Denmark's economic vulnerability to a loss of satellite-based PNT

A study for the Inter-Ministerial Space Committee (Det Tværministerielle Rumudvalg)

FINAL REPORT

February 2019

LE London Economics

Commissioned by:

The Inter-Governmental Space Committee, comprising:

Ministries of Finance; Defence; Environment and Food; Transport and Building; Foreign Affairs; Energy, Utilities and Climate; Business and Growth; Higher Education and Science (chair)

About London Economics

London Economics (LE) is a leading independent European economic consultancy, with a dedicated team of professional economists specialised in the space sector.

As a company, our reputation for independent analysis and client-driven, world-class and academically robust economic research has been built up over 30 years. From our headquarters in London, and associate offices in five other European capitals, we advise an international client base.

As a team, we have been pioneering innovative analytical techniques to provide trusted economic advice to decision-makers across the space industry, space agencies and international governments since 2008. Drawing on our solid understanding of the economics of space, expertise in economic analysis and industry knowledge, we use our expertise to reduce uncertainty and guide decision-makers in this most challenging operating environment.

Our consultants are highly-qualified economists with extensive experience in applying a wide variety of best practice analytical techniques to the space sector, including:

- Market sizing, analysis and demand forecasting;
- Business case support (economic and financial feasibility);
- Value-for-Money (Cost-Benefit Analysis, Cost Effectiveness Analysis);
- Impact assessment and policy evaluation (especially public utility and spillover benefits);
- Sophisticated statistical analysis (econometrics, regression);
- Analysis of industry structure and competitive dynamics;
- Commercial due diligence.

Head Office: London Economics, Somerset House (New Wing), Strand, London WC2R 1LA, United Kingdom.
w: londoneconomics.co.uk/space e: space@londoneconomics.co.uk
t: +44 (0)20 3701 7707 🐦: @LE_Aerospace

Acknowledgements

We would like to acknowledge the useful guidance and feedback provided by the Danish Agency for Science and Higher Education throughout this research, and the assistance of more than 20 stakeholders who have kindly contributed their time and expertise to inform this report. Responsibility for the contents of this report remains with London Economics, and the professional opinions expressed in this report are those of the author only.

Authors

Rasmus Flytkjær, Associate Director, Space, rflytkjaer@londoneconomics.co.uk

Cover image: **Image source:** NASA, Artist's impression of a STEREO Spacecraft Viewing CME
https://www.nasa.gov/mission_pages/sunearth/missions/mission_stereo.html
Use of the image does not imply NASA's endorsement of the report.

London Economics Ltd is a Limited Company registered in England and Wales with registered number 04083204 and registered offices at Somerset House, New Wing, Strand, London WC2R 1LA. London Economics Ltd's registration number for Value Added Tax in the United Kingdom is GB769529863.

Table of Contents

Page

Table of Contents

Page

Resumé

Hovedresultater

Danmark er et avanceret, moderne samfund, der bruger teknologi til at løse opgaver. GNSS er en af disse teknologier og bruges bredt i samfundet. At Danmark ikke har en national tidskilde (ulig nabolandene Sverige og Tyskland, og mange andre lande), gør, at applikationer, der kræver tidsstempler med høj nøjagtighed, må bruge GNSS.

Denne rapport baserer sig på undersøgelse af otte fokusområder for sårbarhed overfor et fem-dages udfald af satellitbaserede positions-, navigations- og tidsstyringstjenester og har fundet følgende:

- **Energitransmission** har implementeret GNSS, men har ikke tilladt, at forsyningssikkerheden blev afhængig af teknologien, og er derfor ikke sårbar.
- **Meteorologien, redningstjenesterne, fiskeriet og landbruget** anvender GNSS og ville blive påvirket af et tab af tjenesterne. Offentlige og private brugere ville mærke effektivitetstab, men ville kunne oppebære drift.
- **Vejtransportsektoren** ville opleve øget trafik og reduceret effektivitet, som ville påvirke alle brugere af vejene. Danskere er i den internationale elite med hensyn til rumlig navigation, så det forventes, at trafikken ikke ville gå helt i stå.
- **Det offentliges IT** bruger tilsyneladende ikke GNSS til synkronisering og er derfor ikke sårbar.
- **Finanssektoren** synes ikke at være opmærksom på de risici, der er forbundet med brug af GNSS, som er den eneste bredt tilgængelige kilde til tidsstempling med den nøjagtighed, der kræves i EU's direktiv.

Indledning

Denne rapport besvarer spørgsmålet: *"Hvordan er Danmarks sårbarhed overfor et udfald i satellitbaserede positions-, navigations- og tidsstyringstjenester"?* Spørgsmålet besvares ved at analysere samfundets brug af disse tjenester som helhed, samt ved at sætte særligt fokus på otte områder.

Der er generelt tre typer af menneskeskabte satellitter i kredsløb om Jorden: kommunikations-, jordobservations- og navigationssatellitter. Denne rapport beskæftiger sig med den sidste type, som grupperes under titlen Globale Navigations Satellit Systemer (GNSS).

Der er fire GNSS-konstellationer, nemlig USA's GPS, Ruslands GLONASS, Europas Galileo og Kinas BeiDou. De første to systemer er fuldt funktionsdygtige, mens de to sidste er under udvikling og forventes færdige i 2020.

Global Positioning System (GPS) er det originale GNSS, og dets navn er blevet synonym med satellitnavigationssystemer i biler, hvilket fik stor udbredelse i befolkningen i midten af nullerne. GLONASS genopnåede fuld dækning i 2009 (efter at have mistet sin finansiering efter Sovjetunionens fald) og har været standard i mobiltelefoners navigationschip siden 2011.

Forskellige konstellationer har forskellige tjenester til at dække specifikke behov. Udover det åbne signal, som kan afkodes af alle, udsendes et reguleret signal, som kun kan bruges af godkendte med den rette krypteringsnøgle. Galileo har tillige et redningssignal, som kan sende besked til en nødstedt om, at hjælpen er på vej, og et nøjagtigt signal, som kan bruges til applikationer, der kræver stor nøjagtighed. BeiDou har et kommunikationssignal, som kan bruges til at advare brugere i visse områder mod naturkatastrofer m.v.

GNSS fungerer ved, at alle satellitterne i den samme konstellation udsender et præcist klokkeslæt samt satellittens position. Signalet bevæger sig med (nær) lysets hastighed til brugernes satellitmodtagere. Med signaler fra tilstrækkeligt mange satellitter er det muligt at beregne, hvor langt man er fra signalets udgangspunkt, og derved beregne hvor man er. Da signalet udsendes konstant, er det muligt at beregne ændringer i position og dermed hastighed. Denne information bruges til navigationsapplikationer i biler og andre køretøjer. Sådanne bilnavigationssystemer anvender tillige digitale kort, som sikrer, at bilens position er forankret i vejnettet.

At GNSS udsender et præcist tidssignal, kan udnyttes af brugere, som kræver sådanne oplysninger. Alternativet til GNSS er brug af atomure, som koster hundredtusindvis af kroner, og som skal kalibreres for at sikre den nødvendige præcision. GNSS-ure kan erhverves for en snes kr., og GNSS-brugere udnytter, at konstellationens ejer (eksempelvis US Air Force eller EU) kalibrerer satellitternes atomure hver 12. time, hvilket sikrer at signalet er korrekt. En ekstra gevinst er, at alle satellitter i samme konstellation er synkroniseret til det samme ur, så alle brugere i hele verden – der bruger den samme konstellation – er enige om tid.

Følgende scenarium ligger til grund for undersøgelsen: *et øjeblikkeligt og fuldkomment tab af alle GNSS-tjenester i en sammenhængende periode på fem dages varighed, hvorefter alle tjenesterne gendannes fuldstændigt.*

Rapporten differentierer ikke ved årsagen til udfaldet og dækker kun den nuværende situation uden at fremskrive eventuelle ændringer i fremtiden, og omfatter ikke Færøerne og Grønland. Undersøgelsen er baseret på samtaler med mere end 20 interessenter, som har givet deres besyv med.

Baggrund og motivation

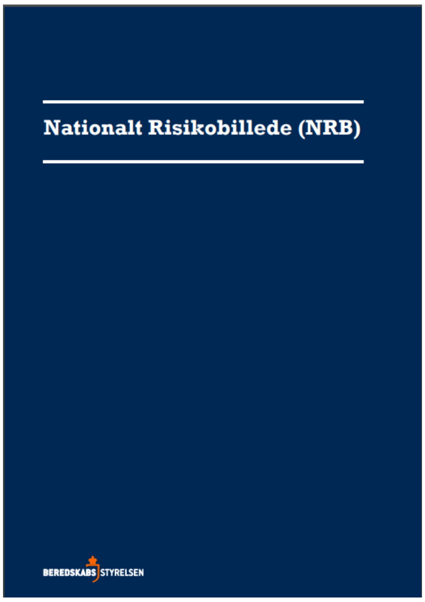
GNSS anvendes i mange forskellige dele af samfundet og har i mange tilfælde erstattet traditionelle navigationsmetoder eller tidsstyringssystemer. GNSS er den billigste og nemmeste løsning på mange forskellige problemer for mange forskellige aktører, og der er derfor en risiko for, at et udfald af disse tjenester kunne have en betydelig effekt på samfundets funktionsdygtighed.

GNSS-signaler er meget svage, idet de har en effekt svarende til en 40W pære, når de forlader satellitten. Efter en rejse på omtrent 20.000 km gennem Jordens atmosfære er det derfor vanskeligt at opfange signalet. Modtagere på Jorden forstærker signalet, så det kan bruges af udstyret, men dets lave effekt bevirker, at det let udsættes for forstyrrelser (interferens). Denne interferens kan være utilsigtet eller bevidst, og fordi systemerne bruges i mange forskellige funktioner, kan visse aktører have incitament til at maskere deres position ved at interferere med signalet. Det er også muligt at snyde modtagere på Jorden ved at udsende signaler, der ligner de ægte signaler fra satellitter, men som giver en anden position eller tid.

Disse sårbarheder gør, at der er en voksende bekymring for, at det moderne samfund har gjort sig så afhængig af GNSS, at eventuelle udfald (lokale eller på systemniveau) kunne have alvorlige konsekvenser.

Foruden radiointerferens er ekstremt rumvejr en reel trussel mod GNSS. Beredskabsstyrelsens Nationale Risikobillede fra 2017[1] nævner rumvejr som en risiko. I tilfælde af et soludbrud kan ionosfæren omkring Jorden blive så aktiv, at GNSS-signalet ikke kan trænge igennem, og i ekstra grelle tilfælde kan satellitter slås ud af kraftige solvinde.

Området har stor opmærksomhed internationalt, hvor Storbritannien, USA, Korea, m.fl. har igangsat initiativer til at få klarlagt risici og taget skridt mod at afhjælpe disse. Ydermere har hændelser i de seneste år vist, at forstyrrelser af GNSS er tiltagende, og kan være alvorlige.


Nationalt Risikobillede (NRB)

BEREDSKABSSTYRELSEN

Kilde: Beredsskabsstyrelsen

Sårbarheder ved GNSS[2]

Der er stigende fokus på sårbarhederne ved GNSS, og mange er blevet identificeret. Det skal nævnes, at GNSS stadig er den bedste, billigste og mest passende løsning på en bred vifte af opgaver relateret til tid, udendørs position og navigation. Bekymringen vedrørende sårbarhed skyldes, at mange dele af samfundet bruger GNSS til løsning af netop disse opgaver.

Man kan gruppere sårbarheder efter tre typer, som beskrives en ad gangen nedenfor. Sårbarhed på **modtagerniveau** hvor sårbarhederne er en konsekvens af lokale betingelser, og hvor sofistikerede modtagere, evt. i kombination med andre sensorer, kan afhjælpe mange af sårbarhederne.

[1] Beredsskabsstyrelsen (2017). *Nationalt Risikobillede*.

[2] Dette afsnit er baseret på tre hovedkilder: European GNSS Agency (2018). GNSS User Technology Report Issue 2; London Economics (2017). *The Economic Impact on the UK of a Disruption to GNSS; og* Government Office for Science (2018). *Satellite-derived Time and Position: A Study of Critical Dependencies*

Type	Navn	Beskrivelse
Modtagerniveau	Jamming	Det svage signal fra GNSS-satellitterne bevirker, at støjsignaler på samme frekvens gør det umuligt at beregne position. Støjsignaler kan skabes bevidst eller ubevidst og kan komme fra mange kilder. Jamming er ulovligt, men det er let at finde jammere på internettet til lave priser. Incitamentet til jamming kan eksempelvis være et ønske om at bruge arbejdspladsens bil til private formål, uden det kan ses i flådestyringssystemet.
	Spoofing	I stedet for støj kan man også generere falske signaler, der ligner ægte GNSS-signaler. Disse kan bruges til at snyde GNSS-modtagere til at beregne en fejlagtig position. Spillet Pokémon Go var ansvarligt for en hurtig udvikling i spoofing, da spillere observerede, at det var lettere at finde de bedste monstre i tæt bebyggede områder (Central Park i New York skulle efter sigende være bedst). Hvis ens telefon troede man var der, havde man de bedste muligheder for at avancere i spillet. I løbet af de sidste 30 år er spoofingudstyr således faldet fra ca. 1 mio. kr. til omkring 40 kr. Nylige hændelser har vist konsekvenserne af et spoofingangreb: ■ Ved en stor GNSS-konference i USA september 2017 bevirkede en læk fra en GNSS simulator, at alle smartphones i nærheden troede de var i Frankrig i 2014 – telefonerne skulle gendannes for at kunne hente nye e-mails igen. ■ I Sortehavet i juni 2017 rapporterede adskillige skibe, at deres position var angivet til lufthavnen i Sochi. Der skete ingen uheld, men man kan spekulere på, hvordan det var gået, hvis positionen havde været forkert, men troværdig. ■ En artikel fra 2018 viser, at man kan udnytte den måde, vejnettet er anlagt i store amerikanske byer, til at spoofe position og narre chauffører til at dreje en gang for meget. 95% af deltagerne i eksperimentet opdagede ikke, at de kørte den forkerte vej.
	Meaconing	Meaconing er spoofing hvor man genafspiller ægte GNSS-signaler. Disse vil naturligvis ikke længere angive korrekt tid, og kan også modelleres til at angive forkert position.

Kilde: London Economics analyse

Sårbarheder på **miljøniveau** er konsekvenser af det område, hvor brugeren opholder sig. Brugeren har ikke indflydelse på disse risici og kan i reglen ikke afhjælpe dem ved at opgradere GNSS-modtageren.

Type	Navn	Beskrivelse
Miljøniveau	Rumvejr og ionosfære	Ionosfæren er et lag af atmosfæren 80-600 km over Jorden. Ladede ioner i ionosfæren kan påvirke GNSS-signaler, bremse dem og gøre, at det er vanskeligt at beregne en position. Ionosfærisk scintillation kan fremkomme ved ekstremt rumvejr og bevirke, at GNSS-signalerne blokeres i ionosfæren. Dette fænomen er hyppigere ved polerne og ækvator end over Danmark. Satellitter er bygget til at modstå rumvejr, men et særligt alvorligt udbrud på niveau med det mest alvorlige, registrerede udbrud, Carrington-hændelsen i 1859, kan muligvis ødelægge satellitterne i kredsløb om Jorden.
	Rumskrot	Rumskrot giver anledning til voksende bekymring for rummet. Flere og flere satellitter bevirker, at risikoen for kollision mellem satellitter eller mellem satellitter og eksisterende rumskrot vokser. I Medium-Earth Orbit (MEO), hvor GNSS-satellitterne er i kredsløb, følger ESA i øjeblikket 203 stykker rumskrot på mere end 10 cm. Hvis et af disse kolliderer med en satellit, som efterfølgende bliver til rumskrot og kolliderer med flere (osv.), kan GNSS holde op med at virke, og kredsløbet forurenes så meget, at det ikke længere kan bruges. Der er endnu ikke trængsel i MEO, men fænomenet bør ikke desto mindre tages med i betragtning.
	Geografiske faktorer	For at beregne position ved GNSS kræves direkte sigte til mindst fire satellitter. I byer kan det imidlertid være vanskeligt at opnå den nødvendige dækning, da signalerne ikke kan trænge igennem bygninger. Signalerne kan imidlertid reflekteres af bygninger, og der er derfor en del støj, som avancerede modtagerne skal bruge tid og strøm på at filtrere fra (hvis et signal har rejst via en bygning, har det rejst længere end direkte, og positionens nøjagtighed falder derfor).
	Radio-interferens nær GNSS frekvenser	GNSS bruger forskellige frekvenser afhængigt af konstellation og tjeneste. Alle GNSS har en frekvens i det øvre L-bånd (1559-1610 MHz), som ofte omtales som L1. At alle konstellationer bruger samme frekvensområde gør, at modtagere kan bruge samme hardware til at tilgå signaler fra flere konstellationer. Interoperabilitet gør, at man kan anvende signaler fra forskellige konstellationer til at beregne position med få synlige satellitter. Foruden L1 anvender Galileo E5 og E6; GPS L2 og E5; BeiDou B2 og B3 og GLONASS L2, L3, og E5. På trods af de mange forskellige frekvenser er GNSS-signaler sårbare overfor interferens i nære frekvenser. Den lave effekt af GNSS-signaler bevirker, at evt. ændringer i andre signaler vil kunne jamme GNSS. *LightSquared* var en amerikansk virksomhed, der i 2011 ansøgte om at bruge et spektrum nær L1 til en internettjeneste. Ansøgningen blev afvist grundet bekymring om påvirkningen af GNSS.

Kilde: London Economics analyse

Den sidste type sårbarhed omhandler **menneskelig faktorer** i interaktionen med systemerne. Disse kan sammenfattes som menneskelige fejl, strategiske beslutninger eller særdeles sofistikerede angreb på systemerne. Lokale brugere har ingen mulighed for at afhjælpe disse risici.

Type	Navn	Beskrivelse
Menneskelige faktorer	Problemer med jord-stationer	Alle GNSS-satellitter kontrolleres af et netværk af jordstationer, som opdaterer data med jævne mellemrum. Ved to lejligheder siden GNSS blev åbnet for forbrugere, har sådanne opdateringer resulteret i fejl på systemet. GPS uploadede i 2016 forkerte data til en satellit der skulle tages ud af tjeneste. Dette bevirkede, at alle tider blev forkerte. GLONASS begik en tilsvarende fejl i 2014, hvor alle satellitterne udsendte signaler med en forkert position i tre dimensioner. Derved opstod stor usikkerhed i positionen beregnet på Jorden. Disse er eksempler på, at selv computerstyrede systemer er sårbare overfor menneskelige fejl.
	Intern inkonsistens	Engang imellem tilføjes skudsekunder til UTC fordi Jordens rotation ikke er perfekt. GNSS-tid tager ikke altid højde for disse ændringer, så visse systemer kan komme i problemer. Derudover er der et muligt problem under opsejling. GPS data er af begrænset længde, og der er derfor kun 1024 tilgængelige ugenumre i systemet. Pr. 6. april 2019 ændres GPS ugenummeret fra 1024 og tilbage til 1. Ældre modtagere kan få problemer med denne tilpasning, som ikke er begrænset til denne specifikke uge.
	Selektiv tilgænge-lighed og anden forringelse	Det oprindelige GPS havde en funktion, der tillod, at man kunne forringe det civile signal således, at man kunne drage fordel af "asymmetrisk adgang til positionering". Denne funktion er officielt ikke længere til stede, men det er formentlig stadig muligt at forringe signalet i forbindelse med konflikter. Selvom det ikke er sandsynligt, er det muligt, at de stater og institutioner, der har et GNSS holder op med at vedligeholde det. Dette skete for Rusland, som lod GLONASS miste fuld dækning i 15 år efter Sovjetunionens kollaps.
	Cyberangreb	GNSS styres fra få, stærkt beskyttede jordstationer rundt om i verden. Et cyberangreb på en eller flere af disse stationer kunne have dramatiske konsekvenser for den angrebne konstellation.
	Anti-satellit missiler	Adskillige af de store rumnationer har vist, at de kan nedskyde en satellit i kredsløb. Skulle dette ramme en GNSS-satellit, kan man let forestille sig en kædereaktion, som kunne udrydde mange satellitter (se rumskrot).

Kilde: London Economics analyse

Det næste afsnit sammenfatter mulige initiativer, man kan tage for at afhjælpe disse sårbarheder.

Hvad kan man gøre?

Selvom ovenstående tabel kan synes overvældende, og at det kan virke svært at imødegå de kendte sårbarheder, er der meget, man kan gøre for at begrænse konsekvenserne af eventuelle hændelser.

På **modtagerniveau** kan modtageren udstyres med notchfiltre, som kan bortfiltrere signaler, der ikke er fra GNSS-satellitter. Sådanne filtre virker godt mod konstant (naturlig) interferens, men kan ikke bruges til at modvirke de såkaldte chirpjammere, som springer inden for GNSS-frekvenserne og bruges ved bevidst jamming. Da jamming og spoofing traditionelt udsendes fra eller tæt på jordoverfladen, kan man anvende avancerede antenner, som kan se bort fra signaler der ankommer under en vis vinkel. Disse antenner kan modvirke utilsigtede effekter ved jamming eller spoofing (medmindre gerningsmanden sender dem op med drone). Andre antenner med rod i det militære kan endvidere identificere hvilken retning de falske signaler kommer fra, og se bort fra specifikke retninger, men disse antenner kan kun bruges i statiske eller meget lavt dynamiske applikationer.

Et spoofingangreb er kun succesfuldt hvis brugeren ikke opdager, at vedkommende bliver spoofet. Når den bliver operationel, vil Galileos Open Service Navigation Message Authentication (OS-NMA)-funktion gøre det muligt at detektere et spoofingangreb, og man kan derfor sikre, at brugeren advares og ikke ledes i uføre. Sofistikerede meaconingangreb kan ikke detekteres af OS-NMA, da signalet er et originalt GNSS-signal.

Brugen af flere GNSS er helt generelt en anbefalelsesværdig strategi. Mange af de identificerede menneskeskabte risici er relevante for enkelte konstellationer, så jo flere signaler der kommer ind, des bedre chance for at filtrere dårlige signaler fra. Det samme gør sig gældende for geografiske faktorer, hvor direkte sigte til fire satellitter fra den samme konstellation er meget vanskeligere at opnå, end til fire satellitter fra forskellige konstellationer.

Uden for selve GNSS-modtageren kan man også øge robustheden ved at **bruge andre kilder**. Brugere af GNSS til tidsstyring har oscillatorer i deres ure, som kan holde tid i en vis periode efter et udfald. Perioden afhænger af oscillatorens kvalitet og de krav der stilles til nøjagtighed, men spænder fra nogle minutter (til et par kr.) til måneder (til flere hundredetusinde kr.). I de fleste apparater er der allerede andre typer af sensorer som gyroskoper, barometre og odometre. Disse bruges allerede til navigation i biler og kan give en (unøjagtig) position i tunneller og andre steder, hvor GNSS ikke dækker. Derudover er mange typer brugerenheder, specielt smartphones, udstyrede med sensorer for mange andre typer af signaler. Der eksisterer databaser over placering af Wi-Fi hotspots, Bluetooth-sendere og mobilmaster, som alle kan bruges til at beregne position. Googles database over Wi-Fi hotspots er oprindeligt dannet af Google Streetviews biler og kalibreres med den crowd-sourcede information, som telefoner sender til Google for at beregne positionen uden adgang til GNSS. Radio- og tv-signaler kan desuden bruges til at estimere position, hvis man ved hvor disse kommer fra. Disse signaler kaldes signals-of-opportunity og kan være en væsentlig kilde til robusthed.

Der eksisterer også **alternative radionavigationssignaler**, eksempelvis STL, som er en kommerciel tjeneste, der udbyder tidsstyringstjenester og positionering i lavdynamiske applikationer. STL anvender den frekvens, der tidligere blev brugt til bippere, men som efter mobiltelefonens indtog ikke længere er nødvendig. Denne frekvens er tæt på GNSS E5, men STL adskiller sig fra GNSS ved at bruge et krypteret signal, som er meget stærkere end GNSS, og derfor ikke kan jammes eller spoofes. eLoran er en anden type, som baseres på det gamle Loran-C-system og som vil kunne genskabes til præcis tid og til navigation, hvis der er politisk vilje. Endelig kan brugere af GNSS til tidsstyring anvende internetbaserede tjenester eller (hvis kravene ikke er så strenge) tidssignalet fra Mainflingen nær Frankfurt, som stiller mange vækkeure.

I andre lande eksisterer også **kablede forbindelser** til det Nationale Metrologiinstitut, som kan levere tid over fibernet eller andre netværk.

Den mest oplagte måde at gardere sig mod en forstyrrelse af GNSS er imidlertid at sikre, at **traditionelle metoder** stadig er en mulighed.

Danmarks afhængighed af GNSS

I et avanceret samfund som det danske er mange dele afhængige af GNSS til mange forskellige opgaver. I Danmark er *Lov om Tidens Bestemmelse*[3] fra 1893 stadig den gældende definition af tid, og baseret på middelsoltiden for den 15. længdegrad. Sammenholdt med at Danmark ikke har et atomur, der kan levere præcis tid, er GNSS de facto den bedste og eneste leverandør af tids-og synkroniseringstjenester med høj præcision i Danmark.[4] Ifølge Rumstatistikken fra 2018 bruger 15% af danske virksomheder rumtjenester, heraf benyttes de af 15% til tidsstyring og -synkronisering.

[3] LOV nr 83 af 29/03/1893, Retsinformationen, https://www.retsinformation.dk/eli/lta/1893/83

[4] Dansk Institut for Fundamental Metrologi (2018). *Input til analyse af konsekvenser for Danmark af et nedbrud i de satellitbaserede PNT-tjenester.* Inputdokument til denne undersøgelse, ikke offentliggjort.

Disse brugere findes inden for mange sektorer, herunder den finansielle sektor, energiselskaber og teleindustrien.

Blandt de 15% af virksomheder, der anvender rumtjenester, gør 67% det med henblik på logistik og distribution.[5] De 19% af danske landmænd, som dyrker 51% af jorden, bruger GNSS med RTK (Real-Time Kinematic – en teknik, der øger nøjagtigheden af den beregnede position) til præcisionslandbrug.[6] Derudover ejer ca. halvdelen af befolkningen en GPS til bilen, og i 2015 fandt Danmarks Statistik, at 63% af befolkningen bruger GPS-funktionen i deres mobiltelefon.[7]

I mange sektorer er brug af GNSS et lovkrav herunder den maritime transport, fiskeriet, lastvognsskrivere og det fælleseuropæiske eCall system, som sikrer, at forulykkede biler sender oplysninger (herunder position) til alarmcentralen. Med udgangen af 2018 implementeres endvidere Advanced Mobile Location (AML), som sikrer, at alle opkald til alarmcentralen medsender den position, der er beregnet af den mobiltelefon, der placerer opkaldet, så man kan spare tid til at finde ud af hvor ulykken er, fokusere på ulykkens type og fremskynde udrykning.

RUMSTATISTIK

– Rumområdets betydning for den danske økonomi i tal

Januar 2018

Kilde: Styrelsen for Forskning og Uddannelse

Landmålingssektoren er fuldkommen afhængig af GNSS, der har så godt som erstattet alle andre måder at arbejde på. Uden GNSS skal alle målinger refereres til et kendt sted, men med GNSS kan man tage uafhængige målinger og derved skabe et overblik.

Redningstjenester er en anden type brugere af GNSS, som studeres nærmere i næste afsnit. Søredning er ikke omfattet af de særlige fokusområder nedenfor, men denne applikation er også afhængig af GNSS. En nødstedt i besiddelse af en sender i det international Cospas-Sarsat-system kan aktivere denne og sende sin position til nødberedskabet. Systemet bruger ikke GNSS til primær positionering, men, afhængig af type, er op til 96% af senderne i stand til at sende GNSS-positionen, som er mere nøjagtig end den primære metode. Nødmeddelelser, der indløber via VHF-radio, skal også stedfæstes, og GNSS er den oplagte løsning. På redningsmissionen anvendes GNSS til at navigere til den nødstedte. Skønt kaptajnen på redningsbåden (og piloten i helikopteren) må forventes at kunne navigere uden GNSS, er det satellitbaserede system at foretrække pga. af dets præcision – navnlig under vanskelige forhold som høj sø, tåge og i mørke.

I sammenligning med andre lande er Danmark dog, måske, ikke lige så afhængig af GNSS til navigation. Et papir fra University College London og University of East Anglia viser, at ud af en halv million brugere af et spil designet til at forstå spillerens spatiale navigationsfærdigheder, er danskere næstbedst efter finnerne.[8] Med andre ord er danskerne bedre end de fleste til rumlig navigation.

[5] Styrelsen for Forskning og Uddannelse (2018). *Rumstatistik – Rumområdets betydning for den danske økonomi I tal*. Available at: https://ufm.dk/publikationer/2018/filer/rumstatistik-2018_endelig.pdf

[6] Danmarks Statistik (2018). *Avanceret Teknologi Indtager de Danske Marker*. Available at: https://dst.dk/da/Statistik/nyt/NytHtml?cid=30775 [accessed 30/10/2018]

[7] The data are available for download at: https://www.dst.dk/da/Statistik/emner/uddannelse-og-viden/informationssamfundet/it-anvendelse-i-befolkningen

[8] Coutrot, A., Silva, R., Manley, E., de Cothi, W., Sami, S., Bohbot, V. D., Wiener, J.M., Hölscher, C., Dalton, R.C., Hornberger, M., Spiers, H.J. (2018). *Global Determinants of Navigation Ability*. Current Biology Volume 28, Issue 17, P2861-2866.E4, September 10, 2018

Særlige fokusområder

For at komme et spadestik dybere med analysen af Danmarks afhængighed af og sårbarhed overfor udfald i GNSS, undersøges otte særlige fokusområder på tværs af offentlige og private aktører.

El-transmission Bochim Sang/Shutterstock.com	El-transmissionsnettet bruger GNSS til tidsstempling af observationer. Det eksisterende SCADA-system sender observationer, når noget ændrer sig. Disse er tidsstemplede, men kræver kun nøjagtighed på 1 sekund. Den næste generation af SCADA i el-transmission bruger Phasor Measurement Units (PMU) til at holde styr på, om fasen afviger fra 50 Hz. Dette system kræver konstant monitorering og tidsstempler med 100-150 nanosekunders nøjagtighed. Ved at bruge PMU kan man øge udnyttelsen af nettet, fordi den højere overvågningsgrad gør, at man kan reducere den buffer, der er implementeret på nettet. Energinet, Danmarks transmissionsselskab, har PMU'er på nettet, men disse anvendes kun til akademisk evaluering af dets ydelse. Man har besluttet ikke at implementere løsningen til drift, fordi man ville gøre sig fuldstændig afhængig af GNSS uden at have kontrol over dets funktion. Der findes mange metoder til at detektere fejl på et transmissionsnet. Differentialmetoden virker ved, at man sammenligner observationer i to knuder. Evt. uventede udslag kan så sted- og retningsbestemmes, idet man kan se, hvor forskellen findes. I Danmark har man udlagt transparent fibernet mellem knuderne for at sikre, at man ikke er afhængig af et tidsstempel på målingerne. I andre lande bruges bl.a. GNSS til tidsstempling, og observationerne sendes på traditionelle kabler. Energinets opmærksomhed på risici ved GNSS og deraf følgende beslutning om ikke at gøre sig afhængig deraf gør, at der ikke er nogen sårbarhed overfor et udfald. Øget udnyttelse af nettet kunne være brugbart, men hvis det blev realiseret på bekostning af øget sårbarhed, kunne konsekvenserne være store. Adgang til en alternativ, præcis tidskilde kunne muliggøre bedre effektivitet af nettet. Energinet har kendskab til både jamming og spoofing på udstyr i elnet og stiller derfor krav til maskering af GNSS-antennerne til PMU'er.
Nødtjenester chuyuss/Shutterstock.com	Nødberedskabet er meget afhængigt af GNSS, og afhængigheden er stigende. I dag indløber ca. 10% af **nødopkald** via 112-app'en, som sender mobiltelefonens position, men med udgangen af 2018 implementeres Advanced Mobile Location i danske nødopkald, så alle mobilopkald bruger GNSS. eCall er allerede trådt i kraft, og de første biler med funktionen er på markedet. Om få år vil forulykkede biler derfor også indsende en GNSS-baseret position til alarmcentralen. Tid er meget værdifuld i en nødsituation, og studier har vist, at præcis angivelse af ulykkens placering reducerer responstiden. Efter alarmcentralen har samlet de nødvendige oplysninger, **udvælges det rette køretøj** til opgaven baseret på position og status. Også her er GNSS en vigtig kilde til positionering. Køretøjet **navigerer** derefter til åstedet ved hjælp af GNSS-navigation og digitale kort. Meget få køretøjer er udstyret med papirkort, og grundet kredsenes størrelse, kan man ikke forvente, at politi-, ambulance-, og brandfolk kender lokalområdet godt nok til at navigere uden hjælpemidler. Brugen af GNSS gør, at personalet i udrykningskøretøjet kan forberede sig på opgaven eller skrive rapport i stedet for at skulle navigere. Især ved **politiopgaver bruges GNSS til opgaveløsning**. I forbindelse med menneskejagter eller borgere der har forladt fx et plejehjem, er det vigtigt at vide hvilke områder der er afsøgt, og et GNSS-spor på en skærm bruges til at skabe overblik. Ved den store **menneskejagt i september 2018** mobiliserede politiet i Espe på Fyn, fordi GPS-overvågningen havde vist, at en eftersøgt lejebil var der. En defekt antenne på bilen havde forstyrret GPS-signalet, med samme effekt som ved spoofing. Bilen blev fundet i Holbæk. I forbindelse med terrorangreb eller lignende kan man forestille sig, at politiet og andre tjenester kunne blive udsat for jamming eller spoofing, så det er vigtigt, at man har et alternativ til GNSS og bevarer de nødvendige kompetencer. Der er tilstrækkeligt med personel til rådighed til, at man kan erstatte det elektroniske flådestyringssystem med et traditionelt kort med markører for hvert køretøj. Dette vil selv sagt være mindre effektivt, men kunne sikre fortsat drift. Denne løsning er mulig fordi Sikkerhedsnettet (SINE) har bekræftet, at selvom det anvender GNSS, kan det blive ved med at fungere i mindst fem dage efter et GNSS-nedbrud. Det er derfor muligt at bevare kommunikationen, selv hvis det civile net overbelastes.

Meteorologi

Thomas Nedergaard, via DMI.dk

Det er velkendt, at meteorologer anvender satellitbilleder til at lave vejrudsigter med kort og længere sigte. At meteorologer også er afhængige af GNSS, er måske ikke så kendt. Som i mange andre dele af samfundet er meteorologernes brug af GNSS en konsekvens af, at GNSS er den nemmeste måde at holde styr på, hvor noget befinder sig.

Meteorologer bruger **målinger fra skibe og bøjer**, som bevæger sig rundt på havet. Målingerne omfatter bl.a. tryk og temperatur ved havoverfladen, som sendes tilbage ved hjælp af satellitkommunikation, og som bruges i vejrmodeller.

En anden type målinger foretages ved hjælp af **radiosonder**. Disse opsendes periodisk med vejrballoner fra forskellige steder i Europa og bruges til at måle tryk, temperatur, luftfugtighed og vind. GNSS giver position og højde og har tillige erstattet barometre, som tidligere blev sendt op.

DMI's **lynpejlesystem** er en anden bruger, som ved hjælp af synkroniserede sensorer på jorden kan tælle og stedfæste lyn i Danmark. Synkroniseringen er afgørende for at beregne, hvor lynet slog ned. Disse oplysninger bruges bl.a. af forsikringsselskaber til at bestemme, om der er grundlag for at udbetale erstatning.

Endelig bruges GNSS til **radiookkultation**, som udnytter, at GNSS-signalet reagerer på atmosfæren. Så hvis man kan observere et signal og beregne hvordan det teoretisk skulle have bevæget sig, kan man observere forskellen og regne baglæns for at udregne temperatur og fugtighed i atmosfæren.

DMI har bekræftet, at kommunikationen mellem instituttets supercomputer i Island og hovedkontoret i Storkøbenhavn ikke bruger GNSS, men i stedet har to separate leverandører af internetbaseret tid, som man har verificeret, er uafhængige af GNSS.

Et tab af GNSS ville have betydning for DMI, men instituttet ville stadig kunne fungere og levere langt hovedparten af sine tjenester. Jo længere udfald, des større bliver betydningen. Bøjer driver eksempelvis ikke meget, så den tidligere position er nok en god approksimation til den faktiske position – i starten. Et nedbrud i GNSS vil forringe nøjagtigheden af vejrforudsigelser, hvilket kan få betydning for DMI's kunder og brugere.

Det er dog relevant at sikre sig, at det kommunikationssystem, der leverer resultater fra bøjer og skibe, ikke er sårbart overfor et udfald af GNSS.

Landbruget

Henryk Sadura/Shutterstock.com

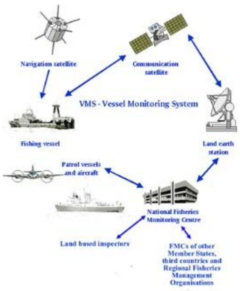
Både offentlige og private aktører inden for landbruget anvender GNSS. **Landbrugsstyrelsen** er ansvarlig for udbetalingen af 7 mia. kr. i EU landbrugsstøtte. Styrelsen bruger avanceret GNSS-udstyr til at kontrollere, at det areal, der er indberettet af landmændene i ansøgningen om støtte, er korrekt. **Private landmænd** anvender også GNSS. 51% af dansk landbrugsjord sås, gødes og høstes med GNSS-vejledning, som giver mulighed for at sikre, at man bruger så lidt af marken som muligt til at bære landbrugsmaskiner. Ved at analysere satellit-, drone- eller ortofotos kan man også bruge GNSS til at sprede den optimale mængde af gødning og pesticider, så man kun behandler de planter, der trænger. Landmænd kan spare 2-4% på brændstof og 4-9% af alle produktionsinput ved at bruge GNSS.

Både offentlige og private brugere inden for landbruget bruger GNSS intensivt i visse perioder og meget begrænset i andre. Et udfald i januar ville have meget begrænset betydning for både offentlige og private aktører, hvorimod et udfald samtidig med gødskning i maj og kontrol af efterafgrøder i september ville vanskeliggøre arbejdet for såvel landmænd som Landbrugsstyrelsen.

Landmænd ville om nødvendigt køre uden GNSS, men de effektivitetsgevinster, som GNSS bringer, ville blive tabt, og derudover kan man forvente, at landmænd, der har anvendt GNSS i mange år, ville have mistet nogle af de evner, de tidligere havde. Det er derfor sandsynligt, at man ville miste mere end effektivitetsgevinsterne ved GNSS. Landbrugsstyrelsen ville formentlig søge alternative metoder til kontrol, herunder billeder fra satellitter og fly.

Der er ingen specifikke trusler mod landbruget, da ingen udefrakommende har incitament til at forstyrre erhvervet. Landmænd kunne få økonomisk gevinst af at indrapportere større arealer og spoofe kontrolfunktionen, men da Landbrugsstyrelsen bruger historiske billeder og målinger, er det næppe sandsynligt, at alle systemerne kan snydes. Man kan praktisk ikke konstruere et system, der kan erstatte GNSS for hele landet, men det er muligt, at særligt ressourcerige storlandmænd kunne være interesserede i et lokalt netværk af såkaldte "pseudolites" (pseudo-satellitter), som kunne skabe et lokalt positioneringsnetværk, der er uafhængigt af GNSS.

Fiskeriet


Navigation satellite
Communication satellite
VMS - Vessel Monitoring System
Fishing vessel
Land earth station
Patrol vessels and aircraft
National Fisheries Monitoring Centre
Land based inspectors
FMCs of other Member States, third countries and Regional Fisheries Management Organisations

Europa-Kommissionen

Ligesom i landbruget er der to grupper af GNSS-brugere i fiskeriet. Det europæiske Vessel Monitoring System (VMS) administreres i Danmark af **Fiskeristyrelsen**, som kan følge hvor alle fiskerbåde over 12m befinder sig. Fiskerbåde rapporterer deres GNSS-afledte position, retning og hastighed hver anden time, så man kan følge med i hvor der fiskes og sikre, at der ikke fiskes i miljøbeskyttelseszoner. Da fiskerbåde er forbundet med internettet gennem VMS (via Inmarsat satellitkommunikation), er det også muligt for Fiskeristyrelsen at opdatere listen over miljøbeskyttelseszoner i realtid, og derved reagere på evt. nye oplysninger om økosystemet.

Private brugere af GNSS er **fiskere**, som bruger systemet til at navigere til gode fiskesteder og til at sikre, at de ikke overtræder loven. Fiskere sparer også tid ved at bruge VMS til logning og indrapportering digitalt i stedet for papirbaserede systemer. Ydermere kan GNSS anvendes til sofistikeret monitorering af fiskerbåden. Ved at placere mange antenner på båden kan man beregne krængning og dermed få advarsler om farlig sejlads, før båden får slagside.

Brugen af GNSS blandt private fiskere er meget vigtig, som vist i et "eksperiment" på den Koreanske Halvø. Nordkorea jammede GPS-signalet over Sydkorea i 2016, hvilket resulterede i, at 70 ud af 332 fiskerbåde, der var stævnet ud den morgen, vendte om.

Et udfald af GNSS ville næppe være katastrofalt for Danmark, men det ville betyde en øget rapporteringsbyrde for fiskere (ca. 1.000 logbøger over fem dage) og for Fiskeristyrelsen, som ville skulle indtaste disse. Endvidere ville man miste muligheden for at beskytte udsatte områder, som kunne blive beskadiget. Der er alternative systemer på plads til at holde styr på, hvor fisk er fanget, så sandsynligheden for at fiskere ville jamme eller spoofe VMS-systemet synes ikke stor.

Vejtransport

Kaspars Grinvalds/Shutterstock.com

Bilnavigation bragte oprindeligt GNSS til befolkningen. Ifølge Danmarks Statistik har ca. 50% af befolkningen en "GPS", og 88% af befolkningen har adgang til en smartphone. Der er således ikke mange bilejere, som ikke kan anvende GNSS til navigation, hvis de vil.

GNSS er imidlertid ikke blot en teknologi for forbrugere, men mange kommercielle transportfirmaer bruger den også til at navigere og ikke mindst til flådestyring. Flådestyringssystemer tillader hovedkontoret at holde styr på, hvor køretøjerne befinder sig, således at man kan respondere hurtigt og effektivt på nye opgaver.

Flextrafik er en regional, offentlig tjeneste, som giver mulighed for, at befolkningen kan køres til relevante aftaler, eksempelvis på hospitaler. Flextrafik har ingen køretøjer, men bruger private taxaer til at dække behovet. Fra hovedkontoret planlægges ture, og systemet kan samarbejde med satellitnavigationssystemer i bilerne, således at chaufføren kan finde vej. Man bruger ikke GNSS til at se hvor bilerne er, men i stedet bruges indberetninger fra chaufføren. Værdien af GNSS i dette system ligger i behandling af klager og monitorering af turen. Hvis en kunde klager over en udeblevet bil, kan Flextrafik kontrollere, hvor bilen har været, og respondere på klagen. Man bruger også data til at kalibrere ture sådan, at hvis specifikke dele viser sig at tage længere tid end forventet, kan dette inkorporeres i planen.

Flextrafik dækker et stort område, og man kan derfor ikke forvente, at chaufføren har lokalt kendskab til at navigere uden hjælpemidler. Det er uvist, hvor mange biler der har papirkort, men dette forventes at være få. I tilfælde af tab af GNSS vil man derfor være afhængig af, at mobilnettet stadig virker, så man kan navigere med digitale kort ved selv at flytte billedet.

Et udfald af GNSS må forventes at placere mange bilister i en tilsvarende situation, og selvom mange har tilstrækkeligt lokalt kendskab, må man forvente, at nogle bilister forlænger deres rejsetid, og kører mindre forudsigeligt, hvilket vil påvirke alle bilister.

Storebæltsbroen er et vigtigt trafikalt knudepunkt i Danmark, som passeres af mere end 30.000 biler om dagen. Man bruger GNSS til synkronisering af IT systemer og flylys m.v., men der er ikke en kritisk afhængighed. Med andre ord ville Storebæltsforbindelsen ikke blive påvirket af et udfald. Trafikken kunne stadig køre.

For at begrænse sårbarheden overfor et udfald, er det vigtigt at bibeholde befolkningens evne til at navigere ved kort og uden en blå plet på en skærm.

Offentlig IT Statens IT	IT-systemer kræver synkroniseret tid for at fungere, og GNSS er i mange tilfælde den billigste og bedste måde at opnå dette – især fordi man kan sikre, at alle dele af systemet bruger den samme referencetid, uanset hvor de er. Danmarks offentlige sektor er meget digitaliseret, og landet er nummer 4 på EU's indeks. I Danmark varetager **Statens IT** det offentliges behov. Statens IT har 5.000-6.000 servere forskellige steder i landet, som servicerer 16 ministerier og 19.000 brugere. Statens IT har bekræftet, at man ikke bruger GNSS til synkronisering, men i stedet har en internetbaseret leverandør. Det har ikke været muligt at undersøge, hvilket ur der til syvende og sidst leverer tiden, og om det er afhængigt af GNSS. Det anbefales derfor kraftigt, at de relevant myndigheder forsikrer sig om, at der ikke er risiko for, at et jamming- eller spoofingangreb på leverandøren kan give problemer for det offentliges IT-systemer.
Finanssektoren Mahlum (Wikimedia Commons)	Den finansielle sektor er helt afhængig af præcis tid. Højfrekvente transaktioner tidsstemples således, at den pris, som gjaldt præcis i handelsøjeblikket, kan afregnes. GNSS er den billigste kilde til tidsstempling, og har den yderligere fordel, at alle aktører, der bruger den samme konstellation, er enige om tiden. EU's Markets In Financial Instruments Directive (MIFID II)[9] foreskriver, at organisationer, der foretager højfrekvent handel, skal kunne tidsstemple transaktioner med mindst 100 mikrosekunders nøjagtighed i forhold til UTC. Dette krav kan ikke opfyldes af DCF77, men kræver internet-baserede kilder eller GNSS (eller evt. STL). Kommissionens Delegerede Regulativ foreskriver, at virksomheder kan anvende GNSS til at opnå denne nøjagtighed, hvis de kan gøre rede for, hvordan de behandler forskellen mellem GNSS-tid og UTC. Direktivet foreskriver endvidere, at eventuelle overtrædelser af bestemmelserne kan sanktioneres med bøde fra 5 mio. Euro op til 10% af virksomhedens omsætning i foregående år. Af andre anvendelser af GNSS i finanssektoren kan nævnes børshandel og netværks-synkronisering ved digitale betalinger, kontanthævning m.v. Den finansielle sektor har ikke bidraget til denne undersøgelse, men andre interessenter har udtrykt bekymring over sektorens manglende forståelse af risici ved brug af GNSS. Der er således en frygt for, at et GNSS nedbrud eller jamming/spoofing-angreb på specifikke datacentre kunne bringe sektoren i fare. Det anbefales, at en undersøgelse af sektorens tidsstyringsudstyr iværksættes. Hvis sårbarhed konstateres i forbindelse med en sådan hændelse, kunne konsekvenserne for sektoren og samfundet blive alvorlige. Derudover kunne eventuelle sanktioner være meget dyre for institutionerne.

Konklusion og anbefalinger

Danmark er et avanceret, moderne samfund, der bruger teknologi til at løse opgaver. GNSS er en af disse teknologier og bruges bredt i samfundet. At Danmark ikke har en national tidskilde (ulig nabolandene Sverige og Tyskland, og mange andre lande) gør, at applikationer, der kræver tidsstempler med høj nøjagtighed, må bruge GNSS. Det anbefales at undersøge, om der er behov for en national tidskilde, og om der er efterspørgsel efter en internetbaseret tjeneste med specifikke performanceparametre. Private, kommercielle brugere bør overveje, om det er værd at finde alternative kilder som STL (der er fra en kommerciel udbyder, og derfor ikke er gratis at bruge), og staten bør overveje sin position i forhold til eLoran, som navnlig i Storbritannien nævnes som en mulig løsning på mange problemer med GNSS-sårbarhed. En dansk station i et genskabt eLoran-net kunne dække mange tidsstyringskrav i Danmark og forbedre geometrien til navigation i Nordsøen.

Imidlertid har samfundsvigtige virksomheder, som Energinet, udvist behørig skepsis overfor GNSS, og givet afkald på effektivitetsgevinster pga. den sårbarhed, der er forbundet med en stor afhængighed af en enkelt kilde. Det anbefales, at fremtidige effektiviseringsinitiativer anlægger samme tilgang.

[9] European Commission (2014). *DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU*

Det tyder på, at Finanssektoren er bagud i forhold til internationale konkurrenter (herunder Storbritannien), og en undersøgelse af sektorens udstyr ville være nyttig, så man kan sikre sig, at et jamming- eller spoofingangreb ikke kan bringe sektoren i problemer. Storbritanniens Cabinet Office udgav i 2018 en rapport, som anbefaler, at alle samfundsvigtige funktioner (i Storbritannien har man offentliggjort en liste med 13) rapporterer om GNSS-sårbarhed til de relevante instanser.

Det offentliges IT er en væsentlig brik i samfundets puslespil, og en nærmere undersøgelse af dets afhængighed af GNSS (både i Statens IT og andre tjenester) anbefales også.

Landbruget, fiskeriet og meteorologien er i stand til at fortsætte driften med mindre forstyrrelser, mens nødberedskabet må forventes at blive hårdt ramt, men dog kunne opretholde drift.

Vejtransport er afhængig af GNSS, men danskernes evner til at navigere bevirker, at man må forvente, at trafikken vil blive langsommere, men ikke at den går helt i stå.

Udover de områder, der er undersøgt i denne rapport, anbefales det, at man sikrer, at det civile telekommunikationsnet er robust overfor et udfald af GNSS. Mange af de områder, der er analyseret i denne rapport, klarer sig med begrænset sårbarhed, fordi det antages, at telekommunikationen er robust, og at man derfor kan bruge dens tjenester til backup. Det ville være godt at få klarlagt.

Det bredere transportsystem kunne også undersøges nærmere. Maritim transport bruger GNSS til mange væsentlige formål, og det ville være nyttigt at undersøge, om kaptajnerne på de skibe, der leverer varer til Danmark, kan navigere uden GNSS. I fremtiden bliver luftfarten mere afhængig af GNSS, hvor primær overvågning af fly skifter fra radar til ADS-B, som er GNSS-baseret. Længere ude i fremtiden kunne togdriften også blive GNSS-afhængig, hvis Danmark implementerer European Rail Traffic Management System.

Derudover er det kendt, at DAB-radio og tv-signaler bruger GNSS til synkronisering. Selvom disse tjenester kan virke mindre vigtige sammenholdt med de andre områder i rapporten, er det værd at huske, at Beredskabsstyrelsens vejledning ved alarmering med sirener foreskriver, at man skal gå inden døre og søge information, eksempelvis fra tv og radio, men i stigende grad fra Mobilvarslings-app'en, hjemmesider, og sociale medier.

Sidst, men ikke mindst, og udover disse teknologiske og andre anbefalinger, er det vigtigt at nævne, at evnen til at navigere uden GNSS er flygtig. En undersøgelse fra University College London viser, at man slår hjernen fra, når man slår GPS'en til.[10] Bilister der kører med GPS er således ikke opmærksomme på, hvor de kører, og har svært ved at genskabe ruten senere. Det anbefales, at man underviser i navigation og kortlæsning (evt. ved orienteringsløb uden GNSS-støtte), så befolkningen har noget at falde tilbage på.

[10] University College London (2017). *Satnav 'switch off' parts of the brain*. Available at: http://www.ucl.ac.uk/news/news-articles/0317/210317-satnav-brain-hippocampus [accessed 26/09/2018]

1 Introduction

1.1 What is satellite-based Position, Navigation, and Timing (PNT)?

There are three broad categories of artificial satellites in space: Communication, Earth Observation, and navigation, available from Global Navigation Satellite Systems (GNSS) constellations in Medium-Earth Orbit (MEO). There are currently four GNSS:

- **GPS**: The original GNSS, which was made available in 2000, and is available in all commercial GNSS receivers.;
- **GLONASS**: Russia's system, which reached full operational capability in 2009, and has been widely available in smartphones since the release of the iPhone 4s – the first smartphone with GLONASS was launched in 2011;[12]
- **Galileo**: Europe's GNSS funded by the EU and procured through ESA. Galileo will reach full operational capability in 2020, and became available at the time of the iPhone 8/X – the first smartphone with Galileo was launched in 2016;[13]
- **BeiDou**: China's system, which currently provides local services over the Chinese landmass. Global coverage is in development, and expected by 2020, Apple has not yet made BeiDou available in its iPhones, but Samsung has included it since the Galaxy Note 3 from 2013.[14]

Box 1 Early history of GPS

The launch of the Russian Sputnik satellite in 1957 planted the first seed of satellite-based position, navigation and timing (PNT) services. US military and scientists tracked the location of the satellite by comparing the time at which different measurement stations on the ground received the 'pings' emitted by the satellite.

Within two decades, the *Global Positioning System (GPS)* was launched and operational and used by the US military. GPS uses the same approach as was used to locate Sputnik, but in the opposite direction. All 30 satellites in the constellation (including spares) emit their location and time. Ground-based receivers with access to signals from a sufficient number of satellites can therefore compute the distance to each satellite (as the signal travels at approximately the speed of light), and trilaterate their precise location.[11]

As 'GPS' alludes to, the original purpose of the constellation was for **positioning (P)** but given the frequency of update and availability of the service, the signals were soon used for **navigation (N)** purposes by adding direction and velocity to equation. The devices commonly known as GPSs that introduced the system to the mass market use software systems to match the position derived from GNSS with local maps.

Beyond positioning and navigation, GNSS is used for **timing (T)** because the atomic clocks on the satellites in space are extremely high grade, so the time signal sent from the satellite is very reliable, and free at point of use. This means that a relatively simple GNSS receiver (starting price as low as

[11] GPS World (2012). *A brief history of GPS*. Available at: https://www.pcworld.com/article/2000276/a-brief-history-of-gps.html [accessed 02/06/2018]

[12] Lenta.ru (2010). *Putin showed the Russian analogue to iPhone 4*. Available at: https://lenta.ru/news/2010/12/28/ohwow/ [accessed 27/09/2019]

[13] European GNSS Agency (2016). *First European Galileo-ready smartphone to hit stores in July*. Available at: https://www.gsa.europa.eu/newsroom/news/first-european-galileo-ready-smartphone-hit-stores-july [accessed 27/09/2018]

[14] Qualcomm (2013). *Qualcomm Collaborates with Samsung to be First to Employ China's BeiDou Satellite Network to Enhance Location-Based Mobile Data and Services for Smartphones*. Available at: https://www.qualcomm.com/news/releases/2013/11/21/qualcomm-collaborates-samsung-be-first-employ-chinas-beidou-satellite [accessed 27/09/2018]

a couple of tens of DKK), can be used to access precise time that would otherwise require the purchase of an atomic clock costing 100s of thousands of DKK. For this reason, sectors and agents that require precise time increasingly turn to GNSS as the preferred provider. In particular, network operators such as telecoms and power transmission companies, and international financial institutions turn to GNSS because the systems are internally synchronised, which means all users all over the world have the same reference time.

All global systems use a frequency in the upper L-band (1559-1610 MHz). These frequencies are commonly referred to as L1[15]. As the frequencies are very close, it is relatively easy for receiver manufacturers to include all the constellations in their solutions. This is especially the case as the constellation owners have agreed interoperability between the signals. This means that receivers no longer need to access signals from four satellites from the same constellation, but instead can rely on signals from any four satellites. In urban canyons, where tall buildings obscure a large proportion of the sky, this can be the difference between having line-of-sight to four satellites (i.e. the ability to fix a position) or not.

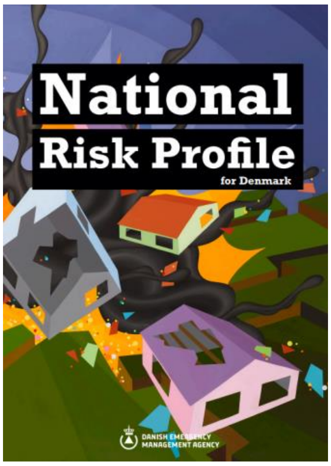
In addition to the L1 band, individual constellations broadcast signals in additional bands. Galileo uses E5 and E6, GPS uses L2 and E5, BeiDou use B2 and B3, and GLONASS uses L1, L2, L3, and L5.[16]

A commercial, satellite-based PNT service is available from Satellite Time and Location (STL) that uses the frequency band previously allocated to pagers to provide its service. The STL service is hosted on Iridium satellites in Low-Earth Orbit (LEO), and is independent of some of the vulnerabilities suffered by GNSS. For this reason, outage of STL is not in scope of the study, but the service could be used as a mitigation against certain GNSS vulnerabilities.

1.2 Motivation for the study

The ubiquity of GNSS as the preferred solution for PNT has fostered growing concern in the international PNT community.[17] There is consensus that GNSS is the best solution available to meet PNT-related challenges, but it is not perfect.

Figure 1 National Risk Profile



Source: Danish Emergency Management Agency

The signal strength of GNSS is a particular concern. At source (i.e. the satellite), the power is equivalent to a 40W lightbulb, and the signal needs to travel 20,000km, through the Earth's atmosphere, to reach the user. The signal is therefore very faint when it arrives and needs specialised equipment to be received and amplified. The faint signal strength means that it risks being overpowered by interference in the frequency band. Interference can also be intentional (e.g. jamming and spoofing events are on the rise), or natural (e.g. the effect of space weather – radio bursts resulting from solar flares affect GNSS signals and degrade the accuracy in user receivers).

These vulnerabilities mean there is a need to understand just how reliant modern economies are on PNT from space.

[15] The signal in the same frequency band can also be referred to as E1/G1/B1 for Galileo, GLONASS, and BeiDou, respectively

[16] European GNSS Agency (2018). GNSS User Technology Report Issue 2, available at: https://www.gsa.europa.eu/european-gnss/gnss-market/gnss-user-technology-report

[17] Several countries have studied the vulnerabilities of their economies, including UK, US, Canada, and Korea. In addition, the 1st Galileo User Assembly in November 2017 identified the protection against vulnerability as a key requirement for users across many applications.

Space weather was specifically identified as a one of thirteen events studied in the Danish *National Risk Profile* published by the Danish Emergency Management Agency in 2017.[18] Spaceweather is a known risk to satellites in space but it is difficult to defend against. The National Risk Profile further identified GNSS spoofing as a cyber event that could significantly affect the ability of emergency services to respond to crises.

There is a feeling in the navigation community (e.g. the British Royal Institute of Navigation), that the general public has lost the ability to navigate using a paper map and a compass, because their smartphone does the navigation for them. Similarly, the low cost and generally reliable performance of GNSS means that certain professional users could be in deep trouble if GNSS were denied. For example, a sextant is still mandated carriage on vessels under the Safety-of-Life-At-Sea (SOLAS) convention;[19] however, the actual ability of mariners to use it has been questioned.

1.3 Research objective

The objective of this study is to perform an overarching risk assessment, supported by several case studies with specific focus on the consequences associated with loss of space-based PNT services within the domains of the ministries represented in the *Inter-Ministerial Space Committee*.

1.3.1 Definition of scenario of outage

An initial task was to define a scenario of disruption to satellite-based PNT services that is suitable for Denmark. The following scenario was agreed:

An instantaneous and complete loss of all GNSS services for a consecutive period of five days after which time all GNSS services are fully and instantaneously re-instated.

This scenario is consistent with the study conducted in the UK,[20] and therefore maximises comparability across the two studies. The UK study chose a five-day outage as a reasonable worst-case scenario that aligns with scenarios in the UK National Risk Assessment, UK Business Continuity Planning Assumptions, and the UK National Risk Register.

1.4 Caveats and limitations

This research has been conducted by a team of independent professional economists with specialist knowledge of GNSS technology and markets. The study relies on secondary research as well as interviews with more than 15 stakeholders across GNSS in general and its use in specific case studies. Nonetheless, the reader should bear in mind the following high-level limitations and caveats:

- The report portrays information across a selected set of case studies covering a wide range of activity in the Danish economy. It **does not purport to present a comprehensive, economy-wide finding**.
- Greenland and the Faeroes are not in scope of the present study.
- The study is based on consultations with civil servants and private operators across the case studies. While all efforts have been made to ensure the information is truthful, the

[18] Danish Emergency Management Agency (2017). *National Risk Profile 2017*.

[19] UK Maritime and Coastguard Agency (no date). *Regulation 19 - Carriage requirements for shipborne navigational systems and equipment*. Available at: http://solasv.mcga.gov.uk/regulations/regulation19.htm [accessed 02/06/2018]

[20] London Economics (2017). *The Economic Impact on the UK of a Disruption to GNSS*. Available at: https://www.gov.uk/government/publications/the-economic-impact-on-the-uk-of-a-disruption-to-gnss

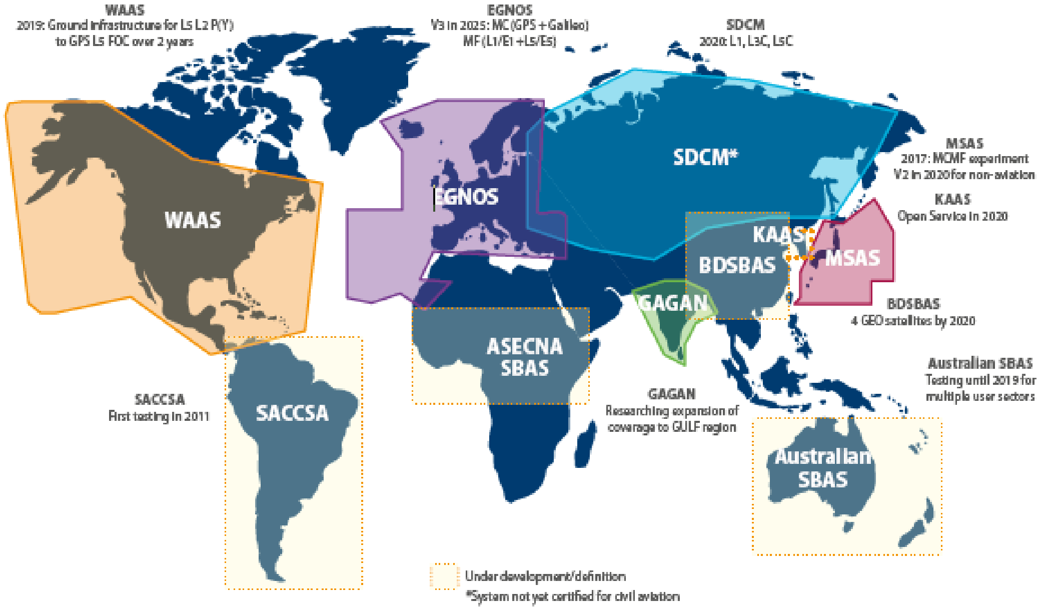
nature of consultation means that **certain biases** (e.g. optimism bias) might be present in the findings.

- Though the report discusses vulnerabilities and mitigations, it is **agnostic to the source of GNSS disruption**. In certain case studies and for specific causes of GNSS loss, the impact would go far beyond the results presented here.
- The report considers GNSS as a single set of satellites, irrespective of constellation. While discussion over the inherent risk mitigation of employing multiple systems is present, the case studies are based on a full outage of GNSS and does not distinguish constellations.
- The report is based on information collected in 2018, and although future developments are mentioned, the findings relate to the **current situation** in the main. The GNSS market is characterised by great dynamism and new applications emerge constantly. The findings might therefore not apply in the relatively near future.

2 Fundamentals of (satellite-based) PNT

GNSS is the infrastructure that allows users to compute their position, velocity and local time using signals from satellites in space. Four systems provide global coverage: GPS (US), GLONASS (Russia), Galileo (EU), and BeiDou (China). In addition, regional systems in Japan (QZSS), India (IRNSS) and China (BeiDou regional component) provide enhanced performance in specific regions. Furthermore, satellite-based augmentation systems (SBAS) improve accuracy and integrity of signals for Safety-of-Life operations across most of the globe, as illustrated in the figure below.

Figure 2 Satellite-based augmentation systems (SBAS) in the world


WAAS
2019: Ground infrastructure for L5 L2 P(Y) to GPS L5 FOC over 2 years
EGNOS
V3 in 2025: MC (GPS + Galileo) MF (L1/E1 + L5/E5)
SDCM
2020: L1, L3C, L5C
MSAS
2017: MCMF experiment V2 in 2020 for non-aviation
KAAS
Open Service in 2020
BDSBAS
4 GEO satellites by 2020
Australian SBAS
Testing until 2019 for multiple user sectors
GAGAN
Researching expansion of coverage to GULF region
SACCSA
First testing in 2011
WAAS
EGNOS
SDCM*
KAAS
BDSBAS
MSAS
GAGAN
ASECNA SBAS
SACCSA
Australian SBAS
Under development/definition
*System not yet certified for civil aviation

Source: European GNSS Agency (2018). GNSS User Technology Report Issue 2, available at: https://www.gsa.europa.eu/european-gnss/gnss-market/gnss-user-technology-report

GNSS are assessed on the key performance parameters presented in Box 2.

Box 2 GNSS key performance parameters

Availability: Percentage of time over a specified time interval that a sufficient number of satellites are transmitting a usable ranging signal within view of the user.

Accuracy: The difference between true and computed position (absolute positioning).

Continuity: Ability to provide the required performances during an operation without interruption once the operation has started.

Integrity: The measure of trust that can be placed in the correctness of the position or time estimate provided by the receiver.

Time To First Fix (TTFF): A measure of a receiver's performance covering the time between activation and output of a position within the required accuracy bounds.

Robustness: A qualitative, rather than quantitative, parameter that depends on the type of attack or interference the receiver is capable of mitigating.

Authentication: The ability of the system to assure the users that they are utilising signals and/ or data from a trustworthy source, and thus protecting sensitive applications from spoofing threats.

Source: European GNSS Agency (2017). GNSS Market Report Issue 5. Available at: https://www.gsa.europa.eu/2017-gnss-market-report

2.1 Timing (and synchronisation)

Satellite-based **timing** and synchronisation refers to the use of a GNSS receiver for the purpose of accessing accurate time that is traceable to Universal Coordinated Time (UTC). In addition, GNSS offers a reference frequency. This information can be used across a variety of different user groups and for many different purposes[21]:

- **Telecommunications**: Precise time is used to synchronise networks and ensure that the wireless communications can transfer between base stations without loss of call quality. GNSS is also used to provide frequency alignment on all base stations in a network. Precise time is also used for time slot allocation and event logging. The GNSS reference frequency is used by teleports to ensure communications with satellites are on the correct frequency.
- **Electricity**: Precise time is used to detect faults on the transmission network and identify the direction of travel of a fault. This requires accurate time stamping of all observations as minor discrepancies in reference time could lead to the wrong conclusions. The use of the GNSS reference frequency makes it possible to compare the frequency on the network against the desired frequency (in Denmark, 50Hz).
- **Finance**: The financial sector relies on accurate time for time stamping at financial institutions and stock exchanges. These time stamps are required to ensure trades are settled the correct price, and to be able to recreate a transaction in chronological order and establish causal links. The European Commission's second *Markets in Financial Instruments Directive* (MiFID 2)[22] specifies the accuracy with which different types of financial institutions must be able to trace their time source to UTC.[23]

In general terms, accessing UTC traceable time requires two elements: a time source that is traceable to UTC and a delivery mechanism with known uncertainties. The appeal of satellite-based PNT is that each GNSS as a time source is traceable to UTC.[24] In addition, the delivery mechanism through radio waves has known uncertainties so the time derived by the user's equipment is within a known range from UTC.

2.2 Position and navigation

Users of satellite-based PNT for position and navigation purposes cover a wide range of applications across a vast set of market segments. Applications can be grouped by **position**, where the location of the user is important. Such applications include[25]:

- Road tolling, smart tachograph, and eCall in the road transport sector;
- Automatic dependent surveillance broadcast (ADS-B) in aviation;
- Search and rescue beacons on land, sea, and in the air;

[21] For more details and global market forecasts for GNSS, please see European GNSS Agency (2017). *GNSS Market Report Issue 5*. Available at: https://www.gsa.europa.eu/2017-gnss-market-report

[22] DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN

[23] Please see Annex to the COMMISSION DELEGATED REGULATION supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the level of accuracy of business clocks. Available at: http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160607-rts-25-annex_en.pdf

[24] European Space Agency, Navipedia (2011). *Time References in GNSS*. Available at: https://gssc.esa.int/navipedia/index.php/Time_References_in_GNSS [accessed 07/08/2018]

[25] For more details and global market forecasts for GNSS, please see European GNSS Agency (2017). *GNSS Market Report Issue 5*. Available at: https://www.gsa.europa.eu/2017-gnss-market-report

- Automatic Identification System (AIS) for merchant and fishing vessels;
- Fitness trackers, points of interest, and ride hailing apps for consumers electronics;
- Safety-relevant and passenger information systems in rail;
- Variable rate application in agriculture; and
- Construction, land, and marine surveying activities.

The majority of **positioning** applications of GNSS use communications networks to report on the position and properties of the receiver. For example, in search and rescue applications, the beacon when activated submits the location of the receiver to a Mission Control Centre that then relays the information to the coastguard or emergency services with jurisdiction in the area of the distressed. Some positioning applications work in the opposite direction where a local database is matched against the position derived from GNSS. Such applications include variable rate application in agriculture and passenger information systems in rail.

Navigation users rely on multiple GNSS position fixes to compute heading and velocity in addition to position. This information interacts with a plotted route to track progress towards a destination. It is based on this simple set of information that satellite navigation apps or devices for pedestrians, cars, aircraft, and vessels are able constantly calibrate the route to the destination and enable real time turn-by-turn navigation. The same fundamental idea is used for tractors and construction machinery with automatic steering capabilities.

3 Vulnerabilities of satellite-based PNT and mitigations

There exist a number of known threats to GNSS availability and fidelity.[26] These can be broadly categorised into three areas – receiver vulnerabilities, environmental challenges, and problems due to human interactions with the system. This section introduces these vulnerabilities as well as mitigations and discusses the need for a backup system to GPS.

3.1 Receiver vulnerabilities

3.1.1 Jamming

The most common forms of blocking or interference with GNSS signals typically occur due to malfunctioning electronics, or from natural sources.[27] There is, however, also the potential for more malicious sources of interference to arise in cases of intentional disruption. Both intentional and unintentional jamming issues arise due to the inherently low power nature of GNSS signals, which means that misleading signals or even unavailability can occur from relatively weak interference sources.[28]

As a result, it is possible to obtain relatively inexpensive devices on the internet, which can cause highly effective localised jamming. Even attempting to use signals from multiple GNSS constellations or multiple frequencies to mitigate the effects can fail, as it is possible to interfere with the entire region of the electromagnetic spectrum used by GNSS. Such devices can be acquired by a wide range of potential users, from governmental or military organisations through to criminals, or even individual citizens seeking privacy in personal time from their employer’s fleet management system.

3.1.2 Spoofing

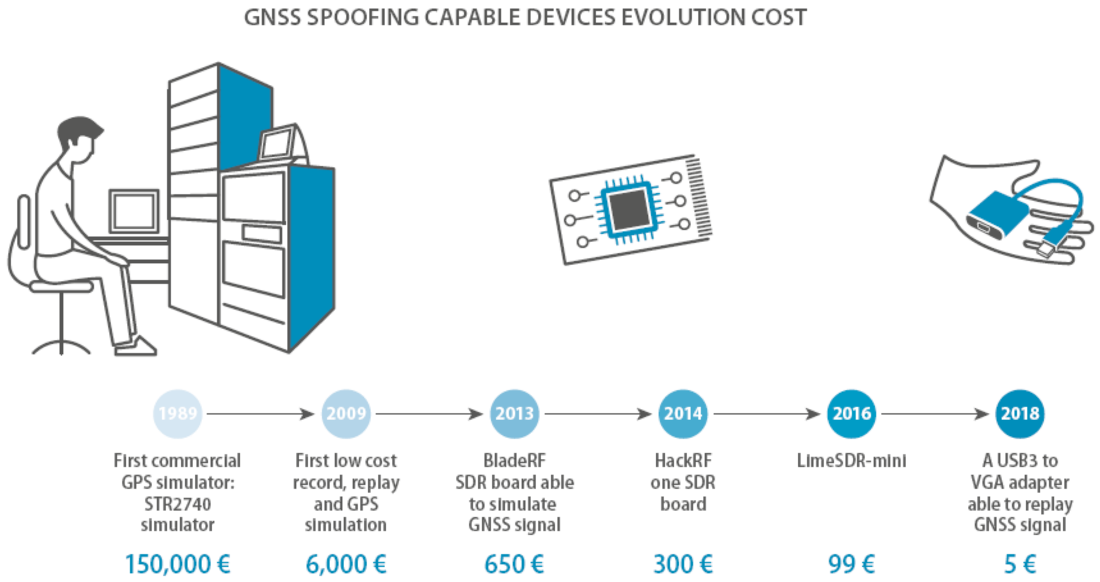
A less blunt method of manipulating GNSS signals is to convince a GNSS receiver that it is in fact in an entirely different location, or ‘spoof’ the signal. The motivations for such activity can arise from the desire to avoid paying location-based road charging, or to cheat at your favourite location-based smartphone game (e.g. Pokémon Go), as well as more serious or malicious objectives. The more benign examples demonstrate how such capabilities are even available at the relatively novice or hobbyist level, and as a result have developed significantly over the last few years as illustrated in the figure below.

[26] This section draws heavily on research and findings from an Innovate UK funded study: London Economics (2017). *The Economic Impact on the UK of a Disruption to GNSS*. Available at: https://londoneconomics.co.uk/blog/publication/economic-impact-uk-disruption-gnss/

[27] For more information, please see the outputs of the Horizon 2020 project Strike 3: http://www.aic-aachen.org/strike3/downloads/POSNAV2016_Paper_German.pdf

[28] Government Office for Science (2018). *Satellite-derived Time and Position: A Study of Critical Dependencies*

Figure 3 Spoofing devices over time


GNSS SPOOFING CAPABLE DEVICES EVOLUTION COST
1989
2009
2013
2014
2016
2018
First commercial GPS simulator: STR2740 simulator
First low cost record, replay and GPS simulation
BladeRF SDR board able to simulate GNSS signal
HackRF one SDR board
LimeSDR-mini
A USB3 to VGA adapter able to replay GNSS signal
150,000 €
6,000 €
650 €
300 €
99 €
5 €

Source: European GNSS Agency (2018). GNSS User Technology Report Issue 2, available at: https://www.gsa.europa.eu/european-gnss/gnss-market/gnss-user-technology-report

A recent incident at the ION GNSS conference in Portland, Oregon in September 2017 illustrates that spoofing can be a subtle threat, and also problematic to resolve.[29] In this particular incident, the cause was an accidental signal leak from GNSS testing equipment that was set to 'France, 2014'. The smartphones in the conference hall accepted the erroneous input and old text messages started to appear. Certificates for email accounts were invalidated by the asynchronous data, and many phones took hours to recover, if at all. Even this assembly of leading experts in the field of GNSS struggled to detect and mitigate the problem.

An incident with potentially more serious consequences was observed in the Black Sea in June 2017, where several ships received spoofed GNSS signals providing inaccurate positioning data.[30] On this occasion, some of the ships were able to identify the misleading signal and navigate via other means, however this was not the case with 100% of shipping in the area. Though fortunately there were no reported serious impacts, the potential for chaos in a similar scenario in a busy shipping lane is apparent.

During the great Danish manhunt that isolated the island of Zealand from the rest of the country in September 2018, a stolen Swedish rental car wanted in connection with a crime was tracked (using GNSS) to a location in Espe on the island of Funen. A faulty antenna on the vehicle interfered with the GNSS tracking system and located the vehicle approximately 100 kilometres from where it was found later that day. Although not confirmed as such, on this occasion, the faulty antenna had the same effect as a spoofing incident.[31]

[29] Scott, L. (2017). *Spoofing Incident Report: An Illustration of Cascading Security Failure* available at http://www.insidegnss.com/node/5661

[30] Lied, H. (2017). *GPS freaking out? Maybe you're too close to Putin* available at https://nrkbeta.no/2017/09/18/gps-freaking-out-maybe-youre-too-close-to-putin/

[31] Københavns Politi (5 November 2018. *Fejlagtige GPS-signaler førte til politiaktion i Espe*. Press release. Available at: http://www.mynewsdesk.com/dk/koebenhavns-politi/pressreleases/fejlagtige-gps-signaler-foerte-til-politiaktion-i-espe-2785687 [accessed 05/11/2018]

An experiment presented in a recent research paper[32] goes one step further by matching the spoofing attack to the route plotted in the satellite navigation device in the car. The experiment takes place in Manhattan and Boston, where the grid layout of the roads means that the environment surrounding the original route plotted on the satellite navigation devices appears very similar to the spoofed route (which involves one wrong turn). The spoofing attack successfully fooled 95% of participants into driving to the wrong destination.

3.1.3 Meaconing

Rebroadcasting genuine GNSS signals, either unintentionally or deliberately, is known as 'meaconing'. A potential beneficial application of meaconing is enabling a proxy GNSS signal in areas with limited coverage such as indoor locations. The end-result however is the generation of a misleading position, owing to the relative time delay from the original broadcast of the GNSS signal via satellite. As a result, the impact of an accidentally rebroadcast signal or maliciously reproduced signal would be similar to those from a spoofing incident, but as the signals would be genuine GNSS signals with a delay, they would be harder to identify.

3.1.4 Mitigations

At the receiver level, a number of potential mitigation strategies exist:

- Avoidance of **jamming** can be achieved through insertion of notch filters in the receiver front-end.[33] This way, receivers are able to filter the jammer's signal, but this is only effective against continuous wave interference. Chirp jammers (commonly found in 'personal privacy devices' for cars), are different, and cannot as easily be removed at the receiver level. Instead, as jammers are usually found on or near the ground, clever antennas can be employed to simply disregard signals arriving from below a certain angle. This way only signals from the same direction as the satellites are let into the receiver, and the risk of overpowering is reduced. Antennas that are even more sophisticated can nullify signal from the direction at which the jamming signal is detected. Such antennas are costly and have a fundamental need to operate in a no-to-low dynamic environment.
- In terms of **spoofing**, mitigation can come in two forms. Technically, spoofing is only successful if the spoofed agent remains unaware, so the simplest mitigation against spoofing is *detection*. Galileo has a unique way of assisting with this through its Open Service Navigation Message Authentication (OS-NMA), which allows the receiver to verify that a signal has indeed arrived from a satellite in space, and therefore identify signals that have not. The OS-NMA is due to be offered in experimental form in 2019 and fully fledged at full operational capability in 2020. Other means of spoofing detection include analysis of the received signals to identify inconsistencies. The faint nature of GNSS signals become a strength in this respect, as the spoofed signal needs to be calibrated to a similar level for the receiver to accept it. Inside a GNSS receiver is an oscillator that is used to steer frequency and, in many cases, keep time. A receiver should be able to reject a spoofed GNSS signal if this is inconsistent with the time kept in the oscillator. Beyond the GNSS-receiver itself, many GNSS-enabled devices are connected to Wi-Fi and cellular networks.

[32] Zeng K, Liu S, Shu Y, Wang D, Li H, Dou Y, Wang G, Yang Y (2018). *All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems*. 27th USENIX Security Symposium (USENIX Security 18). Available at: https://www.usenix.org/conference/usenixsecurity18/presentation/zeng

[33] A detailed account of the layout and setup of receivers is beyond the scope of this report. The interested reader is encouraged to study European GNSS Agency (2018). *GNSS User Technology Report Issue 2*, available at: https://www.gsa.europa.eu/european-gnss/gnss-market/gnss-user-technology-report

If the location (or date) offered by GNSS is inconsistent with the location available from Wi-Fi hotspots and cellular masts, or the implied journey violates the laws of physics, then in time, devices could be improved to reject the spoofed signals. Even more useful than detection, *mitigation* against spoofing is a more complicated activity, and can only be achieved by encrypting the whole navigation message, and letting users decipher on their devices using secure keys. Galileo and GPS offer such services to EU members and NATO members through their Public Regulated Service (PRS) and Precise Positioning Service (PPS) services, respectively. In addition, Galileo will offer a Signal Authentication Service (SAS) on a commercial basis to subscribers.

- As **meaconing** is a particular type of spoofing, the physical mitigation strategies still apply, however, the use of OS-NMA does not clearly solve the problem because the signals are genuinely from the satellites, just delayed.

3.2 Environmental challenges

3.2.1 Space weather and ionospheric disruption

Varying levels of electromagnetic radiation naturally emitted by the sun is the primary cause of space weather interference to GNSS systems. These effects can take a number of forms, most typically from disturbing the Earth's ionosphere, a layer of atmosphere 80-600km above the ground. The ionosphere contains electrically charged ions with a sufficient density to slow the GNSS signals as they pass through.[34] Ionospheric scintillation can be caused by space weather, local time, and geomagnetic activity, and describes an event in which the electrically charged ions can modify the GNSS signals and make it impossible to obtain a position fix. Scintillation is more common over the equator or the poles than over mid-latitude areas, such as mainland Denmark.[35]

Short-term solar storms can also have consequences both in space and on earth, with the level of impact scaling with intensity. A sudden burst of radio waves over the course of minutes or hours can result in jamming effects of GNSS devices described above, whilst more intense superstorms lasting several days could potentially damage GNSS satellites in orbit, causing disruption to services. Whilst GNSS satellite constellations are designed to be resilient to high intensity space weather, an event of a truly extreme nature last occurred in 1859 (the Carrington event), and as such the effects of a similar occurrence on modern spacecraft systems are difficult to estimate due to their extremely low occurrence rate.

3.2.2 Space debris

A global issue of increasing concern relates to the ever-growing population of orbital debris generated by several decades of space activity. Whilst satellites have the capability to avoid larger, trackable objects, smaller high velocity fragments occurring in orbit are almost impossible to detect. A catastrophe-level event in future years is not inconceivable unless debris mitigation activities are successful. If one satellite is severely damaged by a high energy collision, then the resulting debris field could lead to a chain reaction of collisions with other spacecraft that occupy similar orbits. This could lead to GNSS outages if such an event was to occur with the orbital plane of a GNSS

[34] NovAtel (no date). *An introduction to GNSS*. Available at: https://www.novatel.com/an-introduction-to-gnss/chapter-4-gnss-error-sources/error-sources/ [accessed 03/06/2018]

[35] National Oceanic and Atmosphere Administration, Space Weather Prediction Center (no date). *Ionospheric Scintillation*. Available at: https://www.swpc.noaa.gov/phenomena/ionospheric-scintillation [accessed 03/06/2018]

constellation. Medium-Earth Orbit used by GNSS satellites is currently of low concern from a space debris perspective with 203 pieces of space debris of more than 10cm.[36]

3.2.3 Geographical constraints

GNSS receivers require visibility of at least four satellites in order to acquire a position fix. This becomes more challenging in a non-flat location, e.g. urban environments, and can lead to failure to acquire an accurate location. In addition, urban environments can often generate misleading signals via inadvertent reflections also known as 'multipath'. Multipath arises when a signal bounces off a surface on its journey from satellite to receiver. As such, the signal will travel further than if the receiver had line-of-sight (LOS) to the satellite, and as each nanosecond is equivalent to a 30cm error, computations quickly lose accuracy as a result.

In addition to the problems with multipath, GNSS is generally accepted as an outdoor-only solution as the signal strength makes it unsuited for indoor usage.

3.2.4 Near-channel radio interference

The most important example of near-channel interference was the one that was avoided. In 2011, a satellite communications services company called *LightSquared* filed for access to radio-spectrum at the low end of the GNSS L1 band. The request was denied because technical analysis found a great risk of disruption of L1 and therefore degradation of the performance of all GPS receivers. In addition, in-band interference is a growing concern as the multitude of GNSS satellites broadcasting on the same frequency makes it increasingly difficult for receivers to reject noise and noisy multipath signals.

3.2.5 Mitigations

Environmental challenges are inherently difficult to mitigate against from a technical perspective. If a major *space weather* event occurs, it cannot be avoided. The International Space Environment Service (ISES) is a collaborative of space weather service-providers across all continents.[37] Advance warning could inform users of heightened risk of ionospheric scintillation, which would implore users to seek alternative PNT sources. GNSS devices that can use more than one frequency are generally more resilient to ionospheric disturbance as the different frequencies are affected in different ways. *Space debris* is not a major concern in MEO, but the implications of a collision means the risk should continue to be monitored to allow satellites to steer clear of any incoming piece of debris. Receivers capable of receiving signals from multiple constellations have demonstrated greater performance capabilities in *multipath* environments, as they are more likely to obtain a position fix using only LOS signals. However it should also be noted that poorer quality receivers will struggle to discern the target signal should there be too great a background noise from other GNSS on the same frequency.[38] In the case of *near-channel radio interference*, the best mitigation is to reduce the risk in the first place by ensuring that spectrum allocation (the remit of the International Telecommunications Union, ITU) is as considered as possible. Avoiding usage of the spectrum near GNSS for non-navigational purposes is the only way to avoid this risk materialising.

[36] European Space Agency, European Space Operations Centre (2018). *ESA's Annual Space Environment Report*. Available at: https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf [accessed 03/06/2018]

[37] International Space Environment Service, http://www.spaceweather.org/; members include: Australia, Austria, Belgium, Brazil, Canada, China, Czech Republic, India, Indonesia, Mexico, Poland, Russia, South Africa, South Korea, Sweden, UK, US, and ESA.

[38] GSA (2017). *GNSS Market Report Issue 5*

3.3 Human factors

3.3.1 Ground station anomalies

Human error is always a risk to any computerised system, and GNSS is no exception. In late January 2016, widespread disruption across telecoms and broadcasting was experienced across parts of Europe and the US. The root cause of the issue was isolated to an erroneous upload to a GPS satellite, with one UK telecoms operator reporting a resultant disruption over a four-day period.[39]

A similar event befell GLONASS on 1st April 2014, when all satellites in the constellation started issuing data on the position of the satellites (ephemerides) that were off by up to 200km in all three dimensions (meaning the satellites were not where the broadcast messages said they were).[40] The timing signal, however, was unaffected. GLONASS satellites were affected by the error for up to 11 hours.[41] The event provided a real-world experiment as to what happens if only one GNSS constellation provides inaccurate information. At the time, only Asia had meaningful coverage of at least one GNSS beyond GPS and GLONASS, and the incorporation of BeiDou meant that receivers in coverage were able to identify that GPS and BeiDou provided similar positions and GLONASS did not, so they could filter GLONASS out of the solution. In Europe, on the other hand, where only GPS and GLONASS were available, receivers were not able to select which constellation was correct and behaved in different ways as a result. Some oscillated between the two positions while others computed the average position between the two constellations. Neither of those solutions provided the user with relevant information.[42]

These two significant events remain the only system-level disruptions to a GNSS since it was opened to the mass market.

3.3.2 Internal inconsistencies

Leap seconds are periodically added to UTC to account for imperfections in the Earth's rotation but are not necessarily accounted for in GNSS timing systems. This could imply inconsistencies of time and lead to failures or errors in GNSS-reliant systems.

Additionally, some poorer quality receivers may need to 'reset' their date periodically, as GNSS data messages have a limited length, which eventually must reset from their maximum value to their minimum.[43] This can result in inconsistencies and follow-on consequences for receivers without adequate software coding. The next rollover for GPS is due on 6 April 2019, which could potentially affect many systems. However, as receiver manufacturers generally aim to increase the useful life of receivers, many have switched the week parameter from the factory, so the problem is not isolated to that week.

[39] Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (2016). *'GPS Receiver Impact from the UTC Offset (UTCO) Anomaly of 25-26 January 2016'* Available at http://www.gps.gov/systems/gps/performance/2016-UTC-offset-anomaly-impact.pdf

[40] GPS World (2014). *The System: GLONASS in April, What Went Wrong*. Available at: http://gpsworld.com/the-system-glonass-in-april-what-went-wrong/ [accessed 10/08/2018]

[41] Frank van Diggelen (2014). *How GLONASS Failed for 11 Hours and Multi-GNSS Survived.* Available at: https://web.stanford.edu/group/scpnt/pnt/PNT14/2014_Presentation_Files/7.van_Diggelen-GLONASS-multi_GNSS.pdf [accessed 10/08/2018]

[42] Frank van Diggelen (2014). *How GLONASS Failed for 11 Hours and Multi-GNSS Survived.* Available at: https://web.stanford.edu/group/scpnt/pnt/PNT14/2014_Presentation_Files/7.van_Diggelen-GLONASS-multi_GNSS.pdf [accessed 10/08/2018]

[43] Government Office for Science (2018). *Satellite-derived Time and Position: A Study of Critical Dependencies*

3.3.3 Selective availability

Although officially removed from GPS satellites, access to asymmetric GNSS information in times of conflict may still be a feasible option. It is also plausible (if unlikely) that a nation or entity may cease to maintain GNSS capability, for example in the event of extreme financial pressures. In fact, this threat materialised for GLONASS. The constellation achieved sufficient coverage at 25 satellites in 1995 but dropped to 16 only two years later. By 2001, there were 9 operational GLONASS satellites, rising back to full coverage at 26 in 2010. Since then, Russia has maintained global coverage of GLONASS. However, this example demonstrates that perpetual service of all currently active constellations cannot be assumed.

3.3.4 Cyber-attack

GNSS satellites are controlled from a few, highly secure, ground stations around the world. Nevertheless, if a malicious agent gained control of the ground station at time of active spacecraft control (e.g. upload of new satellite data), then the systems could be rendered useless.

Even the corruption of signal from one constellation could represent a problem for multi-constellation receivers, as studies have shown that not all GNSS receivers have the capability to detect an erroneous signal and filter it out of its data input.[44]

3.3.5 Anti-satellite missiles and space warfare

Several of the major space-faring nations have conducted anti-satellite missile tests previously, demonstrating the capability to eliminate or disable active spacecraft in orbit. Indeed, these capabilities are likely to be enhanced, possibly advancing to space warfare, in the near future.[45] It is likely that in the event of a major conflict, satellite capabilities would be one of the first strategic targets. There is also the unlikely event of an act of terrorism, which targets in-orbit spacecraft. Should another test or malicious action occur, it would also likely increase the probability of residual space debris effects (see 'Space debris' above), potentially causing a chain reaction.

3.3.6 Mitigations

It is very difficult to mitigate against human factors of vulnerability. The most effective, available, mitigation against *ground stations anomalies, selective availability, anti-satellite missiles,* and *cyber-attacks* is the use of multiple constellations and multiple frequencies in the receiver (MCMF) – because, whilst applicable to all constellations, each vulnerability is most likely to occur to only one constellation at the time. If a receiver can use at least three constellations in the position solution, it is possible to ensure that the affected constellation can be removed (at least three constellations are required to identify the odd-one-out). *Internal inconsistencies* can be alleviated by ensuring the firmware of the receiver is up-to-date, as manufacturers tend to identify the problems and issue patches ahead of time.

3.4 Summary of vulnerabilities

The vulnerabilities presented in the previous sections are summarised in the table below.

[44] Government Office for Science (2018). *Satellite-derived Time and Position: A Study of Critical Dependencies*

[45] O'Connor, T. (2018). *Russia and China are testing missiles that could blast U.S. satellites out of space.* Available at http://www.newsweek.com/russia-china-testing-missiles-could-blast-us-satellites-out-space-869044

Table 1 Summary of vulnerabilities, by type

Receiver	Environment	Human factors
Jamming	Space weather and ionosphere	Ground station anomalies
Spoofing	Space debris	Internal inconsistencies
Meaconing	Geographical constraints	Selective availability
	Near-channel radio interference	Cyber-attack
		Anti-satellite missiles

Source: London Economics

3.5 A backup system?

There is wide-spread discussion on the need for a backup to GNSS.[46] The reality is that due to the free availability of GPS and decades of R&D into the best utilisation of that technology, no single solution can be established as a backup to GNSS across all the applications it serves. However, various solutions exist to address specific vulnerabilities for specific user groups.[47]

3.5.1 Timing and synchronisation users

The use of GNSS for timing and synchronisation is generally the least well-known, but as it underpins many critical infrastructures of modern society, it is among the most important. Users of GNSS for timing and synchronisation need access to a timing source that is traceable to UTC in order to ensure synchronised networks use the same time reference. Many users also rely on GNSS for phase and frequency synchronisation.

Timing users can rely on an internal component of the GNSS-clock to keep time. This component is called an oscillator, which contains a crystal that oscillates with known frequency. The number of oscillations per second is known, so a count of oscillations can be converted to time elapsed. The quality of the oscillator, and the user requirements determine how long the application can continue to function in a GNSS-deprived situation. The price of oscillators ranges from less than DKK 1 to more than DKK 100,000. Free-running for five days, the cheapest oscillators drift by more than 100ms while the most sophisticated drift less than 0.001ms (1µs).[48]

Timing users are recommended to access precise time from three sources whose delivery mechanisms are vulnerable to mutually exclusive threats. GNSS will always remain one of those sources, but there is currently no consensus on the other two sources. Some candidate time sources and delivery mechanisms include:

- **eLoran**: The ‘enhanced Long-Range Navigation’ system is an evolution of the Loran-C system that was commissioned in the 1960s. Similar to GNSS satellites, eLoran stations transmit their location and precise time, and receivers can then compute local time based on the known propagation of the signal. Unlike GNSS, eLoran is a ground-based system that operates at a low frequency of 90-110 kHz, and unlike GNSS, the signal is considerably stronger, and transmission requires a 200m mast (which makes spoofing challenging). There is currently one eLoran transmitter in Western Europe, namely in Anthorn in the UK.

[46] E.g. Bloomberg Businessweek (2018). *The World Economy Runs on GPS. It needs a Backup Plan*. Available at: https://www.bloomberg.com/news/features/2018-07-25/the-world-economy-runs-on-gps-it-needs-a-backup-plan?utm_source=nextdraft&utm_medium=email [accessed 06/08/2018] and Munich Satellite Navigation Summit 2017 (2017). *Session 3. GNSS – Is It Time for Backup?*. Available at: https://www.munich-satellite-navigation-summit.org/program-2017-day-2 [accessed 06/08/2018]

[47] E.g. European Commission (2018). *European Radio Navigation Plan*

[48] For more details on drift, holdover and price of oscillators, please see Annex 2.

Until 2016, the North Sea was covered by stations in Norway, France, UK, Germany, and Denmark (Faroes). Similar systems to eLoran exist in many countries, including the US, Russia, Australia, South Korea, India, China, and Iran.[49] The Russian system, Chayka, covers all of mainland Denmark and could therefore be of particular interest.[50] Combined eLoran and GNSS receivers are available for timing on the commercial market.[51]

- **Satelles Time and Location (STL)**: A commercial satellite-based system that uses the Iridium constellation of communications satellites in LEO, and the spectrum that was previously allocated to pagers. While STL is technically a satellite-based PNT solution, it is vulnerable to different risks than GNSS. For example, the signal strength is 300-2,400 times that of GNSS, which makes the signal very difficult to jam or spoof. As the solution is a commercial offering that will involve subscription, the signal must be encrypted, and only customers will be able to decode the signal, which makes it nearly impossible to spoof. Unlike GNSS, STL payload does not include clocks, so the system depends on a signal from the ground that is then relayed to users via the satellites. Iridium satellites are in the very congested LEO, which contains more assets and more space debris than MEO (where GNSS satellites are), but LEO is better shielded from solar radiation due to the Earth's magnetic field. STL-enabled timing servers are available on the market. These also use GNSS, and are enabled for incorporation of eLoran.[52]
- **Longwave signals**: DCF77 from Frankfurt and MSF60 from Anthorn are both accessible in Denmark. The signals are provided by the German Physikalisch-Technische Bundesanstalt (PTB) and the National Physical Laboratory (NPL) in the UK and are therefore traceable to UTC at source. The delivery mechanism is susceptible to environmental disruption – especially at sunrise and sunset, so the accuracy at user level is not comparable with GNSS. It is, however, sufficient for many applications.
- **Cabled connections**: Some National Laboratories that provide certified timing offer access to UTC traceable time from their own laboratories. This information is transferred using copper or fibre-optic cables. The solution needs a reliable network, preferably straight from the source clock to the user, to ensure the accuracy can be maintained. If the network has too many nodes and too many potential routes, then accuracy and reliability is lost. Such services are, as yet, not available from a Danish operator and no Danish entity contributes to the calibration of UTC.[53] As a point of reference, the solution available from the UK National Physical Laboratory, which comes with a service-level agreement, and at considerable cost.

In addition to the timing sources above, a different way of accessing accurate time is through the traceable transport of time from a reliable clock. Many transport mechanisms exist, including:

- **Precision Time Protocol (PTPv2)**: Defined in IEEE standard 1588, version 2 from 2008, the protocol is normally used for time transport over Ethernet cables and can work on point-to-point networks, local area networks (LAN) and wide area networks (WAN). PTP is among the most precise transport protocols and is suitable for distribution of time within an organisation's network.

[49] Chuck Shuhe (2018). *Enhanced Loran Technology Overview, Strengths & Weaknesses, Implementation Status*. UrsaNav. Conference presentation at Securing Position, Navigation & Timing; Trinity House, London; 14/06/2018.

[50] International Research & Technical Centre of Advanced Navigation Technologies (2017). *Russia's Chayka (Loran) Coverage*. Available at: https://rntfnd.org/wp-content/uploads/Chayka-coverage-2017.jpg [Accessed 06/08/2018]

[51] E.g. http://www.ursanav.com/partners/chronos-technology-ltd/

[52] E.g. https://spectracom.com/sites/default/files/document-files/PRISMA-VelaSync-High-Speed-Time-Server_rev-F.pdf

[53] Bureau International des Poids et Mesures (2016). *BIPM Annual Report on Time Activities*. Available at: https://www.bipm.org/utils/en/pdf/time_ann_rep/Time_annual_report_2016.pdf

- **Network Time Protocol (NTP)**: The protocol is used to distribute time over a standard network and is widely used for easy and generally free access to time. In Denmark, the available NTP servers are run by private individuals on a hobby basis.[54]
- **White Rabbit**: Developed at the European Organization for Nuclear Research (CERN), White Rabbit is a very accurate time distribution service that can deliver sub-nanosecond performance over short distances.
- **Telephone delivery**: The speaking clock (Frk. Klokken) is an example of time delivered via telephone. The Danish speaking clock relies on GPS-time, so is not an alternative source in case of GNSS outage.[55]

3.5.2 Position and navigation users

Position and navigation applications are inherently different from timing and synchronisation because an alternative solution exists, which was used before GNSS. Such 'traditional methods' are available for most applications and include the use of paper maps with a compass for navigation, sextants for maritime positioning, and VOR, DME, or ILS[56] for aircraft approaches. The availability of traditional methods differs greatly by application as aviation has largely maintained its infrastructure, so aircraft can use these to navigate while the number of people who carry maps while on foot or in cars is expected to be low.

While these traditional methods should be considered in the resiliency plan of businesses, this section primarily focuses on technological solutions.

One cross-cutting mitigation against GNSS outage is the use of **other sensors**. The most important such sensors are accelerometers, gyrometers, magnetometers, odometers, and other sources of relevant information. If the receiver can sense whether it has moved in a certain direction or been stationary, that could be an important input in computation of a GNSS-deprived position. In addition to sensors within the receiver, the use of **Signals-of-Opportunity Positioning (SOP)** can improve the resilience of a position fix and help understand the position in a GNSS-deprived scenario. All radio signals can be used for SOP, but some are better suited than others, depending on whether a critical mass of usage has been achieved.

- **Wi-Fi**: The location of Wi-Fi hotspots is kept in a crowd-sourced database and held by mobile software companies such as Google Android and Apple. This information is not perfect as any one hotspot may be moved at any time. However, especially in cities where dozens or hundreds of hotspots can be visible at any time, the crowd-sourced database is updated with sufficient frequency that it remains useable.
- **Bluetooth**: Similar to Wi-Fi, but not as developed owing to smaller number of Bluetooth beacons.
- **Cellular**: In the days before GNSS was ubiquitous in mobile phones, the 'ping' from a cell tower was often used in court cases to determine a suspect's location.[57] The necessity of identification of the cell mast in use means that a coarse position can be obtained from the knowledge of the location of the mast.

[54] EURAMET (2011). *Countries' Legal Time Regulations and Practices*.

[55] Dansk Institut for Fundamental Metrologi m.fl. (2000). *Handlingsplan for det Metrologiske Hovedområde: Tid og Frekvens*.

[56] VHF Omnidirectional Range, Distance Measurement Equipment, and Instrument Landing Systems, respectively

[57] One such example is the well-known PFA case where Kurt Thorsen was sentenced to six years in prison in part because his mobile phone placed him in a certain location. https://ing.dk/artikel/indsigt-mobilregistrering-uden-kontrol-30419?amp

- **Broadcast signals**: Ultimately, the information required to compute a position from a sufficient number of signals is the location of the transmitter and the duration of the signal's journey. Using signals from analogue and digital radio and TV broadcasts, it is often possible to acquire a sufficient number of transmitters to derive a position.[58]

In addition to these options, users of GNSS for positioning and navigation can also use STL and potentially eLoran (if a sufficient number of transmitters becomes available). The General Lighthouse Authorities of the UK and Ireland conducted a test on the use of eLoran in a GNSS denied environment in 2014 when eLoran was fully operational.[59] The test showed that a vessel that entered a GNSS jammed zone (of the North Sea) would experience a large number of alerts from a wide range of electronics on the bridge and overload the mariner's decision-making capacity. With an eLoran-enhanced solution, the vessel would realise it was being jammed and maintain an acceptable location for the duration of the outage.

A final option remains for applications confined to a small area and requiring high levels of accuracy. Locata and Omnisense are two companies that sell pseudolites (pseudo-satellites), which can be used to construct a local positioning network at very high accuracy. The systems are not cheap and require a strong business case. Largely autonomous mines in Australia were among the first users of this type of technology alongside large warehouses with robotic operations.

[58] For more information on a military application of SOP, please see BAE Systems (no date). *Navigation via Signals of Opportunity (NAVSOP)*. Available at: https://www.baesystems.com/en-uk/product/navigation-via-signals-of-opportunity-navsop

[59] General Lighthouse Authorities of the United Kingdom and Ireland (2014). *Resilient PNT using eLoran during GNSS Denial*. Available at: http://onlinepubs.trb.org/onlinepubs/conferences/2014/MTS2014/Hargreaves.pdf [accessed 06/08/2018]

4 Denmark's reliance on satellite-based PNT

4.1 Timing and synchronisation

4.1.1 Denmark's definition of time and national infrastructure

Denmark defines 'time' in the Law on Determination of Time from 1893 (*Lov om Tidens Bestemmelse*[60]). This law defines time-of-day all over the country, except the Faroe Islands, by the mean solar time on the 15th Easterly longitude.

<u>Lov om Tidens Bestemmelse</u>

§ 1: For alle Dele af Landet med Undtagelse af Færøerne skal Tiden herefter bestemmes lige med Middelsoltiden for den 15de Længdegrad Øst for Greenwich.

LOV nr 83 af 29/03/1893, Retsinformationen, https://www.retsinformation.dk/eli/lta/1893/83

This definition of time, in combination with the unavailability of a Danish timescale means that, on the face of it, Denmark's users of precise time have two options: either they use GNSS as a primary and sole source of time; or they supplement the use of GNSS with verification from the longwave transmitter near Frankfurt that distributes the German UTC-reference time, UTC(PTB), maintained by the German metrology institute, Physikalisch-Technische Bundesanstalt.[61]

4.1.2 Users of satellite-based PNT for timing and synchronisation

Given the paucity of alternative sources of accurate timing and synchronisation information, GNSS is the provider of choice for a wide range of applications that rely on accurate time. A wide range of applications that use or could use GNSS exist across a vast set of sectors. The *Space Statistics* from 2018,[62] reports that 15% of the 15% of Danish companies that rely on *space services*, use them for timing and synchronisation. GNSS is the only widespread space-based technology for these purposes, so it reasonable to assume that 2% of Danish companies use GNSS for these purposes.

The table below summarises the applications that use GNSS specifically for timing and synchronisation purposes and allocates these by GNSS intensity (i.e. the degree to which GNSS is used in Denmark). Details on definitions and market size is available in GNSS Market Report 5.[63]

Table 2 High-level split of timing applications by GNSS intensity

Low	Medium	High
Small cells	SCADA for power transmission†	Banking and trading†
PMU in power transmission†		Cellular telephony
Stock exchanges*		Fixed-line telephony
		Secure telecommunications†
		Teleports

Note: Transactions in the Nordic stock markets clear in Stockholm, which is why the Danish stock exchanges have low GNSS intensity. The degree to which the Stockholm exchange relies on GNSS has not been investigated in this study. †: applications covered in case studies in Section 5. This table considers the use of GNSS rather than the implications of a loss. In other words, an application may have a high GNSS intensity without suffering damage from a loss of GNSS due to a suitable backup system.

Source: London Economics analysis and GNSS Market Report 5

[60] https://www.retsinformation.dk/eli/lta/1893/83

[61] Dansk Institut for Fundamental Metrologi (2000). *Handlingsplan for det Metrologiske Hovedområde: Tid og Frekvens*.

[62] Styrelsen for Forskning og Uddannelse (2018). *Rumstatistik – Rumområdets betydning for den danske økonomi i tal*. Available at: https://ufm.dk/publikationer/2018/filer/rumstatistik-2018_endelig.pdf

[63] European GNSS Agency (2017). *GNSS Market Report Issue 5*. Available at: https://www.gsa.europa.eu/2017-gnss-market-report

4.1.3 Availability of alternative timing and synchronisation sources

As alluded to in previous sections, Denmark's users of accurate timing and synchronisation have few options available to them when seeking a source. There are internet-based NTP-servers, but these are not operated by institutions that can guarantee or monitor the validity of the information. NTP-technology also offers limited accuracy, and many such services source time from GPS.

A potential alternative that is currently available is the Iridium STL service that sources time from the US Naval Observatory (the same source as GPS), but uses different satellites in different orbits using different signal strength to deliver time to users. The accuracy is provided by Spectracom, and as a commercial service, guaranteed through service-level agreements. Users of STL remain vulnerable to severe space weather events that could disable satellites in orbit, and the fact that both systems rely on the same ultimate reference clock is a weakness. However, the likelihood that the US Naval Observatory fails to deliver accurate time to both STL and GPS *at the same time as all other GNSS fail* is extremely low.

Cabled connections available in Denmark are not sufficient for the majority of applications currently relying on GNSS-time, and the longwave transmission from Frankfurt is also too inaccurate.[64] Denmark's neighbouring countries, Sweden and Germany, each have a UTC-synchronised timescale (in Borås and Braunschweig, respectively). As both timescales are reachable from Denmark over land (and bridge), they could provide precise time to Danish users if the necessary infrastructure was to be constructed.

4.2 Positioning and navigation

Use of GNSS for positioning and navigation purposes is much more widespread than the narrower and exclusively professional use of GNSS for timing.

Danish Agencies collect many pieces of data that help improve the understanding of the use of GNSS in the country. The *Space Statistics* from 2018,[65] for example reports on the use of space-based services in the economy, and although GNSS is not identified separately, the fact that of the 15% of Danish companies that use space services, 67% rely on them for logistics and distribution, and 12% for physical precision works suggest that GNSS is the most widely used space signal. Other purposes might integrate GNSS in the solution, but the link is less obvious.

A specific survey of Danish farmers finds that 19% of Danish farmers us GNSS with RTK augmentation. Importantly, however, it also shows that these are the largest holdings working 51% of farmland.[66]

Statistics Denmark keep a representative survey on the population's use of IT,[67] which has produced GNSS-relevant results. For example, in 2015 it found that 63% of the Danish population aged 16-64 used the GPS function in their mobile phone. Among the 20-39-year-olds this proportion was 84%.

[64] DFM (2018). *Input til analyse af konsekvenser for Danmark af et nedbrud i de satellitbaserede PNT-tjenester.* Unpublished bespoke input document to the present study.

[65] Styrelsen for Forskning og Uddannelse (2018). *Rumstatistik – Rumpmrådets betydning for den danske økonomi I tal*. Available at: https://ufm.dk/publikationer/2018/filer/rumstatistik-2018_endelig.pdf

[66] Danmarks Statistik (2018). *Avanceret Teknologi Indtager de Danske Marker*. Available at: https://dst.dk/da/Statistik/nyt/NytHtml?cid=30775 [accessed 30/10/2018]

[67] The data are available for download at: https://www.dst.dk/da/Statistik/emner/uddannelse-og-viden/informationssamfundet/it-anvendelse-i-befolkningen

In 2018, the survey found that 88% of the population have a smartphone in the home, around half have a dedicated GPS navigation device, and one-in-five own a GPS watch for fitness tracking.

GNSS, position and navigation are integral parts of Search and Rescue activities. Whether reported via the Cospas-Sarsat beacon system or VHF radio, accurate positioning is imperative for a successful rescue mission. Cospas-Sarsat is an international organisation that maintains the infrastructure for beacons on 406 MHz to be able to report distress. Three types of beacons exist, covering the aviation (Emergency Locator Transmitter – ELT), maritime (Emergency Position-Indicating RadioBeacon – EPIRB), and personal domains (Personal Locator Beacon – PLB), which can be used on land, sea and in the air. The majority of these beacons are GNSS-enabled, and the position derived from GNSS is sent to the relevant authorities alongside Cospas-Sarsat's primary means of location, Doppler. Galileo's Search and Rescue service is due for full operating capability in 2020 and will add a return-link function to the Cospas-Sarsat beacon system where a person in distress will receive a message that help is on the way.

The Danish Defence respond to approximately 350 marine Search and Rescue alarms every year,[68] and in 2016, two of those events were reported via Cospas-Sarsat.[69] Approximately 6,000 beacons are registered in Denmark. Using GNSS for positioning distress messages via Cospas-Sarsat and VHF ensures that the authorities know the destination for the responding vessels or helicopters.

Equally important is the use of GNSS for navigation purposes in responding to an emergency. While rescuers are professional mariners and pilots that are expected to be able to navigate without GNSS, the convenience and accuracy of the system means that it is the default method. This is especially true in adverse weather conditions, where fog, high seas (or darkness) make non-GNSS navigation methods more challenging.

In addition, the use of GNSS for specific applications is mandated by various international organisations. For example:

- On the road, where EU regulation requires all vehicle models type approved after 31st March 2018 to be fitted with the eCall system.[70] The system automatically makes an emergency call if the vehicle's airbags are triggered, and submits basic information about the car, including its location, to emergency services. The Smart Tachograph is another EU mandated application where heavy goods vehicles need to share their location periodically as of 2019. This is to enforce the rules on driving time.[71]
- At sea, the EU mandates the use of VMS in fishing vessels and the IMO mandates the use of GNSS for navigation and traffic management purposes, among others.[72]
- As of 2020, all aircraft in the US and Europe need to be equipped with a GNSS-enabled Automatic Dependent Surveillance Broadcast (ADS-B) transmitter, mandated by the European Commission.[73]

[68] Forsvaret (2018). *Eftersøgning og redning*. Available at: https://www2.forsvaret.dk/viden-om/indland/redningstjeneste/Pages/Redningstjenesten2.aspx [accessed 31/10/2018]

[69] Cospas-Sarsat (2018). *Report on system status and operations C/S R.007 No. 33: January – December 2016*.

[70] European Emergency Number Association (2018). *EU legislation on eCall enter into force 31 March.* Available at: http://www.eena.org/news/eu-legislation-on-ecall-enters-into-force-on-31-march#.W6uQeHtKiCg [accessed 26/09/2018]

[71] Joint Research Centre (2018). *Smart Tachograph*. Available at: https://dtc.jrc.ec.europa.eu/dtc_smart_tachograph.php [accessed 26/09/2018]

[72] International Maritime Organization (2002). *Regulation 19.2 of SOLAS Chapter V*

[73] European Commission (2011). *Commission Implementing Regulation (U) No 1207/2011*.

The table below summarises the applications that use GNSS for positioning and navigation purposes. More detailed information on definitions and market size is available in GNSS Market Report 5.[74]

Table 3 High-level split of position and navigation applications by GNSS intensity

Low	Medium	High	
Infrastructure monitoring (construction)	Consumer drones	Pilotage	Maritime navigation
Infrastructure monitoring (off-shore)	Aircraft under Visual Flight Rules navigation	Fisheries navigation†	Maritime Long-Range Identification
eCall†	Regional aircraft navigation	VMS†	Marine Engineering
Rail asset management	Search & Rescue (ELT)	Maritime traffic management	Hydrographic surveying
Passenger information	In-vehicle navigation†	Search & Rescue (EPIRB)	Oil & gas surveying
Digital camera geo-tagging	Smart Tachograph	Search & Rescue (AIS-MOB)	Cadastral surveying
Offender tracking	Child tracking	Search & Rescue (PLB)	On-the-spot checks†
Smart street lights	Health/medical tracking	Maritime Search and Rescue	Construction surveying
Golfing assistants	Lone worker tracking	RTK systems	Construction machine control
Portable computers	Smartphone emergency call†	Mapping	ADS-B
Tablets applications	Bridge monitoring†	Advanced driver assistance systems level 0-2	Commercial aircraft navigation
Agriculture asset monitoring	Dangerous goods tracking	Fleet management†	General & Business aircraft navigation
Insurance telematics	Forestry	Automated port operations	Commercial drones
Leisure maritime navigation	Meteorology†	Smartphone navigation	Personal tracking
		Tractor guidance†	Goods tracking
Train driver advisory system		Variable rate application†	Fitness trackers
		Automatic tractor steering†	

Note: †: applications covered in case studies in Section 5. This table considers the use of GNSS rather than the implications of a loss. In other words, an application may have a high GNSS intensity without suffering damage from a loss of GNSS due to a suitable backup system.

Source: London Economics analysis and GNSS Market Report 5

4.2.1 Availability of alternative positioning and navigation sources

Alternative positioning and navigation predominantly comprise the traditional methods used before GNSS became commonplace and replaced them. These methods remain available at the theoretical level, but a real concern exists in the navigation community over the ability of people to navigate.

In a 2017 experiment, researchers from University College London[75] investigated the brain activity of 24 volunteers tasked with navigating the streets of Soho in Central London with and without satellite navigation devices. The findings suggest that when people navigate manually, they the hippocampus and prefrontal cortex of their brain have high activity, which is interpreted as learning the route. When navigating by satellite navigation, these effects are much smaller, and suggest the test subjects did not actually learn the routes. These findings shed some light on the ability of people to go back to non-GNSS aided navigation if necessary.

In a separate academic study, researchers from University College London and University of East Anglia created a mobile app to test people's spatial navigation abilities.[76] More than half a million

[74] European GNSS Agency (2017). *GNSS Market Report Issue 5*. Available at: https://www.gsa.europa.eu/2017-gnss-market-report

[75] University College London (2017). *Satnav 'switch off' parts of the brain*. Available at: http://www.ucl.ac.uk/news/news-articles/0317/210317-satnav-brain-hippocampus [accessed 26/09/2018]

[76] Coutrot, A., Silva, R., Manley, E., de Cothi, W., Sami, S., Bohbot, V. D., Wiener, J.M., Hölscher, C., Dalton, R.C., Hornberger, M., Spiers, H.J. (2018). *Global Determinants of Navigation Ability*. Current Biology Volume 28, Issue 17, P2861-2866.E4, September 10, 2018

people in 57 countries participated, and the study found that people in the Nordic countries are among the best spatial navigators alongside North Americans, Australians and New Zealanders. The authors speculate that a national interest in the sport of orienteering is a contributing factor in the success of the Nordics, alongside strong socio-economic factors.

4.3 Comparison with other countries

As a modern economy, Denmark relies on technological solutions. The country's public sector is highly digitised and cash transactions are rare. These factors suggest that the country does rely on PNT to a greater-than-average extent among its usual comparators.

According to a 2011 survey of National Measurement Institutes conducted by the European Association of National Metrology Institutes (EURAMET),[77] Denmark is one of nine countries[78] in which (*de facto*) legal time is not disseminated using NTP servers.

That GNSS is the only available source of traceable time (at a high accuracy) means that it is likely Denmark is more dependent on GNSS than countries with a national timescale and time distribution infrastructure. The major question is whether Danish operators have implemented the GNSS-based solution in a robust way. If the oscillators in use are sufficiently sophisticated, then an outage of GNSS would not be a problem. The same holds if the applications that rely on GNSS have not replaced other methods because of concerns over its vulnerability. In this instance, efficiencies at normal conditions could have been realised at the expense increased vulnerability.

[77] The European Association of National Metrology Institutes (2011). *EURAMET Countries' Legal Time Regulations and Practices*.

[78] The other countries are: Iceland, Portugal, Slovakia, Hungary, Croatia, Bosnia and Herzegovina, Cyprus, and Bulgaria.

5 Case studies

5.1 Agriculture

5.1.1 Introduction and use of GNSS

The agriculture sector uses GNSS for both public and private operations, which are discussed below, in turn.

Public sector users of GNSS include the Danish Agricultural Agency that is responsible for the distribution of the EU Common Agricultural Policy (CAP) payments to Danish farm holdings. DKK 7bn are distributed to Danish farms every year, so it is important to ensure that the funds are allocated based on actual parameters and not just reports. Every year, 5% of applicants are subjected to on-the-spot checks where the information provided in the CAP application is verified on the ground. It is for this purpose that GNSS receivers augmented with RTK (Real-Time Kinematic) are used. RTK is an augmentation system that allows the user's receiver to correct ionospheric disturbances because there is a strong correlation of such disruption in the same geographic area. An RTK reference station measures the difference between its actual location and the location estimated by GNSS and broadcasts this information to users in the vicinity.

Figure 4 Surveying equipment

Source: Henryk Sadura/Shutterstock.com

GNSS eases the work of the inspectors because they are able to take precise measurements without the need to for a geodetic reference point.

The Danish Agricultural Agency's 100 inspectors perform approximately 3,000 physical on-the-spot checks per year concentrated between 1st June and 1st December.

The **private users** of GNSS are farmers using the solution (with RTK) for automatic steering purposes and for variable rate application of seeds, fertiliser, and pesticides. Statistics Denmark report that 19%, of Danish farmers working 51% of the farmland use GNSS solutions with RTK augmentation.[79] An earlier survey in 2013, showed that 7% of farmers used GNSS with RTK, while 18% used any GNSS at all,[80] suggesting the use of any GNSS in agriculture widespread.

Figure 5 Precision farming

Source: Sasa Prudkov/Shutterstock.com

The farming community might not be the most obvious candidate user of a high-precision, high-tech solution, but the benefits are tangible, and the farmers

[79] Danmarks Statistik (2018). *Avanceret Teknologi Indtager de Danske Marker*. Available at: https://dst.dk/da/Statistik/nyt/NytHtml?cid=30775 [accessed 30/10/2018]

[80] Styrelsen for Forskning og Uddannelse (2018). *Rumstatistik – Rumpmrådets betydning for den danske økonomi I tal*. Available at: https://ufm.dk/publikationer/2018/filer/rumstatistik-2018_endelig.pdf

are aware. A 2015 study by SEGES[81] referenced in the space statistic shows that farmers can save 2-4% on fuel and 4-9% on all inputs when using GNSS-based precision agriculture relative to a non-GNSS solution. In a sector with a small margin and a high number of bankruptcies,[82] any technological solution that can reduce cost and increase yield is keenly appreciated.

5.1.2 Case-specific vulnerabilities

The vast expanse of agricultural land and its general proximity to public roads means that agricultural GNSS users (be they public or private sector) are more likely than most to experience accidental jamming from 'personal privacy' devices in passing vehicles. However, the extent of such events is often short as these vehicles tend to pass by quickly. In the case of on-the-spot checks, the reaction to a disturbance to the signal is simply to take a second measurement, which should be sufficient to ensure any discrepancy between measured and actual data is removed. Farmers relying on precision agriculture use sophisticated devices that generally include other sensors such odometers, gyroscopes, and other Micro-Electro-Mechanical Systems (MEMS) that can be used for holdover over limited time.

GNSS-based verification is just one of the methods employed by the Danish Agricultural Agency to confirm compliance with the CAP applications of farmers, with the use of satellite and aircraft imagery forming an important secondary check. While GNSS is a key input and source of efficiency, the Agency is not fully dependent on the technology, and any farmer who misrepresents their land would need to be more sophisticated even than spoofing GNSS to get away with it.

The technological development in agriculture is fast, and the prospect of fully autonomous tractors is likely not too distant. Such vehicles would have greater reliance on GNSS as the alternative (human operation) might not be physically possible. Stakeholders in agriculture should bear the vulnerability of GNSS in mind when implementing autonomy.

5.1.3 Impact of a GNSS outage

Agriculture is a very seasonal sector, and as such, the impact of a GNSS outage greatly depends on the time of year at which it happens. A GNSS outage in January would practically impact neither public nor private sector users. If, on the other hand, the outage was to overlap with the application of fertiliser in May or the check of catch crops in September, then the private and public stakeholders, respectively, could be severely disrupted.

Whilst on-spot-checks are one of a few control tools available to the Agency, it remains an authoritative input in the verification of an application. As such, the lack of availability of GNSS for up to five days would effectively halt this procedure within the Agency. The lost time would have to be made up as GNSS signals resurfaced, but if the outage overlapped with the busiest time of year, it would be very difficult to squeeze in further checks as GNSS returned. A greater reliance on aircraft or satellite imagery might be necessary to cope with the backlog.

Farming is among the most difficult sectors to estimate the benefits of GNSS, and the loss associated with its outage. As farmers increasingly rely on precision agriculture solutions to steer the tractor and apply seeds, fertiliser, and pesticides more efficiently, it is highly likely that the ability of farmers

[81] Højholdt, M. (2015). *Reduktion af brændstofforbruget med RTK-GPS*. Available at: https://www.landbrugsinfo.dk/Maskiner-markteknik/Traktorer/Sider/reduktion-af-braendsstofforbruget-med-rtk-gps_pl_15_2194_2439.aspx [accessed 28/09/2018]

[82] Landbrugsavisen (23rd February 2017). *Kort: Her er der flest landbrugskonkurser*. Available at: https://landbrugsavisen.dk/kort-her-er-der-flest-landbrugskonkurser [accessed 21/09/2018]

to complete those tasks has degraded. In practice, this means that the loss of the efficiency benefits that are measured against the counterfactual farmer (i.e. best practice non-GNSS) is likely not the full effect. The reduced ability of farmers might translate into soil compaction beyond the predefined paths around the field, crushing of crops under the tractor, greater pass-to-pass overlap requiring more fuel and a blanket application of fertiliser or pesticides, reducing crop yield. According to Statistics Denmark, more than 5,000 Danish farms use RTK-GPS in the tractors and/or combine harvesters.[83]

Reduction in yield would not only affect the farmers through loss of sales, but the scarcity might increase the price of agricultural output. Such a price increase would benefit the farmer, but could be detrimental for the food processing industry, consumers, and exports.

In summary, **the impact of a five-day GNSS loss significantly depends on the timing of the event**, and the impact could range from nil to a week's overtime required in the Agency and loss of all efficiency gains (about 4-9% of the cost of inputs), yield reduction and further inputs required for farmers.

5.1.4 Mitigations

The accuracy requirements of the agriculture sector mean that no other wide-area positioning technology is currently available for users. Bespoke systems exist where a local network of pseudo-satellites (pseudolites) can be installed and provide coverage over a small area. However, the infrastructure cost and cost of implementation in the equipment has not seen adoption of such technologies aside from a few large mining companies. The option exists and might develop in the future.

Spoofing (although very unlikely) would be significantly more difficult to implement if the equipment were to use Galileo with OS-NMA as soon as that becomes available.

5.2 Emergency services

5.2.1 Introduction and use of GNSS

All emergency services rely on GNSS, but to varying extent. The primary applications of GNSS are fleet management and navigation, but ongoing developments in the emergency call domain mean that further reliance is envisaged in the near future.

Emergency response chain:

- Emergency call.
- Tasking of vehicles.
- Navigation to location.
- Solving of the emergency.
- Navigation to next location.

To understand the use of GNSS in emergency services, it is useful to consider the different stages of responding to an emergency, as listed on the right.

Emergency call

The emergency call is the first link in the chain. Following initial teething problems with emergency calls from mobile phones, the current procedure uses the location of the caller to ensure the most appropriate PSAP (Public Safety Answering Point) gets the call. The current method of allocation

[83] Danmarks Statistik (2018). *Satellit-Teknologi Vinder Frem hos Unge Landmænd.* Available at: https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=29269

relies on the cell tower in use, and therefore does not rely on GNSS. Calls from landlines are always allocated to the nearest PSAP using established methods.

A call from a landline is geo-located because a known location is attributed to each line and operators therefore know exactly where the caller is. For calls from mobiles, this same certainty is only available if the caller has had presence of mind (and pre-planning) to use the emergency app (the 112 app). Approximately 10% of emergency calls in Denmark are currently made through the 112 app.

Geo-located emergency calls bring significant benefits to the PSAP and by extension the emergency services and the people in distress. A study by the London Ambulance Service[84] found that calls from mobiles are, on average, 42 seconds longer than calls from landlines, and that the most important information ('Location and Chief Complaint') is relayed 27 second faster in calls from landline. While other factors are likely to affect the length of call (e.g. call quality, a caller from a mobile is less likely to know who the victim is, etc.), the fact that calls from landlines are geo-located means the location is a matter of confirmation rather than explanation. The value of time in emergency response is estimated for Sweden at €1,300 per minute,[85] so any efficiency makes a sizeable difference.

Denmark is due to implement Advanced Mobile Location (AML) by the end of 2018. AML is a system that enables the smartphone to send a text message with its location to the PSAP. The system is currently supported in Android phones from Gingerbread onwards (2016), and in iPhones implementing software updates from spring 2018. The solution is fully implemented in Iceland, Ireland, UK, Finland, Estonia, and Lithuania, and partially implemented in Belgium, Austria, and Slovenia.[86] As the system relies on the mobile phone's location, non-GNSS sources of location such as Wi-Fi and Bluetooth are used, especially in cities. However, the location of Wi-Fi access points is crowd-sourced based on the prevailing location of the phones that use the access points, and that is ultimately GNSS-based.

Figure 6 Ambulance

Source: chuyuss/Shutterstock.com

The pan-European eCall system for cars is still in its infancy, with regulation only applying to new car models after 1st April 2018. eCall is a system that makes an emergency call if the airbag is engaged, and which also allows the occupants of the cars to dial 112 in case of an emergency. The system sends basic information about the vehicle including speed, number of occupants, and location to the emergency services such that rescuers can react even if the occupant(s) is unable to speak.

Tasking of vehicle(s)

A crucial way in which GNSS is used for emergency services is for fleet management purposes. Relying on the Danish tetra-network (SINE), all emergency vehicles communicate their location and

[84] Included in European Emergency Number Association (EENA) (2014) 112 Caller Location & GNSS available at: http://ec.europa.eu/DocsRoom/documents/5372/attachments/1/translations/en/renditions/native [accessed 06/12/16]

[85] Jaldell, Henrik (2004) Cost-benefit analysis and life-saving operations, University of Karlstad. Based on data from the Swedish Rescue Services statistical unit.

[86] EENA (2018). *Annual Report 2017*. Available at: http://www.eena.org/download.asp?item_id=256

status to central dispatch in real-time, and the tasking of vehicles is optimised because the controller knows exactly which vehicle is in the vicinity and available.

Navigation to location

The emergency vehicles that have been tasked with the problem then navigate to the destination using a GNSS-enabled solution, thus freeing up the co-driver to familiarise and prepare themselves for the emergency, make notes for reports and help making the fast-paced blue-light transfer as safe as possible. Emergency vehicles use electronic maps that run off the civil telecommunication network.

Solving the emergency

This step depends on the nature of the emergency, and fire and health-related emergencies typically do not use GNSS to solve the emergency.

Police emergencies are different, and especially those cases that involve searches do use GNSS. Whether the search is for a suspect or an individual who has left a care home, the police force uses GNSS inputs in a GIS database to track their personnel and ensure that all parts of the search area have been covered.

In addition, all policemen carry two GNSS receivers, one that communicates on the civil telecoms network and one using the secure Tetra-network, SINE. An important function of these systems is the ability to sound an alarm that the policeman is in distress, the GNSS location allows colleagues to intervene as efficiently as possible in such events.

All police forces need to be able to run an operation using the equipment and infrastructure of a different force. It is therefore important that all systems are aligned and the location of all vehicles and staff is known. This includes all emergency services as many events require collaboration between services.

Navigation to next location

This step too uses GNSS to navigate to the hospital, next incident, patrol area, or back to base.

5.2.2 Case-specific vulnerabilities

The use case does not have any specific vulnerabilities, but the large area served means that it is possible that vehicles might suffer from jamming from ‘personal privacy devices’. The occasional news stories describing difficulties for emergency services entering certain parts of larger cities could also lead to concerns that GNSS jamming or spoofing might become a problem in those areas.

The SINE uses GNSS for synchronisation, and the integrity of the network in the face of a prolonged jamming or spoofing attack is therefore paramount to the services’ continued ability to function. The SINE has been confirmed to be robust to a five-day outage of GNSS.[87]

[87] The exact duration of attack that could be mitigated is not available due to security concerns.

5.2.3 Impact of a GNSS outage

The GNSS reliance of emergency calls is still limited, but when Denmark implements AML and the eCall system achieves greater penetration, then the efficiency of handling emergency calls will reduce in case of a GNSS outage. This consideration is important because it is tempting to harvest efficiency benefits of such systems and reduce the personnel accordingly. The impact of loss of GNSS is not confined to the foregone benefits of the efficiencies GNSS brings but can easily be compounded if the traditional methods can no longer be used.

For fleet management applications, this effect is even more pertinent. The Danish Emergency Management Agency and Police have confirmed that there is sufficient and recently trained staff available for manual management of the fleet. This could be expected to involve a large map and pins or other markers that could represent vehicles. The fact that SINE is robust to an outage is important as it ensures speech and data communication can continue to flow between vehicles and dispatch. However, a much greater volume of radio communication would be required to continue operations.

For navigation of vehicles absent GNSS, the most likely mitigation is to let the co-driver navigate the vehicle. This will allow the emergency services to continue to solve the issues they are required to do (albeit with increased travel time likely) but would mean the co-driver would no longer be able to complete the tasks they currently perform. As vehicle navigation relies on digital maps over the civil network, and only few vehicles carry paper maps, the robustness of the civil network should be investigated further.[88]

In summary, **loss of a five-day GNSS loss would have a negative impact on the emergency services**. The economic loss associated with a GNSS outage would stem from the extra personnel that would need to be drafted in quickly to ensure all systems could continue to function.

5.2.4 Mitigations

It is important to ensure that sufficient staff remains available to solve the problems using traditional means. This includes a task to ensure people remain able to navigate using a paper map, or a smartphone-based map that they would need to move manually.[89] Given the size of the areas served by police and ambulances in particular, the likelihood that it is possible to rely on the personnel's local knowledge is slim. Switching the navigation solution for vehicles to rely on local, downloaded maps, could alleviate risks associated with the loss of civil communications.

It is possible to use alternative systems for coarse navigation, but the accuracy on offer is currently not sufficient for the application. If Denmark were to build an eDLoran network (with partners), it would be possible to achieve 5m accuracy. Such performance would be sufficient with good map-matching technology but would require further investigation to ensure the receivers and antennas are fit for emergency vehicles.

[88] The impact of a GNSS outage on the civil telecommunication network is not in scope of the present study.

[89] The telecoms industry is a known user of GNSS for synchronisation purposes, so the network might be vulnerable to an outage of GNSS. If so, the use of smartphone-based maps would not be a viable option. The robustness of the telecoms industry in Denmark has not been studied as part of this report.

5.3 Electricity transmission

5.3.1 Introduction and use of GNSS

Electricity transmission might not be the most obvious application for satellite-based position, navigation, and timing. Indeed, the infrastructure is stationary (so its position is known), and rarely moves (so needs no navigation). It is the third service from GNSS satellites, the often-unreported timing service, that is crucial for electricity transmission networks in Denmark and around the globe.

GNSS is relevant in different applications of the electricity transmission domain and different countries have implemented different systems. For example, **SCADA**[90] systems used to control and detect systems need to timestamp the data to ensure the information is available in the right order.

Figure 7 Transmission lines

Source: Bochim Sang/Shutterstock.com

The current requirements for the SCADA system on the Danish transmission grid is in the order of 1 second, which is comfortably met by GNSS and DCF77. The system is used to identify inefficiencies, improve the utilisation of the network and provide inputs for political and regulatory decisions.

The next step from conventional SCADA systems is to adopt a system of data collection using Phasor Measurement Units – **PMUs**. PMUs rely on synchronised measurements from all measuring points to determine faults on the system and allow early intervention if the frequency deviates from the 50 Hz standard. The accuracy requirements for PMUs are in the order of 100-150 ns, and need to be consistent across vast areas, including Denmark's neighbouring countries. GNSS is the cheapest and best source for such information and is an integral part of the PMU roll-out in Europe and further afield. PMUs are not currently implemented operationally in Denmark, but the grid operator uses a number of PMUs for *ex post* evaluation of the performance of the network. The upgrade to PMU-based monitoring could allow more efficient use of the grid by allowing the operational buffer to be reduced substantially. Whilst not currently implemented operationally, the move towards PMU-based monitoring is underway, and likely to be implemented in the next decade. The stringent accuracy requirement on PMUs (100-150 ns) means that GNSS is the only current option. The implied reliance on one source (a single point of failure) has meant the operator is reluctant to embrace the technology for fear of causing an overreliance.

There are many ways to monitor the health of the network and avoid aggravating faults. One such method is the differential **fault detection** method, which compares measurements either end of a line to identify anomalies. There are different ways to implement this solution. One is to timestamp the observations to enable sequential comparison to help identify a fault's direction of travel. As the measurement is timestamped, this method can use a conventional communication system to relay information. In Denmark, however, the method is implemented using a transparent fibre optic network along the transmission network. This means that timestamping is not required for the functioning of the application. The implication is that **fault detection on the Danish transmission network is fully resilient to a loss of GNSS.**

[90] Supervisory control and data acquisition

5.3.2 Case-specific vulnerabilities

As a critical national infrastructure in all but formal domestic definition,[91] the electricity transmission network is a pillar of modern society in Denmark and therefore, one would imagine, a potential target for cybercrime. The disparate nature of the network (located throughout the country) makes it liable for accidental and deliberate jamming, and the Danish operator is aware of spoofing attacks on foreign networks.

The specification for the PMUs used on the Danish network places a requirement on the GNSS antenna which needs to be shielded from signals below 20 degrees. This measure removes the risk of accidental jamming from passing personal privacy devices. Integration of Galileo – specifically the OS-NMA when available – in future PMUs is recognised as an option to mitigate against spoofing attacks.

The lack of suitable, independent, and readily available timing sources means that GNSS will always be an integral part of the solution in energy transmission.

5.3.3 Impact of a GNSS outage

The cautious approach to electricity transmission (avoidance of a single point of failure) means that GNSS is not integral in any operational activities of the operator. The PMUs currently used for *ex post* evaluations of the network will not be able to maintain synchronisation for the five-day duration of the outage. In fact, the oscillators used would drift in a matter of hours rather than days.

In summary, the ability of the network to supply electricity would not be affected by the outage, and consequently, any impact is confined to the inability to evaluate the performance of the network retrospectively.

5.3.4 Mitigations

A key mitigation strategy is already implemented at the antenna-level for PMUs. The shielding from signals below 20 degrees means that accidental jamming from personal privacy devices is all but impossible. The strategy also protects against spoofing from the ground, but a potential risk still exists with respect to targeted jamming or spoofing with devices mounted on drones. Galileo OS-NMA can mitigate against spoofing, but jamming could still be a problem.

To allow the Danish grid operator to fully reap the benefits of more accurate monitoring through PMUs, an alternative source of synchronisation is required. This source would need to be referenceable to UTC to ensure the cross-border nature of the network is protected. Options include STL and eLoran as well as cabled connections (e.g. using the transparent fibre used in the existing SCADA system). A cabled connection would require a source clock that was independent of GNSS, and ideally calibrated to UTC by a measurement institute.

[91] Denmark does not define its critical national infrastructures formally, but the energy sector is considered a European Critical Infrastructure in Directive 2008/114/EC owing to its cross-border nature.

5.4 Financial transactions

5.4.1 Introduction and use of GNSS

The financial sector might not be an obvious candidate for use of GNSS. However, as an industry where time literally is money, and prices change so fast that financial institutions have always clustered near stock exchanges, the importance of accurate timestamps is ever-increasing.

Figure 8 Copenhagen Stock Exchange

Source: Mahlum via Wikimedia Commons

The European Commission's Markets In Financial Instruments Directive II (MIFID II)[92] came into force in January 2018. The Directive defines the requirements on timestamping of financial transactions depending on their nature. The most stringent requirements are placed on activity "using high frequency algorithmic trading techniques,"[93] which have a maximum allowable divergence from UTC of 100 microseconds. This level of precision is beyond that which can be expected from a terrestrial radio signal such as DCF77 from Frankfurt, so GNSS is one of very few applicable sources. Indeed, the Commission Delegated Regulation stipulates that users are allowed to source UTC traceable time from satellite systems provided they account for the discrepancy between the satellite system's reference time and UTC.[94]

Timestamping is required to ensure that the price that triggered a transaction is also the price at which the transaction settles. It is also important for audit purposes as accurate timestamps using the same reference source make it possible to create a chronological chain of events and establish causal links.

The Directive proposes sanctions for its violation in the order of at least €5m for legal persons and up to 10% of the entity's turnover in the previous year.

In addition to timestamping, financial institutions rely on precise time to synchronise IT systems and use GNSS sourced time at nodes that can then be distributed in a time sensitive network to edges further from the source.

Stock exchanges in the Nordic region are consolidated in the Nasdaq Nordic group, and several stakeholders have confirmed that financial transactions clear in Stockholm. The Danish stock exchange therefore is not a key user of GNSS. But the Swedish exchange almost certainly is.

The e-nettet is a Danish company charged with digitisation of the finance industry. It works behind the scenes to ensure transactions between Danish financial institutions run smoothly. The network is strongly reliant on synchronised time to be able operate and is aware of risks associated with overly relying on single points of failure. A stakeholder has confirmed the e-nettet is most likely resilient, but the organisation itself has not responded to invites of contribution to this study.

[92] European Commission (2014). *DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU*

[93] European Commission (2016). *ANNEX to the COMMISSION DELEGATED REGULATION supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the level of accuracy of business clocks*. Available at: http://ec.europa.eu/finance/securities/docs/isd/mifid/rts/160607-rts-25-annex_en.pdf

[94] European Commission (2016). *COMMISSION DELEGATED REGULATION (EU) …/... of 7.6.2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the level of accuracy of business clocks*

5.4.2 Case-specific vulnerabilities

The concentration of financial institutions and their datacentres in cities mean that there is a risk of terrestrial interference from an increasing number of sources and spectrum. There might be financial gains to be made from spoofing of signals which would make the financial sector more vulnerable than other sectors.

Key stakeholders in the public and private sector have not been accessible for this project, but suppliers of solutions have expressed concern over the general awareness of vulnerabilities and limitations of GNSS as a primary or sole source of time. It is recommended that the sector's equipment and infrastructure be registered to ensure or confirm that a coordinated jamming event cannot incapacitate the Danish financial sector – both in terms of trading and consumer-facing operations.

5.4.3 Impact of a GNSS outage

The impact of a GNSS outage is not possible to discuss based on the limited information that is available. However, there is a concerning perception that financial institutions have lagged behind on compliance with MIFID II requirements in terms of the quality of business clocks. If this perception is true, then Danish companies could be saddled with significant fines from the regulator in case of an event.

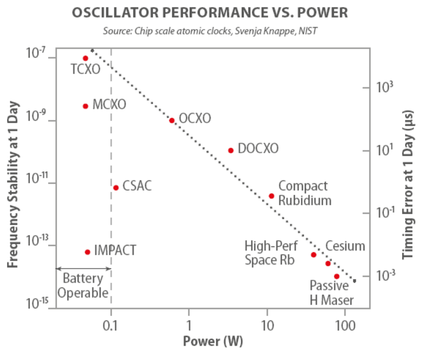
Additionally, a weakness in the financial industry's IT infrastructure in terms of synchronisation could make it impossible to perform transactions, which in an increasingly cashless society (in 2015 cash accounted for 20% of transaction value)[95] would be very inconvenient at least.

5.4.4 Mitigations

There are possible mitigations against the vulnerabilities of GNSS and the risks associated with its outage. The most obvious candidate is to ensure that the oscillator in the GNSS clock is of sufficient quality to ensure holdover for a sufficient amount of time. Figure 9 summarises the holdover capability and power consumption of a wide range of oscillators.

Additional mitigations include the use of alternative signals. In the longer term, this might include eLoran for Denmark, but in the shorter term, the most obvious candidate is STL.

Figure 9 Oscillator quality



Source: European GNSS Agency (2018). GNSS User Technology Report Issue 2

Internet-based timing services can also be used, but if they are, it is important to ensure that the ultimate source of time is not GNSS-dependent as such sources have been known to distribute GNSS time.

[95] Forbrugerrådet Tænk (2017). *Kort, kontanter eller mobil: Hvordan skal du betale?* Available at: https://taenk.dk/test-og-forbrugerliv/privatoekonomi-og-aftaler/kort-eller-kontanter-hvordan-skal-du-betale [accessed 19/10/18]

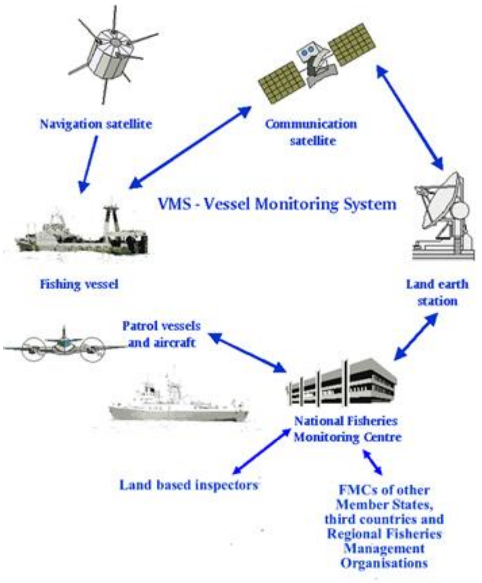
5.5 Fisheries

5.5.1 Introduction and use of GNSS

Similar to agriculture, the fisheries sector uses GNSS for both public and private purposes. **Public sector** users rely on GNSS to track vessels using the pan-European VMS (Vessel Monitoring System). The system mandates the use of a GNSS receiver and an (Inmarsat) satellite communication link on all vessels over 12m in length. The vessels need to report location, course, and speed every two hours.

The system is implemented to ensure that the provenance of the fish reported at auctions can be independently verified. It is also used to protect Natura2000 zones and other protected areas.

Figure 10 Vessel Monitoring System


Navigation satellite
Communication satellite
VMS - Vessel Monitoring System
Fishing vessel
Land earth station
Patrol vessels and aircraft
National Fisheries Monitoring Centre
Land based inspectors
FMCs of other Member States, third countries and Regional Fisheries Management Organisations

Source: European Commission

Given the connected nature of the VMS, it is possible for the national authority to effectuate a 'Real-Time Closure' of specific areas of the sea to enable environmental protection as soon as the information is available. This system is based on coordinates and has been made much easier by the use of GNSS.

Private sector users rely on the VMS to enable an electronic log that eases the reporting of operations when they reach the shore. The electronic log has replaced a paper log (which is still in use for vessels under 12m) and added efficiency because a lot of the information is logged automatically, and only the actual catch information needs to be inserted. The electronic log is submitted to the authorities electronically via satellite communication (Inmarsat).

However, the VMS-based electronic log is not the only GNSS-based tool used by fishermen. GNSS-enabled navigation equipment is commonplace, and the ability to navigate accurately to rich areas makes the work of fishermen easier and more efficient. By fitting multiple GNSS antennas on a vessel, it becomes possible to monitor the tilt, list, pitch, and roll of the vessel, and thus ensure that risks are identified before they materialise. The drag generated by a trawler is so strong that the vessel could capsize, and GNSS-based solutions can provide early warning of that.

Communication via satellites in GEO (Inmarsat) requires GNSS to function. This is because the satellite needs to focus its beams to the right location for communication to be possible. Satellite communication connects vessels to the shore and enables access to detailed and bespoke weather forecasts, as well as communication with the fishing company, and reporting of electronic logs.

5.5.2 Case-specific vulnerabilities

Sea fisheries are not likely to be affected by accidental jamming except in rare cases related to military manoeuvres or similar events. It is therefore unlikely that a wide-area disruption would occur. At the more local level, the fishermen might have incentive to jam or spoof their own VMS receivers to be able to 'go dark' and fish illegally in protected areas. However, other vessels in the vicinity would also be affected, and it is therefore likely that any violation could be identified and addressed. The mechanisms in place to trace the origin of a catch go beyond VMS, so a self-jamming fisherman would need to overcome many other obstacles.

5.5.3 Impact of a GNSS outage

GNSS outage would have significant impact on both public and private sector stakeholders in fisheries. The EU directive stipulates that the Fisheries Monitoring Centre (FMC) of each member state is to maintain surveillance of all vessels every four hours in case the VMS stops working. If the vessels fail to report in at that frequency, the FMC will contact the vessel to get a status report.

Electronic logs will cease to function, which means the vessels will be required to revert to paper logs. This imposes a time requirement on the fishermen and on the administration alike. In fact, a five-day outage of GNSS would imply creation of approximately 1,000 paper logs that would need to be digitised by the Agency.

The importance of GNSS for the purpose of fishing has not been the subject of detailed studies. However, an 'experiment' in South Korea tells the story. The North Korean regime has engaged in periodic jamming of GNSS over its Southern neighbour's waters. One such event in 2016 resulted in 70 out of 332 fishing vessels that had left port in the morning returning early as a result of this specific GPS failure.[96]

The loss of GNSS would imply inability to monitor fisheries in environmentally protected areas, and real-time closure of specific areas would no longer be possible. For this reason, environmental damage is likely to ensue as a result. The temptation for fishermen to knowingly fish illegally is considered unlikely to be acted upon. Illegal fishing is considered to be limited to accidental catches of protected species and no deliberate activity occurs. The fact that fish auctions need to confirm the provenance of the fish in terms of areas and vessels means that there are other checks in place beyond VMS. And the fishermen know the data are compared routinely.

The lack of availability of Inmarsat-based satellite telephony would make processes more cumbersome, but all of Danish waters are in VHF range, so the vessel would not be completely cut off from communication with the shore.[97]

In summary, **loss of GNSS would impose substantial additional clerical work** on the fishermen and the Agency, **might cause environmental damage to protected areas**, and would almost certainly **reduce the efficiency of catches**.

5.5.4 Mitigations

It worth considering mitigation at of the GNSS dependence separately for the different applications. Firstly, VMS and electronic logs are based on a pan-European system relying on global infrastructure. As such, including a potential Danish eLoran system would not necessarily be possible as there are no plans to construct a similar system in the Mediterranean. STL could offer positioning services of sorts, but at substantially degraded accuracy (20m-50m).

Secondly, the reliance on Inmarsat for satellite communications could be mitigated using LEO-based communication such as Iridium, but for VMS, this too would require European agreement.

Fishermen could use STL or eLoran (if it becomes available) to access much coarser positioning information that might allow them to continue operations in a GNSS-denied scenario.

[96] Reuters (01 April 2016), South Korea fishing boats turn back after North 'disrupts GPS'. Available at: http://af.reuters.com/article/worldNews/idAFKCN0WY3I5 [accessed 25/09/2018]

[97] Fisheries in the Faroes and Greenland are not in scope for this case study.

5.6 Meteorology

5.6.1 Introduction and use of GNSS

Meteorological forecasts are a crucial input into the functioning of many critical infrastructures in Denmark. The accuracy of weather forecasts depends on the quality of the inputs used in the process. The Danish Meteorological Institute (DMI) was founded in 1872 and is an institution under the Ministry of Energy, Utilities and Climate.[98]

The Meteorological community has adopted GNSS in recent decades to improve the accuracy and efficiency of measurements and data inputs. DMI is the lead institution for EUMETSAT's[99] Satellite Application Facility on **Radio Occultation Meteorology**. Radio Occultation is a method where GNSS signals are used to infer information on the climate and atmosphere. The propagation of GNSS signals varies with the amount of water vapour in the atmosphere, and Radio Occultation makes it possible to exploit this fact and compute a measure of water vapour and temperature using satellite-based instruments analysing the signals that travel through the various layers of the atmosphere from the opposite side of Earth. Radio Occultation is the most obvious way in which meteorological forecasts use GNSS, but there are many others.

Figure 11 Launch of a radiosonde

Source: Thomas Nedergaard, via DMI.dk

Radiosondes are another provider of meteorological inputs where GNSS has become a key component. Radiosondes are launched periodically from specific locations across Europe (approximately 300 km apart). Radiosondes are attached to Hydrogen-filled balloons and gather and report meteorological parameters such as temperature, humidity, wind drift and speed. GNSS is used to provide location and altitude. Previously, radiosondes carried barometers, but this payload has been saved by using GNSS.

Buoys and ships carry meteorological sensors to estimate a wide range of variables, including pressure and sea surface temperature. Neither buoys nor ships are stationary, so their location is very important for an appropriate integration of the information they gather. Both buoys and ships can use satellite communication to transmit the collected data. Inmarsat satellite communication relies on GNSS to ensure the correct satellite communicates with the terminal. Without GNSS, the data might never reach the meteorological office.

DMI's **lightning detection system** uses GNSS for synchronisation of the ground stations used for the system. The ground stations are designed to detect the intensity and direction of the electromagnetic wave released by the lightning. Adequate synchronisation of the ground stations allow graphical representation of lightning strikes as well as offering inputs into climate models and for use by insurance companies and emergency services.[100]

[98] DMI (2017). *Introduction to DMI*. Available at: http://www.dmi.dk/en/about/ [accessed 17/09/2018]

[99] European Organisation for the Exploitation of Meteorological Satellites

[100] DMI (2013). *DMI's lynpejlesystem*. Available at: http://www.dmi.dk/laer-om/temaer/vejr/lyn-og-torden/dmis-lynpejlesystem/ [accessed 17/09/2018]

5.6.2 Case-specific vulnerabilities

As demonstrated in the previous section the use of GNSS for meteorological purposes can be split between space-based measurements and meteorological sensors that require position and timing information. As such, the potential sources of outage differ from other applications.

Vulnerabilities arising at the **receiver** level (jamming, spoofing, meaconing) cannot be ruled out for the ground-based sensors that need to report position and require synchronisation, but meteorological infrastructure is more likely to suffer collateral damage than be a target. Radiosondes and radio occultation are not likely to be affected by these terrestrial vulnerabilities.

The meteorological applications of GNSS are as likely to be affected by **environmental** and **human** factors as other domains. However, if a powerful space weather event were to incapacitate, meteorological operators might be severely hit across all the space-based assets, and the GNSS outage would be the least of their worries.

5.6.3 Impact of a GNSS outage

As an integral part of the mechanism through which weather forecasts are derived, the loss of GNSS for a period of up to five days will influence the accuracy and reliability of the forecasts. However, if the outage is contained to five days, the effect will be limited. Buoys are relatively stable and the information that comes through (if the satcom link works) will remain accurate of an approximate area. The operational value of meteorological sensors on-board ships is likely to deteriorate quickly as the ship travels. Lightning will continue to be detected, but it will no longer be possible to map the lightning strikes at the same level of accuracy.

One major application that is not meteorological at its core, but absolutely vital for DMI is the communication between the Head Office in Copenhagen and the supercomputer in Iceland. It has been confirmed that communication between the two locations is independent of, and therefore resilient to an outage of, GNSS.

In summary, the **impact of a loss of GNSS in terms of meteorology is limited assuming the duration of the outage is not too long**. Radio occultation, which would stop working entirely, is not a core input in the weather models, and assuming a stickiness in location of buoys (and access to satcom) and availability of supplementary data from aircraft, the weather models would continue to operate at good accuracy.

The economic loss associated with a five-day outage of GNSS in the meteorological domain is found to be limited. A loss of accuracy on the weather forecast data would impact a wide range of users, especially in the energy sector, potentially leading to an economic loss.

5.6.4 Mitigations

The loss of radio occultation cannot be mitigated, but all other applications have some available options. Whether they can be implemented depends on costs and technological considerations such as the size and weight of solutions.

Radiosondes and lightning detection could incorporate alternative sources of location, altitude and synchronisation. Options include STL and eLoran, but the geometry and signal characteristics (specifically the required size of antenna) of STL means this solution appears the best suited if the accuracy is sufficient. A further benefit of STL is that it is currently operational and could be tested immediately.

Weather buoys and ship-based sensors could be upgraded with STL capability (eLoran is unlikely to ever extend as far into the ocean as required), but a major unknown is the satcom system used to relay the information. If the satcom system employed is also vulnerable to GNSS outage, then the best mitigating strategy is to consider a differing technology to add resilience there.

The overarching question is whether the risks of outage and the importance of the GNSS-derived information is sufficient to warrant an upgrade of the equipment and subscription to the commercial STL service.

5.7 Public sector IT

5.7.1 Introduction and use of GNSS

The Danish economy is highly digitised, ranking first in the EU for overall digitisation according to the European Commission's DESI index for 2017.[101] For public services, Denmark ranks 4th in the EU, meaning its public sector is geared towards the use of digital services.

Figure 12 Datacentre security

Source: Statens IT

It is conceivable that satellite-derived PNT plays two separate roles in the public sector's functions. IT systems all require accurately **synchronised time** to be able to operate. Timestamps on queries and edits make it possible to recreate a chain of events.

In many cases, IT networks are spread across multiple servers. As an example of this, the Danish Agency for Government IT Services currently serves 16 ministries and 19,000 users using its 5,000-6,000 servers in at least three locations. Synchronisation is an important requirement to be able to respond to a query that requires information from more than one of these servers. Synchronisation is also crucial to enable light maintenance certain servers without loss of service.

GNSS solutions are used by many IT services companies because they are relatively cheap and have the great advantage that all satellites in a constellation are calibrated to the same reference clock every 12 hours. In other words, every server in the same system, no matter where it is on Earth, can be synchronised to the same clock.

The Danish Agency for Government IT Services, however, have confirmed that they do not access time from GNSS, but instead rely on internet-based services. The identity and service level agreement are confidential.

However, investigation into the provider's source of time is recommended. Many internet-based timing servers are known to source time from GNSS and distributing using NTP-level accuracy.[102] If the Danish Agency for Government IT Services relies on such a service to achieve synchronisation then it would unknowingly be vulnerable to a loss of GNSS.

[101] European Commission (2017). *Digital Economy and Society Index 2017 – Denmark*. Available at: http://ec.europa.eu/newsroom/document.cfm?doc_id=43001 [accessed 19/10/2018]
[102] Government Office for Science (2018). *Satellite-derived Time and Position: A Study of Critical Dependencies*

Beyond IT synchronisation purposes, government systems could be imagined relying on geo-tagged information and data. Specific examples of such usage are quoted in the other sections in this chapter.

5.7.2 Case-specific vulnerabilities

As described above, the Agency for Government IT Services does not directly rely on GNSS but might do so indirectly. The following discussion therefore assumes that the chosen internet-based time service provider distributes GNSS time (if this turns out to be the case, the following discussions are therefore relevant).

Depending on the resilience of the time service provider, GNSS services could be lost as a result of a localised jamming incident. The distributed nature of the network and conceivable distance between the provider’s antenna and the Government servers would make it very difficult to protect against such an attack. If the service provider counts other critical services among its customers (e.g. finance), then attacks would be more likely as a perpetrator might gain financially.

5.7.3 Impact of a GNSS outage

Assuming the time service provider depends on GNSS, an outage would imply a loss of synchronisation between the network and the wider world (at least if the system is not resilient and has sufficient holdover capability). Synchronisation within the network might be acceptable if the same clock provides time to all locations.

If a loss of GNSS were to impact the network’s integrity, then it is most likely that Government IT services would cease functioning, which given Denmark’s high degree of digitisation in Government would impact its ability to operate.

The indirect reliance on GNSS would also make it difficult to identify and remedy a terrestrial source of an outage, as it would simply require additional steps to locate the problem.

The impact of loss of GNSS is seemingly nil, but it is important to ensure the clock that ultimately synchronises the whole network is not GNSS-dependent for that statement to hold.

5.7.4 Mitigations

Ensuring that no single source of time is relied upon is the foundation of a resilient network. It is generally recommended that three mutually independent sources be used and that these should have different vulnerabilities. A network-based source is encouraged as it propagates differently to radio-based sources. GNSS is one of those radio-based sources, and while it should never stand alone, its convenience and price point means it is often the primary source. The third source can be a different radio-based solution such as eLoran or STL, or if lower accuracy is required, DCF from Frankfurt.

5.8 Road transportation

5.8.1 Introduction and use of GNSS

Figure 13 Car navigation system

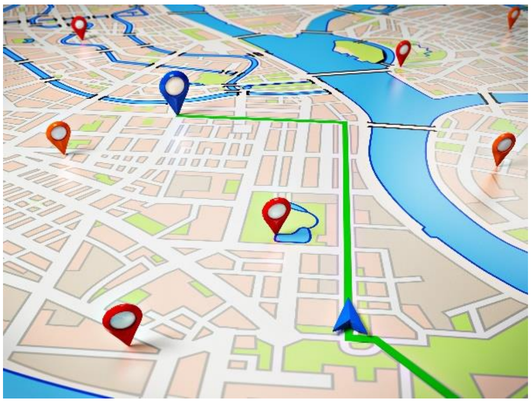
Source: Kaspars Grinvalds/Shutterstock.com

Road transportation was the original mass market user of GNSS as consumers saw the value of an electronic navigation assistant based on satellites. In the mid-2000s the price of satellite navigation devices for cars had reduced to a degree that consumers began to take note.[103] In many languages, 'a GPS' is unequivocally a portable navigation device for cars. Since then, in-built navigation systems have gained prominence and the availability of map applications for smartphones has meant that any driver who wants to use GNSS can do so.

According to Statistics Denmark[104] for 2018, 88% of the Danish population have a smartphone in the home and around half have a dedicated GPS navigation device.

In road transportation, GNSS is not just a consumer technology. Professional drivers in haulage and taxi companies depend on navigation equipment to find their way and reach the destination on time.

Figure 14 Fleet management system



Source: Vadim Georgiev/Shutterstock.com

An equally important application made available by GNSS is fleet management. The ability to track vehicles and know where they are and how they have been driven, enables targeted maintenance programmes and a more efficient use of the vehicle. It also allows headquarters to optimise the traffic and reduce the amount of time vehicles drive empty from one location to another.

Flextrafik is a public service offered at the regional level in Denmark to help people get to eligible appointments at hospitals, doctors, and similar. The service relies on private taxi companies that register their vehicles for Flextrafik's use as appropriate. Each driver is allocated journeys over the period of their availability, and the centralised planning system is able to adjust the plans over the course of the day to respond to changes in the traffic situation or similar.

The drivers receive the next destination in a bespoke satellite navigation device, but the system could function using addresses and conventional maps.

The most important role for GNSS is in the audit and post-processing of data. As the location of all vehicles is known at all times, complaints of late-shows or no-shows can be easily investigated and settled.

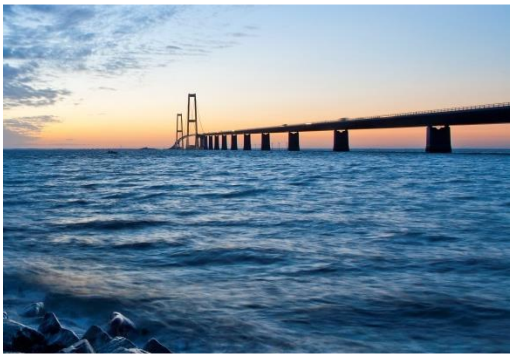
[103] Lendino, J. (2012) *Early GPS Systems, Portables, and Cell Phones*. Available at: https://uk.pcmag.com/consumer-electronics-reviews-ratings/64623/news/the-history-of-car-gps-navigation?p=2 [accessed 27/09/2018]

[104] The data are available for download at: https://www.dst.dk/da/Statistik/emner/uddannelse-og-viden/informationssamfundet/it-anvendelse-i-befolkningen

The data are also used in anonymised form to improve the knowledge of traffic flows. With 1,700 vehicles in use across Zealand, Flextrafik's data give a good indication of bottlenecks and open road. This is used to adjust the expected duration of journeys to improve safety and reduce driver stress.

Denmark's Great Belt Bridge connects the East and West of the country and carries more than 30,000 vehicles every day. The bridge uses GNSS for synchronisation purposes, in the IT system, for monitoring applications, and for the flashing aviation lamps at the top of the pylons. GNSS does not provide mission-critical inputs, and the systems are therefore not vulnerable to a loss of GNSS.

Figure 15 Great Belt Bridge



Source: Sund & Bælt

5.8.2 Case-specific vulnerabilities

Similar to other wide-ranging applications there is a risk of passing through the range of a personal privacy device, but there are no major additional risks.

5.8.3 Impact of a GNSS outage

The road transport network is strongly dependent on GNSS, and an outage would have significant impact on the flow of traffic. The effects would be more pronounced in dense traffic areas, where one driver slowing down or acting erratically as a result of more limited information is more likely to affect others.

The least affected stretches of road are likely the motorways, where drivers are able to familiarise themselves with the route and know which junction to exit. It is considered likely (although not verified) that the mobile communication network would remain available, so drivers could use smartphone-based map applications and move them manually instead of paper maps. Nevertheless, the efficiencies offered by GNSS would be lost, and further detriment would arise through increased congestion and the use of waypoint navigation (i.e. stopping, working out the next three landmarks, driving that part of the route, and then repeating until the destination is reached).

It is important to consider the full impact of drivers arising from a loss of GNSS. The transport network is such that travel times prolongs as congestion increases. Even if the majority of traffic is made up of drivers that know the way and do not need to use navigational aids, these drivers will be affected by a loss of efficiency in other drivers whose increased travel time and – potentially – more erratic driving behaviour will spill over to the rest of road users.

In the main, Flextrafik's clients are transported between their home and well-known, signposted destinations. Considering three legs of the journey: 1) to client's home, 2) to destination, 3) back to client's home, it is likely that the first leg would be longer as the driver would need to navigate using alternative means. The second step, in isolation, would not necessarily be much longer, but would be affected by the network effect described above. The third leg would most likely only be marginally longer as most clients would be able to direct the driver the last stretch.

What would be lost to Flextrafik is the post-drive audit. In a situation where more stress is expected on the road network, more complaints could be anticipated, so the loss of efficiency gains from GNSS is not the only detriment felt.

Stakeholders from the Great Belt Bridge have confirmed that a loss of GNSS would have no impact on the operational capabilities of the bridge.

In summary, **the road transportation sector would be significantly affected by a loss of GNSS**, and many of the economic agents that use it every day would suffer losses of time, likely fuel, and possible damages.

5.8.4 Mitigations

The most important mitigation against the impacts that a loss of GNSS might have in the road transport sector is to up the ability of drivers to navigate. Specifically, ensuring that the skills that already exist are not allowed to deteriorate. It would be possible to use alternative systems for coarse navigation, but the accuracy on offer is currently not sufficient for turn-by-turn navigation.

6 Conclusion

This study has analysed Denmark's dependence on GNSS through two measures. Firstly, applications of GNSS for Positioning and Navigation, and Timing have been grouped by the intensity of use in Denmark, and secondly, through case study analysis of 8 distinct areas of society. The case studies have evaluated the scenario of '*an instantaneous and complete loss of all GNSS services for a consecutive period of five days after which time all GNSS services are fully and instantaneously re-instated'*.

It emerged from this analysis that Denmark's existing infrastructure for **accurate time** is less developed than in many other countries, which implies that users that need very accurate time for their applications need GNSS to be an integral part of their solution. Whilst risks and vulnerabilities arising from receiver or environmental challenges can be mitigated with a good oscillator, more fundamental problems with GNSS is likely to result in severe problems across many sectors as there is no obvious 'plan B' to GNSS. A reference to UTC in the legal definition of time, along with a national time-scale disseminating legal time, could mitigate this risk and add an ultimate fall-back option of physical transfer of a synchronised clock from the laboratory to the user in need. Another alternative is to construct infrastructure that could provide traceable time from the Swedish or German UTC timescales to Danish territory.

Like most modern societies, the use of GNSS for **positioning and navigation** purposes is highly prevalent in Denmark, and as such, many efficiencies have been realised in both public and private sector operations. Recent academic research suggests that Danes are among the very best spatial navigators globally (second only to Finland), so the implication of loss might be less severe for the functioning of the road network than could be feared. However, the equipage of paper maps in vehicles is dwindling, with only a select few police vehicles even carrying the resource. Reliance on the civil telecommunication network for professional and private users has been identified, and the resilience of this resource needs to be appraised.

A detailed list explaining the relevant risks that might cause a GNSS disruption, organised by three broad categories (see Table 4), and with discussion of available and potential mitigations against the specific vulnerability has been provided.

Table 4 Summary of vulnerabilities, by type

Receiver	Environment	Human factors
Jamming	Space weather and ionosphere	Ground station anomalies
Spoofing	Space debris	Internal inconsistencies
Meaconing	Geographical constraints	Selective availability
	Near-channel radio interference	Cyber-attack
		Anti-satellite missiles

Source: London Economics

The case studies analysed in this report are equally liable to environmental risks and human factors, while receiver-level risks depend on the application itself, its environment of use and which other agents operate there. Applications with a safety or liability critical focus are more likely to be subjected to deliberate receiver-level vulnerabilities while applications covering a wide area are more likely to be hit by accidental interference.

Table 5 Summary of case study findings

Case study	Summary of findings	Critical assumption(s)
Agriculture	Private users of GNSS would be **significantly affected** and likely suffer economic and financial loss (depending on timing of the outage). Public sector users would **continue to operate but less efficiently**.	Timing of the event is critical. CAP monitoring has back-up systems that continue to work.
Emergency services	Emergency services would **continue to operate, but much less efficiently**. Additional staff would be needed quickly.	Civil telecommunication network continues to work and provide maps.
Electricity transmission	The transmission network would **continue to operate**, and fault detection would not be affected. Retrospective analysis of network performance would not be possible.	PMU-based monitoring is currently used for 'academic' purposes. If implemented operationally, efficiency would improve but GNSS become a single-point-of-failure
Financial transactions	Available information does not allow a statement to be made.	A unit in the regulator transposing the MIFID II ought to undertake investigation of compliance with the Directive's requirements on business clocks.
Fisheries	Loss of GNSS would impose **substantial additional clerical work for public and private sector, might cause environmental damage and would reduce efficiency**.	Alternative monitoring systems beyond VMS are strong enough to deter fishermen from illegal fishing.
Meteorology	**Limited impact** provided the outage is no longer than five days.	The functionality of the other satellites on which weather forecasting is based is independent of the event that removed GNSS. It remains possible to communicate with buoys even without GNSS.
Public sector IT	**Available information suggests no impact.**	This is true only if the internet-based timing source used in the public IT system is independent of GNSS, which should be verified.
Road transportation	**Significant impact expected** resulting in increase in travel time and reduced efficiency for professional and leisure road users.	There is no extraordinary effect from affected bridges or ferries.

Source: London Economics analysis based on stakeholder consultations. More details in section 5.

6.1 Recommendations

Limitations on scope and budget means that this study provides deep dives into the use and dependence of GNSS in only a small number of specific areas of the Danish economy. The report provides a qualitative assessment of how GNSS is used and likely implications of a loss but has not monetised this effect, as that is beyond the scope. Primarily, this is due to the interconnected nature of modern society, and it is only when a critical number of areas are considered that a meaningful estimate can be derived. To be able to appreciate the full impact of a GNSS outage, further research, including other areas of society, would be needed.

The partial picture emerging from the **finance sector** suggests that more information is needed to understand its vulnerability to a loss of GNSS. With GNSS the only identified source of traceable time at the required accuracy, it is recommended that the regulator adds 'properties of business clocks' to its reporting requirements to verify that the requirements specified in MIFID II are met. This recommendation is consistent with the wider Recommendation 1 of the UK Cabinet Office's review into critical dependencies in critical infrastructures.[105]

[105] Government Office for Science (2018). *Satellite-derived Time and Position: A Study of Critical Dependencies*

It is recommended that further aspects are considered, with specific emphasis placed on the **civil telecommunications network**. Although it is considered *likely* that civil telecommunications are robust, a number of case studies in this report rely on this assumption to hold in order to be able to report the limited impact that is found. The regulator should ensure that this is in fact the case and take remedial action if it is not.

The wider transport system also warrants further analysis:

- **Maritime transport** is required to use GNSS by IMO mandate, and shrinking navigable sea space due to oil rigs and wind turbines means that GNSS-based positioning, integrated with charts, is a critical input in modern maritime operations – especially in adverse weather conditions. The current and future situation in the shipping industry should be analysed.
- **In aviation**, a mandate is coming into force in 2020 that requires aircraft in Europe and North America to use ADS-B for positioning reports. This system can reduce the ground-based infrastructure currently employed to track aircraft and offer information where there previously was none (because there is no ground infrastructure). ADS-B is entirely dependent on GNSS, and the impact of ADS-B driven efficiency gains should be analysed.
- **The rail transport network** currently uses GNSS, with the Danish Train Operating Company (DSB) an early adopter of driver advisory systems that use GNSS (and many other inputs) to help the driver meet the requirements of the timetable while reducing wear and tear on the brakes and conserving as much energy as possible. Future developments in rail include the European Rail Traffic Management System that is expected to incorporate GNSS and thus save trackside signalling infrastructure when implemented.

Beyond these areas, **TV and radio broadcasting** relies on GNSS to synchronise transmissions, and it would be relevant to study the robustness of these solutions to a GNSS outage. Whilst broadcast TV and radio might be considered a luxury in the context of this report, it plays a crucial role in the event of a disaster. The Danish Emergency Management Agency are able to use sirens to warn individuals in the local area of emergencies such as major fires or toxic air. In these cases, broadcast TV and radio are a crucial source of information.

Another important recommendation relates to the **timeframe of the analysis**. Certain developments have been proposed and it is reasonable to assume that they would materialise in the future. Understanding the impact on GNSS vulnerability of solutions that bring efficiency gains is important to allow decision makers to weigh the gains against the potential losses.

Finally, this study has considered GNSS as one set of satellites and not clearly distinguished the relative importance of constellations. With Galileo scheduled to reach full operational capability in 2020, additional research into uptake of Galileo, i.e. the degree to which GPS-only risks are mitigated and the effect of Galileo’s differentiators such as the OS-NMA or Search and Rescue service would be relevant.

In a broader sense, it is recommended that further work be undertaken to: identify the need for a Danish timescale and distribution service of traceable time; and investigate commercial considerations on the suitability and value-for-money of a subscription (e.g. STL) to, or development (e.g. eLoran) of, an alternative radio-based timing service.

Beyond navigation technology, it is encouraged that existing navigation competencies in Denmark are maintained. Danes are second only to the Finns in capabilities of spatial navigation, and maintaining these skills are an important mitigation against the implications of a loss of GNSS from a navigational perspective.

The Danish space strategy seeks to generate efficiencies through the use of space. GNSS has proven to be a great bringer of efficiency – when it works. Ensuring that future initiatives to increase efficiency consider the vulnerability of the system is imperative.

6.2 Comparison with UK findings

In 2017 Innovate UK published a report on *The Economic Impact on the UK of a Disruption to GNSS,*[106] also completed by us (London Economics Space team).

Denmark and the UK differ geographically and culturally. A clear cultural difference exists in the attitude towards 'security'. In the UK, matters of security are part of the national conversation, while in Denmark such matters are not frequently discussed in the public domain. The findings from this report show that many critical infrastructure operators are aware of risks and have incorporated mitigations in their solutions – even if they do not tend to broadcast that fact.

The UK study covered the whole economy, whilst this report has focused on eight case studies. As such, the findings cannot be compared in their entirety. Some general conclusions can be drawn.

A cross-cutting difference between the UK and Denmark is scale. Denmark is a smaller country with half the population density of the UK (approximately one-twelfth of the population in one-sixth of the landmass). Local knowledge is therefore more prevalent in Denmark and there is less of a need to rely on technological solutions.

This is clearly exemplified in the **road transportation** network where the associated knock-on effects from increased congestion anticipated from a loss of GNSS are less severe in Denmark. Traffic in UK cities is significantly more congested than in Denmark. The disturbance to business-as-usual implied by a loss of GNSS will therefore not affect Denmark to the same extent, as there is more capacity to absorb any overflow. TomTom rank cities by congestion level and show that 21 UK cities are more congested than Copenhagen, the highest-ranked of the three Danish cities in the database.[107] The UK road transport network is therefore more vulnerable to an outage of GNSS because the infrastructure is running closer to capacity.

Danish stakeholders expressed less concern of a loss of GNSS in **emergency services**, and the implementation of fault detection processes on **electricity transmission** means that this case is also less vulnerable than its UK counterpart.

The **finance sector** in the UK appears more aware of GNSS vulnerabilities. The finding that the UK sector is resilient to a GNSS outage was not replicated for Denmark, and further work is encouraged to establish concrete facts.

Public sector IT was not considered in the UK study so cannot be compared. The finding that it is resilient should be investigated in a relevant forum as it hinges on unverified assumptions.

For **agriculture, fisheries**, and **meteorology**, the findings for UK and Denmark are analogous. For agriculture and fisheries this is expected as the cases are currently based on the same procedures and regulation from the EU.

[106] London Economics (2017). *The Economic Impact on the UK of a Disruption to GNSS*. Available at: https://londoneconomics.co.uk/blog/publication/economic-impact-uk-disruption-gnss/

[107] TomTom Traffic Index. Available at: https://www.tomtom.com/en_gb/trafficindex/list?citySize=ALL&continent=ALL [accessed 19/10/18]

Index of Tables, Figures and Boxes

Tables

Figures

Boxes

ANNEXES

Annex 1 Glossary

ADS-B	Automatic Dependent Surveillance Broadcast
AIS	Automatic Identification System
AIS-MOB	AIS Man Over Board
AML	Advanced Mobile Location
CAP	Common Agricultural Policy
CERN	European Organization for Nuclear Research
DESI	Digital Economy and Society Index
DME	Distance Measurement Equipment
DMI	Danish Meteorological Institute
eCall	Pan-European Emergency Call system
eDLoran	Differential eLoran
EENA	European Emergency Number Association
eLoran	Enhanced Long-Range Navigation
ELT	Emergency Locator Transmitter
EPIRB	Emergency Position Indicating Radio Beacon
ERTMS	European Rail Traffic Management System
ESA	European Space Agency
EU	European Union
EUMETSAT	European Organisation for the Exploitation of Meteorological Satellites
EURAMET	The European Association of National Metrology Institutes
FMC	Fisheries Monitoring Centre
GLONASS	GLObalnaya NAvigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
ILS	Instrument Landing Systems
IMO	International Maritime Organization
ION	Institute of Navigation
IRNSS	Indian Regional Navigation Satellite System
ISES	International Space Environment Service
ITU	International Telecommunications Union
LAN	Local area networks
LEO	Low-Earth Orbit
LOS	Line-of-sight
MCMF	Multi-Constellation, Multi-Frequency
MEMS	Micro-Electro-Mechanical Systems
MEO	Medium-Earth Orbit
MiFID II	Market in Financial Instruments Directive II
NATO	North Atlantic Treaty Organisation
NTP	Network time protocol
OS-NMA	Open Service Navigation Message Authentication
PLB	Personal Locator Beacon
PMU	Phasor Measurement Unit
PNT	Position, Navigation, and Timing
PPS	Precise Positioning Service
PRS	Public Regulated Service
PSAP	Public Safety Answering Point
PTB	Physikalisch-Technische Bundesanstalt
PTP	Precision Time Protocol
QZSS	Quasi-Zenith Satellite System
RTK	Real-Time Kinematic

SAS	Signal Authentication Service
SBAS	Satellite-Based Augmentation System
SCADA	Supervisory control and data acquisition
SINE	SIkkerhedsNEttet (Danish Tetra network)
SOLAS	Safety-Of-Life-At-Sea
SOP	Signals-of-Opportunity Positioning (SOP)
STL	Satelles Time and Location
Tetra	Terrestrial Trunked Radio
TTFF	Time To First Fix
UK	United Kingdom
US	United States
UTC	Universal Coordinated Time
VHF	Very High Frequency
VMS	Vessel Monitoring System
VOR	VHF Omnidirectional Range
WAN	Wide area networks

Annex 2 Oscillator quality, drift and price

Table 6 Oscillator holdover capacity

Oscillator	Cost	Accuracy (ms) free run three days	Accuracy (ms) free run five days	Required accuracy		
				Mobile billing systems < 1s (1000ms)	Financial transaction < 1ms	Mobile networks, Smart Grid, DVB, DAB, CFT† < 1µs (0.001ms)
TCXO	< DKK 1	38.88	108.00	✓✓	✗✗	✗✗
OCXO LQ	DKK 100s- DKK 1,000s	7.78	21.60	✓✓	✗✗	✗✗
OCXO SQ		1.94	5.40	✓✓	✗✗	✗✗
OCXO MQ		0.58	1.62	✓✓	✓✗	✗✗
OCXO HQ		0.19	0.54	✓✓	✓✓	✗✗
OCXO DHQ		0.039	0.108	✓✓	✓✓	✗✗
Rubidium	DKK 10,000+	0.008	0.022	✓✓	✓✓	✗✗
Rubidium XPRO	DKK 100,000+	0.000	0.000	✓✓	✓✓	✓✓

Notes: Calculations assume a constant ambient temperature (i.e. drifts due to fluctuations in temperature are not accounted for). †: Computer-automated financial trading. ✓✓: Holdover sufficient for five days; ✓✗: Holdover sufficient for three but not five days; ✗✗: Holdover insufficient for three days.

Source: London Economics (2017). The Economic Impact on the UK of a Disruption to GNSS. Available at: https://londoneconomics.co.uk/blog/publication/economic-impact-uk-disruption-gnss/.

Somerset House, New Wing, Strand,
London, WC2R 1LA, United Kingdom
info@londoneconomics.co.uk
londoneconomics.co.uk
@LondonEconomics
+44 (0)20 3701 7700