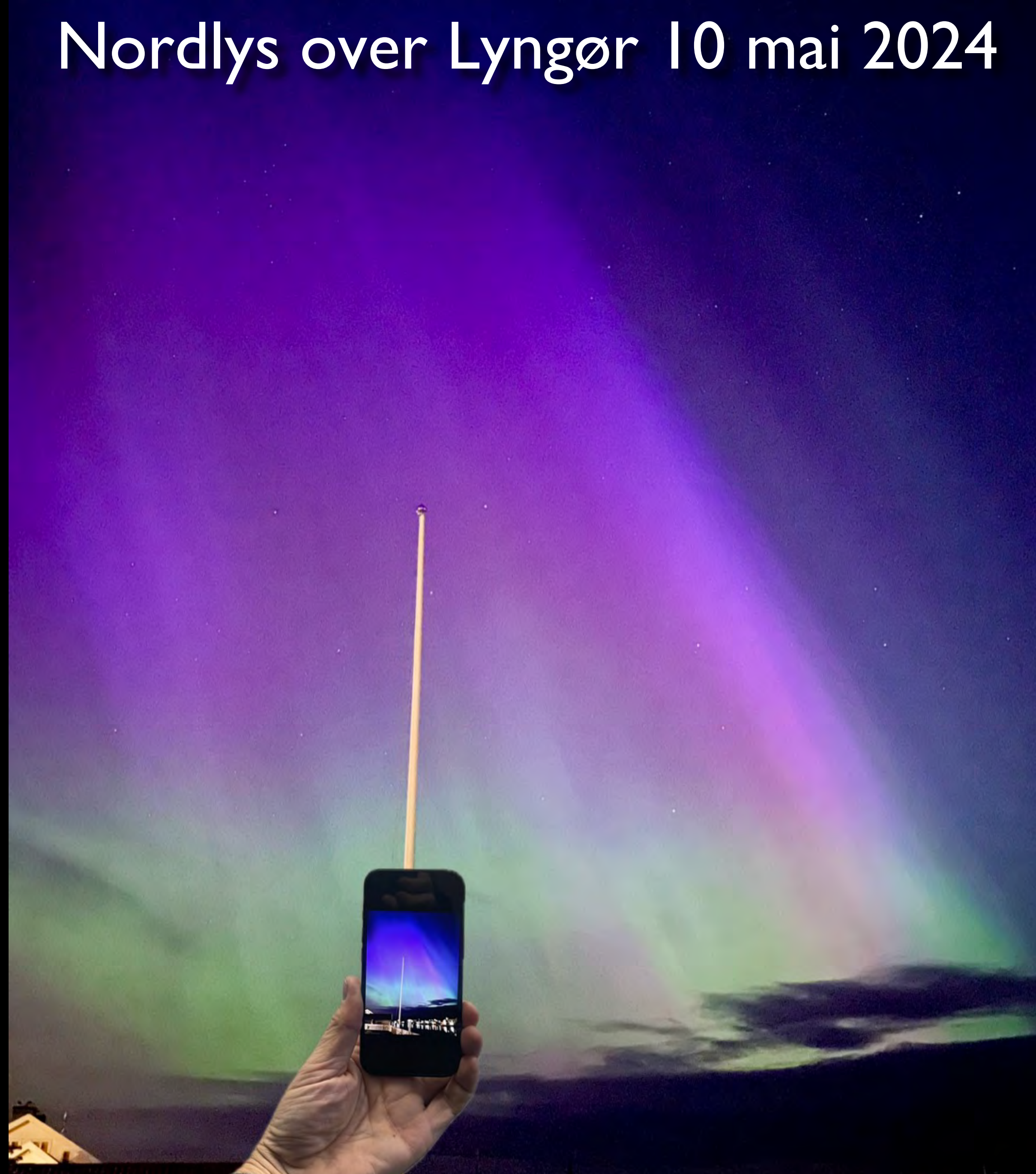
SpaceX Starlink satellitter falt ned etter en geomagnetisk storm 3 februar 2022

40 av 49 satellitter gikk tapt og brant opp i atmosfæren.

Solstormen førte til at friksjonen økte med 50%



Nordlys over Lyngør 10 mai 2024



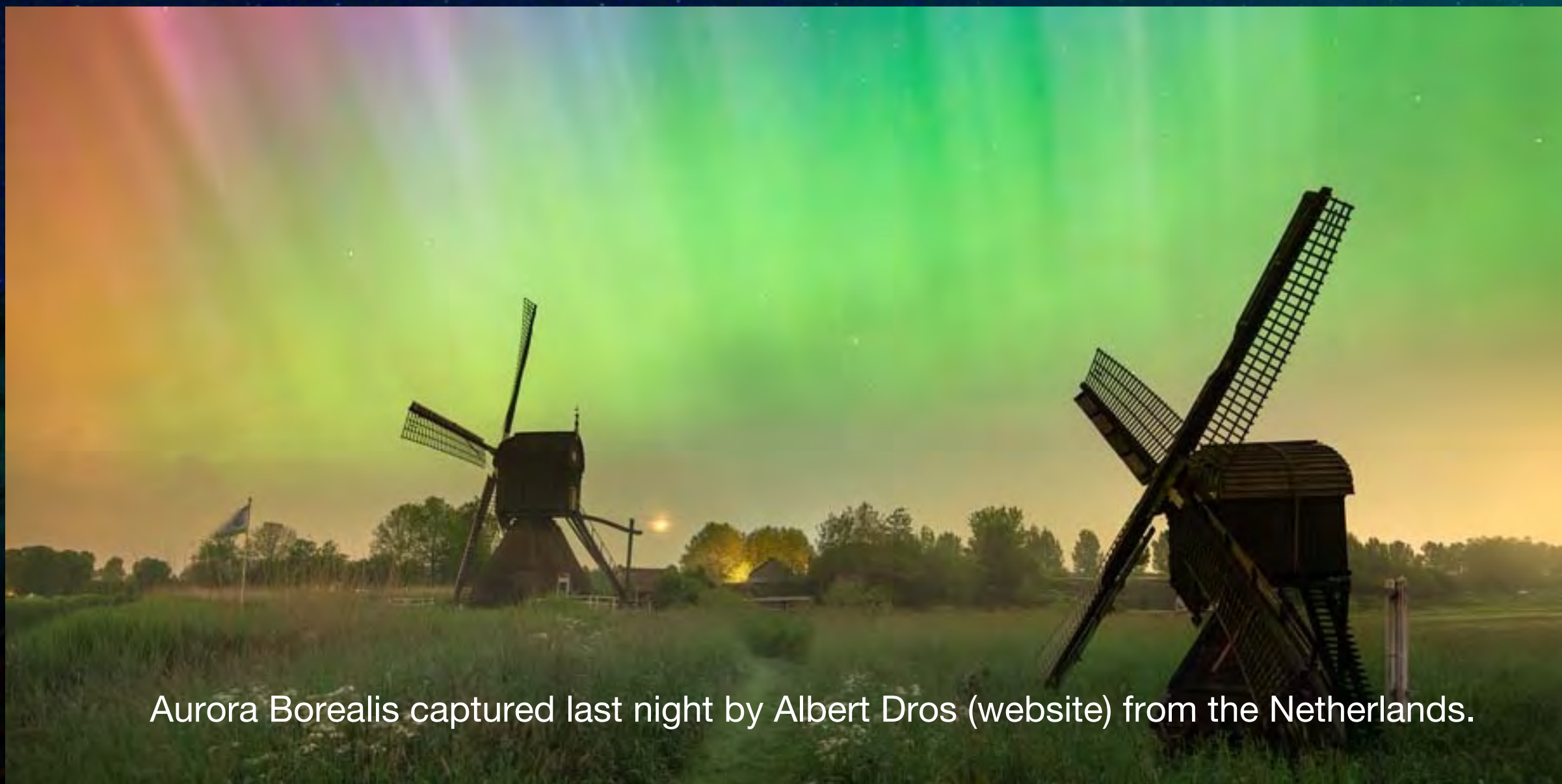
Taken by Kyle Las Vegas, NV



Taken by Marc Hochreutener in Eggersriet, Switzerland



Aurora Borealis captured last night by Albert Dros (website) from the Netherlands.

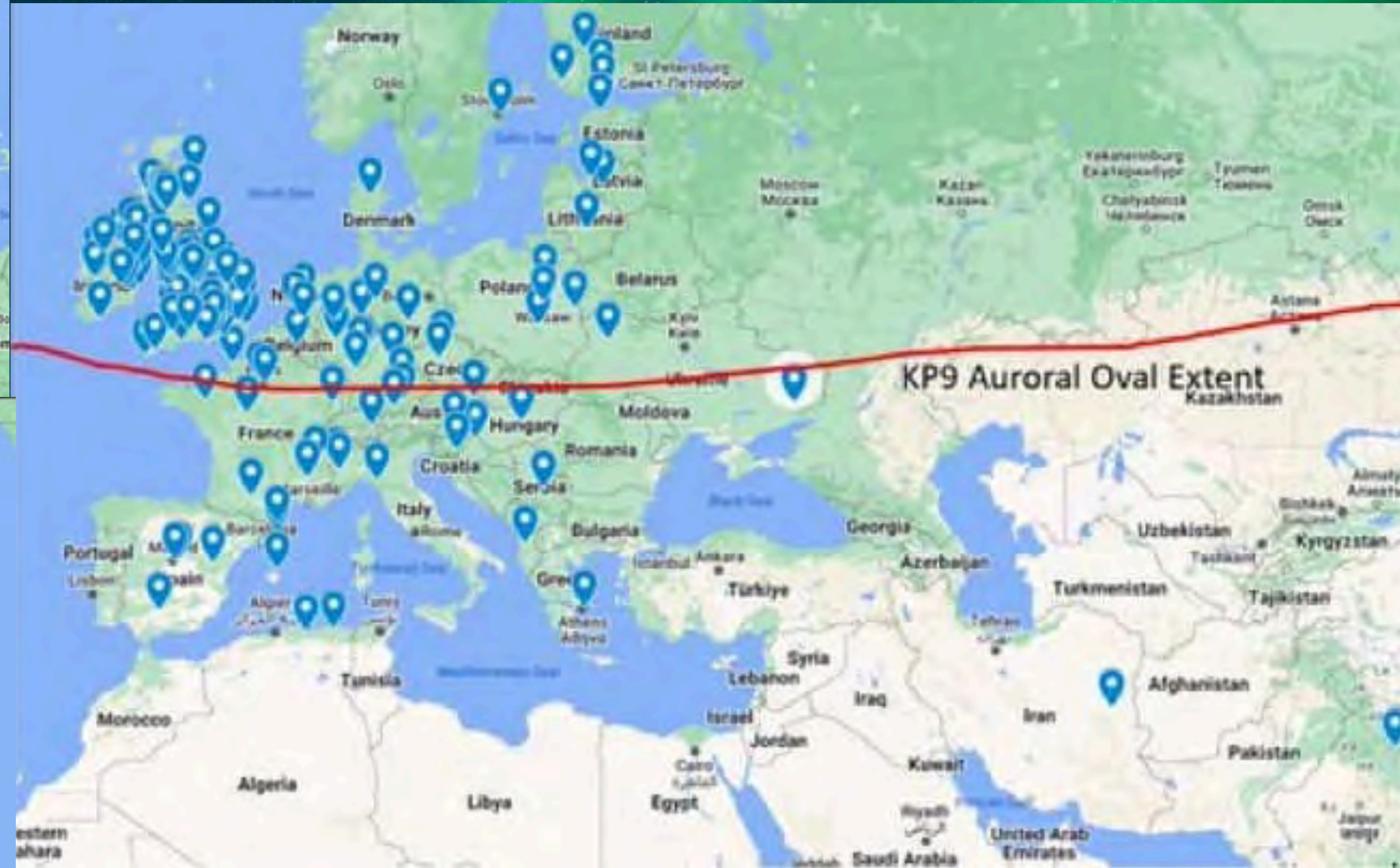
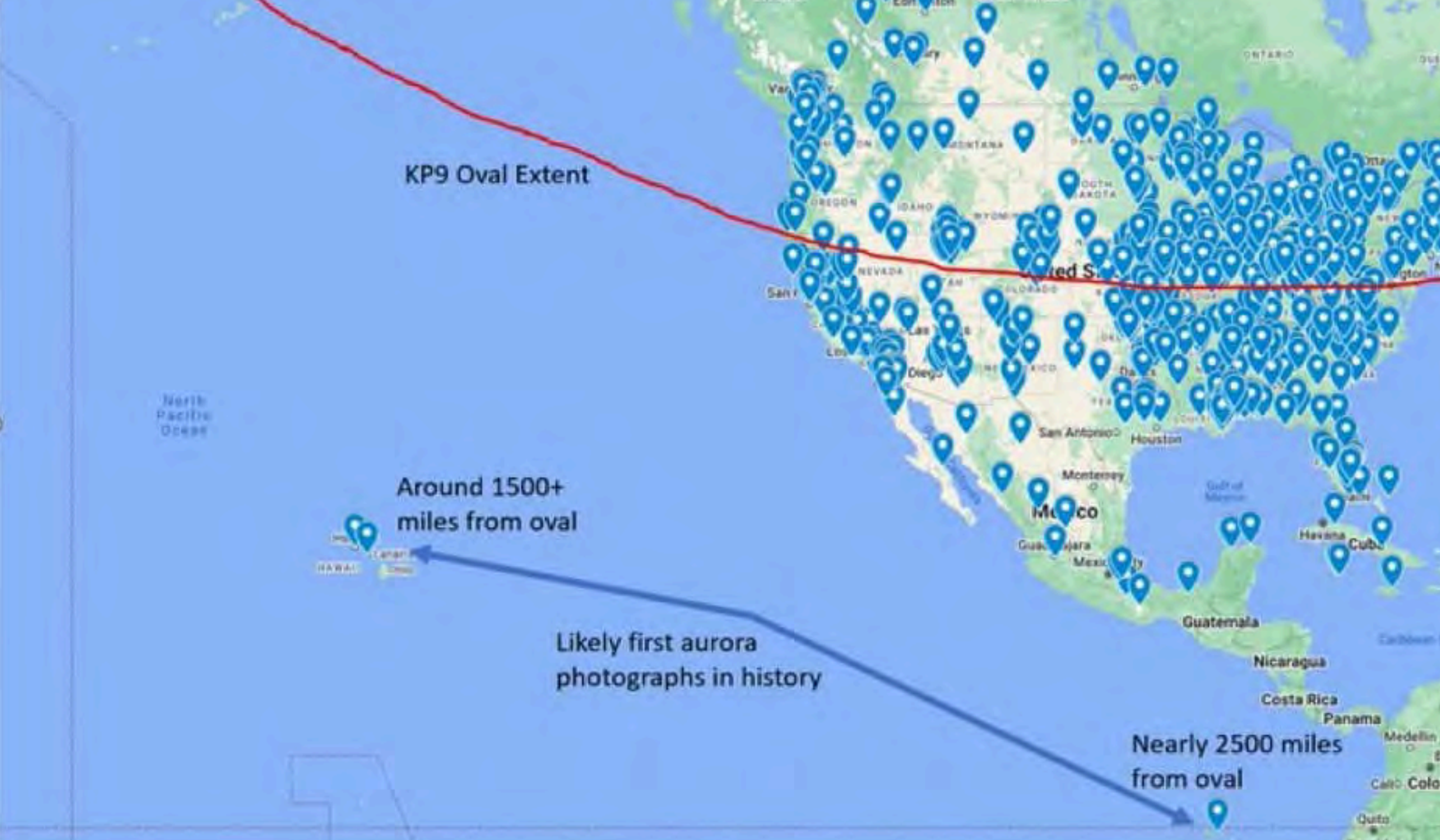


Taken by Denis Martinez on May 11, 2024 @ LAS GRUTAS- ARGENTINA

@DenisMartinez



100 millioner mennesker fikk sett nordlys for første gang



Noen effekter av denne stormen

TRACTORS

Solar Storm Knocks Out Farmers' Tractor GPS Systems During Peak Planting Season

JASON KOEBLER · MAY 12, 2024 AT 9:39 AM

The accuracy of some critical GPS navigation systems used in modern farming have been "extremely compromised," a John Deere dealership told customers Saturday.



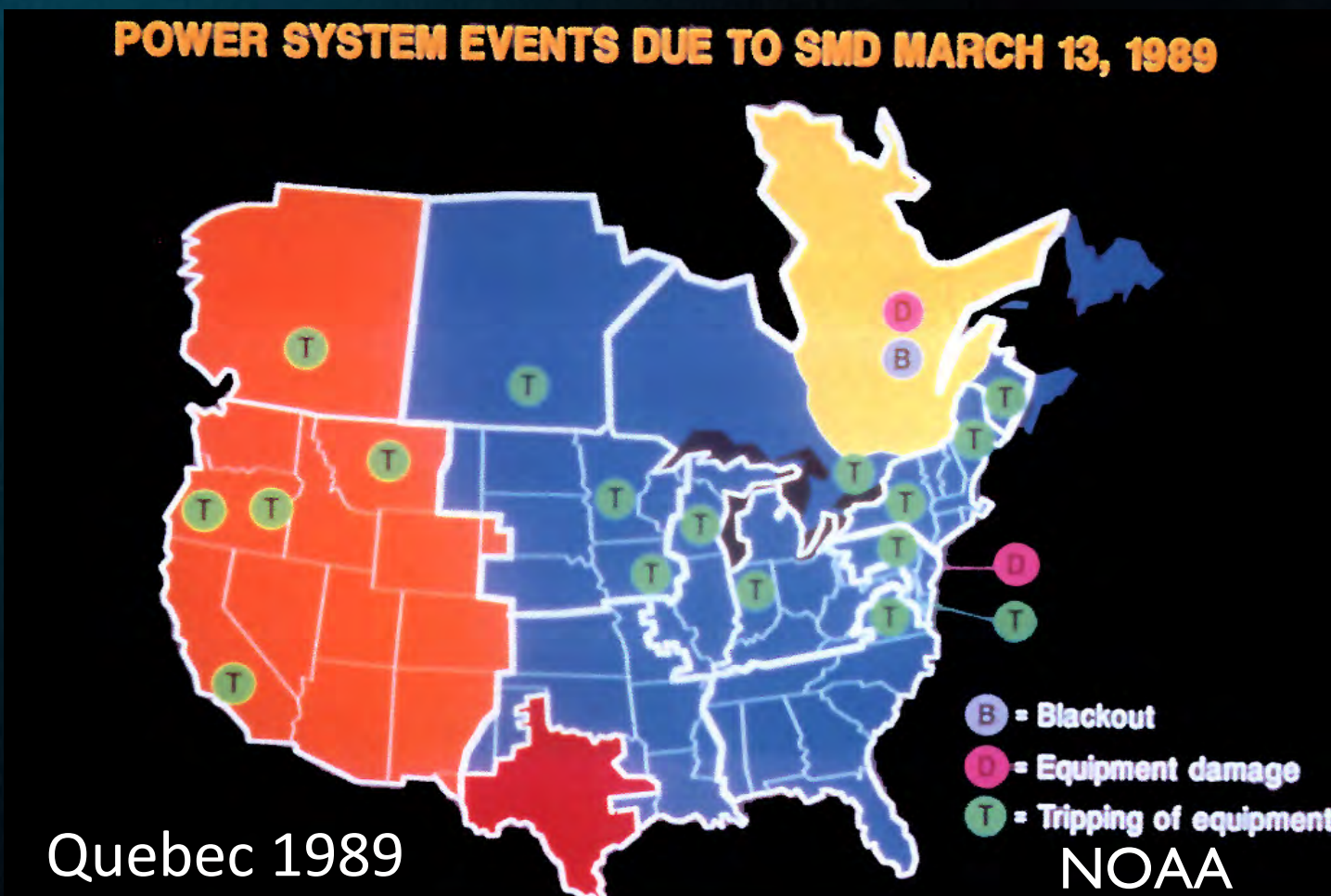
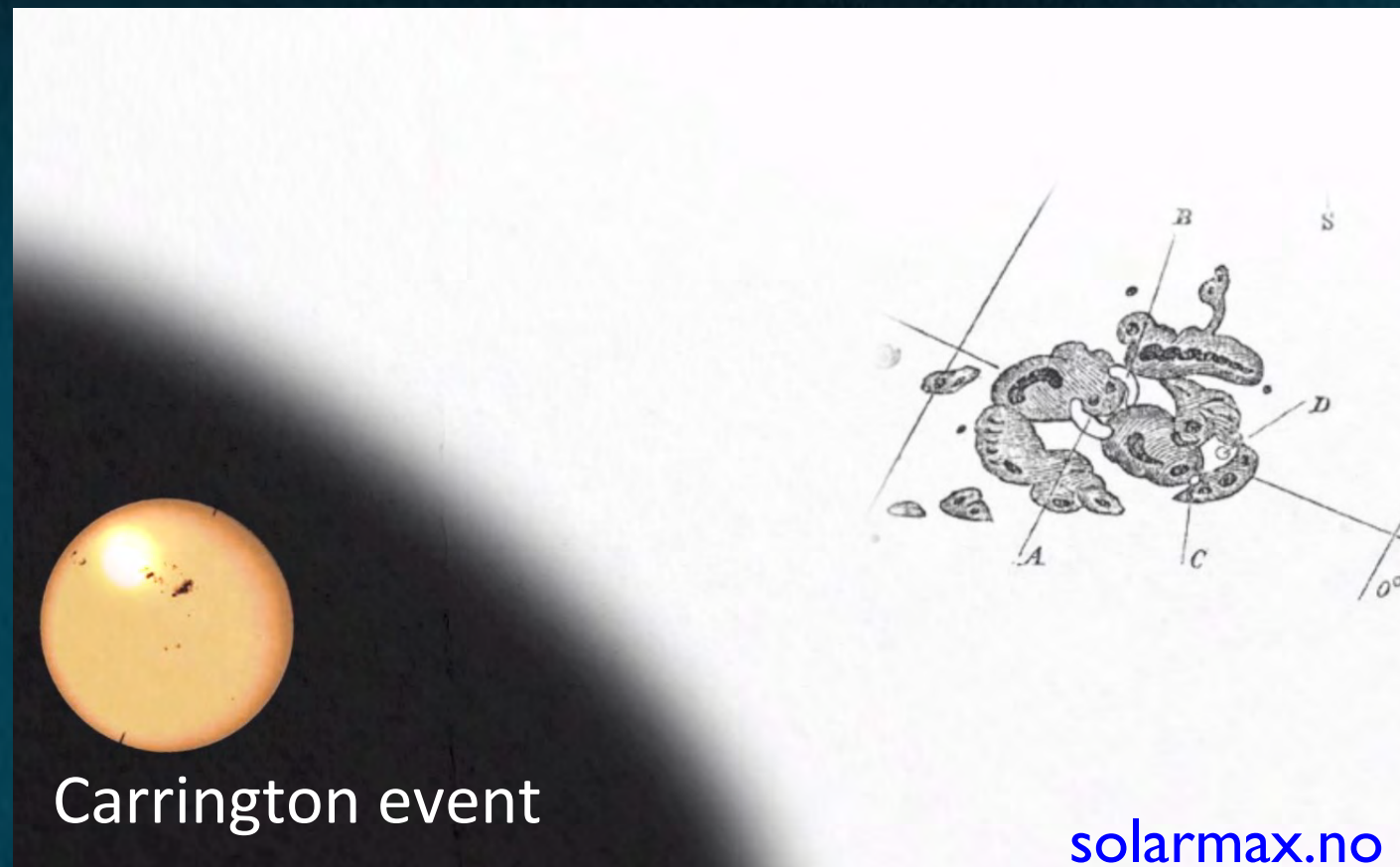
IMAGE: JOHN DEERE



Starlink Reports 'Degraded Service' as Severe Geomagnetic Storm Impacts Earth

May 11, 2024 • Ben Townsend

Superstormer - Carrington 1859



Extreme Solar Weather Has Happened Before



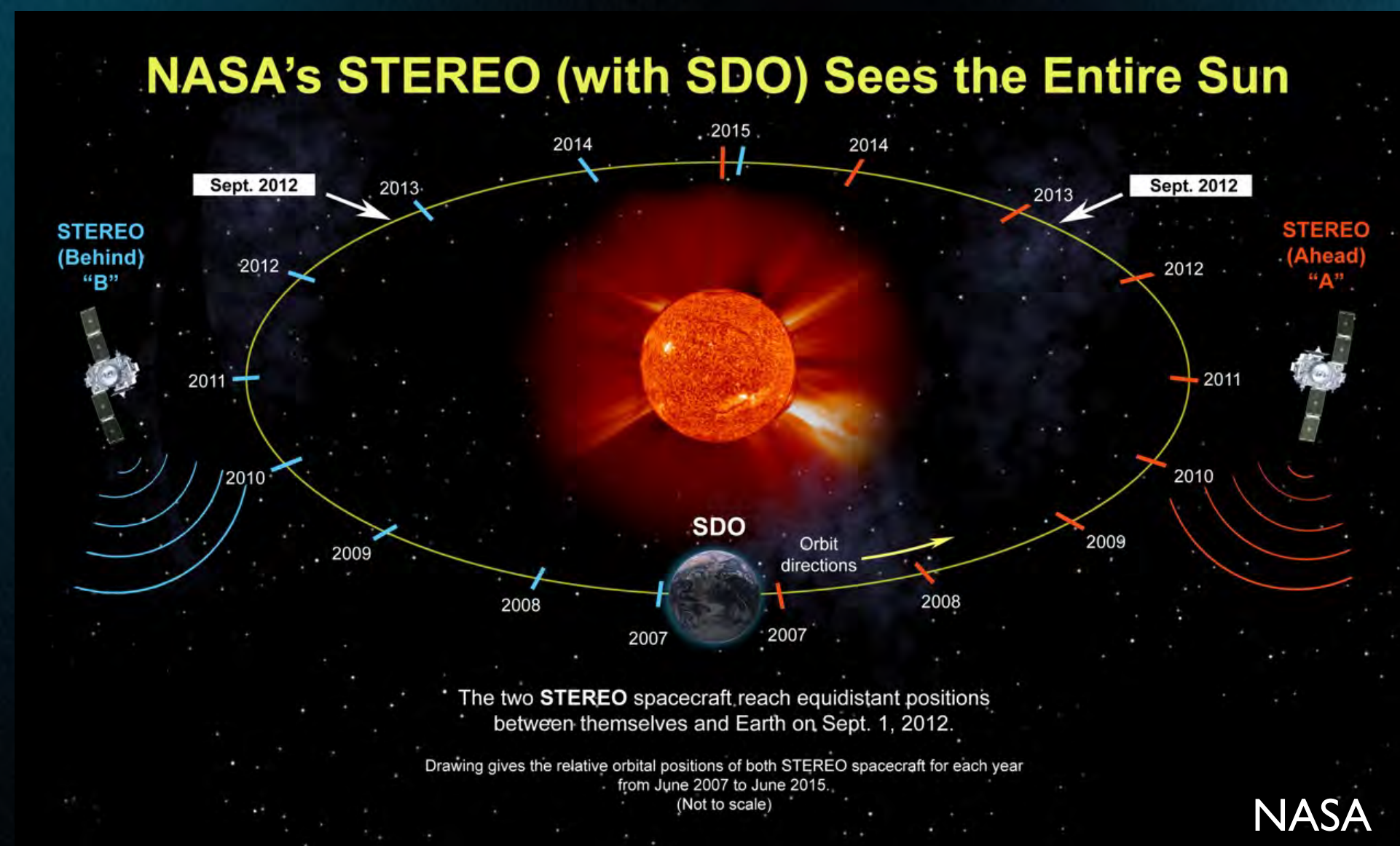
Photo from www.telegraphlore.com

- **1847** – “Anomalous current” noted on telegraph line between Derby and Birmingham. First recorded impact of solar weather on technology.
- **August 28-29, 1859** – Telegraph service disrupted worldwide by geomagnetic superstorm.
- **September 1-2, 1859** – Carrington-Hodgson event is largest geomagnetic storm in 500 years.
- **May 16, 1921** – The “Great Storm” disrupted telegraph service, caused fires, burned out cables. **Storms like this may occur roughly every 100 years.**
- **March 13, 1989** – Geomagnetic storm collapsed Quebec power grid. Northeast U.S. and Midwest power grid came within seconds of collapse.
- **October 19 – November 7, 2003** – “Halloween Storms” interrupted GPS, blacked out High Frequency (HF) radio, forced emergency procedures at nuclear power plants in Canada and the Northeastern United States, and destroyed several large electrical power transformers in South Africa.

NOAA

2012: 9 dager unna en «katastrofe»

Den 23 juli 2012 observerte en av NASA's Stereo-sonder en superstorm med en hastighet på 8 millioner km/t.



MailOnline Science

Home | News | U.S. | Sport | TV&Showbiz | Australia | Femail | Health | **Science** | Money

Science Home | Pictures | Gadgets Gifts and Toys Store

Businessman sets up private toll road | Prince Charles' 'fury' as former | Diana's favourite DJ Mike Smith dies at | Best hotel in Britain is Birmingham's

Solar flare almost blasted Earth back to the dark ages two years ago, NASA scientists reveal

CBSNEWS Video US World Politics Entertainment Health MoneyWatch SciTech Crime Sports Photos More

By ELIENE AUGENBRAUN CBS NEWS July 25, 2014, 3:07 PM

Solar "superstorm" just missed Earth in 2012

One of the top five fastest coronal mass ejections (CME) that scientists have ever observed, and the fastest observed by STEREO, blasted away from the sun on July 22, 2012. NASA/STEREO

18 Comments / 563 Shares / 141 Tweets / Stumble / @ Email / More +

GO BEHIND THE SCENES ON THIS SUMMER'S HOTTEST SHOW! CBS

READY FOR ACTION: TALES FROM UNDER THE DOME WATCH NOW

Presented by **edge**

Most Popular

- 01 Obama: "We tortured some folks" after 9/11 57912 views
- 02 Body of boy who'd been dead for days found in home 44838 views
- 03 First American Ebola patient arrives in U.S. from Africa 29795 views
- 04 Teen severely burned in online "fire challenge"

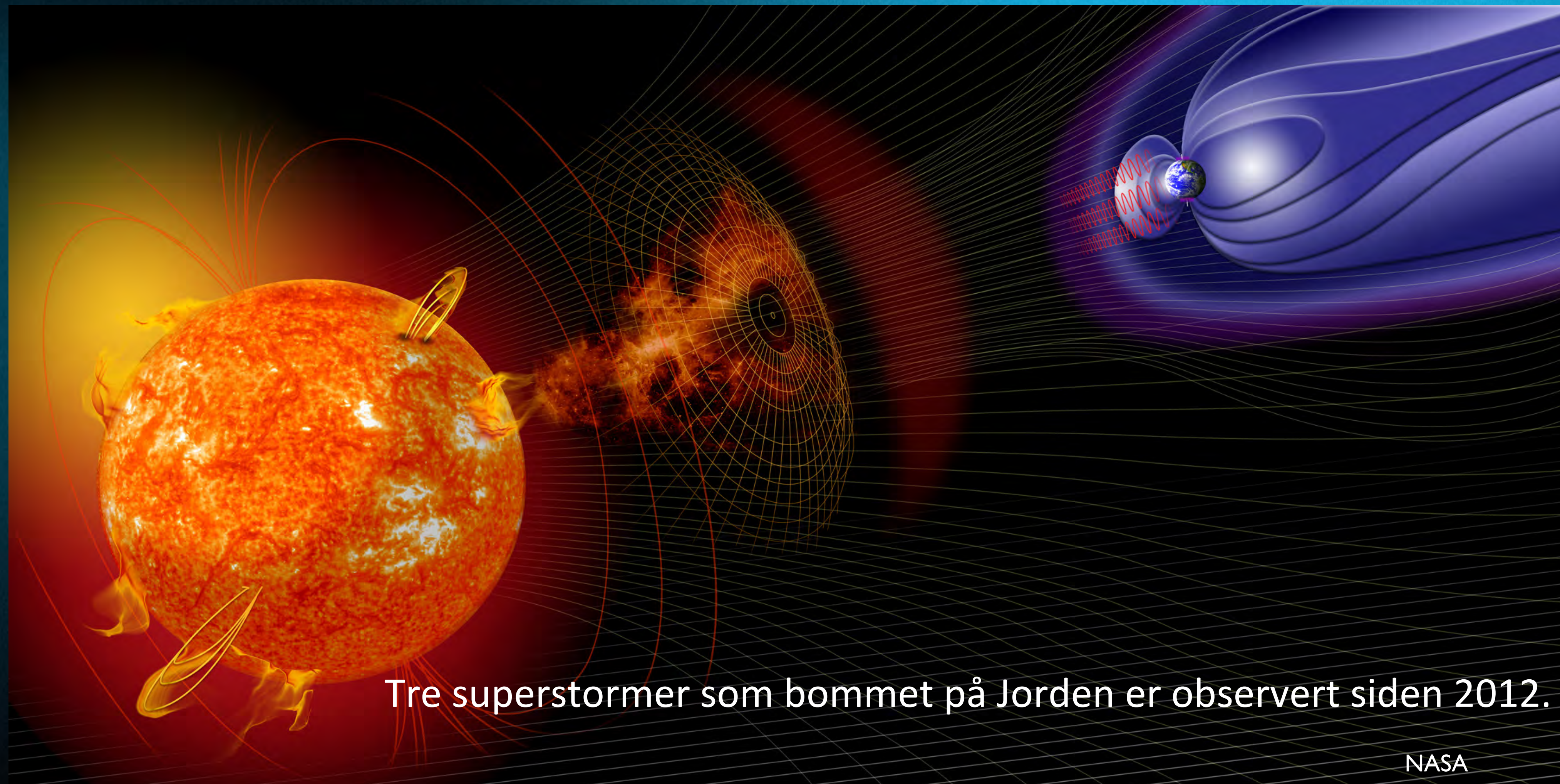
ed away from the sun as fast as 3000 km/s

t one week earlier, the blast site would have

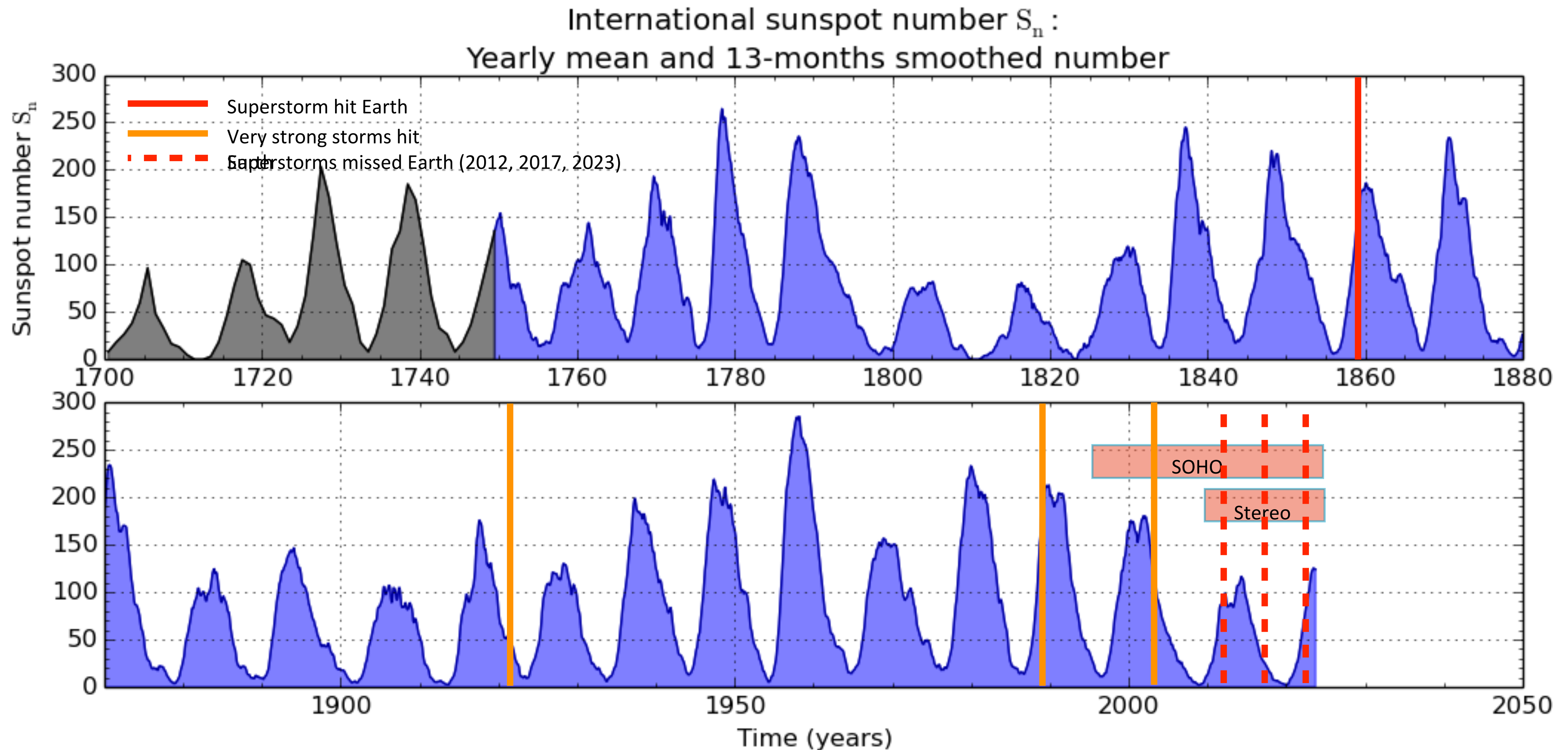
read power blackouts, disabling everything

ave exceeded \$2 trillion or 20 times greater Katrina

Hvor ofte inntreffer superstormer?



Superstormer de siste 150 år



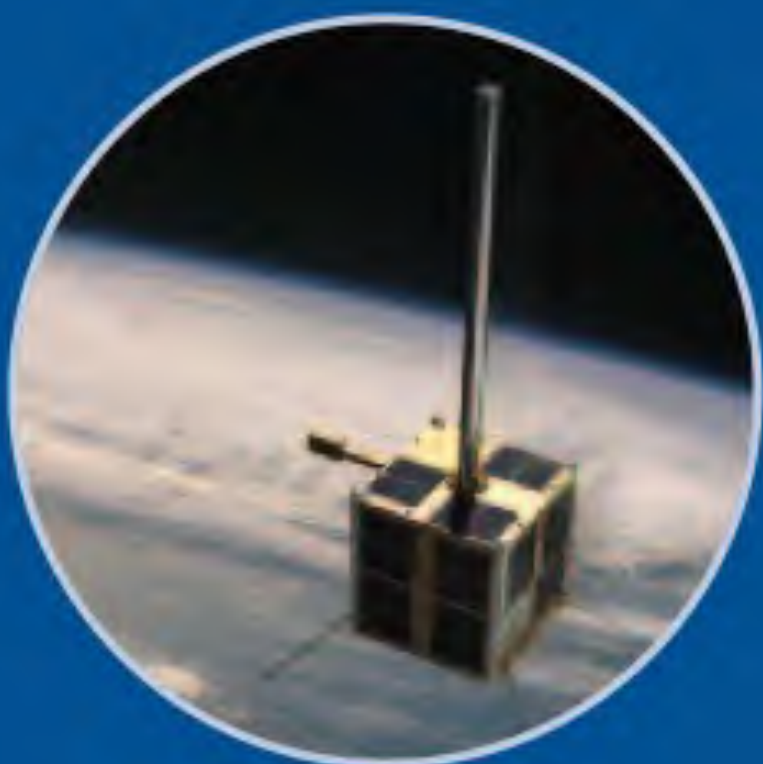
SILSO graphics (<http://sidc.be/silso>) Royal Observatory of Belgium 2024 April 18

The red lines are previous strong storms - where the 1859 storm was the only real super-storm. The two dotted lines are the recent super-storms that was on the far side of the Sun. It is only after SOHO (1995) we have been able to observe CMEs and super-storms. So we have no idea how many superstorms the Sun has produced between 1859 - 1995.



NRK

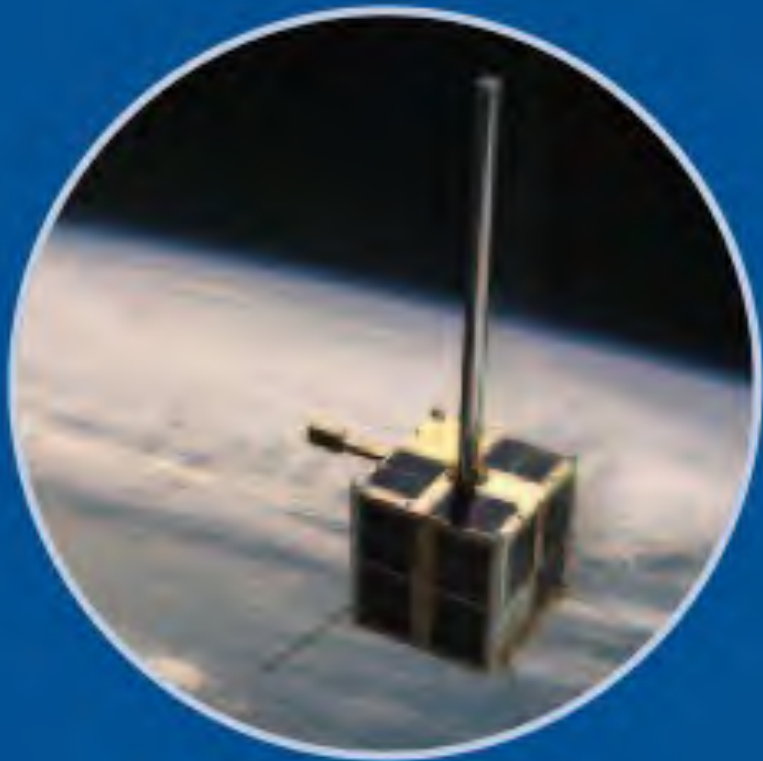
Hva er du avhengig av?



Har du oversikt over hva du bruker satellitter til?

Hva er din plan B om du mister disse tjenestene?

Hva skjer om du mister disse tjenestene?



- Klarer du å oppdage tap, forstyrrelse eller falske signaler?
- Er det krise om de blir borte en liten stund – eller lenge?
- Kan du hente signaler fra flere satellittsystemer?
- Kan du få signaler fra andre systemer mens satellittene er borte?
- Kan du få utført oppgavene på en annen måte (teknologi, opplæring og prosedyrer)?

Bevisthetsøvelse for avhengighet av GNSS

 DSB

Fagområder ▾ Tjenester og ressurser ▾ Søk Q

Hjem / Øvelser / Alle øvelser / Bortfall av satellittbaserte tjenester

Bortfall av satellittbaserte tjenester

Om øvelsen

Scenarioet i denne diskusjonsøvelsen handler om hvilke konsekvenser det vil kunne få for en norsk kommune at satellittbaserte tjenester faller bort eller forstyrres. Øvelsen har følgende formål:

- Avdekke i hvilken grad kommunen er avhengig av satellittbaserte tjenester.
- Kartlegge hvilke konsekvenser bortfall av slike tjenester kan medføre for kommunens kjernefunksjoner/samfunnskritiske funksjoner.

Fakta om øvelsen

- **Type øvelse:** diskusjonsøvelse
- **Tid:** Estimert ca. 2 timer å gjennomføre
- **Passer for:** norske kommuner
- **Målgruppe:** Representanter fra ulike sektorer i kommunen (beredskap, teknisk etat, helse og omsorg, skole, IT, osv.).

 Direktoratet for romvirksomhet

Videoforelesninger

Navigasjon

Tema 2025: Digital Beredskap

Bestill et foredrag

Tilby dine foredrag

Valg

 Print artikkel

 Gå tilbake



Foredragsdugnaden: Digital Beredskap

Foredragsdugnaden er et sentralt tiltak under Nasjonal sikkerhetsmåned, og gir eksperter innen digital sikkerhet en unik mulighet til å dele sin kompetanse med virksomheter over hele landet. Gjennom dugnaden tilbys foredrag kostnadsfritt til bedrifter og organisasjoner som ønsker å styrke sin digitale beredskap.



Hensikten er todelt:

Dugnaden gir virksomheter – særlig små og mellomstore – tilgang til praktisk, relevant kunnskap fra fagfolk med solid erfaring.

Samtidig gir den fagpersoner og selskaper innen cyber-, informasjon- og digital sikkerhet en arena for å bidra direkte til økt bevissthet og kompetanse i samfunnet.

<https://www.dsb.no/ovelser/alle-ovelser/bortfall-av-satellittbaserte-tjenester/>



Takk for oppmerksomheten



Pål Brekke
Fagsjef, Romforskning
paal@spaceagency.no



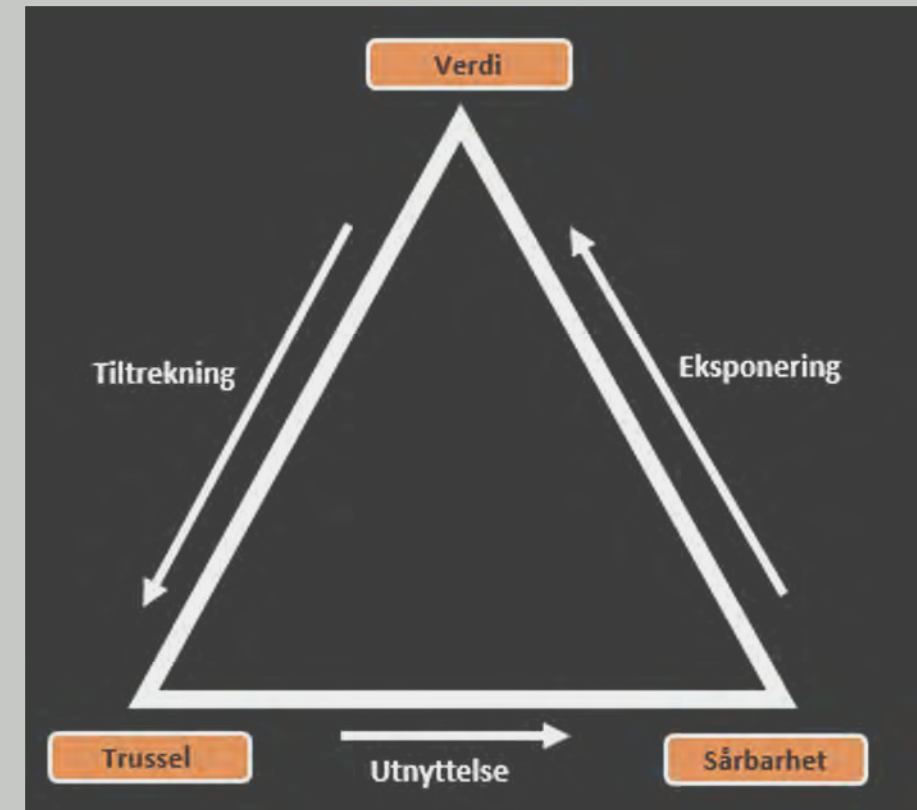
Helhetlig beskyttelse

- Reparasjonsberedskap

Chris McCabe
Fagdirektør NSM

Sannsynlighets og/eller konsekvensreduserende tiltak

- Sannsynlighetsreduserende sikkerhetstiltak:
 - Sikkerhetstiltak som bidrar til å forhindre en uønsket hendelse.
 - Resiliens (motstandsevne)
 - Eks. Sikring: barrierer, deteksjon, verifikasjon, reaksjon
- Konsekvensreduserende sikkerhetstiltak:
 - Sikkerhetstiltak som bidrar til å redusere følgene av en hendelse.
 - Eks. Redundans (dublerte funksjoner)
 - Reetableringsplaner



Grunnsikringstiltak



Sikringstiltak ved normaltilstand

Påbyggingstiltak

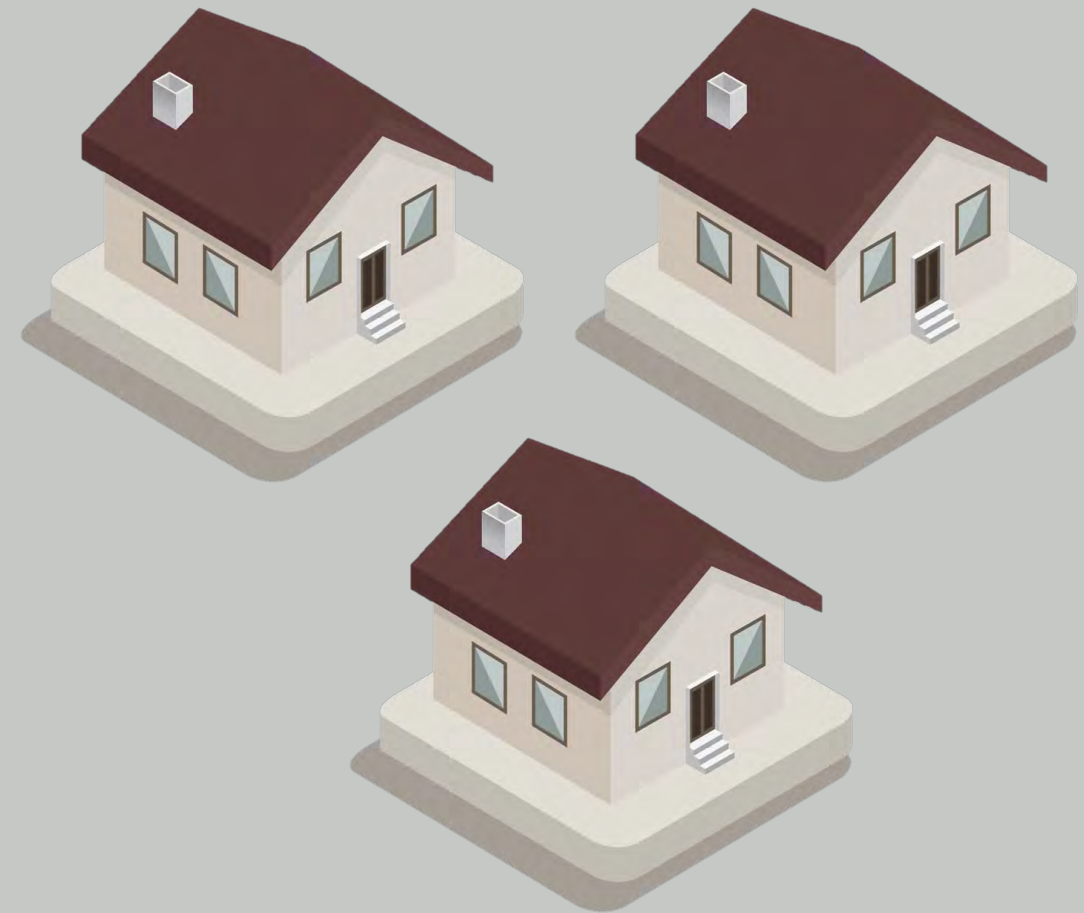
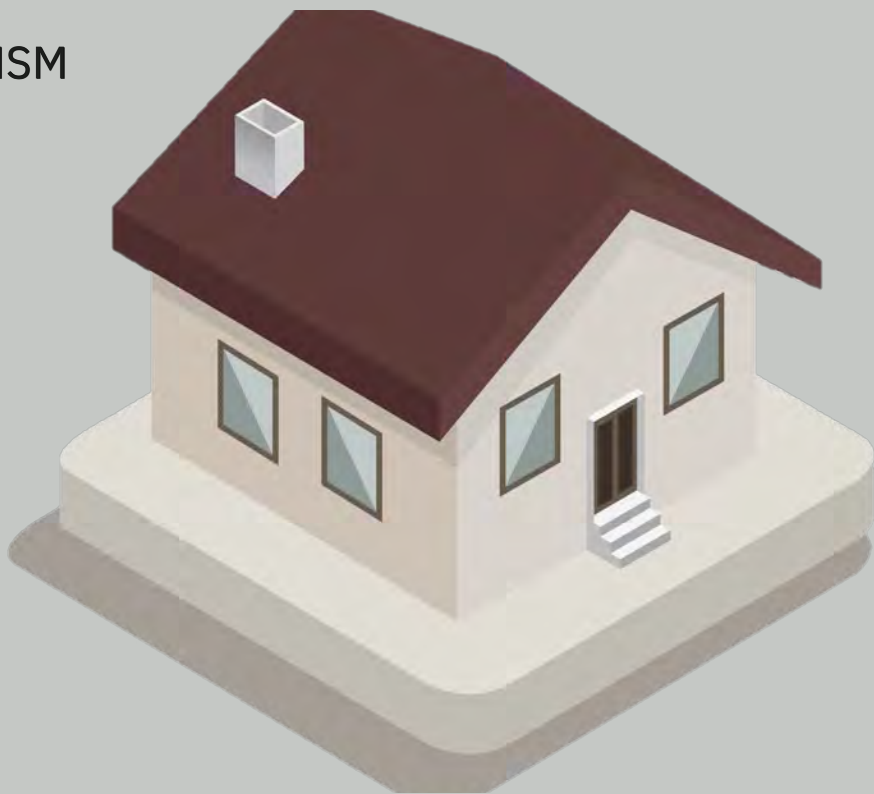


Sikringstiltak dersom
grunnsikringstiltakene ikke er
tilstrekkelig ved økt risiko

Skadebegrensende tiltak



Sikringstiltak ved beredskap eller
situasjoner hvor andre tiltak ikke
strekker til



Konsekvensreduserende tiltak

«Sikring mot sabotasje krever at virksomheter legger mer vekt på reserveløsninger og etablerer god reparasjonsberedskap. Både myndigheter og den enkelte virksomhet må få bedre forståelse av konsekvensene dersom tilgangen på viktige varer eller tjenester faller bort». – RISIKO 2025



Reparasjonsberedskap

Det er vanskelig å bygge fysiske barrierer rundt alt!

«Det er utfordrende å etablere fysiske sikringstiltak som kan forhindre sabotasje mot ubemannet infrastruktur i distriktene. NSM anbefaler å prioritere reserveløsninger og motstandsdyktighet, overvåkings- og deteksjonstiltak samt å øve på beredskapsplaner. Dette for å sikre rask respons og gjenoppretting ved bortfall av kritiske innsatsfaktorer som kraft, transport, internett, vann eller posisjon, navigasjon og tidsbestemmelse (PNT).» - RISKO 2025

Like viktig som sikringstiltak er redundans og
reserveløsninger



Reparasjonskompetanse

Råd:

1. Se på muligheten for å bygge redundans for de viktigste funksjonene
2. Lagre/ oppbevare enkeltkomponenter og reserveløsninger
3. Kartlegg reparasjonskompetansen (håndverkere)
4. Kartlegg hvor lenge man kan være uten produksjonen før det påvirker andre tjenester, og hvor lang tid det vil ta å gjenopprette funksjonen etter ødeleggelse

Takk for oppmerksomheten!

Uten ekom stopper Norge

Sikkerhet og beredskap i stadig mer krevende tider

Erik Wehler
Sikkerhetsdirektør
erik.wehler@telia.no



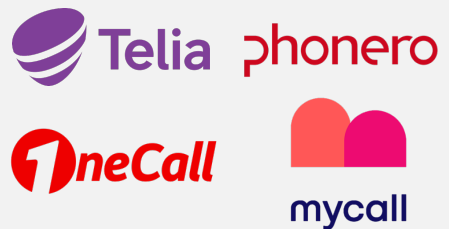
Vi er en del av Telia Company

>170 år

hvor vi har knyttet
mennesker og bedrifter
sammen

**SEK 89
milliarder**
inntekter i 2024

~26 millioner
abonnenter i Norden
og Baltikum



Fastnett



**Unik digital
infrastruktur**



Mobilnett



Transportnett og datasentre





Telia er leverandør til:
**Norges viktigste
samfunnskritiske aktører**



Nasjonal digitaliserings-
strategi 2024–2030:

- Norge skal bli verdens
mest digitaliserte land

...når t-banen i
OSLO SKAL KJØRE



...når du trenger hjelp fra
POLITIET



...når flere hundre tusen
PAKKER OG BREV
skal frem hver dag



...når du blir tatt i å
KJØRE FOR FORT
- i en fartsboks



Uten Telia
STOPPER
Norge



...når du spiller på lotto, tipper eller
SPILLER PÅ HEST



...hvis man ikke ønsker at
BILEN STOPPER



...når hvert sekund
TELLER



...når du trenger konnektivet
OVERALT, ALLTID



Sannsynligheten for sabotasje på norsk jord vurderes som høy
- Fiberkabler, energiforsyning og satellittbaserte tjenester er spesielt utsatte mål.

Statlig etterretningsvirksomhet og sabotasje
- Russland og Kina driver intensiv etterretningsaktivitet i Norge.

Totalforsvar og beredskap
- Norge er mer sårbart enn før, og sivil-militært samarbeid må styrkes.





Mistenker sabotasje mot et 30-tals
basestasjoner langs den svenske
østkysten



A middle-aged man with short brown hair, wearing a dark blue blazer over a black shirt, is speaking into a silver microphone. He is gesturing with his right hand. The background is a large, out-of-focus map of Europe. The text is overlaid on the left side of the image.

– Vi som selskap prøvde
å forberede oss i over ett
år. Men virkeligheten var
annerledes enn vi ventet.

*- Volodymyr Kabanenko, tidl. teknisk visedirektør i
Ukrainas største mobilselskap, Kyivstar*





Ny nasjonal sikkerhetsplan for digital infrastruktur



Norden - ny strategisk region NATO



Sikkerhet og beredskap over landegrenser



Teste og øve på sikkerhet og beredskap



The image is a collage of three photographs. The left photo shows a woman with glasses pointing at a large digital screen displaying a flowchart, with a man looking on. The middle photo shows two construction workers in safety vests and hard hats, one holding a tablet and the other on a phone, standing in front of scaffolding. The right photo shows a man and a woman sitting on a sofa in a modern office, looking at a laptop. The text 'Risikovurderere' is overlaid on the top left, 'Bygge motstandskraft' is overlaid across the middle, and 'Teste og øve' is overlaid on the bottom right.

Risikovurderere

Bygge motstandskraft

Teste og øve





kraftCERT



Beredskap i kraftsektoren

Digital hendelseshandtering

Espen Nodeland, KraftCERT

Christian Damslora, NVE

Foto: NASA – ISS

KraftCERT/ InfraCERT

- SektorCERT for Havtil og NVE
- Medlemmer i kraft, petroleum, vann og avløp, industri
- Eid av medlemmer, non-profit, støttet av NVE & Havtil

KraftCERT/ InfraCERT

- Hva vil en angriper kunne utføre med et cyberangrep på kraft?
- Mediebildet vs trusselbilde
- Ukraina: erfaringer og observasjoner

Trusselbilde

KraftCERTs trusselvurdering 2025 - nøkkelfunn

Det er **meget lite sannsynlig** at noen vil kunne skape langvarige strømutfall med digitale angrep.

Angrepene er svært vanskelige

Systemene er svært godt beskyttet

Digitale angrep kan skape kortvarige strømutfall og driftsforstyrrelser, men det er **meget lite sannsynlig** at dette blir bredt og langvarig.

Det er **meget sannsynlig** at virksomheter kartlegges både teknisk og organisatorisk. Andre vurderinger har pekt på at slik kartlegging har særlig nytteverdi i fysiske angrep dersom en konflikt går høyere opp i eskaleringsnivå.

Kraftbransjen i høgspenn etter nytt damangrep

Den norske kraftbransjen intensiverer sikkerhetsarbeidet etter det som skal vere enda eit russisk hackarangrep.



RISAVATNET I BREMANGER: I april blei eit damanlegg i Bremanger sabotert. PST kopla sabotasjen til ein «prorussisk gruppe», og etterforskar nå eit liknande angrep.

FOTO: PREBEN NEDREBERG HOLMØY / NRK



[Håvard Nyhus](#)
Journalist

Publisert i går kl. 14:22

Mediebildet

1: Bremanger

- Ikke knyttet til kraftproduksjon
- Ingen skadelige konsekvenser
- Automasjonen krever ikke passord

2: "Østlandet"

- Ingen kobling til kraft eller annen kritisk infrastruktur
- Nevnt i medieoppslag der det påstås sammenheng eller likhetstrekk
- Angrepet skjedde våren 2025, men brukt i media på sensommeren.

Ukraina – observasjoner og erfaringer

Invasjonen i 2022 – cyberangrep med lite effekt

Russland forsøkte cyberangrep i innledende faser i 2022 = egentlig svært små praktiske konsekvenser, men en del store medieoppslag.

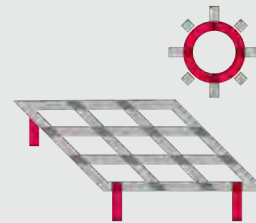
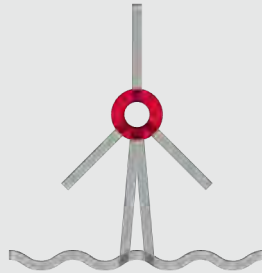
Kraftsystemet gjennom krigen

Kraftsystemet i Ukraina rammes av droner og raketter.

Ukraina har vist enorm motstandsdyktighet i sitt kraftsystem. Store deler av landet fortsetter i stor grad som normalt

Men: det har kostet, både arbeidsinnsats og koordinering av Ukraina og reservedeler fra mange bidragsland inklusive Norge. Forsvar mot både cyber og fysiske angrep på kraftsystemet må først og fremst handle om motstandsdyktighet .

Kraftforsyningens beredskapsorganisering



1948

NORGES SIVILE BEREDSKAP



UTGITT AV DIREKTORATET FOR SIVILT BEREDSKAP

1972



Industriens og

Man vil i denne forbindelse understreke at bedrifter som ikke på forhånd er gitt noen bestemt prioritet, må oppfattes som reservebedrifter som vil måtte trekkes inn i det prioriterte produksjonsprogram hvis den totale kapasitet i bransjen reduseres som følge av krigshandlinger, hvis tilgangen på råvarer blir bedre enn forutsatt osv. Slike reservebedrifter vil eventuelt også kunne gis krigsviktige oppdrag som kan innebære en omlegging i forhold til bedriftens normale produksjon.

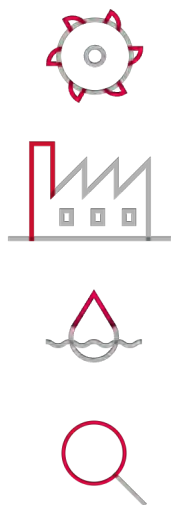
Kraftforsyningen

Alle sider av samfunnet er etter hvert så gjennomført elektrifisert at **svikt** i den elektriske kraftforsyningen medfører **alvorlige konsekvenser på nær sagt alle områder.** Under en krig vil forstyrrelser i kraftforsyningen, foruten å gå ut over sivilbefolkningens essensielle

Kraftforsyningens beredskapsorganisasjon - KBO

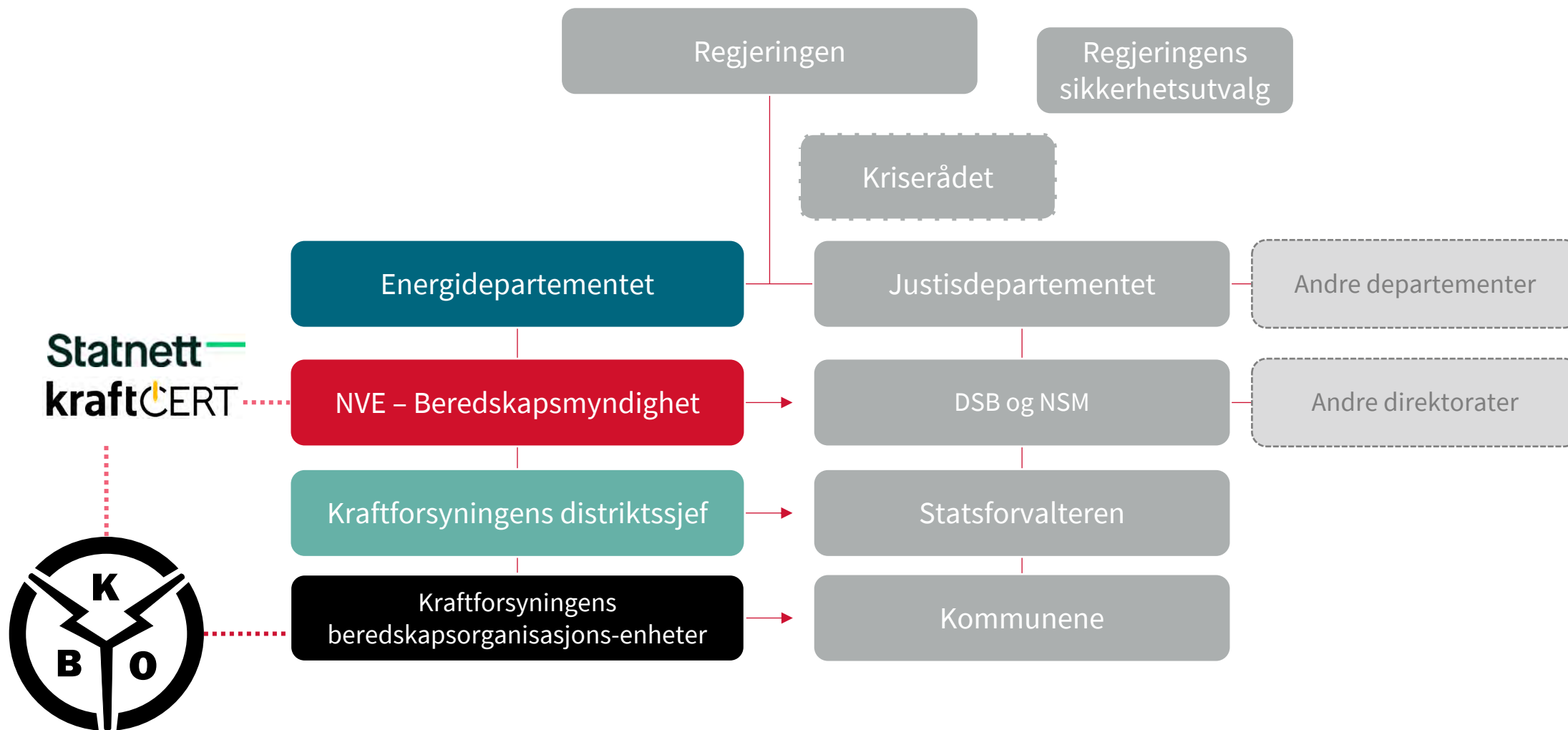
KBO-enheter

- Nettselskap (ca. 50 %)
- Produksjon (ca. 35 %)
- Industri (ca. 5 %)
- Brukseierforeninger (ca. 5 %)
- Andre (ca. 5 %)



- KBO-enheter er de som eier og driver anlegg med vesentlig betydning for kraftforsyningen

Planer, roller og ansvar og beslutningsprosesser



Organisering av kraftforsyningen - ansvarshierarki

➤ Energidepartementet – overordnet ansvar

➤ NVE – beredskapsmyndighet

- Samordne beredskapsarbeidet
- Regelverk/forskrift

➤ Statnett – systemansvar

- Balanse mellom forbruk og produksjon
- Håndtere effekt- og energiknapphet

➤ KraftCERT– digitale hendelser

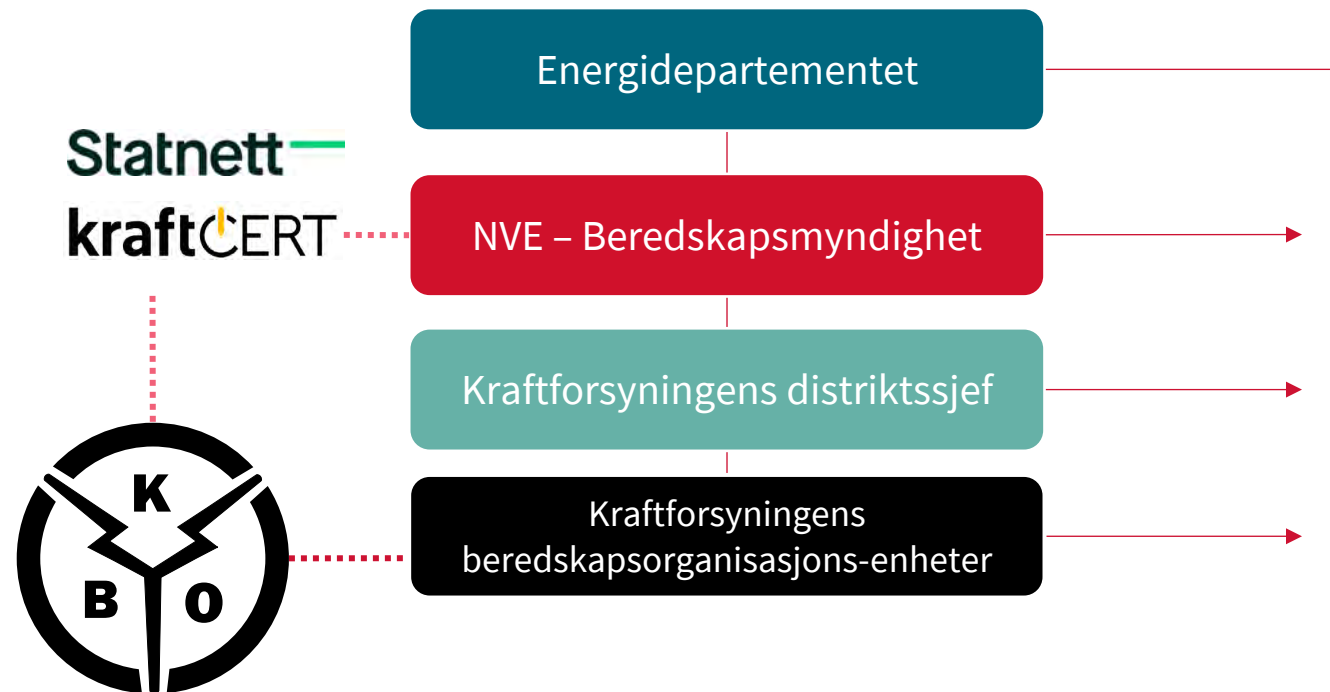
- CERT-miljø for energisektoren
- Operativ handteringen av cyberhendelser

➤ Kraftforsyningens Distriktssjefer (KDS)

- Delegert ansvar fra NVE
- Regionalt ansvar

➤ Viktige virksomheter

- KBO-enheter – lokalt ansvar
- Konsesjon + klassifiserte anlegg / vedtak









NVE DIGITAL VEILEDER

AREALPLANLEGGINGENERGIMILJØ OG LANDSKAP
TILSYN OG BEREDSKAPVANN OG VASSDRAG

Søk

[NVE digital veileder](#) > [Temaveileder: Øvelsesscenario for digitale hendelser i kraftforsyningen](#) >

Temaveileder: Øvelsesscenario for digitale hendelser i kraftforsyningen

Publisert 28.02.25 Sist endret 09.03.25

[Sjå](#) [Sjå](#)

Oversikt over øvelsene →

Bruerveiledning →

Tilpasning av øvingsscenario ✓

Evaluerings ✓

Øvelsesscenariene ✓

Cyberøvelser for virksomheter i kraftforsyningen

Det er utviklet 20 øvingsscenarioer for cyberangrep tilpasset kraftselskaper og nettoperatører. Scenariene er realistiske og dekker hendelser både innen IT- og OT-systemer. Scenariene er tilpasset to forskjellige øvingsformer: diskusjonsøvelse og spilløvelse.

Scenariene er tilpasset et sammensatt trusselbilde der angrep både fra statlige aktører med betydelige kapasiteter og kriminelle som først og fremst søker økonomisk vinning, kan forventes. Scenariene dekker et bredt spekter av mulige øvingsmål, og er valgt for å gi bredde i tilgjengelige øvinger, og kunne passe både for virksomheter som har lite erfaring med øvingsvirksomhet, og mer modne virksomheter som ønsker større utfordringer.

Oversikt over øvelsene

OT-øvelser:

- Scenario 01 - Dataangrep på automasjonssystem (OT)
- Scenario 02 - Avansert vedvarende trussel (APT)
- Scenario 03 - Brudd på integritet i sanntidsdata
- Scenario 04 - Fjernaksesskompromittering
- Scenario 05 - Forsyningskjede-angrep
- Scenario 06 - Kritisk systemnedetid
- Scenario 07 - Løsepengevirus-angrep
- Scenario 08 - Nettverkssegmenteringsfeil
- Scenario 09 - Teknologisk innovasjon
- Scenario 10 - Zero-day exploit

IT-øvelser

- Scenario 11 - Angrep på mobile applikasjoner
- Scenario 12 - Brannmurkonfigurasjonsfeil
- Scenario 13 - Brudd på autentiseringsmekanismer

Evaluerings



Øvelsesscenariene



Scenariene er tilpasset et sammensatt trusselbilde der angrep både fra statlige aktører med betydelige kapasiteter og kriminelle som først og fremst søker økonomisk vinning, kan forventes. Scenariene dekker et bredt spekter av mulige øvingsmål, og er valgt for å gi bredde i tilgjengelige øvinger, og kunne passe både for virksomheter som har lite erfaring med øvingsvirksomhet, og mer modne virksomheter som ønsker større utfordringer.

Oversikt over øvelsene

OT-øvelser:

- Scenario 01 - Dataangrep på automasjonssystem (OT)
- Scenario 02 - Avansert vedvarende trussel (APT)
- Scenario 03 - Brudd på integritet i sanntidsdata
- Scenario 04 - Fjernaksesskompromittering
- Scenario 05 - Forsyningskjede-angrep
- Scenario 06 - Kritisk systemnedetid
- Scenario 07 - Løsepengevirus-angrep
- Scenario 08 - Nettverkssegmenteringsfeil
- Scenario 09 - Teknologisk innovasjon
- Scenario 10 - Zero-day exploit

IT-øvelser

- Scenario 11 - Angrep på mobile applikasjoner
- Scenario 12 - Brannmurkonfigurasjonsfeil
- Scenario 13 - Brudd på autentiseringsmekanismer
- Scenario 14 - Brudd på personvern
- Scenario 15 - DDoS-angrep
- Scenario 16 - Man-in-the-Middle (MitM) angrep
- Scenario 17 - Sosial manipulasjonsangrep
- Scenario 18 - Tyveri av legitimasjon

Sky-øvelse

- Scenario 19 - Kompromittering av skytjenester

IoT-øvelse

- Scenario 20 - IoT-angrep

Lenke til rapport: [NVE Ekstern rapport 5/2025: Cyber-øvelser for virksomheter i kraftforsyningen](https://veiledere.nve.no/temaveileder-ovelsesscenario-for-digitale-hendelser-i-kraftforsyningen/oversikt-over-ovelsene/)

Takk for oppmerksomheten!

kraftCERT



NVE: cadd@nve.no

KraftCERT: cert@kraftcert.no



DSBs samordningsrolle i fred, krise og krig

Tonje Espeland
seksjonssjef
DSB



15. september 2025



«Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare».

Meld St. 10 (2016–2017) Risiko i et trygt samfunn

DSB skal

- Forebygge ulykker og kriser i samfunnet
- Ha oversikt over risiko og sårbarheter i samfunnet
- Bistå JD og øvrige departementer ved koordinering av håndtering av større kriser og katastrofer, herunder sikkerhetspolitisk krise og krig

Forberedt på krise og krig

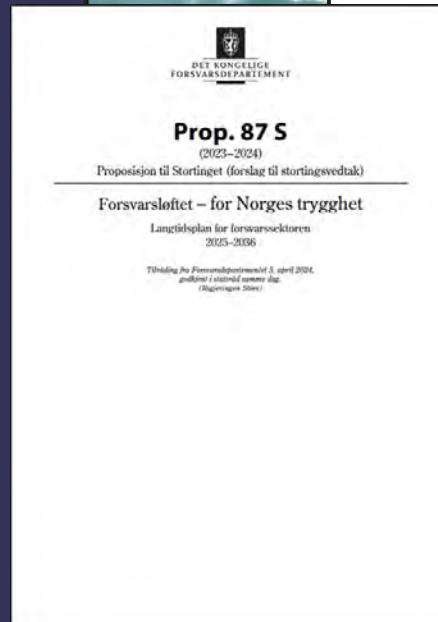
Mål for regjeringens arbeid med sivil motstandskraft

1. Et sivilt samfunn som er forberedt på krise og krig



2. Et sivilt samfunn som motstår sammensatte
trusler

3. Et sivilt samfunn som understøtter militær innsats



Nasjonale planleggingsgrunnlag

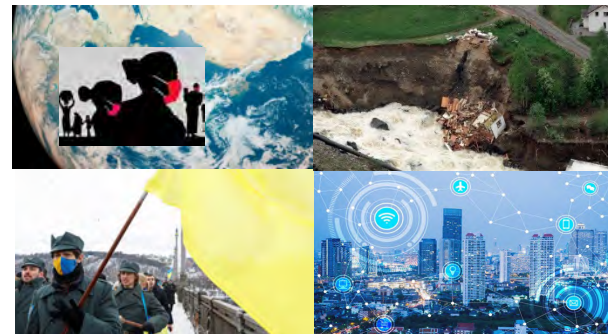
- hva vi skal beskytte og all-hazard trusselbilde



Hvilke funksjoner er det viktig å sikre?



Hva må vi sikre oss mot?



Hvordan forberede og håndtere?

DSBs analyser av krisescenarier



- Digitalt angrep mot finansiell infrastruktur
- Digitalt angrep mot ekom-
infrastruktur
- Vurdering av
samfunnskonsekvenser

DSBs samordningsrolle i bredt

- Ansvarsprinsippet står sterkt
- Samordning – både vertikalt og horisontalt – er krevende
- Skape resultater uten å ha styringsmyndighet over de ressursene som trengs for å oppnå disse resultatene
- Avhengig av medvirkning fra aktørene som skal samordnes
- Samordningsmyndigheter på de ulike forvaltningsnivåene:
 - Justis- og beredskapsdepartementet
 - DSB
 - Statsforvalter
 - Kommune

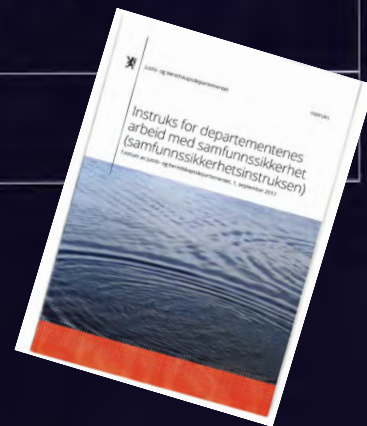


*Instruks for DSBs koordinerende
roller, kgl. res. 24. juni 2005*

**Direktoratet for samfunnssikkerhet
og beredskap – det generelle
koordineringsansvaret og ansvaret for
koordinering av tilsyn med aktiviteter,
objekter og virksomhet med potensial
for store ulykker**

Kongelig resolusjon 24.06.2005

- ✓ Oversikt
- ✓ Initiativ
- ✓ Bistand



DSBs samordningsrolle i krisehåndtering

- DSB skal gjennom sin samordningsrolle bidra med et å gi et **helhetlig situasjonsbilde** og **danne felles forståelse av tverrsektorielle samfunnskONSEKVENSER** av en hendelse
- FØR – UNDER – ETTER
- Tverrsektorielle samordningskonferanser
- Situasjonsrapportering fra kommuner, statsforvaltere og DSB til Justis- og beredskapsdepartementet

Tema

Retningslinjer for bruk av samordningskanal



2025



Samhandling NSM og DSB ved digitale angrep og cyberhendelser

NSM skal:

- etablere og vedlikeholde nasjonalt situasjonsbilde, sårbarhetsbilde og risikobilde og dele dette med relevante miljøer.
- ha beredskapsplaner for håndtering av større digitale angrep, sikkerhetspolitiske kriser og væpnet konflikt knyttet til det digitale rom.

DSB skal:

- Ha oversikt over risiko og sårbarhet, forebygge uønskede hendelser og sørge for god beredskap og effektiv ulykkes- og krisehåndtering.



Nasjonalt rammeverk for håndtering av digitale angrep og cyberhendelser

Sikre en nasjonal hendelseshåndteringsmodell som gir grunnlag for effektivt samspill mellom virksomheter, sektorvise responsmiljøer og det nasjonale sektorovergripende nivået for ivaretagelse av cybersikkerhet.

Totalforsvaret

Summen av landets sivile og militære ressurser, som jobber sammen for å forebygge og håndtere kriser, væpnede konflikter og krig



Totalforsvarsåret 2026

- I samarbeid med sivile aktører og Forsvaret planlegger DSB Totalforsvarsåret 2026.
- Forslag til overordnet mål: Styrke Norges evne til å forebygge og håndtere sikkerhetspolitisk krise og krig.
 1. Styrke motstandsdyktigheten i kritiske samfunnsfunksjoner
 2. Styrke sivil evne til å understøtte Forsvaret
 3. Styrke totalforsvarets evne til å yte vertlandsstøtte
 4. Styrke evnen til å beskytte befolkningen i krig
 5. Styrke motstandsdyktigheten i befolkningen.

Øvelser i Totalforsvarsåret



Øvelser i Totalforsvarsåret 2026



dsb.no/ovelser/

- Øvelsesbanken – ulike scenario for diskusjonsøvelser for virksomheter
- Øvelsesveiledning – materiell
- Kurs i øvelsesplanlegging



Øvelser

Her finner du ulike øvelser basert på scenarioer som kan ramme din virksomhet.

Diskusjonsøvelser



Bortfall av satellittbaserte tjenester

Scenarioet i denne diskusjonsøvelsen handler om hvilke konsekvenser det vil kunne få for en norsk kommune at satellittbaserte tjenester faller bort eller forstyrres.



Samfunnskritiske funksjoner ute av spill

Scenarioet i denne øvelsen tar utgangspunkt i banken som din organisasjon benytter blir hacket med følger som stanser alle transaksjoner.



Samfunnskritiske systemer ute av spill

Scenarioet i denne diskusjonsøvelsen er et mellesvaringsp som summer det elektriske nettsystemet internasjonalt, og hvordan dette kan påvirke din virksomhet.



Kompromitterte servere

Scenarioet i denne øvelsen handler om hvordan trusselaktører kan gå inn på organisasjonens servere, enten for å bruke serverne som mellomledd, eller for å erverve informasjon fra organisasjonen.



Direktørsvindel

Scenarioet i denne øvelsen handler om forsøk på svindel der meldinger, som tilsvarende kommer fra en toppleder, ber medarbeidere om å betale faktura eller overføre penger til konti som er ulagte for bedriften.



Sikkerhetsvarsel

Scenarioet i denne diskusjonsøvelsen handler om hvordan organisasjonen kan få sikkerhetsvarsel fra utenforstående hackere.



Vitende insider

Scenarioet handler om en ansatt som deler sensitive informasjon med nye samarbeidspartnere, og legger til rette for eksposen om blottlegging.



Uvitende insider

Scenarioet i denne diskusjonsøvelsen handler om en ansatt ulagte innrede trussel.



Personopplysninger på avveie – Phishing

Scenarioet i denne øvelsen handler om deling og lagring av informasjon, og hvordan problemet med utlekk.

dsb.no/sikkerhverdag/





Takk for oppmerksomheten

Tonje Espeland

Seksjonssjef krisehåndtering

+47 98 61 54 38

Tonje.Espeland@dsb.no