Metodstöd för analys av GNSS-beroenden

Delområde: Tid och frekvens

ÅSA DAVIDSSON, BENGT JOHANSSON, SARA NILSSON,
SOFIA BERGSTRÖM, MIKAEL ALEXANDERSSON

FOI-R--5838--SE
ISSN 1650-1942 December 2025

Åsa Davidsson, Bengt Johansson, Sara Nilsson,
Sofia Bergström, Mikael Alexandersson

Metodstöd för analys av GNSS-beroenden

Delområde: Tid och frekvens

Titel	Metodstöd för analys av GNSS-beroenden – Delområde: Tid och frekvens
Title	Method support for analysing GNSS dependencies – Subarea: Time and frequency
Rapportnr	FOI-R--5838--SE
Månad	December
Utgivningsår	2025
Antal sidor	32
ISSN	1650-1942
Uppdragsgivare	MSB
Forskningsområde	Civilt försvar och krisberedskap
FoT-område	Inget FoT-område
Projektnr	E13978
Godkänd av	Daniel Faria
Ansvarig avdelning	Försvarsanalys

Bild: Fotograf Mikael Alexandersson. Bild föreställande störsändare av mindre format

Sammanfattning

Den ökande digitaliseringen innebär utöver ett omfattande beroende av tekniska system ett beroende av satellittjänster för att de tekniska systemen ska fungera. Tid och frekvens via globala satellitnavigeringssystem (GNSS) är exempel på sådana satellittjänster. Det innebär att påverkan på GNSS kan medföra störningar hos tekniska system som i sin tur påverkar aktörer och deras uppdrag.

Denna rapport innehåller ett metodstöd till aktörer som ska göra sårbarhetsanalyser, bland annat de risk- och sårbarhetsanalyser (RSA) som statliga myndigheter, regioner och kommuner enligt lagstiftningen ska genomföra. Metodstödet är tänkt att underlätta arbetet med att identifiera hur aktörers verksamhet påverkas vid störning eller vilseledning av GNSS avseende tid och frekvens.

I rapporten presenteras en arbetsgång i sju steg för hur en analys av beroendet av GNSS kan genomföras. I rapporten ges också ett urval exempel på sådana beroenden.

De sju stegen är: i) bemanning av analysgrupp, ii) kartläggning av prioriterade åtaganden, iii) identifiering av kritiska beroenden av tekniska system, iv) identifiering av de tekniska systemens beroenden av tid och frekvens via GNSS, v) kartläggning av redundans i systemen, vi) undersökning av hur prioriterade åtaganden påverkas av störning eller vilseledning, vii) kunskapsöverföring internt och externt via RSA-rapporteringen.

Nyckelord: tekniska beroenden, GNSS, tid, frekvens, störning, vilseledning, metodstöd, risk- och sårbarhetsanalys

Summary

The increasing digitalisation of society entails not only extensive dependence on technical systems, but also a dependence on satellite services that allows for these technical systems to function. The time and frequency services provided by Global Navigation Satellite Systems (GNSS) are examples of such satellite services. This means that interference with GNSS can cause disruptions in technical systems, which in turn affect actors and their abilities to carry out tasks.

This report contains methodological support for actors conducting vulnerability analyses, including the risk and vulnerability analyses (RVAs) that government agencies, regions, and municipalities are required to carry out under current legislation. The method support is intended to aid in identifying how an actor's operations may be affected when GNSS time and frequency services are jammed or spoofed.

The report outlines a seven-step workflow for analysing GNSS dependences. It also includes examples of relevant dependencies.

The seven steps are: i) staffing the analysis group, ii) mapping prioritised commitments, iii) identifying critical dependencies on technical systems, iv) identifying the technical systems' dependencies on time and frequency via GNSS, v) mapping system redundancies, vi) examining how prioritised commitments are affected by jamming or spoofing, vii) ensuring internal and external knowledge transfer through RVA reporting.

Keywords: technical dependencies, GNSS, time, frequency, jamming, spoofing, methodological support, risk and vulnerability analysis

Innehållsförteckning

1 Inledning

Samhällets ökade digitalisering har inneburit att många samhällsviktiga tjänster idag helt eller delvis är beroende av digitala system inklusive globala satellitnavigeringssystem (GNSS) [1]. Användningen av dessa system ger många fördelar men beroendet av dem skapar även sårbarheter[1] hos de verksamheter som ska upprätthållas i kris och, i värsta fall, under krig. Det inledande kapitlet redogör för problematiken med tekniska beroenden av GNSS och hur denna rapport syftar till att bemöta denna problematik.

1.1 Problembeskrivning

GNSS används i dag i ett stort antal applikationer. Välkänt är dess roll i olika former av navigationssystem såväl till lands, sjöss och i luften. Mindre känt är förmodligen GNSS roll i att säkerställa korrekt tid och frekvens i olika tekniska system som är beroende av detta.

En del av problematiken med beroende av satellittjänster är att det inte alltid är uppenbart för slutanvändaren att satellittjänster används för att säkerställa en samhällsfunktion. Eftersom det finns okända beroenden av satellittjänster försvåras identifieringen av sårbarheter i kritisk infrastruktur och i viktiga samhällsfunktioner. För att veta om sårbarheterna är acceptabla i fred, kris eller krig kräver det att sårbarheterna är kända [2]. Genom att identifiera de tekniska system som är beroende av GNSS kan förståelsen öka för hur verksamhetens prioriterade åtaganden påverkas om dessa system drabbas av störning eller bortfall av GNSS. Identifierade sårbarheter kan sedan arbetas in i verksamhetens risk- och sårbarhetsanalys (RSA).

Exempel på beroenden som finns dagligen men som man kanske inte reflekterar över är att tidsangivelse via GNSS kan användas för att jämföra övervakningskameror i utredningar. Exempelvis saknades korrekt tid i övervakningskamerorna vid mordet på Anna Lindh 2003. De 21 kameror som användes för att utreda mordet hade alla olika tidsangivelser med felaktigheter mellan 30 minuter och 3 dygn, vilket försvårade utredningen när förövarens rörelser skulle kartläggas [3]. Ett annat exempel återfinns inom hälso- och sjukvården där frekvens (och tid) används inom avancerad medicinsk utrustning för att blanda olika substanser. När korrekt mängd av ett ämne ska tillföras utgår man från den tid det tar att fylla på det i stället för att väga ämnet. Mer välkänt är kanske att en stabil frekvens behövs för att elnätet ska fungera [1].

Påverkan på GNSS är ett hot som är reellt och tyvärr vanligt förekommande i dagens konfliktzoner. Det har också blivit allt vanligare i Sverige och Sveriges närområde. Påverkan består såväl av att GNSS-signaler överröstas, vilket kallas för störning, som att en egengenererad GNSS-signal skickas ut för att lura en GNSS-mottagare, vilket benämns vilseledning [4]. Enligt den svenska nationella säkerhetsstrategin kan IT-relaterade incidenter orsaka störningar i samhällsviktig verksamhet[2] och i förlängningen därmed påverka den nationella säkerheten [5]. Incidenter kan orsakas av olyckor och systemfel [5], men även antagonistiska hot mot Sverige har i allt högre grad blivit en realitet [4].

Försvars- och säkerhetsstrategin för rymden [6] lyfter bland annat att Sverige ska öka sin motståndskraft för att säkerställa tillgång till robusta rymdtjänster. Ett sätt att öka motståndskraften är att Sverige ska verka för *att aktörerna inom beredskapssektorerna bygger upp kunskap om beroendet av rymdtjänster och genomför sammanfattande risk- och sårbarhetsanalyser inom respektive sektor* [6]. Ett av målen med det civila försvaret är att grundläggande samhällsfunktioner ska kunna bibehållas i krig. För att uppnå det måste en bred förståelse för beroende av rymdtjänster finnas. Denna typ av beroenden finns inom samtliga tolv beredskapssektorer [6].

Risk- och sårbarhetsanalyser är ett viktigt verktyg i arbetet med att minska risker och sårbarheter i den egna verksamheten. Det är även ett verktyg för att skapa en överblick över de samlade

[1] Sårbarhet definieras i MSBFS 2024:5 ”egenskaper eller bristande förmåga som innebär förhöjd sannolikhet för en oönskad händelse eller mottaglighet för negativa konsekvenser av en händelse.”

[2] Samhällsviktig verksamhet definieras i MSBFS 2024:5 ”verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer viktiga samhällsfunktioner.”

riskerna och sårbarheterna på olika nivåer i samhället. Slutligen utgör RSA ett beslutsunderlag för åtgärder. Såväl processen att ta fram RSA som själva produkten kan på så sätt bidra till ökad säkerhet i samhället. Statliga myndigheter likväl som kommuner och regioner är ålagda att regelbundet göra risk- och sårbarhetsanalyser för det egna ansvarsområdet. Vikten av att beakta GNSS och sårbarheter kopplat till sådana beroenden inom ramen för dessa analyser har blivit större i takt med ökande teknikberoenden.

1.2 Uppdrag, syfte och målgrupp

Under 2025 fick FOI i uppdrag av Myndigheten för Samhällsskydd och Beredskap (MSB)[3] att utveckla en första version till ett metodstöd som kan stötta vid arbetet med att identifiera hur verksamheter påverkas vid störning eller vilseledning av GNSS avseende tid och frekvens. Denna rapport beskriver resultatet av detta arbete, vilket utarbetats med stöd av befintlig litteratur och expertis inom FOI rörande GNSS och metodutveckling. Metodstödet har utformats för att passa in i nuvarande RSA-arbete. Därför har avstämningar under arbetets gång skett med MSB. Metodstödet är tänkt att på sikt kunna användas i aktörers arbete med verksamhetsnära risk- och sårbarhetsanalyser, vilka idag saknar GNSS-perspektivet.

Syftet är, med andra ord, att bidra med metodstöd för aktörer som behöver identifiera hur deras samhällsviktiga verksamhet och prioriterade åtaganden påverkas vid en störning eller vilseledning av GNSS avseende tid och frekvens. Stödet ska underlätta att i verksamheter identifiera de tekniska system som är beroende av GNSS och öka förståelsen för hur GNSS-påverkningar kan inverka på dessa system.

Det föreslagna metodstödet riktar sig främst till de statliga myndigheter som enligt 7§ i Förordning (2022:524) om statliga myndigheters beredskap ska göra risk- och sårbarhetsanalyser men kan användas även av kommuner och regioner som ska göra motsvarande enligt lagen (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap. Även andra aktörer kan ha nytta av materialet i sin kontinuitetsplanering.

I och med den breda målgruppen och mängden tekniska system som omfattas, kan inte metodstödet inriktas på en specifik verksamhets tekniska beroenden utan är istället av generell karaktär för att passa en bred målgrupp. Stödet är utformat för att vara kunskapshöjande.

1.3 Rapportens inriktning och avgränsning

Det presenterade metodstödet fokuserar på de tekniska beroenden av GNSS som rör tid och frekvens. Metodstödet är konstruerat för att underlätta identifiering av beroenden och att analysera vilka konsekvenser störning och vilseledning av GNSS skulle få för aktörernas prioriterade åtaganden. Metodstödet inkluderar inte tekniska beroenden kopplade till positionering via GNSS.

Metodstödet består av en systematisk arbetsgång med illustrativa exempel på hur olika tekniska systems funktion beror av tid och frekvensangivelser från GNSS. Exemplen är inte heltäckande och speglar inte alla möjliga beroenden av GNSS i samhället. Däremot kan exemplen hjälpa användaren att skapa en övergripande förståelse för var och för vilka ändamål sådana system kan förekomma. För att öka bakgrundsförståelsen för hur GNSS-påverkan kan se ut och vilka konsekvenser den kan få presenteras även ett scenario som speglar ett möjligt händelseförlopp.

Att bedöma allvarlighetsgraden av GNSS-påverkan och vilka möjliga åtgärder för att minska verksamhetens sårbarheter som finns är viktiga delar av olika aktörers arbete med att bygga robusthet och resiliens. Varken allvarlighetsgrad eller möjliga åtgärder inkluderas dock i detta metodstöd. Metodstödet har inte testats hos aktörerna vilket kan motivera fortsatt bearbetning och utveckling av metodstödet när användbarheten för aktörerna har testats.

[3] Myndigheten byter namn till Myndigheten för civilt försvar den 1 januari 2026.

Metodstödet är tillämpbart för både fredstida krissituationer och höjd beredskap. Urvalet av exempel som presenteras har gjorts på ett sådant sätt att de ska vara möjliga att publicera i en öppen rapport.

1.4 Rapportens disposition

Rapporten och dess metodstöd är upplagd enligt följande. I kapitel 2 ges en övergripande beskrivning av GNSS och dess användningsområden och hur en inverkan på olika aktörers tekniska system kan påverka samhällsviktiga verksamheter. Exempel på hur GNSS används i några olika beredskapssektorer presenteras liksom ett antal aktuella exempel hur påverkan på GNSS har gett effekter på samhällsviktig verksamhet. Slutligen presenteras i kapitlet ett scenario som illustration av en händelse där GNSS påverkas och som kan fungera som en bakgrund för användarna av metodstödet.

Kapitel 3 beskriver mycket kortfattat den roll som risk- och sårbarhetsanalyser har i det svenska beredskapssystemet. I kapitlet presenteras också en konceptuell modell som illustrerar hur det föreslagna metodstödet kan förstås i relation till dagens system för risk- och sårbarhetsanalyser.

Kapitel 4 presenterar en systematisk arbetsgång för hur GNSS kan tas in i arbetet med risk- och sårbarhetsanalyser. Kapitlet beskriver de olika processteg som ingår, vilka frågeställningar som bör behandlas i respektive steg och ett antal exempel som underlättar förståelsen för de olika processtegen.

Slutligen avslutas rapporten i kapitel 5 med en utblick mot möjligt framtida utvecklingsarbete inom området.

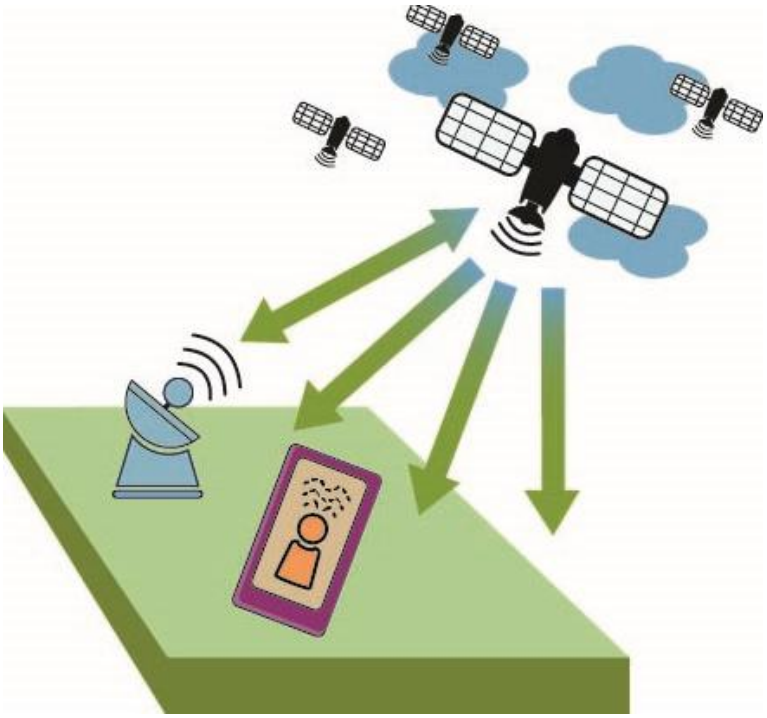
2 GNSS – funktion, användning och sårbarheter

För att kunna genomföra metodstödets systematiska arbetsgång och besvara dess frågor behövs en grundförståelse för vad GNSS är och hur det används. Detta kapitel ger därför en bakgrundsbeskrivning av vad GNSS är samt hur systemet levererar tid och frekvens. Kapitlet beskriver även hur störning och vilseledning kan påverka leveransen av tid och frekvens via GNSS. Det ges även exempel på var i samhället GNSS-tid och frekvens kan användas och exempel från verkliga händelser där GNSS har störts eller vilseletts. Slutligen presenteras ett scenario.

2.1 GNSS

GNSS står för *Global Navigation Satellite Systems* och är ett samlingsbegrepp för satellitnavigeringssystem som är globala. Idag finns fyra system som räknas som GNSS: amerikanska GPS, ryska GLONASS, europeiska Galileo och kinesiska BeiDou. Systemen drivs oberoende av varandra och sänder både öppna och krypterade signaler på flera radiofrekvenser. Krypterade signaler är främst för militär användning medan de öppna signalerna kan användas av vem som helst. En mer utförlig introduktion till GNSS finns i FOI-rapporten *Globala satellitnavigeringssystem: En översikt över öppna signaler och tjänster* [7].

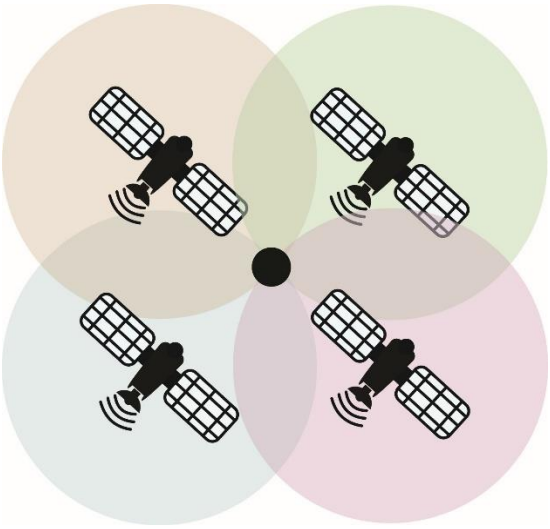
Alla GNSS är uppbyggda på liknande sätt och kan delas in i tre segment: rymdsegment, marksegment och användarsegment. Rymdsegmentet består av satelliter i olika omloppsbanor runt jorden som sänder ut navigationsdata. Satelliterna sänder signaler på specifika radiofrekvenser, vilket kan liknas med att radiostationer har sin egen frekvens som de sänder på. Marksegmentet, eller kontrollsegmentet som det också kallas, kontrollerar rymdsegmentet och ser till att satelliterna sänder ut data med korrekt information om bland annat satellitens placering. Användarsegmentet består av alla GNSS-mottagare som finns på jorden. Eftersom GNSS-mottagare bara lyssnar efter GNSS-signaler och gör positionsberäkningen lokalt går det att ha ett obegränsat antal mottagare samtidigt. Satelliterna kan inte heller veta hur många eller vilka som använder signalerna [7]. Figur 1 är en enkel illustration av hur de olika segmenten relaterar till varandra.



Figur 1. Rymdsegmentet skickar signaler till användarsegmentet där varje användares GNSS-mottagare kan beräkna sin position, hastighet och tid. Marksegmentet ser till att rymdsegmentet fungerar.

Trenden idag går mot att allt fler mottagare använder signaler från flera system och även använder signaler på fler radiofrekvenser. En modern mobiltelefon använder signaler från alla fyra GNSS. GPS, det amerikanska systemet, är äldst och är för många i dagligt tal synonymt med GNSS eller handhållna navigationssystem. Det är också det system som fortfarande är mest använt i världen [8].

En GNSS-mottagare tar emot signaler från satelliterna och kan med hjälp av dem beräkna position, hastighet och tid. Mottagaren kan vara allt från ett chip i en mobiltelefon till en mer dedikerad mottagare framtagen för att beräkna positioner med millimeternoggrannhet. För att en mottagare ska kunna beräkna position, hastighet och tid krävs det att den tar emot signaler från minst fyra satelliter, där tre satelliter tillsammans ger en skärningspunkt motsvarande mottagarens position och den fjärde satelliten används för att estimera GNSS-mottagarnas klockfel. Figur 2 visar en mottagare som har beräknat sin position med fyra satelliter [7]. Om en mottagare hade haft en perfekt synkroniserad klocka hade endast tre satelliter behövts för att beräkna dess positionen.



Figur 2. Positionsbestämning med hjälp av fyra satelliter.

2.2 Tid och frekvens

Många förknippar GNSS endast med position men en viktig del, både i beräknandet av positionslösningen och som fristående tjänst, är distribution av noggranna tid och frekvensangivelser. Alla satelliter har atomur som håller tiden och som regelbundet synkroniseras med markstationer och med varandra. Därför är GNSS en lättillgänglig och smidig källa till tid, till en betydligt lägre kostnad än andra alternativ då en GNSS-mottagare är långt billigare än till exempel atomur [9].

Tid är ett mått på när något har hänt, när något sker och när något kommer att hända och används för att beskriva en sekvens av individuella händelser. Tid mäter vi med dagar, timmar, minuter och sekunder. Sverige som land har en gemensam tid som kallas normaltid, eller vintertid i dagligt tal. I Sverige är forskningsinstitutet RISE ansvarigt för att upprätthålla normaltiden men även för att distribuera den till olika användare runt om i landet. RISE använder ett antal atomklockor för att fastställa en extremt noggrann tid och ser till att den överensstämmer med den gemensamma internationella tidsskalan. Den tidsskalan heter på svenska koordinerad universell tid, förkortas UTC, och är ett viktat medelvärde av tidsskalor som mäts in i olika laboratorium runt om i världen [10]. Standardenheten för mätning av ett tidsintervall är en sekund (s).

För att mäta en tidkällas kvalitet används två begrepp: noggrannhet (eng. *accuracy*) och precision (eng. *precision*). Noggrannheten beskriver hur långt från ett referensvärde mätningen är och precision beskriver hur mycket olika mätningar varierar inbördes. En klocka som konsekvent tappar en sekund varje dag har alltså hög precision men är inte noggrann.

Frekvens är mått på hur många gånger en händelse inträffar under ett specifikt tidsintervall. Standardenheten för att mäta frekvens är hertz (Hz) och är ett mått på antalet händelser per sekund. Tid och frekvens är tätt sammankopplade då en hertz är lika med en händelse per sekund [9], [11].

Inom traditionell radio används oftast frekvens för att beskriva svängningshastigheten hos den våg som bär informationen i radiosignalen. Olika kanaler tilldelas olika frekvenser för att inte störa varandra. Vid användande av GNSS som frekvenskälla är det inte samma typ av frekvens som avses, utan förmågan att hålla takten i ett system. Detta kan jämföras med en metronom. Här används frekvens synonymt med att få olika delar i ett system att svänga i takt vilket betyder att systemen kan arbeta ihop. Att svänga i takt innebär inte enbart att svängningarna är lika snabba utan också att de ligger i fas så att systemen inte motverkar varandra.

2.2.1 Systemklockor och stratumnivåer

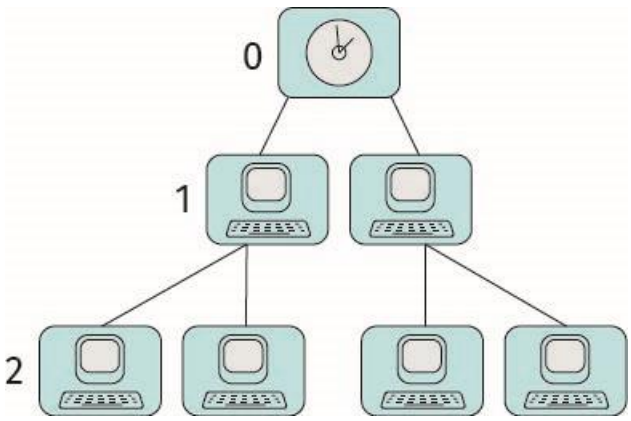
Enskilda system mäter tid genom att ha en någon form av intern eller extern oscillator. En oscillator är en elektrisk komponent som ger en stadig takt (frekvens) och som räknar hur många taktslag som förekommit. Det som är gemensamt för alla klockor är att de kommer att börja driva om de inte synkroniseras mot en referensklocka och hur snabbt klockan driver beror på hur bra oscillator den har [12].

Det finns olika typer av oscillatorer med olika egenskaper och noggrannhet. Den enklaste typen, kristalloscillatorer, håller takten genom att en kristall, oftast i kvarts, hamnar i självsvängning när den utsätts för ett elektriskt fält. Atomur är också en typ av oscillator som håller frekvensen genom att mäta energin som frigörs när elektroner hoppar mellan olika energinivåer. Den senare är både betydligt dyrare och betydligt mer noggrann.

Om ett system har tillgång till internet, kan tiden tas därifrån med hjälp av olika protokoll. Det vanligaste protokollet är network time protocol (NTP) [13] vilket har använts sedan år 1985. Inom NTP skickar en klient en fråga till en NTP-server som svara med vad tiden är. Noggrannheten brukar anges vara 10–100 millisekunder.

Ett begrepp som ofta dyker upp i samband med NTP är stratumnivåer. Det definierar en hierarki av tidskällor där Stratum 0 är den högsta nivån i hierarkin med högts noggrannhet och utgörs av en fysisk referens som ett atomur eller GNSS (vilka har atomur i varje satellit). Stratum 1-källor tar sin tid från stratum 0, stratum 2 tar sin tid från stratum 1 och så vidare upp till nivå 16. Stratumnivån anger alltså avståndet från referenskällan vilket också indirekt speglar noggrannheten på tiden. Figur 3 ger en översikt på ett system med två stratumnivåer.

Ett annat protokoll för överföring av tid är PTP, precision time protocol [14]. PTP används typiskt i avgränsade miljöer då kraven på noggrannhet är högre. PTP kräver en särskild hårdvara vilket gör att det blir mer kostsamt att ha fler användare. Komplexiteten och kostnaden blir högre för PTP jämfört med NTP som är mjukvarubaserat. Noggrannheten på PTP anges vara 10–100 mikrosekunder.



Figur 3. Ett system med två stratumnivåer där nivå noll är en tidreferens. Alla nivåer i systemet är beroende av att tidreferens i nivå noll fungerar.

2.2.2 Tidskravställning

De flesta tekniska system kräver betydligt högre noggrannhet än en sekund. Det finns en tolerans för hur fel tidmätningarna kan vara innan systemet inte längre fungerar. Tiden för hur länge en klocka kan hålla sig inom feltoleransen utan att synkroniseras mot en referensklocka kallas för *holdover*. Alla klockor har olika holdover-tid men generellt har bättre klockor längre holdover-tid då dessa driver mindre.

Många typer av tekniska system ställer krav på en tidsnoggrannhet på en eller några få mikrosekunder, medan det i till exempel 5G-nät handlar om krav på nanosekundnivå [15]. Krav för tid brukar förekomma i kravställande dokument på två sätt, som krav på maximal avvikelse i tidssynkronisering och noggrannhet i tidsstämpling.

Grad av tidssynkronisering kan mätas som tidsskillnaden mellan systemklockan och en referensklocka. Ofta väljs en referensklocka som är synkroniserad med UTC. Själva synkroniseringen innebär att justera systemklockan att överensstämma med referensklockan. I vissa fall räcker det att systemet vet om att tidsskillnaden är inom toleransen och inga justeringar behöver därför göras. Behovet av tidssynkronisering är viktig i vissa system, främst inom kommunikation. Kommunikationssystemen bygger på att enskilda sändare får en tidslucka där en sändare har tillstånd att sända. Om olika sändare har olika tidsuppfattning är det troligt att flera sändare sänder i samma tidslucka vilket resulterar i att mottagarna får problem att avkoda vad som sänds och uppfattar de andra sändarna som en störsändare [9].

Vissa system kan kräva att händelser som sker i systemet, till exempel en banktransaktion, ges en tidsstämpel. Tidsstämpel bör då innehålla vilken timme, minut och sekund som händelsen skedde, ofta ner till milli- eller mikrosekundnivå. Olika system har olika tolerans för hur stor skillnad det får vara mellan referensklockan och den tidsangivelse tidsstämpeln ger [9].

2.2.3 Frekvenskravställning

I tekniska system som är beroende av korrekt frekvensangivelse krävs frekvenssynkronisering, på engelska *syntonization*. Precis som vid tidssynkronisering mäts och justeras skillnaden i frekvens mellan en systemklocka och en referensklocka. På samma sätt som för tid har tekniska system en förmåga att hålla frekvensen under en kortare tid, det kallas för frekvensstabilitet. Detta bygger också på interna eller externa oscillatorer som kan ha olika egenskaper och noggrannhet [9]. Exempel på vanliga frekvensenheter finns i Tabell 1.

Tabell 1. Några frekvensenheter och dess förkortningar.

Enhet	Förkortning	Händelser per sekund
Puls per sekund	pps	1
Kilohertz	kHz	10^3
Megahertz	MHz	10^6
Gigahertz	GHz	10^9

2.3 Exempel på hur GNSS används i samhället

Tid från GNSS har länge varit det billigaste och smidigaste sättet att få en noggrann tid i samhället. Följande är tre exempel på var GNSS-tid och frekvens skulle kunna förekomma i beredskapssystemet:

Finansiella tjänster

Vid finansiella transaktioner är en noggrann och spårbar tid till UTC av vikt. Inom exempelvis *high frequency trading* (HFT) kan tusentals transaktioner ske inom en sekund och det är viktigt att veta i vilken ordning de skedde. Varje transaktion måste ha en tidsstämpel och noggrannheten kan behöva vara inom 100 mikrosekunder från UTC för att följa internationella riktlinjer. Korrekta tidsstämplar blir även av hög betydelse i utredningar om ekonomisk brottslighet för att säker ställa händelseförlopp. Tidssynkroniseringsfel har lett till att börser har tvingats stänga, dock har stängningarna inte kunnat kopplas till problem med GNSS utan illustrerar bara vikten av korrekt tid [15].

Elektroniska kommunikationer och post

Inom telekom och kommunikation är noggrann tid och frekvens viktig för att synkronisera nätverk så att de kan kommunicera med varandra. Det finns internationella standarder utfärdade av Internationella teleunionen (ITU) för hur stabila frekvenssignaler ska vara för att nätverk från olika operatörer ska fungera tillsammans. Att ha en stabil frekvens är nödvändigt för att mobilnät som 3G och 4G ska fungera. 5G har ännu högre krav på en stabil frekvens. Tekniker som *time division duplexing*, TDD, som används i bland annat mobiltelefoni kräver också noggrann tid [15], [9].

Energiförsörjning

Elnät består ofta av flera separata system, både mellan länder men även nationellt, och kräver en noggrann tidssynkronisering. Svenska kraftnät använder till exempel i stor utsträckning GNSS för tidssynkronisering i sina stationer [16]. Tidssynkronisering behövs för att kontrollera generatorer, frekvens- och effektkontroll, avlastning med mera. Tidssynkronisering är också viktigt för metoder som *travelling wave fault detection*[4] vilket är till för lokalisering av fel i ledningarna. Frekvensen i elsystem påverkas av balansen mellan tillförd och använd energi, vilket kräver konstant monitorering och åtgärder. Större avvikelser av normalfrekvensen kan riskera skada utrustning hos såväl producenter som användare och i värsta fall hota hela systemets funktionalitet. För att undvika störningar behöver anslutna anläggningar hålla samma frekvens som råder i systemet som helhet. För att övervaka nätet mäts effekt och ström i olika noder flera tusen gånger per sekund. Internationella krav säger att tidnoggrannheten på dessa mätningar måste vara inom en mikrosekund och om de inte följs kan det leda till att områden blir utan ström. I Storbritannien används GNSS-tid för att synkronisera elnätet. Övergång till holdover-lösningar vid bortfall av GNSS skulle typiskt skapa tidsfel på två millisekunder inom ett par timmar. Nya understationer kan enligt internationell standard behöva en tidnoggrannhet på 1 mikrosekund vilket innebär att problem snabbt kan uppkomma vid GNSS bortfall [15], [9].

2.4 Störning av GNSS

Avsiktlig störning av GNSS kan delas in i två huvudkategorier:

- **Störning,** på engelska kallat för *jamming*, är att avsiktligt sända brussignaler på samma radiofrekvenser som GNSS-signalerna för att överrösta dem. GNSS-mottagaren kan då få en sämre förmåga till navigering och tidgivning eller i värsta fall inte kunna navigera eller ge tid överhuvudtaget.
- **Vilseledning,** på engelska kallat för *spoofing*, är att avsiktligt sända ut signaler som härmar riktiga GNSS-signaler men med falsk information om position eller tid och vissa fall både och. En vilseledd mottagare kan ge ifrån sig en felaktig position och tid. Bakomliggande system kan då felaktigt verka vara opåverkade.

De amerikanska styrkorna använde GPS med stor framgång under första Gulfkriget 1991 och sedan dess har intresset för och möjligheten att störa ut fiendens GNSS bara ökat [17]. Störtekniken har utvecklats mycket och idag påverkas GNSS dagligen både i och utanför konfliktzoner. Genom hemsidor som sammanställer data från trafikflygplan går det att se att störning förekommer i delar av Östersjön sedan Rysslands invasion av Ukraina i februari 2022 [18]. Vilseledningsattacker har blivit betydligt vanligare sedan början av 2024 [19].

Utrustning för störning, så kallade störsändare, finns i en mängd olika storlekar. De allra minsta kan sättas i ett cigarettändaruttag i en bil och därefter skapa en liten störbubbla på några meter runt fordonet. De största störsystemen kan ha en påverkan på över 100 km. Störningen genomförs då oftast av statliga aktörer [19].

[4] Travellling wave fault detection är en metod där det utnyttjas att vid fel i ledningar kommer spänning vid felet att gå mot noll medan strömmen dubbleras. En högfrekvenspuls kommer då att färdas från felet i ledningen med ljusets hastighet och om ankomsttiden för pulsen mäts i vardera änden av ledningen kan närmsta kraftledningsstolpe identifieras. Detta kräver att klockorna i nätet är synkroniserade.

När en GNSS-mottagare blir utstörd är det första symptomet att systemen slutar leverera position eller att positionen hoppar mellan olika platser. En positionsavvikelse kan vara relativt lätt att upptäcka. Ett mindre uppenbart beroende är att många system använder GNSS för att synkronisera tid och frekvens. Vissa system som enbart använder GNSS för korrekt tid och frekvens kommer då att bli påverkade och inte kunna leverera rätt tid eller frekvens. Det kan även visa sig att system som tros vara GNSS-oberoende inte är det då källan de hämtar tid ifrån i sin tur är beroende av GNSS.

Vilseledning av GNSS kan orsaka stora problem, men kan också vara mycket svårt att upptäcka. Eftersom GNSS-mottagarna tar emot en signal som innehåller information tror mottagaren att allt är som det ska och kan därför låta bli att varna att något är fel. I synnerhet en liten succesiv förändring av tidssignalen kan vara svår att upptäcka och resultera i att mottagaren vilseleds och inte varnar användaren. En annan fara med vilseledning kan vara om den falska tiden är satt långt fram i tiden. Det är då lätt för en människa att upptäcka felet men det kan då ha fått stora konsekvenser i och med att vissa mjukvarulicenser har nått sitt utgångsdatum.

Att öva med GNSS-störning eller vilseledning är i princip omöjligt. Detta då sändning i frekvensbandet inte är tillåtet förutom för satelliter. Det medför att system och personal oftast inte har erfarenhet av hur störning av GNSS påverkar eller har svårt att förutsäga konsekvenserna. Eftersom olika mottagare och eventuella stödsystem skiljer sig åt inbördes går det inte att uttala sig generellt om hur störning och vilseledning kan påverka.

2.5 Verkliga exempel på GNSS-störning

Följande är exempel på verkliga händelser där GNSS på något sätt har påverkats, antingen genom fel från satelliterna eller genom störning och vilseledning.

2.5.1 Ett litet klockfel skapar stor oreda

Den 26 januari 2016 orsakade en uttjänt GPS-satellit omfattande problem över hela världen. En uttjänt satellit skulle avvecklas men istället laddades felaktig mjukvara upp. Det ledde till att ungefär hälften av alla GPS-satelliter fick ett tidsfel på 13 mikrosekunder relativt UTC-tid. Tidsfelet pågick under några timmar. Incidenten fick stor påverkan världen över. Flertalet incidentrapporter redogör för problem hos olika kommunikationslösningar eller broadcastsändningar [20]. Bland annat brittiska BBC rapporterade att digitalradiosändarna fick problem att synkronisera sändningen och därför kom att störa varandra då de sände vid fel tillfälle [21]. En tillverkare av tidsservrar i Storbritannien var tidiga med att rapportera om händelsen och anger att det under fyra dagar kom in nära 5000 larm från olika länder [22]. De noterar också att det inte var någon samstämmighet i vilka mottagare som påverkades av incidenten. Även i jämförelse mellan mottagare av samma typ kunde det skilja mycket på grund av olika inställningar i mottagaren.

2.5.2 Minicall

Under några månader vintern 2006–2007 drabbades personsökare i Sverige från företaget Minicall av problem som gjorde det svårt att till exempel kalla in personal till sjukvården. Basstationerna som kommunicerade med Minicall-enheterna använde GPS-signaler för att synkronisera sändningen, men på grund av ett fel med GPS-mottagningen stängdes basstationerna ner. Problemet krävde att de lokala GPS-mottagarna i basstationerna byttes ut manuellt vilket tog ungefär en månad på grund av stora avstånd och vinterklimat [3], [23], [24].

2.5.3 Störning och vilseledning av trafikflygplan

Sedan Rysslands invasion av Ukraina i slutet av februari 2022 har störning och vilseledning av trafikflygplan blivit allt mer vanligt. Under 2023 var det ett fåtal störincidenter i Östersjöområdet men 2024 och 2025 har rapporterna om GNSS-störning ökat kraftigt [25]. Till en början förekom mest störning men sedan 2024 har även vilseledning blivit all mer vanligt. Vid störning är det främst flygplanets navigeringssystem som blir påverkat. Om flygplanets GNSS-mottagare blir utsatt för vilseledning kan det få kaskadeffekter i andra system som är beroende av position och tid. Till exempel kan flygplanets väderradar sluta fungera om flygplanet har en falsk position och planet kan då få svårt att detektera åskväder. Om flygplansklockan uppdateras med en falsk tid från GNSS-mottagaren kan flygplanet få problem med sina datalänkar och tappa kontakt med marksystem [19].

2.6 Ett scenario för antagonistisk störning av GNSS

Scenariot är utformat för illustrera ett hot som är både rimligt och som kan orsaka särskilt allvarliga konsekvenser i fredstid [26]. Scenariot kan läsas enskilt för att ge stöd till förståelsen av tekniska beroenden av tid och frekvens via GNSS. Scenariot är inte baserat på en verklig händelse och det är inte säkert att de system som nämns i scenariot skulle påverkas på det beskrivna sättet. Scenariot kan även användas tillsammans med metodstödets arbetsgång (presenteras i kapitel 4).

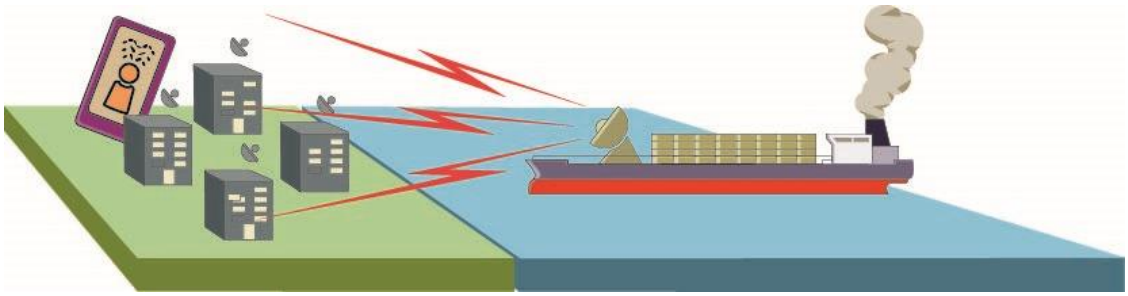
Scenariot har en generisk utformning utan geografisk avgränsning för att bidra till inspiration att identifiera beroenden utifrån den egna verksamheten. I scenariot befinner sig störsändarna på internationellt vatten (figur 4), vilket gör det svårt för svenska myndigheter att avlägsna störutrustningen. Landbaserad störutrustning skulle kunna användas, men om störsändarna befinner sig inom Sveriges gränser skulle den förhoppningsvis snabbt tas om hand av svenska myndigheter.

En längre tid under hösten har det i media dagligen rapporterats om GNSS-störningar över Östersjön. Störningarna har varit återkommande och har påverkat flyg- och sjötrafiken genom att GNSS-mottagarna ombord inte har fungerat. Samtidigt har skuggflottor befunnit sig längs territorialgränsen ett flertal gånger, men alltid befunnit sig på internationellt vatten. Det finns indikationer på att skuggflottan är utrustad med störutrustning och att detta ligger bakom GNSS-störningarna i området. Experter inom GNSS tror att det kan röra sig om någon form av ny utrustning som skuggflottan testar innan det ska användas skarpt. På land har infrastruktur och människor varit relativt förskonade från den störning som flyg- och sjötrafiken utsatts för men ett antal gånger har även system på land slutat att fungera på grund av störning. Alla störincidenter har hittills varat under några timmar och större delen av dygnet har GNSS fungerat.

En regnig fredagseftermiddag i november börjar plötsligt rapporter strömma in om att navigeringssystem baserat på GNSS slutat att fungera. Man kan inte längre se sin egen position i kartappar. Ledningscentraler kan inte lokalisera ambulanser och poliser. Lantmäteriet som har ett väl utbyggt nät av referensstationer med GNSS-mottagare börjar uppleva att kustnära stationer inte längre fungerar korrekt. Snart inkommer också rapporter om funktionsfel och varningar som kan ha koppling till problem med satellitnavigeringssystem från det övriga samhället.

Över helgen blåser det upp till storm i delar av det påverkade området. Samtidigt börjar klockorna i transformatorstationerna i elnätet att driva då de inte längre kan synkroniseras mot GNSS-tid. När sen träd faller över elledningar uppstår problem med att lokalisera felet i ledningen då metoden som används förlitar sig på att klockorna i nätet är synkroniserade. Efter några dagar slutar delar av mobilnätet att fungera på grund av att klockorna i basstationerna har drivit för mycket.

Efter ytterligare några dagar kommer det in rapporter om att störningsattacken verkar vara över, men den positionsangivelse som rapporteras i olika system stämmer inte med det som användare tror att den ska vara. Tiden ser först ut att stämma men när den jämförs mot exakt tid så upptäcks ett fel på några millisekunder. Även datanätverk som har tillgång till reservsystem slutar plötsligt att fungera då de synkroniserats mot den falska tiden och kan inte kommunicera med andra nätverk. Nu är området även utsatt för vilseledning. Störning och vilseledning fortsätter att påverka området konstant i flera veckor. Allt eftersom veckorna går slutar fler och fler system att fungera då de klockor som finns i back-up systemen fortsätter att driva och inte längre går tillräckligt noggrant.



Figur 4. Fartyg med störsändare riktade mot samhället.

3 Risk- och sårbarhetsanalyser och metodstödets roll

Att upprätthålla samhällets funktionalitet är en central uppgift inom det civila försvaret. MSB pekar idag ut viktiga samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet – i vardagen, krisen och kriget. De viktiga samhällsfunktionerna utgör grunden för att identifiera samhällsviktig verksamhet som bedrivs av offentliga och privata aktörer [27]. Att säkerställa den samhällsviktiga verksamheten kan ses som aktörers (privata och offentliga) prioriterade åtaganden under kris, höjd beredskap och då ytterst krig.

I detta kapitel redovisas kortfattat vad risk- och sårbarhetsanalyser spelar för roll i det svenska beredskapssystemet och hur metodstödet kan förstås i relation till detta system.

3.1 Risk- och sårbarhetsanalyser i det svenska beredskapssystemet

Enligt gällande lagstiftning ska RSA genomföras av såväl statliga myndigheter [28] som av kommuner och regioner [29]. Analysen ska genomföras både för den egna verksamheten och för respektive ansvarsområde. Regioner, kommuner och beredskapsmyndigheter ska redovisa dessa resultat. För beredskapsmyndigheterna benämns rapporteringen risk- och sårbarhetsbedömningar (RSB) [30].

Enligt MSB ska RSA bidra till:

- Beslutsunderlag för beslutsfattare och verksamhetsansvariga.
- Underlag för kommunikation om samhällets risker till allmänheten och anställda.
- Underlag för samhällsplanering.

Analyserna bidrar också till den nationella bilden av hot, risker, sårbarheter och förmåga som presenteras i den nationella risk- och sårbarhetsbedömningen (NRSB). Vad som ska redovisas i RSA respektive RSB specificeras i MSB:s föreskrifter för regioner och kommuner [31], [32] och statliga myndigheter [33].

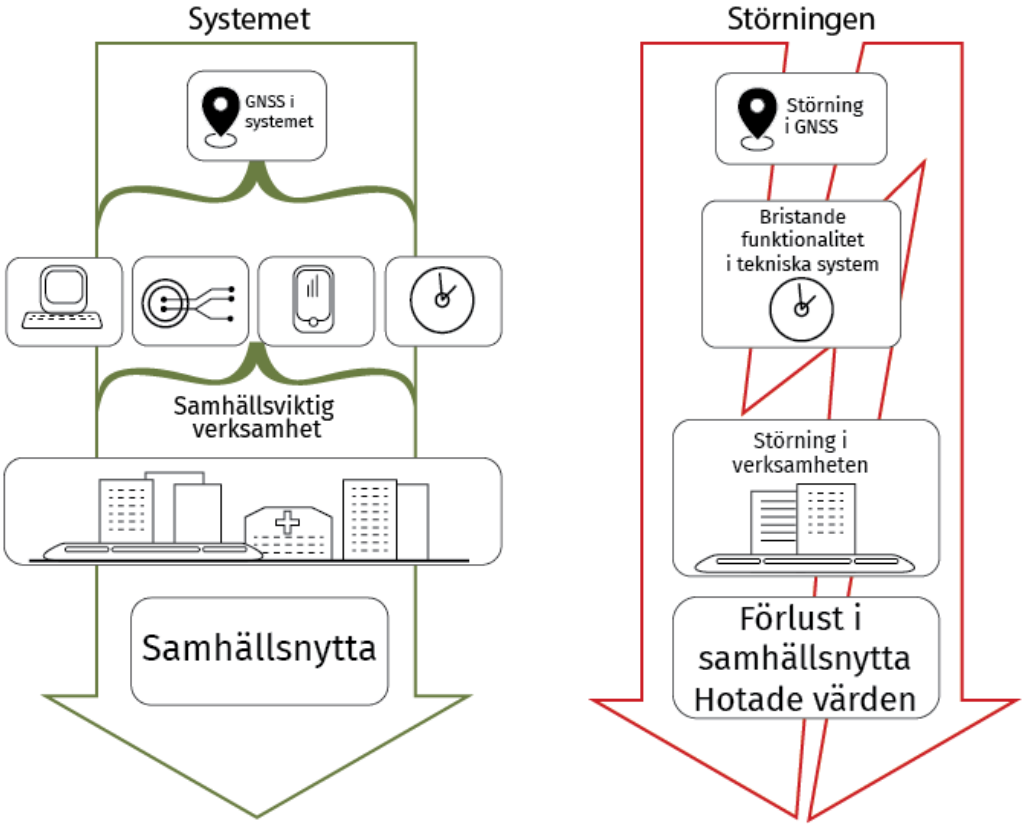
Myndigheter, kommuner och regioner ska i RSA och RSB själva identifiera de hot och risker som ska bedömas. MSB har uppmärksammats på att det finns en svaghet i systemet i och med att hot och risker som bedöms inte är samordnade, vilket försvårar arbetet med NRSB [26]. Istället har MSB utformat gestaltningar[5] i form av händelser för de särskilt allvarliga hoten som kan användas för riskbedömning och utgöra grund för NRSB [26].

I den senaste NRSB har inte störningar av GNSS varit med bland de hot som redovisas i den sammanfattande rapporten. Till den nationella risk- och förmågebedömningen 2012 bidrog dock FOI med ett antal hotscenarier varav störning av GNSS var ett. Scenariot beskrev såväl störningar av position som tid och frekvens. Det scenario som presenterades innebar att GNSS var otillgängligt under två veckor [34]. Med tanke på att detta scenario nu är äldre än tio år fanns ett behov av att uppdatera scenariot, vilket ett förslag på redovisades i avsnitt 2.6.

3.2 Konceptuell bild över metodstödets roll

Det föreslagna metodstödet är tänkt att stötta aktörerna med att i RSA-processen inkludera GNSS-påverkan avseende frekvens och tid. En viktig del av detta är att skapa en systemförståelse för kopplingen mellan påverkan på GNSS, den effekt på tekniska systems funktion som blir följden och de konsekvenser det innebär för samhällsviktiga verksamhet som bedrivs inom organisationen eller sektorn (figur 5).

[5] Gestaltningen uttrycks av MSB utifrån händelsens intensitet, varaktighet och utbredning (NRSB 2025).



Figur 5. Konceptuell bild som illustrerar metodstödets sammanhang och perspektiv. Till vänster speglas GNSS roll i samhällsviktig verksamhet och hur det kan bidra till samhällsnytta. Till höger illustreras hur en påverkan på GNSS potentiellt kan leda till förlust i samhällsnytta och att samhälleliga värden hotas.

Den analysansats som föreslås utgår från att skapa en systemförståelse kring vad som är organisationens eller sektorns samhällsviktiga verksamhet som behöver skyddas, och en kartläggning av de tekniska system som är centrala för verksamhetens funktionalitet. Denna del är relevant även i andra RSA-sammanhang. För förståelsen av effekterna av en störning i GNSS krävs även en kartläggning av vilka system som är beroende av GNSS.

Utifrån denna systemförståelse är det möjligt att analysera konsekvenserna av en störning vilken kan leda till kortare eller längre perioder av försämrad funktion av GNSS-tjänster. Analysen startar med en bedömning av hur detta avbrott påverkar funktionaliteten i de olika tekniska system som är beroende av GNSS. Nästa steg innebär att analysera på vilket sätt avbrottet i de tekniska systemen påverkar verksamheten. Ett ytterligare steg kan vara att vidga analysen till de effekter verksamhetsstörningen får i samhället i stort. Detta ligger dock utanför den tekniska analys som denna rapport handlar om, men kan vara av stort värde att studera när riskerna i samhället av GNSS-beroendet ska bedömas.

Flera av analysstegen kräver god teknisk förståelse. Det innebär att det är viktigt att i processen involvera personer med teknisk kompetens och GNSS-fokus för att inte missa viktiga aspekter.

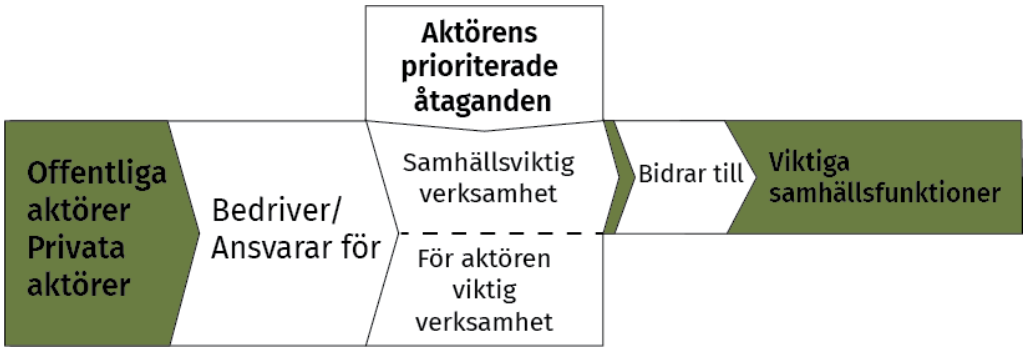
I nästkommande kapitel utvecklas metodstödet utifrån de olika steg som diskuterats ovan, inkluderade såväl teknisk information som exempelbeskrivningar. Tanken är att det ska fungera som stöd för att konkretisera vad GNSS-påverkan kan innebära och att ge ingångar till att förstå var GNSS kommer in i den egna verksamheten och de effekter potentiell påverkan kan få.

4 Systematisk arbetsgång för att identifiera tekniska beroenden av tid och frekvens via GNSS

I detta kapitel presenteras metodstödets systematiska arbetsgång med processteg och frågeställningar samt exempelbeskrivningar, som kan hjälpa aktörer att analysera och förstå hur deras verksamheters prioriterade åtaganden påverkas vid störning och vilseledning av GNSS avseende tid och frekvens.

Med *verksamhet*[6] menas här den aktivitet som genomförs av den organisation eller sektor som analysen gäller. Organisationen eller sektorn har ett antal åtaganden och mål för verksamheten. Vissa åtaganden kan ses som särskilt prioriterade. Samhällsviktig verksamhet är sådana åtaganden som är särskilt prioriterade från ett samhällsperspektiv. Det är ytterligare försvårande om de prioriterade åtaganden som utgörs av samhällsviktig verksamhet påverkas på grund av störning och vilseledning av GNSS.

Prioriterade åtaganden (figur 6) används i FORSA [34] som ett sätt att beskriva de uppgifter som är särskilt viktiga att upprätthålla för att undvika oacceptabla konsekvenser, bland annat samhällsviktig verksamhet. Det bör noteras att det även kan finnas andra åtaganden som också är prioriterade för verksamheten, men inte utgör en samhällsviktig verksamhet för aktören [34]. Av den anledningen används i detta metodstöd begreppet prioriterade åtaganden just för att fånga in fler åtaganden som aktören uppfattar som prioriterade utöver de som inte kan karaktäriseras som samhällsviktiga.



Figur 6. Figuren illustrerar hur begreppen prioriterade åtaganden, samhällsviktig verksamhet och viktiga samhällsfunktioner kan förstås i relation till varandra och de aktörer som bedriver eller ansvarar för dessa.

Den systematiska arbetsgången innehåller sju olika processteg, fördelat på tre faser (figur 7). Arbetsgången startar med en inledande fas som säkerställer att personal med kunskap om den egna verksamheten och de tekniska system som används identifieras och inkluderas i den arbetsgrupp som ska genomföra analysen. Den första fasen handlar också om att planera genomförandet.

Den andra fasen består av steg 2–6 och omfattar den faktiska beroendeanalysen av verksamheten. Det är i denna fas som beroenden [35] [36] av GNSS identifieras och förstås utifrån hur verksamheten är avhängig att GNSS fungerar. Den sker genom en stegvis genomgång av verksamheten för att identifiera dess prioriterade åtaganden (steg 2), vilka tekniska system som är grundläggande för dessa prioriterade åtaganden (steg 3), vilka av dessa system som är beroende av tid och frekvens via GNSS (steg 4), vilken grad av redundans det finns i systemen (steg 5) samt slutligen hur verksamhetens prioriterade åtaganden påverkas om tid och frekvens via GNSS inte kan levereras.

[6] Begreppet verksamhet är dubbeltydigt i svenskan. Det används både om aktör som bedriver någon form av aktivitet och om själva aktiviteten.

Figur 7. Figuren visar en översikt av metodstödets systematiska arbetsgång bestående av sju steg och tre faser.

Den tredje och avslutande fasen består av arbetsgångens sjunde och sista steg. Den handlar om att ta vara på den kunskap som analysen i steg 2 till 6 har genererat genom att sprida den inom den egna verksamheten, samt sprida erfarenheterna uppåt i beredskapssystemet genom att inkludera analysen av sårbara beroenden av GNSS i rapporteringen av verksamhetens RSA och RSB.

4.1 Steg 1. Bemanna analysgrupp och planera genomförandet

Den första fasen (figur 7) beskriver de initierande aktiviteter som bör ske innan analysen kan börja. Den första fasen innebär att utse och tillsätta personal med nödvändig kompetens för ändamålet, samt utse någon eller några personer som leder och håller samman analysarbetet. Slutligen ingår att planera för genomförandet av arbetsgångens övriga steg.

För att göra en analys av hur störning och vilseledning av GNSS påverkar en organisations verksamhet och ansvarsområden behövs både kunskap om de tekniska systemen och deras beroende av GNSS och kunskap om hur verksamheten fungerar och vad den ska leverera. Detta för att kunna identifiera tekniska beroenden och analysera vilka följder störning och vilseledning av GNSS leder till. Denna kunskap bör inkludera:

- Att veta vilka tekniska system inom verksamheten som är beroende av GNSS för tid och frekvens.
- Att förstå hur respektive tekniskt system påverkas avseende tid eller frekvens om GNSS störs eller vilseleds.
- Att veta vilken redundans som finns inom systemen som kan minska konsekvenserna av störning eller vilseledning.
- Förståelse för hur verksamheten inom organisationen eller ansvarsområdet påverkas om något eller några tekniska systems funktionalitet försämras eller helt faller bort.

Ovanstående kunskap kan behöva sökas från olika delar av verksamheten eller om sådan saknas inom organisationen tas in utifrån [37]. Detta då olika delar inom organisationen arbetar med och har kunskap om olika aspekter av verksamheten och olika systems funktioner och skillnader. Exempelvis kan IT-avdelningen ha kunskap om vissa tekniska system och beroenden, medan kunskap om andra tekniska system och beroenden kan finnas på andra platser inom organisationen [38]. Till analysen behöver även kompetens om organisationens verksamhet och ansvarsområden inkluderas. Detta bör bland annat omfatta:

- Kunskap om verksamheten och dess struktur.
- Kunskap om verksamhetens prioriterade åtaganden och samhällsviktig verksamhet.
- Förståelse för hur verksamheten inom organisationen eller ansvarsområdet påverkas om något eller några tekniska systems funktionalitet försämras eller helt faller bort.

Hur genomförandet sker kan bero på vilka personer som ingår i bedömningsarbetet [37]. Exempelvis kan en person med kunskap om både tekniska systems beroende av GNSS samt verksamhetens prioriterade åtaganden delta i flera eller alla delar av bedömningen. En person som däremot innehar spetskompetens om tekniska systems beroenden av GNSS bör ingå i steg 4–5.

4.2 Steg 2. Kartlägg prioriterade åtaganden

I det andra steget kartläggs organisationens eller sektorns prioriterade åtaganden. Prioriterade åtaganden omfattar både samhällsviktig verksamhet och andra åtaganden som också är prioriterade, men inte samhällsviktiga [34]. En av de mest centrala delarna i en verksamhets RSA är att identifiera samhällsviktig verksamhet [39]. Denna kunskap är lämplig att utgå ifrån för att få en övergripande bild av verksamheten och vilka samhällsviktiga verksamheter som är prioriterade åtaganden och som ska säkerställas.

Om det utöver samhällsviktig verksamhet finns prioriterade åtagande som inte nämns i RSA ska även dessa kartläggas. Det är upp till respektive verksamhet att avgöra vilka åtaganden inom verksamheten detta är. Om kartläggning inte redan har skett kan en verksamhetsanalys vara behjälplig. Alternativt tillvägagångssätt till att använda sig av redan genomförd verksamhetskartläggning i RSA är att använda sig av stödmaterial från exempelvis MSB för att identifiera samhällsviktig verksamhet [40] [41] eller att genomföra en verksamhetsanalys [38].

För att identifiera prioriterade åtaganden inom sektorn eller mellan olika aktörer kan en sektorskartläggning eller beroendeanalys vara till hjälp. Stöd till att genomföra en sektorskartläggning kan inhämtas i Livsmedelsverkets sektorsövergripande RSA [42]. Stödmaterial för att genomföra en beroendeanalys kan inhämtas hos MSB [43].

I kartläggning av verksamhetens prioriterade åtaganden är det lämpligt att beakta både fredstid, höjd beredskap och krig då dessa åtaganden kan skilja sig åt mellan de olika beredskapsnivåerna. Samtidigt förväntas samtliga dessa fall beaktas inom ramen för den lagstadgade RSA-processen.

4.3 Steg 3. Identifiera kritiska beroenden i form av tekniska system

I steg 3 identifieras vilka tekniska system som är nödvändiga för att prioriterade åtaganden ska kunna uppfyllas, så kallade kritiska beroenden. Med tekniska system kan förstås ett system som består av mindre delar, i detta fall digitala, som arbetar tillsammans som ett elnät, datornätverk eller övervakningskamera [44].

Kritiska beroenden kan relateras till företeelser (teknik, personal etc.) som behövs för att det ska gå att uppfylla det prioriterade åtagandet, som är svåra att ersätta och om de försvinner och innebär att verksamheten snabbt får en kraftigt försämrad funktionalitet. Kritiska beroenden kan vara både externa och interna. Interna kritiska system finns inom verksamheten, medan externa

beroenden innebär att de kritiska systemen finns utanför verksamheten [34], [43]. Ett internt beroende av kritiska system har verksamheten rådighet över att genomföra åtgärder för att minska sårbarheten i medan de externa beroendena är svårare att påverka direkt [45].

Det är lämpligt att först lista alla tekniska system som verksamheten använder för att kunna uppfylla sina prioriterade åtaganden och sedan försöka klassificera vilka som är kritiska för funktionen. Information om kritiska beroenden kan exempelvis hämtas från verksamhetsbeskrivningen i RSA [34]. I detta steg behöver man inte fundera på om det tekniska systemet är beroende av GNSS eller ej, det sker i steg 4.

- Identifiera *interna* kritiska beroenden av tekniska system utifrån verksamhetens prioriterade åtaganden.
- Identifiera *externa* kritiska beroenden av tekniska system utifrån verksamhetens prioriterade åtaganden.

Analysen bör även om möjligt inkludera att se över om de kritiska beroendena av tekniska systemen är desamma vid fredstida kris som vid höjd beredskap.

Notera: I FORSA inkluderas kritiska beroenden som en del av de prioriterade åtagandena. I detta metodstöd analyseras istället kritiska beroenden separat för att tydliggöra tekniska beroenden [34].

4.4 Steg 4. Identifiera tekniska systems beroende av tid och frekvens från GNSS

I det fjärde steget identifieras om och på vilket sätt de tekniska systemen är beroende av tid- och frekvenssynkronisering och i vilken grad tid och frekvens huvudsakligen fås från GNSS. Om det tekniska systemet är beroende av tid eller frekvens från GNSS för sin funktion behöver det undersökas hur systemet påverkas om störning eller vilseledning sker. Det kan exempelvis tänkas att ett system inte alls är brukbart vid GNSS-påverkan eller att systemet fungerar men att prestandan är sämre. Ytterligare ett alternativ är att systemet skickar ut felaktig information.

Varje tekniskt system behöver studeras individuellt för att hitta eventuellt beroende av tid och frekvens. I avsnitt 4.4.1–4.4.4 presenteras frågor som bör ställas för respektive system för att identifiera beroende av tid eller frekvens. Till frågorna presenteras även exempel och kortare beskrivningar.

4.4.1 Frågor som bör ställas angående störning av tid

För varje system bör följande frågor om tid ställas:

1. Är systemet beroende av tid?
2. Vilka krav har systemet på tidsnoggrannhet?
    a. Vilka delar av systemet kräver störst tidsnoggrannhet?
    b. Finns kravställande dokument om tid?

Exempel relaterat till tidsnoggrannhet

Kräver systemet en tidsnoggrannhet på milli-, mikro eller nanosekundnivå?

Till exempel för 3G finns det krav på tidsnoggrannhet på 1,5 mikrosekunder medan för 5G är kravet mindre än 500 nanosekunder!

Exempel kravställning

EU-direktivet MiFID II innehåller regler för tidsnoggrannhet på tidsstämpling av orderdata och transaktionsrapporter inom aktiehandel.

3. Vad har systemet för tidskälla?
    b. Är tidskällan beroende av GNSS?

Stödfrågor för att identifiera beroenden

Kan det finnas ett gömt beroende av GNSS? Är systemet kopplat direkt till en tidskälla som har en GNSS-mottagare eller får systemet tid från ett annat system som i sin tur får tid från en GNSS-mottagare? Alla beroenden behöver inte vara

5. Använder andra aktörer utanför verksamheten systemet och påverkas de i sin tur om systemet inte levererar korrekt tid?
6. Om systemet påverkas på grund av GNSS-störning, påverkas andra system inom verksamheten?
    a. Vilka andra system påverkas?

6. Vad har systemet för holdovertid?

Exempel på holdover-tid

En klocka som inte får någon stöttning från en tidskälla kommer att börja driva, det vill säga gå mer och mer fel. Om klockan har krav på en tidsnoggrannhet på 12 millisekunder och klockan driver med 3 millisekunder per dag har systemet en holdover-tid på 4 dagar.

7. Kan systemet detektera att tidskällan störts ut eller inte längre är tillgänglig?
8. Om GNSS-tid blir utstört, kan systemet fungera, utan åtgärd, så att verksamhetens funktion kan upprätthållas?
    a. Behöver manuell kvittering av fel ske för fortsatt drift av systemet?

4.4.2 Frågor som bör ställas om störning av frekvens

För varje system bör följande frågor om frekvens ställas:

1. Är systemet beroende av frekvens?
2. Vilka krav har systemet på frekvensstabilitet?
   a. Vilka delar av systemet kräver störst frekvensstabilitet?
   b. Finns kravställande dokument om frekvens?

Exempel på frekvenskrav i samhället

Elnätet ska hålla en stabil frekvens runt 50 Hz.

3. Vad synkroniserar systemets frekvens mot?
   a. Är frekvenskällan beroende av GNSS?
4. Vilken är den största frekvensavvikelsen som systemet klarar av?
5. Använder andra aktörer utanför verksamheten systemet och finns frekvensberoende däremellan?
6. Kan systemet detektera att frekvenskällan störts ut eller inte längre är tillförlitlig?
7. Om systemet påverkas på grund av GNSS-störning, påverkas andra system inom verksamheten?
   a. Vilka andra system påverkas?

Exempel konsekvenser av frekvensavvikelse

I elnätet kopplas vissa delar av nätet bort om frekvensavvikelsen är för stor för att inte nätet ska kollapsa.

4.4.3 Frågor som bör ställas om vilseledning av tid

För varje system bör följande frågor om tid ställas:

1. Hur skulle systemet påverkas av en felaktig tidsangivelse?
2. Finns det system, exempelvis tidsbegränsade programvarulicenser, som endast gäller till ett visst datum?
   a. Kommer systemet kunna fungera även efter detta datum?

Exempel konsekvenser av en vilseledningsattack

Vid en vilseledningsattack skulle tiden i ett system kunna flyttas flera år in i framtiden och då finns det risk för att programvarulicenser har gått ut. Det kan vara så att även om systemet får tillbaka rätt tid att program ändå inte fungerar.

3. Finns det incidentloggning vars tidhållning är beroende av GNSS?
   a. Vilka konsekvenser kan fel tid få?

Exempel konsekvenser av felaktig tid

Till exempel kan datorer som inte har rätt tid bli nekade åtkomst till nätverk.

4. Kan systemet fungera ihop med andra system inom verksamheten om det inte har korrekt tid?
5. Hur påverkar fel tid i systemklockan möjligheten att skapa digitala certifikat så som Public Key Infrastructure (PKI)?

4.5 Steg 5. Undersök om det finns redundans hos tid- och frekvensgivning från GNSS

I det femte steget studeras i vilken grad det finns redundans hos de tekniska systemen avseende tid- och frekvenshållning, det vill säga om det finns något alternativt system som träder in för att upprätthålla tid och frekvens om GNSS inte längre är tillgängligt. Genom att förstå redundans i systemen är det även möjligt att få en uppfattning om dess sårbarhet i förhållande till leverans av tid och frekvens via GNSS. Redundansen påverkas även av faktorer såsom hur länge ett bortfall varar. Exempelvis skulle en bank klara ett längre bortfall av tid om det finns tillgång till egna tidsservrar av god kvalité som kan ge systemen en lång holdover-tid. Även NTP-servrar kan oftast leverera både tid och frekvens.

Redundans för frekvens och tid

De flesta källor som ger tid kan även ge frekvens.

Exempel på källor som kan ge redundant tid och frekvens:

- Multipla tidsservrar som jämför tid mellan systemen och utesluter felaktiga tidkällor.
- Atomur av olika kvalité. Beroende på hur dyr klockan är kan den ge en tillräckligt bra tid i allt från några dagar till flera år.

Varje tekniskt system behöver studeras individuellt för att hitta eventuellt beroende av tid och frekvens. Nedan ges exempel på alternativ för redundans för tid respektive frekvens, samt frågor som ska ställas för respektive system.

4.5.1 Frågor som bör ställas gällande redundans i tid och frekvens

För varje system bör följande frågor ställas för att förstå dess redundans:

1. Har systemet tillgång till flera tid- och frekvenskällor?
    a. Om systemet har flera tid- och frekvenskällor, är alla beroende av GNSS?
2. Har systemet en eller flera tidsservrar?
    a. Är de beroende av GNSS?
3. Har den alternativa klockan samma tidsnoggrannhet och frekvensstabilitet som den primära klockan?
4. Krävs manuella insatser för att den redundanta klockan ska träda in?
    a. Vilken är omställningstiden om manuella åtgärder behövs? Finns exempelvis personer med kompetens på plats?
5. Meddelar systemet när det byter tid- och frekvenskälla?
6. Finns redundans i det tekniska systemet som gör att det kan fungera trots att tid eller frekvens från GNSS har störts?
7. Hur länge kan systemet klara sig utan GNSS-signaler?

4.6 Steg 6. Undersök hur prioriterade åtaganden påverkas om tid eller frekvens via GNSS störs eller vilseleds

Efter att i steg 2–5 identifierat att det inom verksamheten finns tekniska system som är beroende av GNSS är det dags att fördjupa sig i dessa beroenden. Steg 6 innebär att undersöka vilka av verksamhetens prioriterade åtaganden som kan komma att påverkas och hur det inverkar på funktionerna.

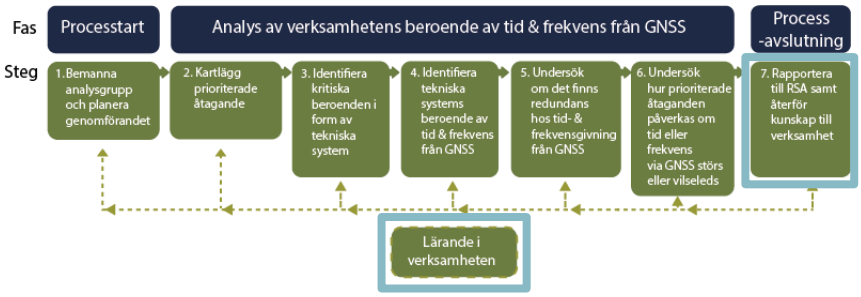
Även om tekniska system använder sig av GNSS-styrd tidgivning via exempelvis en GNSS-tidsserver så behöver störning eller vilseledning av GNSS inte ge en nämnbar påverkan på verksamheten. Exempelvis om det finns alternativa system som träder in eller om det går att förändra arbetssättet för att säkerställa de prioriterade åtagandena. I andra fall kan det motsatta vara fallet, vilket innebär att störning eller vilseledning av GNSS medför att samhällsviktig verksamhet eller prioriterade åtaganden inte kan utföras.

Nedanstående frågor ställs för att förstå vilken betydelse som respektive tekniskt system har för verksamheten. Frågorna ska därför besvaras för respektive system (steg 4) utifrån de viktiga funktioner som verksamheten ska leverera (steg 2):

1) Vilka av de tekniska system som är beroende av GNSS är av avgörande betydelse för att de prioriterade åtagandena ska kunna säkerställas?
2) Finns något alternativt system eller arbetssätt som gör det möjligt att genomföra verksamheten även om det primära tekniska systemet inte fungerar på grund av bortfall av tid eller frekvens från GNSS?
    a) Kan det alternativa systemet eller arbetssättet leverera det som behövs för att verksamheten ska fungera?
    b) Hur länge kan detta alternativa system eller arbetssätt fungera om det primära GNSS-beroende systemet har fallit bort?
3) Vad innebär det för verksamhetens prioriterade åtaganden att det primära GNSS-beroende systemet inte fungerar eller inte fungerar optimalt?
    a) Kan verksamhetens prioriterade åtaganden inte alls uppfyllas?
    b) Kan verksamhetens prioriterade åtaganden delvis uppfyllas och vad är det som i så fall fungerar respektive inte fungerar?
4) Påverkar GNSS-störningens längd i tid hur omfattande konsekvenserna blir? På vilket sätt?
5) Är konsekvensen av GNSS-störning beroende av när på året som störningen inträffar? Hur och varför?
6) Är konsekvensen av GNSS-störning beroende av när på dygnet som störningen inträffar? Hur och varför?

Steg 6 är den sista delen i den systematiska arbetsgångens andra fas.

4.7 Steg 7. Rapportera till RSA samt återför kunskap till verksamhet



Det sjunde och avslutande steget handlar om att säkerställa att den förvärvade kunskapen om tekniska beroenden av GNSS och deras potentiella betydelse för verksamheten beaktas samt redovisas i relevanta organisationers RSA. De sårbarheter som har upptäckts gällande de tekniska systemens beroende av tid och frekvens samt hur störning och vilseledning kan påverka verksamheten bör synliggöras för att också kunna identifiera, prioritera och eventuellt genomföra åtgärder. Genom att beskriva detta i verksamhetens RSA kan kunskapen när den rapporteras vidare uppåt i hierarkin hjälpa myndigheter, till exempel MSB, att få en helhetsbild av de risker och sårbarheter som finns på grund av samhällets beroende av GNSS.

Även annan form av återföring av kunskapen från analysen till organisationen utöver RSA är viktig för att synliggöra potentiella problem samt införa åtgärder. Det kan handla om att se över krav på system och toleranser för systemets robusthet. Det handlar både om att säkra de primära tekniska systemen och om att göra verksamheten robustare ifall de primära systemen fallerar.

5 Avslutande ord

Frågan är egentligen inte *om* tekniska beroenden inom verksamheter och samhällsviktig verksamhet finns, utan *vilka* dessa beroenden är och vad det innebär om tid och frekvens påverkas genom bortfall eller vilseledning. Störning och vilseledning av GNSS är ett återkommande och ökande problem i Sveriges närområde. Det är därför motiverat att aktörer på alla samhällsnivåer bör veta vilka tekniska beroenden av korrekt tid och frekvens via GNSS som föreligger, samt hur aktörens samhällsviktiga verksamhet kan påverkas om GNSS är stört eller vilselett.

Ett första steg för att minska sårbarheter vid tekniska beroenden av tid och frekvens via GNSS är att identifiera var dessa beroenden finns. Metodstödets systematiska arbetsgång kan hjälpa till att identifiera tekniska beroenden och bidra till att skapa förståelse för hur dessa beroenden kan inverka på aktörens prioriterade åtaganden såväl inom egen verksamhet eller inom ramen för deras roll som sektorsansvarig eller geografiskt områdesansvarig. Det ger möjlighet att på sikt införa åtgärder för att stå bättre rustade mot framtida störning och vilseledning, både inom den egna verksamheten men också för Sverige som nation. Genom att i verksamhetens RSA och RSB lyfta beroenden och eventuella sårbarheter kan en nationell överblick av samhällets beroenden av GNSS skapas. En risk med en sådan samlad kunskap är att den skulle kunna skapa en ökad sårbarhet för Sverige och möjliggöra antagonistiska handlingar. Sekretessbedömningar sker dock redan i arbetet med RSA [46] och bör även omfatta tekniska beroenden av tid och frekvens via GNSS.

En förhoppning är att denna rapport kan bidra till att på kort sikt stötta aktörer i att identifiera och förstå sina tekniska beroenden, och skapa förutsättningar för att olika aktörer i ett senare steg genomföra åtgärder som minskar de negativa effekter som kan uppstå i verksamheters funktioner om GNSS störs eller vilseleds. Metodstödet är en första version som inte har testats hos aktörer och den praktiska användbarheten är svår att bedöma helt säkert. Ett test och och en validering skulle göra det ännu mer anpassat efter behoven i beredskapssystemet. Förhoppningen är dock att det redan nu kan vara till hjälp för att identifiera tekniska beroenden och hur verksamheter påverkas vid störning eller vilseledning av GNSS avseende tid och frekvens, för att på så sätt skapa en ökad medvetenhet om verksamheters sårbarheter. Några av de fortsatta utvecklingsområden som har identifierats under arbetets gång är:

- Den systematiska arbetsgången har en generell karaktär som möjliggör egna avgränsningar. Det innebär att det är möjligt att i analysen fokusera enbart på den egna verksamheten, samtidigt kan analysen breddas till att omfatta en sektor eller ett geografiskt område. En fördel med detta är att en bred målgrupp kan använda sig av stödmaterialet och anpassa det till sitt analysbehov. Samtidigt som stödet blir mindre detaljerat.
- Det är önskvärt att i metodstödet inkludera frågor och beskrivningar som kan användas för att identifiera möjliga åtgärder för att minska sårbarheter, och för att värdera hur betydelsefulla konsekvenserna av en GNSS-störning är för verksamheten för att därmed kunna prioritera mellan olika åtgärder. Det är rimligt att anta att vissa följder från GNSS-påverkan har minimal eller ingen inverkan på tekniska system medan andra kan vara helt avgörande för verksamheten. Med hjälp av konsekvensnivåer är det enklare att föreslå lämpliga åtgärdsstrategier inklusive var åtgärder ska prioriteras i de tekniska systemen eller i själva verksamheten.
- Ytterligare ett förslag på vidareutveckling av metodstödet är att det även kan omfatta om och hur det analyserade tekniska systemet kan återställas efter att GNSS-påverkan upphört.

Referenslista

[1] B. Reichel och J. Ingemarsdotter, ”Samhällets beroende av rymdinfrastruktur. En översikt och analys av konsekvenserna för utvecklingen av det civila försvaret,” FOI-R--5610--SE, 2023.

[2] S. Lindström och K. Hallgren, ”Rymden är en ny arena för krigföring i Strategisk utblick – framtida hot,” FOI-R--5103--SE, Stockholm, 2021.

[3] MSB, ”Vikten av var och när. Samhällets beroende av korrekt tids- och positionsangivelse,” 2014.

[4] FOI, ”Omvärldsanalys Rymd 2023. Fokus på försvar och säkerhet,” 2023.

[5] Regeringen, ”En nationell säkerhetsstrategi,” Skr 2023/24:163, 2024.

[6] Försvarsdepartementet, ”Rymdens roll i ett nytt säkerhetspolitiskt läge. Sveriges försvars- och säkerhetsstrategi för rymden,” 2024.

[7] S. Bergström och S. Nilsson, ”Globala satellitnavigeringssystem: En översikt över öppna signaler och tjänster,” FOI-R--5610--SE, 2024.

[8] EUSPA, ”GNSS and Secure SATCOM User Technology report 1,” Publications Office of the European Union, Luxembourg, 2025.

[9] M. A. Lombardi, ”An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Positioning System (GPS),” NIST Technical Note 2189, 2021.

[10] RISE, ”RISE har koll på tiden,” [Online]. Available: https://www.ri.se/sv/rise-har-koll-pa-tiden. [Använd 2025-09-08].

[11] Nationalencyklopedin, ”hertz,” [Online]. Available: https://www.ne.se/uppslagsverk/encyklopedi/lång/hertz. [Använd 2025-11-19].

[12] NIST, ”How Do Atomic Clocks Work?,” [Online]. Available: https://www.nist.gov/atomic-clocks/how-do-atomic-clocks-work. [Använd 2025-09-09].

[13] Internet Engineering Task Force, ”Network Time Protocol Version 4: Protocol and Algorithms Specification,” [Online]. Available: https://datatracker.ietf.org/doc/html/rfc5905. [Använd 2025-11-19].

[14] Internet Engineering Task Force, ”Precision Time Protocol Version 2 (PTPv2) Management Information Base,” [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8173. [Använd 2025-11-19].

[15] Government Office for Science, ”Satellite-derived Time and Position: A Study of Critical Dependencies GPS,” 2018.

[16] V. Hedtjärn Swaling, ”Beroende av korrekt tid i elsystem,” FOI Memo 5069, 2015.

[17] US Air Force, ”Evolution of GPS: From Desert Storm to today's users,” 2016.

[18] L. Höller, ”Researchers home in on origins of Russia’s Baltic GPS jamming,” Defence News, 2/7 2025.

[19] OPS GROUP, ”GPS Spoofing - Final report of the GPS spoofing workgroup,” 2024.

[20] S. Scoles, ”Spoof, Jam, Destroy: Why We Need a Backup for GPS,” Wired, 2 3 2018. [Online]. Available: https://www.wired.com/story/spoof-jam-destroy-why-we-need-a-backup-for-gps/. [Använd 2025-11-20].

[21] C. Baraniuk, ”UK radio disturbance caused by satellite network bug,” BBC, 2 2 2016. [Online]. Available: https://www.bbc.com/news/technology-35463347. [Använd 2025-11-20].

[22] C. Curry, ”The Impact of the GPS UTC Anomaly Event of 26 January 2016 on the Global Timing Community,” i *Proceedings of the 48th Annual Precise Time and Time Interval Systems and Applications Meeting*, Monterey, California, 2017.

[23] A. Pettersson, ”Driftstörningar i Minicall åtgärdade,” Techtidningen, 20 2 2007. [Online]. Available: https://techtidningen.se/driftstorningar-i-minicall-atgardade/. [Använd 2025-11-20].

[24] MSB, ”Störningar i satellitbaserade navigationssystem,” MSB1963 , 2022.

[25] Transportstyrelsen, ”Kraftig ökning av GPS-störningar i Östersjön,” 4 9 2025. [Online]. Available: https://www.transportstyrelsen.se/sv/om-oss/pressrum/nyhetsarkiv/2025/kraftig-okning-av-gps-storningar-i-ostersjon/. [Använd 2025-11-20].

[26] MSB, ”Nationell risk- och sårbarhetsbedömning (NRSB),” 2025.

[27] MSB, ”Lista viktiga samhällsfunktioner - Utgångspunkt för att stärka samhällets beredskap,” MSB 1844 , 2023.

[28] Försvarsdepartementet, ”Förordning om statliga myndigheters beredskap,” 2022:524, 2022.

[29] *Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.*

[30] MSB, ”Om risk- och sårbarhetsanalyser,” [Online]. Available: https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/beredskap-for-aktorer/risk--och-sarbarhetsanalyser/om-risk--och-sarbarhetsanalyser/. [Använd 2025-11-21].

[31] MSB, ”Myndigheten för samhällsskydd och beredskaps föreskrifter om landstings risk- och sårbarhetsanalyser,” MSBFS 2015:4, 2015.

[32] MSB, ”Myndigheten för samhällsskydd och beredskaps föreskrifter om landstings risk- och sårbarhetsanalyser,” MSBFS 2015:4, 2015.

[33] MSB, ”Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters redovisning av risk- och sårbarhetsbedömningar,” MSBFS 2024:5, 2024.

[34] M. Winehav, B. Nevhage, E. Veibäck, P. Larsson, M. Stenström och M. Mobjörk, ”Underlag till nationell riskbedömning 2012. Resultat från den svenska nationella riskbedömningen 2012,” FOI-R--3612--SE, 2013.

[35] Hedtjärn Swaling och Mossberg Sonnek, ”NCS3 - Beroenden till industriella informations- och styrsystem,” 2016.

[36] MSB, ”Översikt över metoder för komplex beroendenanlys på sektoriell & tvärsektoriell nivå,” 2013.

[37] De Sousa, ”Analysing space dependencies,” 2022.

[38] J. Bengtsson , C. Eriksson och M. Olsson, ”IT-system med externa anslutningar - Metod för analys av verksamheters beroenden,” FOI-R--5306--SE, 2022.

[39] MSB, ”Stöd i risk- och sårbarhetsanalys,” [Online]. Available: https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/beredskap-for-aktorer/risk--och-sarbarhetsanalyser/stod-i-risk--och-sarbarhetsanalys/.

[40] MSB, ”Metod för identifiering av samhällsviktig verksamhet,” 2023.

[41] MSB, ”Vägledning för att identifiera samhällsviktig verksamhet som är nödvändig för totalförsvaret,” 2023.

[42] Livsmedelsverket , ”SRSA: sektorsövergripande risk och sårbarhetsanalys - en metodutveckling med utgångspunkt i livsmedelskedjan,” 2015.

[43] MSB, ”Faller en – faller då alla? En slutredovisning från KBM:s arbete”.

[44] Nationalencyklopedin, ”tekniskt system,” [Online]. Available: https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/tekniskt-system. [Använd 2025-11-21].

[45] Västra Götalandsregionen, ”Risk- och sårbarhetsanalys Västra Götalandsregionen 2023–2026,” 2024.

[46] MSB, ”Sekretess i risk- och sårbarhetsanalys,” 2025. [Online]. Available: https://www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/beredskap-for-aktorer/risk--och-sarbarhetsanalyser/sekretess-i-risk--och-sarbarhetsanalys/. [Använd 2025-10-02].

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se