



Gemensamma grunder ► **Arbetssätt**

Samband

Handbok för civilt försvar



**Myndigheten
för civilt försvar**

Samband – Handbok för civilt försvar

Myndigheten för civilt försvar
651 81 Karlstad

Produktion: Advant
Språklig bearbetning: Expertinfo

Publikationsnummer: MCF0098 – mars 2026
ISBN-nummer: 978-91-7927-723-9

Förord

Samband är mer än teknik. Det är förmågan att dela rätt information, i rätt tid, på ett sätt som stödjer ledning och samverkan – även när läget är osäkert, resurserna är ansträngda och flera aktörer behöver agera tillsammans.

Den här handboken är en del av ramverket Gemensamma grunder för ledning och samverkan, och har tagits fram för att stärka just den förmågan. Innehållet bygger på ett aktörsgemensamt arbete inom totalförsvaret, lett av arbetsgruppen Samband Civilt försvar, på uppdrag av Forum Teknik och lokaler för ledning och samverkan. Arbetsgruppen har samlat representanter från beredskapsmyndigheter, regioner och kommuner för att säkerställa bredd och relevans.

Handboken är inte ett kravställande dokument. Den beskriver vad som behöver vara på plats för att sambandet ska fungera i praktiken. Istället erbjuder den gemensamma begrepp, principer och metoder som stöd i det egna arbetet. Den utgår från att aktörer har olika uppdrag, organisationer och tekniska lösningar – men att behovet av fungerande samband är gemensamt.

Förhoppningen är att handboken ska bidra till ökad samstämmighet mellan aktörerna, stärkt samverkan och ett samband som är robust, begripligt och användbart när det behövs som mest.

Arbetet med att utveckla en gemensam grund för sambandet är inte avslutat med denna handbok. Det fortsätter i praktiken – i planering, övning, samverkan och erfarenhetshantering. Era synpunkter och erfarenheter är en del av den utvecklingen och välkomnas därför.

Tillsammans stärker vi förmågan att leda och samverka när det verkligen gäller.

Mer information finns på mcf.se/samband.

Innehåll

1. Handboken – ett stöd för att skapa sambandsförmåga	9
1.1 Varför behövs en handbok för samband?	9
1.2 Vem riktar sig handboken till?	10
1.3 Hur handboken avgränsats och byggts upp	10
2. Samband – avgörande för ledning och samverkan	13
2.1 Centrala begrepp för samband	14
2.2 Grundläggande principer för samband	14
2.2.1 Sambandets syfte	14
2.2.2 Sambandstjänst	15
2.3 Så används samband i praktiken	15
2.3.1 Den som begär information anvisar sambandsväg	15
2.3.2 Sambandsnoder	15
2.4 Interoperabilitet – förmågan att fungera tillsammans	16
3. Hot mot sambandet	19
3.1 Hotaktörerna och deras intressen	19
3.2 Tillvägagångssätt för att hota samband	20
3.2.1 Signalspaning	20
3.2.2 Störsändning (jamming)	21
3.2.3 Falsk signalering (spoofing)	21
3.2.4 Hot från insidan (insiderhot)	21
3.2.5 Artificiell intelligens (AI)	22
3.3 Medvetenhet om hoten och hantering av avvikelser	22
4. Skydda informationen	25
4.1 Informationssäkerhet måste alltid beaktas	26
4.1.1 Informationsklassning – informationen måste alltid värderas	26

4.2	Säkerhetsskydd – när sambandet rör Sveriges säkerhet.....	27
4.2.1	Säkerhetskänslig verksamhet.....	27
4.2.2	Säkerhetsskyddsklassificerade uppgifter.....	27
4.2.3	Höjd beredskap och säkerhetsskydd.....	28
4.3	Signalskydd – för att skydda säkerhetsskyddsklassificerade uppgifter.....	28
4.3.1	Signalskyddssystem.....	30
4.3.2	Signalskyddsnycklar och certifikat.....	30
4.3.3	Signalskyddsgrader.....	31
5.	Sambandssystemet och dess komponenter.....	33
5.1	Vad är ett sambandssystem?.....	33
5.2	Sambandsmedel – tekniken som används.....	34
5.2.1	Användargränssnitt – det som användaren ser.....	34
5.2.2	Bärare – tekniken som överför informationen.....	35
5.2.3	Transmission – hur informationen tekniskt överförs.....	35
5.3	Informationstyper.....	36
5.4	Påverkansfaktorer – när sambandet inte fungerar som planerat.....	37
5.4.1	Väder och naturfenomen.....	37
5.4.2	Solaktivitet och rymdväder.....	37
5.4.3	Tekniska fel och systemberoenden.....	37
5.4.4	Mänskliga fel.....	37
5.5	Exempel på ett sambandssystem.....	38
6.	Metoder – så förmedlas information i praktiken.....	41
6.1	Kontrollera att sambandet fungerar.....	41
6.1.1	Förbindelseprov – hur går det till?.....	42
6.2	Passning – när och hur vi är nåbara.....	42
6.2.1	Passningsalternativ för tal och video.....	43
6.2.2	Passningsalternativ för text och data.....	43
6.3	Prioritering av information – när allt inte kan hanteras samtidigt.....	43

6.4	Sätt att överföra information.....	44
6.4.1	Signaldisciplin – att använda samband på rätt sätt.....	44
6.4.2	Principen T2S2 (Tänk–Tryck–Sänd–Släpp).....	45
6.4.3	Talad informationsöverföring via radio.....	46
	Struktur för talsamtal.....	46
	Trafikuttryck – gemensamt språk för tydlighet och tempo.....	47
	Adressering och anrop.....	48
6.4.4	Återläsning – när korrekthet är kritisk.....	49
6.4.5	Viasignalering – när direkt samband saknas.....	50
6.4.6	Ordonnans – fysisk överföring av information.....	50
6.5	Spårbarhet.....	51
6.5.1	Spårbarhet genom diaries, tidsnummer och loggar.....	51
6.5.2	Spårbarhet genom trafiklista.....	51
6.5.3	Kvittens och mottagningsbevis.....	52
7.	Organisation för sambandstjänst.....	55
7.1	Sambandsorganisation	55
7.1.1	Sambandsfunktion i ett normalläge.....	56
7.1.2	Sambandsfunktion vid hantering av samhällsstörningar.....	56
7.2	Principer för sambandsorganisationens uppbyggnad.....	57
7.2.1	Bemannings, uthållighet och redundans.....	57
7.3	Roller, ansvar och nivåer inom sambandsorganisationen.....	58
7.3.1	Administrativ nivå.....	59
	Sambandschef (Sbch).....	59
	Sambandsansvarig (SA).....	59
7.3.2	Operativ nivå: Sambandsledning.....	60
	Sambandsledare (Sbled).....	60
7.3.3	Operativ nivå: Genomförande.....	60
	Sambandsoperatör (SbOp).....	60
	Sambandstekniker (SbTekn).....	60

8. Sambandsplanering	63
8.1 Varför behövs sambandsplanering?	63
8.2 Sambandsplan – vad är det?	63
8.3 Process för sambandsplanering	64
8.3.1 Steg 1: Lednings- och samverkansanalys	65
8.3.2 Steg 2: Sambandsbedömning – val av sambandssystem: Hur möter vi behoven?	65
Sambandsöversikt som stöd	66
8.3.3 Steg 3: Upprätta sambandsplan	67
PACE – en modell för kontinuitetshantering	68
Sambandsanvisning – från plan till genomförande	69
Beskrivning av sambandsvägar	70
8.4 Relaterade dokument	72
8.4.1 Sambandskatalog	72
8.4.2 Ordonnansplan	72
9. Utbildning, träning och övning	75
9.1 Skillnaden mellan utbildning, träning och övning	75
9.1.1 Utbildning	75
9.1.2 Träning	75
9.1.3 Övning	76
9.1.4 Utvärdering och erfarenhetshantering	76
9.2 Befintliga utbildningar	76
9.3 Utveckling av utbildningar framåt	76
Bokstaveringsalfabetet	78

Kapitel 1

Handboken – ett stöd för att skapa sambandsförmåga

1. Handboken – ett stöd för att skapa sambandsförmåga

Samband är ett samlingsbegrepp för den teknik, de regler och de metoder som vi använder för att överföra information. Denna handbok ger en gemensam grund för samband inom det civila försvaret. Handboken beskriver nationella principer, gemensamma begrepp och arbetssätt som skapar förutsättningar för effektivisering, standardisering och interoperabilitet inom totalförsvaret.

I praktiken använder de flesta aktörer redan samband i sin vardag, eftersom i princip all verksamhet bygger på att information delas mellan människor och funktioner. Att arbeta med samband handlar därför inte om att införa något nytt, utan om att skapa struktur och medvetenhet kring hur informationsöverföring sker. Genom att göra sambandet till en del av kontinuitets- och beredskapsplaneringen blir det lättare att säkerställa att rätt information når fram när det verkligen behövs.

För att aktörer inom krisberedskap och civilt försvar ska kunna leda och samverka krävs att information kan överföras snabbt, tydligt och tillförlitligt. Utan fungerande samband riskerar ledning och samverkan att försvåras i avgörande lägen – i vardagen, vid fredstida kriser, vid höjd beredskap och krig.

1.1 Varför behövs en handbok för samband?

Handboken ger ett gemensamt språk, gemensamma arbetssätt och gemensamma principer för samband inom det civila försvaret genom att

- beskriva regler, metoder och begrepp som tillsammans utgör sambandet
- skapa en gemensam och teknikneutral grund för sambandstjänsten
- ge stöd i att planera, upprätta och använda samband
- öka förståelsen för sambandets betydelse inom totalförsvaret.

Målet är att du som aktör ska kunna säkerställa din egen och den gemensamma sambandsförmågan i din yrkesroll – oavsett beredskapsläge.

1.2 Vem riktar sig handboken till?

Handboken riktar sig särskilt till chefer, samordnande funktioner och medarbetare som i sin roll ansvarar för eller är beroende av fungerande informationsöverföring.

Handboken riktar sig till tre huvudgrupper:

1. Personer som redan arbetar med samband och behöver en samlad och enhetlig grund.
2. Personer som inte har sambandsbakgrund men behöver förstå och använda samband i sin yrkesroll.
3. Personer som behöver en överblick utan att gå in i detaljer.

1.3 Hur handboken avgränsats och byggts upp

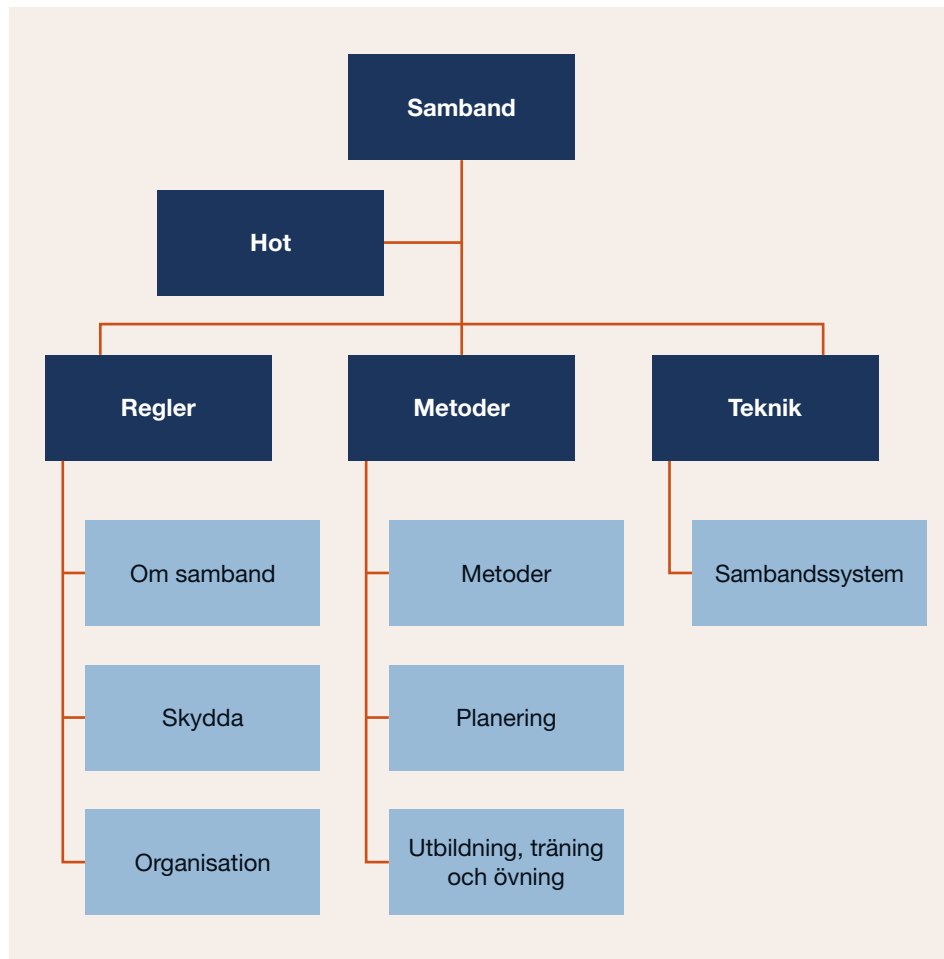
I denna utgåva behandlas samband och informationsöverföring mellan svenska aktörer. Internationella perspektiv och ytterligare systemstöd kommer att utvecklas i kommande versioner.

Handboken är uppbyggd för att spegla sambandsförmåga som en helhet, där flera olika delar behöver fungera tillsammans för att informationsöverföring ska fungera i praktiken. Samband handlar inte enbart om teknik utan även om vikten av att ha gemensamma regler, metoder, organisation och utbildning.

Figur 1 visar hur sambandsförmåga byggs upp av flera samverkande delar. Alla delar behöver inte vara lika omfattande hos alla aktörer – men de behöver finnas med och hänga ihop. Handboken kan därför läsas både sammanhängande och selektivt.

Figur 1 visar hur handbokens kapitel är strukturerade under begreppet samband. Samband delas in i tre huvudområden: *Regler*, *Metoder* och *Teknik*. I *Regler* ingår kapitlen om samband, att skydda informationen och organisation. I *Metoder* ingår kapitlen om metoder, planering samt om utbildning, träning och övning. I *Teknik* ingår kapitlet om sambandssystem. Hot visas som en övergripande påverkansfaktor kopplad till sambandsbegreppet.

Figur 1. Hur bokens kapitel kan sorteras in under sambandsbegreppet



Så tolkar du orden "ska" och "måste"

För att särskilja rekommendationer från juridiska krav används två olika ord i handboken:

Ska används för att markera sådant som behöver vara på plats för att sambandet ska fungera i praktiken. Ordet anger nödvändiga förutsättningar för effekt i ledning och samverkan, men innebär inte ett juridiskt krav.

Måste används enbart när det finns ett uttryckligt krav i lag, förordning eller annan bindande reglering. I dessa fall hänvisar handboken till relevant regelverk.

Kapitel 2

Samband – avgörande för ledning och samverkan

2. Samband – avgörande för ledning och samverkan

Samband är grunden för att kunna överföra information inom och mellan aktörer. Det här kapitlet beskriver vad samband är, och förklarar hur det skiljer sig från kommunikation. Dessutom introduceras några centrala begrepp, vilka principer som gör det användbart i praktiken och några gemensamma arbetssätt som återkommer i resten av handboken.

Det gemensamma begreppet samband

Samband är ett samlingsbegrepp för teknik, regler och metoder som möjliggör informationsöverföring. Begreppet samband används även för att beskriva en förbindelse mellan och inom aktörer.¹



Not 1. Definitionen bygger på Försvarmaktens definition och används här för att skapa samsyn inom totalförsvaret.

2.1 Centrala begrepp för samband

Tabell 1 förklarar de begrepp som återkommer genom handboken.

Tabell 1. Centrala begrepp för samband

Begrepp	Förklaring
Samband	Samlingsbegrepp för teknik, regler och metoder för informationsöverföring. Begreppet används även för att beskriva en förbindelse mellan och inom aktörer.
Informationsförsörjning	Att förse verksamheten med nödvändig information för att lösa sina uppgifter.
Informationsöverföring	Den faktiska förflyttningen av information från en aktör eller funktion till en annan.
Förbindelse	Fysisk eller logisk koppling som möjliggör informationsöverföring mellan funktioner.
Aktör	En formell organisation, antingen offentlig, privat eller ideell, eller spontant socialt nätverk, som har betydelse för hanteringen av samhällsstörningar.
Teknik	De tekniska lösningar som överför information.
Regler	Styrningar som anger hur tekniken och metoderna får och ska användas.
Metoder	Rutiner och instruktioner som underlättar och likriktar användningen av tekniken.

2.2 Grundläggande principer för samband

Begreppen samband och kommunikation används ibland som synonymer. I vardagligt språk används kommunikation brett, till exempel för information till allmänheten, intern dialog eller transport av budskap. Därför bör vi konsekvent säga samband när vi pratar om informationsöverföring som behövs för ledning och samverkan mellan aktörer. Samband är nämligen redan ett vedertaget begrepp i både civila och militära organisationer och hjälper oss att avgränsa innehållet.

2.2.1 Sambandets syfte

För att utöva ledning samt för att uppnå samverkan krävs en förmåga att överföra information, både inom den egna aktören och med andra aktörer. Sambandets syfte är att möjliggöra informationsöverföring. Det gör att aktörer kan skapa en gemensam lägesbild, ge inriktning och samordna åtgärder.

Behovet av samband varierar mellan aktörer beroende på uppgift, informationsbehov och geografisk spridning mellan dem som ska överföra informationen. Därför behöver sambandet kunna anpassas – men bygga på gemensamma begrepp och arbetssätt.

2.2.2 Sambandstjänst

Sambandstjänst är den organiserade verksamhet som ser till att informationsöverföringen fungerar i praktiken, inklusive styrning för hur informationen ska överföras. Syftet med sambandstjänst är att möjliggöra fungerande informationsöverföring.

Sambandstjänsten omfattar allt från att planera, bygga upp och driva de system som gör att information kan överföras mellan olika aktörer, till alla rutiner och den kompetens som krävs för att information ska kunna överföras på ett snabbt, tydligt och säkert sätt. Den omfattar också styrningar för att anordna, upprätta, betjäna, underhålla, skydda och bryta eget samband.

Exempel på vad sambandstjänst kan omfatta:

Radiosystem, nätverk, kryptering, rutiner och utbildning av personal. För totalförsvaret kan sambandstjänst omfatta allt från Rakel och mötestjänster till gemensamma rutiner för kvittens, kontaktvägar och skydd av information.

Hur samband och sambandstjänst förhåller sig till varandra:

Samband är själva förbindelsen, medan sambandstjänst är arbetet som gör att förbindelsen finns och fungerar.

2.3 Så används samband i praktiken

Våra gemensamma arbetssätt styr hur samband används i vardag, vid kriser och vid höjd beredskap och krig. Fokus ligger på ansvar, roller och enkla principer som gör att informationsöverföringen fungerar även när förutsättningarna förändras. Därför är det viktigt att veta hur sambandsvägar anvisas, hur aktörer kan stödja varandra och hur man gör för att hålla informationen kort, tydlig och spårbar.

2.3.1 Den som begär information anvisar sambandsväg

Den aktör som begär information ansvarar för att ange hur informationsöverföringen ska ske, till exempel kanal, kontaktväg och kvittens. Det innebär inte att ett nytt samband måste skapas varje gång. Om det redan finns en planerad eller upprättad sambandsväg som uppfyller behoven kan den användas rutinmässigt.

2.3.2 Sambandsnoder

Om två aktörer saknar möjlighet till direkt samband kan en tredje aktör fungera som sambandsnod och hjälpa till att anvisa kontaktvägar. Det kan ske via en utsedd kontaktpunkt (så kallad POC, Point Of Contact) eller via en sambandsplan. I vissa fall kan nodaktören även förmedla information vidare (viasignalering).



Viktigt att tänka på gällande sambandsnod

En sambandsnod kan inte alltid hantera alla typer av information. Vid säkerhetsskyddsklassificerade uppgifter eller annan skyddsvärd information behöver aktörerna bedöma vilka samband och vilka informationsvägar som är tillåtna och lämpliga.

2.4 Interoperabilitet – förmågan att fungera tillsammans

Interoperabilitet är förmågan hos olika aktörer att fungera tillsammans, både tekniskt, organisatoriskt och i arbetssätt. För samband innebär det att aktörer kan nå varandra, förstå varandra och använda överenskomna metoder – även under press. För att uppnå interoperabilitet behöver val av sambandssystem för samverkan göras gemensamt av de aktörer som berörs.

Handboken tar upp interoperabilitet ur sex perspektiv:

Metod, semantik, teknik, social, organisation och juridik.

Tabell 2. Perspektiv för interoperabilitet

Perspektiv	Handbokens tolkning
Metod	Gemensamma metoder krävs för att kunna överföra information mellan aktörer på ett effektivt sätt.
Semantik	Genom att använda samma begrepp med gemensamma definitioner skapas effektivitet samtidigt som missförstånd och feltolkningar undviks.
Teknik	De tekniska system som används behöver vara gemensamma alternativt ha gemensamma kontaktytor.
Social	Personer som ingår i sambandsorganisationerna behöver dels ha gemensamma förutsättningar i form av utbildningar, dels ha förtroende för varandra.
Organisation	Genom att ha organisationer med väldefinierade roller förenklas kontakterna mellan aktörerna.
Juridik	Författningar, regleringar och annan juridisk styrning behöver antingen tolkas på samma sätt eller att aktörernas olika tolkningar förmedlas till andra inblandade aktörer för att få perspektivförståelse.

! Vanliga fallgropar i samband

- **Begrepp blandas** – till exempel informationsdelning, informationsöverföring, samband och kommunikation.
- **Tekniken får för stort fokus** – medan gemensamma rutiner och roller saknas eller är otydliga.
- **Budskap blir långa och pratiga** – utan tydlig huvudpoäng.
- **Ansvar för sambandsväg är oklart** – det framgår inte vilken roll eller funktion som ska anvisa sambandsväg.
- **Kvittens uteblir** – trots att informationen är kritisk, vilket ökar risken för missförstånd.



? Hur undviker vi fallgroparna?

Använder vi samma begrepp och terminologi inom den egna verksamheten och tillsammans med andra aktörer?

Har vi valt sambandssystem utifrån behov – inte bara teknik?

Och har vi säkerställt att rutiner och roller fungerar i praktiken?

Har vi rutiner för korta och tydliga budskap så att huvudpoängen framgår även under stress?

Har vi beskrivit vilken roll eller funktion som ska anvisa sambandsväg i olika situationer?

Har vi rutiner för kvittens för information som är kritisk eller tidskänslig?

Kapitel 3

Hot mot sambandet

3. Hot mot sambandet

Samband är ett attraktivt mål för hotaktörer som vill påverka, störa eller utnyttja samhällsviktig verksamhet. För att kunna skydda information och upprätthålla fungerande samband behöver vi ha en grundläggande förståelse för hur hot mot samband kan se ut och olika tillvägagångssätt. Det här kapitlet beskriver vanligt förekommande hot mot samband och olika sätt att försöka påverka informationsöverföring.

3.1 Hotaktörerna och deras intressen

Hot mot sambandet kan komma från olika typer av hotaktörer, men i detta sammanhang avses aktörer som har förmåga och intresse av att påverka, störa eller ta del av informationsöverföring. Information som kontinuerligt samlas in rör politik, försvar och ekonomi, men även teknik, innovation och information inom strategiska sektorer.² Samverkan mellan olika hotaktörer gör att säkerhetshoten går in i varandra och förstärks, exempelvis genom att skapa splittring och polarisering.

En central hotaktör är främmande makt, där ett flertal statliga aktörer bedriver underrättelseverksamhet och andra säkerhetshotande aktiviteter riktade mot våra nationella intressen och samhällsviktig verksamhet. Men även våldsbejakande extremister, kriminella nätverk och enskilda individer kan utgöra hot mot sambandet. Dessa kan agera självständigt eller fungera som ombud för andra aktörer. Slutligen kan hot också uppstå inifrån den egna organisationen, till exempel genom bristande rutiner, otillräcklig utbildning eller oavsiktliga fel.

De statliga aktörerna kan ha olika mål, till exempel att stärka bilden av den egna staten, kringgå sanktioner, skapa olika former av beroenden mellan det egna landet och andra länder, anskaffa sig teknik och kunskaper eller att påverka eller störa nationella och internationella samarbeten och kommunikationsmöjligheter. De har ofta både teknisk och organisatorisk förmåga att påverka samband över tid.

Not 2. Källa: Säkerhetspolisens årsberättelse 2024–2025.

Främmande makt använder olika verktyg, inklusive hybridkrigföring, för att påverka oss och våra allierade. Metoderna är anpassningsbara och riktas mot alla samhällsnivåer – från nationell till lokal nivå – samt mot både strategiskt viktiga och mindre uppenbara sektorer. För sambandet innebär detta att hot kan uppträda gradvis, indirekt och i kombination. Tabell 3 illustrerar hur olika medel kan kombineras för att påverka ett samhälle utan öppet militärt angrepp.

Tabell 3. Hybridkrigföring (icke-linjär krigföring)

Strategi	Olika medel	Ombud
Att med militära och civila maktmedel uppnå sina strategiska mål utan att bidra till en direkt militär konfrontation eller storskaligt krig.	Kan omfatta allt från konventionella militära medel och cyberkrigföring till desinformation, sabotage, diplomatiska och ekonomiska påtryckningar samt andra påverkansmetoder.	Kan utföras genom ombud som medvetet eller omedvetet agerar i den angripande maktens intresse.

Källa: MUST:s årsredovisning 2024.

3.2 Tillvägagångssätt för att hota samband

Hotaktörer kan påverka sambandet dels genom att störa möjligheten till informationsöverföring – alltså själva förmågan till samband, dels genom att försöka påverka eller ta del av den information som överförs.

Målet med att störa ut ett sambandsmedel kan vara att

- avbryta sambandet helt
- påverka beslut
- tvinga användaren att byta till ett alternativt sambandsmedel med lägre skyddsnivå som är enklare att inhämta information från.

I jakten på information utvecklas ständigt nya metoder. I detta avsnitt beskrivs några av de vanligaste tillvägagångssätten.

3.2.1 Signalspaning

Signalspaning innebär att information inhämtas ur elektroniska signaler, till exempel i radio eller trådbundna system såsom fiber. Genom olika former av bearbetning kan information utvinnas även utan direkt tillgång till innehållet.

All elektronisk utrustning avger i någon mån signaler till omgivningen. Dessa signaler kan fångas upp via elledningar, datanätverk eller via luften. I vissa fall går det att återskapa information som behandlas i ett system genom att analysera dessa utsignaler. Signalerna kan även användas för att positionera den som sänder.

Beakta även akustisk förmedling av information, till exempel risken att obehöriga kan höra samtal. Inget system bör användas för att förmedla information med högre skyddsnivå än vad utrymmet eller omgivningen är godkänd för. Det är alltid den lägsta skyddsnivån i kedjan som sätter gränsen för vilken information som kan hanteras vid ett givet tillfälle.

Hur system placeras, används och skyddas påverkar därmed risken för signalspaning. Signalspaning är därför en central faktor att beakta vid planering och användning av samband, vilket beskrivs mer i kapitel 4 Skydda informationen och kapitel 8 Sambandsplanering.

3.2.2 Störsändning (jamming)

Störsändning innebär att hindra eller försvåra trådlös informationsöverföring genom att sända störande signaler på samma frekvenser som det sambandsmedel som används. På så sätt kan mottagningen försämrats, eller helt utebli.

Störsändning kan riktas mot exempelvis mobiltelefoner, trådlösa larm, GNSS-system³ och sensorer. Detta påverkar verksamheter som är beroende av trådlös kommunikation eller positionering, till exempel för personal, fordon, fartyg eller luftburna system.

3.2.3 Falsk signalering (spoofing)

Falsk signalering innebär att en aktör sänder vilseledande signaler som får mottagaren att uppfatta dem som äkta. Syftet kan vara att inhämta information, skapa förvirring eller styra beteenden.

Exempel på spoofing:

- Telefon-spoofing – telefonbedrägeri där mottagaren ser ett felaktigt avsändarnummer.
- GNSS-spoofing – när falska positionssignaler sänds för att vilseleda system eller användare om något eller någons faktiska position.

3.2.4 Hot från insidan (insiderhot)

Hot från insidan avser personer inom den egna organisationen som medvetet eller omedvetet ökar risken för att information från sambandet röjs eller att samband försvagas. Det kan handla om att dela känslig information, använda sambandsmedel felaktigt eller bidra till sabotage.

Insiderhot kan uppstå genom avsiktlig påverkan från en extern aktör, men också genom bristande kunskap, stress eller otydliga rutiner. Alla organisationer är i någon grad sårbara för denna typ av hot, vilket gör utbildning, tydliga roller och återkommande övningar särskilt viktiga.

Not 3. Global Navigation Satellite System, ett samlingsnamn för samtliga satellitbaserade navigationssystem.

3.2.5 Artificiell intelligens (AI)

Vi behöver vara medvetna om hur ny teknik påverkar hotbilden mot sambandet. Artificiell intelligens (AI) kan användas för att snabbt bearbeta stora mängder information, identifiera mönster och sammanställa underrättelser.

På kort tid har tekniken ökat både effektiviteten i informationsinhämtning och kvaliteten på den data som inhämtats. Samtidigt innebär tekniken att även hotaktörer med begränsade resurser kan höja sin förmåga. AI kan bland annat användas för att ta fram instruktioner, automatisera angrepp eller sprida vilseledande information i stor skala.

Dessutom kan AI förbättra kvaliteten på

- avlyssnad information
- läckt information
- öppet tillgänglig men sammanställd information
- metadata och mönster.

Varje organisation har ett eget ansvar för att identifiera, värdera och skydda information som inte ska spridas till obehöriga – även mot nya tekniska hot som AI kan förstärka.

3.3 Medvetenhet om hoten och hantering av avvikelser

Medvetenhet om både avsiktliga och oavsiktliga hot är en grundförutsättning för ett fungerande samband. När vi förstår hur hot kan uppstå och vilka tillvägagångssätt som kan användas ökar förmågan att upptäcka avvikelser och agera i tid.

För att hantera avvikelser krävs utbildning, tydliga roller och fastställda rutiner. Säkerhetshotande händelser som rör säkerhetskänslig verksamhet ska hanteras i enlighet med gällande regelverk och ska rapporteras.

Ett exempel på åtgärder kan vara att lämna all utrustning (smarta klockor, bilnycklar, mobiltelefoner med mera) som kan sända och ta emot information utanför rummet där samtalet med känslig information ska äga rum.



Är vi medvetna om hoten mot våra samband?

Vilken information överför vi regelbundet via våra sambandsmedel – och vet vi hur skyddsvärd den är för vår verksamhet?

Finns situationer där vi använder alternativa sambandsmedel utan att skyddsnivån eller hotbilden beaktas?

Hur upptäcker vi avvikelser från normalbilden i vår verksamhet – till exempel oväntade störningar, beteenden eller tekniska förändringar?

Vet berörd personal *hur* och *var* incidenter ska rapporteras samt *vad* som ska rapporteras *till vem* vid misstänkta avvikelser?

Kapitel 4

Skydda informationen

4. Skydda informationen

För att samband ska fungera även i krävande situationer behöver både informationen och de system som används skyddas på ett genomtänkt och proportionerligt sätt. Detta kapitel beskriver hur information skyddas genom informationssäkerhet, säkerhetsskydd och signalskydd samt hur dessa områden hänger ihop i sambandstjänsten.



VIKTIGT!

Att skydda informationen är ett ansvar som berör hela verksamheten – det är inte en isolerad teknisk fråga. Informationssäkerhet, säkerhetsskydd och signalskydd behöver tillämpas samordnat och utifrån verksamhetens förutsättningar.

Hur skyddet ska utformas styrs av lagstiftning och andra bindande krav. Denna handbok beskriver principer och samband mellan områdena, men varje aktör ansvarar för att följa tillämpliga regelverk.



4.1 Informationssäkerhet måste alltid beaktas

Information är en central resurs för alla verksamheter. Förmågan att dela rätt information, i rätt tid och på ett tillförlitligt sätt är avgörande för ledning och samverkan. Om information saknas, är felaktig eller otillgänglig kan det få allvarliga konsekvenser för verksamheten.

Informationssäkerhet handlar om att skydda information mot att obehöriga får tillgång till den, att den förvanskas, förstörs eller blir otillgänglig. Ett systematiskt informationssäkerhetsarbete innebär att verksamhetsutövaren identifierar vilken information som är värdefull, bedömer konsekvenserna av bristande skydd och vidtar proportionerliga skyddsåtgärder.

Informationssäkerhet är teknikneutralt och omfattar information oavsett form.

Skyddet utgår från fyra aspekter:

- Konfidentialitet – att förhindra att obehöriga får tillgång till information.
- Riktighet – att informationen är korrekt och inte manipulerad.
- Tillgänglighet – att informationen finns tillgänglig när den behövs.
- Spårbarhet – att det går att följa hur informationen hanterats.



Informationssäkerhet i samband

Informationssäkerhet gäller oavsett om information överförs muntligt, via radio, i it-system eller genom fysiska handlingar.

4.1.1 Informationsklassning – informationen måste alltid värderas

Informationsklassning innebär att verksamhetsutövaren värderar information utifrån vilka konsekvenser ett otillräckligt skydd kan få. Klassningen används som underlag för beslut om vilka skyddsåtgärder som krävs och bidrar till att informationen varken får för lågt eller onödigt högt skydd.

Även sambandsmedel som används för öppen information kan omfattas av säkerhetsskyddsåtgärder, om de utgör en kritisk förmåga i en säkerhetskänslig verksamhet. Exempelvis kan sambandsplaner, programmeringsföreskrifter och systemarkitektur vara skyddsvärda, även om själva informationsinnehållet inte är säkerhetsskyddsklassificerat.

Myndigheten för civilt försvar tillhandahåller metodstöd för systematiskt informationssäkerhetsarbete och Säkerhetspolisen (Säpo) tillhandahåller vägledning för informationssäkerhet inom säkerhetsskydd.

4.2 Säkerhetsskydd – när sambandet rör Sveriges säkerhet

Säkerhetsskydd syftar till att skydda information och verksamheter som är av betydelse för Sveriges säkerhet eller som omfattas av internationella åtaganden om säkerhetsskydd. Säkerhetsskydd ska förhindra att säkerhetsskyddsklassificerade uppgifter röjs och att säkerhetskänslig verksamhet utsätts för sabotage, spioneri eller andra antagonistiska handlingar.

Alla samhällsviktiga verksamheter är inte säkerhetskänsliga. För att en verksamhet ska bedömas som säkerhetskänslig krävs att en antagonistisk handling skulle få konsekvenser på nationell nivå. Däremot kan en samhällsviktig verksamhet innehålla delar som är säkerhetskänsliga, till exempel vissa funktioner, system eller informationsmängder.

Att en verksamhet ingår i totalförsvaret innebär inte per automatik att den är säkerhetskänslig, men det är en tydlig indikator på att behovet av säkerhetsskydd ska analyseras. Det är verksamhetsutövaren som har skyldighet att utreda verksamhetens behov av säkerhetsskydd.

4.2.1 Säkerhetskänslig verksamhet

En verksamhet är säkerhetskänslig om verksamhetsutövaren

- hanterar säkerhetsskyddsklassificerade uppgifter
- omfattas av internationellt åtagande om säkerhetsskydd
- bedriver signalskyddstjänst.

Säkerhetsskydd utgörs av förebyggande åtgärder inom informationssäkerhet, personalsäkerhet och fysisk säkerhet. Säkerhetspolisen tillhandahåller vägledning inom dessa områden.

4.2.2 Säkerhetsskyddsklassificerade uppgifter

Säkerhetsskyddsklassificerade uppgifter är uppgifter som rör säkerhetskänslig verksamhet och som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), eller som skulle ha omfattats av lagen om den varit tillämplig.

Exempel på uppgifter som kan vara säkerhetsskyddsklassificerade:

- Identifierade sårbarheter i säkerhetskänslig verksamhet.
- Beredskaps- och krigsorganisationer.
- Tillgång till ledningsplatser och ledningsstödsystem.
- Kritiska resurser och förmågor.

Uppgifter värderas och klassificeras utifrån vilken skada ett röjande skulle medföra för Sveriges säkerhet. Säkerhetsskyddsklassificeringen avgör vilka skyddsåtgärder, rutiner och sambandslösningar som får användas vid informationsöverföring.

Tabell 4. Säkerhetspolisens tabell för vägledning för indelning i säkerhetsskyddsklass

Säkerhets-skyddsklass	Den skada som ett röjande av uppgifterna kan medföra för Sveriges säkerhet	Värdeord till stöd för bedömningen om en viss typ av skada föreligger
Kvalificerat hemlig	Ett röjande kan medföra en synnerligen allvarlig skada.	Synnerligen allvarliga negativa konsekvenser av stor omfattning, under lång tid, som utgör ett direkt hot mot den nationella förmågan. Konsekvenserna är inte begränsade till enstaka funktioner. Mycket svårt att återställa.
Hemlig	Ett röjande kan medföra en allvarlig skada.	Allvarliga/betydande negativa konsekvenser av stor omfattning eller av väsentlig art, som innebär ett direkt hot mot den nationella förmågan, om än mot avgränsade funktioner. Svårt att återställa.
Konfidentiell	Ett röjande kan medföra en inte obetydlig skada.	Påtagliga negativa konsekvenser för den nationella förmågan, om än i begränsad omfattning, som äventyrar, vållar skada, hindrar, underlättar för en antagonist eller innebär större avbrott.
Begränsat hemlig	Ett röjande kan medföra endast ringa skada.	Ringa negativa konsekvenser som är begränsade till att påverka, försvåra eller störa den nationella förmågan i mindre omfattning.

4.2.3 Höjd beredskap och säkerhetsskydd

Säkerhetsskyddslagen gäller såväl i fred som i krig. En verksamhet vars funktion är av betydelse för Sveriges säkerhet i ett visst beredskapsläge ska betraktas som säkerhetskänslig även i andra lägen. Den säkerhetskänsliga verksamheten ska kunna bedrivas oavsett beredskapsnivå, vilket ställer krav på att säkerhetsskyddet är planerat, etablerat och fungerande redan i fredstid. Säkerhetsskydd kan därför inte byggas upp först när beredskapen höjs, utan behöver vara integrerat i den ordinarie verksamheten.

4.3 Signalskydd – för att skydda säkerhets-skyddsklassificerade uppgifter

Signalskydd är en del av säkerhetsskyddet och omfattar tekniska lösningar och metoder för att skydda säkerhetsskyddsklassificerade uppgifter, exempelvis vid överföring. Signalskydd kan även användas för att skydda säkerhetskänsliga system, såsom styrsystem. Syftet är bland annat att förhindra att obehöriga kan ta del av eller förändra uppgifterna.

När säkerhetsskyddsklassificerade uppgifter ska överföras digitalt mellan aktörer ska skyddet uppfylla kraven i säkerhetsskyddslagstiftningen. Det innebär att godkända kryptografiska funktioner ska användas när uppgifterna överförs i system utanför den egna verksamhetens kontroll. Försvarsmakten godkänner vilka kryptografiska funktioner (signalskyddssystem) som får användas för att skydda säkerhetsskyddsklassificerade uppgifter.

Signalskydd kan användas oavsett sambandsmedel, men för att ge avsedd effekt behöver signalskydd alltid kombineras med lämpliga rutiner, sambandsmetodik och signaldisciplin.

Signalskydd regleras av ett antal lagar, förordningar och föreskrifter. De viktigaste är säkerhetsskyddslagen, säkerhetsskyddsförordningen och Försvarsmaktens föreskrifter om signalskyddstjänsten. I förordningen om totalförsvar och höjd beredskap framgår bland annat vilka myndigheter som ska ha säkra kryptografiska funktioner och när krypterade meddelanden ska kunna tas emot och sändas.

Regelverk för signalskydd

Signalskydd regleras av

- säkerhetsskyddslagen (2018:585)
- säkerhetsskyddsförordningen (2021:955)
- Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten
- förordningen (2015:1053) om totalförsvar och höjd beredskap
- Myndigheten för samhällsskydd och beredskaps föreskrifter (MSB FS 2025:3) om civila myndigheters signalskyddsberedskap.



Viktigt att beakta gällande signalskydd

- Innan säkerhetsskyddsklassificerade uppgifter behandlas i ett informationssystem utanför verksamhetsutövarens kontroll ska verksamhetsutövaren säkerställa att skyddet uppfyller kravet i säkerhetsskyddslagstiftningen.
- Vid kommunikation till system utanför egen kontroll ska kryptografiska funktioner som godkänts av Försvarsmakten användas.
- Varje verksamhetsutövare ansvarar för att identifiera sitt behov av signalskydd i säkerhetsskyddsanalysen. Signalskyddsorganisationen möjliggör den praktiska tillämpningen.
- Om ni identifierar behov av signalskydd i er säkerhetsskyddsanalys men saknar förmåga, behöver ni planera och vidta åtgärder i god tid innan signalskyddet behöver vara på plats.

För mer information se webbkursen *Signalskydd* – en introduktion som finns på mcf.se.

4.3.1 Signalskyddssystem

Ett signalskyddssystem består av signalskyddsmateriel, signalskyddsnycklar eller certifikat, aktiva kort samt en instruktion för hur systemet fungerar och ska hanteras. Utöver det krävs att gällande regelverk följs och att det finns utbildad personal som kan hantera systemet (se faktarutan Regelverk för signalskydd). Alla dessa delar behöver samverka för att ge optimalt skydd.

Det finns olika typer av signalskyddssystem, till exempel:

- **Talkrypto** i form av kryptotelefon.
- **Datakommunikationskrypto** som länkkrypto och VPN-krypto.
- **Meddelandekrypto** i form av faxkrypto och filkrypto. Används filkrypto kan den krypterade filen till exempel sändas via e-post.

Vilket system som kan användas avgörs av vilken säkerhetsskyddsklass uppgifterna har, verksamhetens behov och tillgänglig signalskyddsförmåga.

Signalskyddssystemen finns för olika nivåer av skydd. Signalskyddsgraden för ett system anger vilken säkerhetsskyddsklass systemet är godkänt för att skydda (se tabell 5).

Tabell 5. Signalskyddsgrader

Signalskyddsgrad	Godkänt för att skydda
SG Top Secret	Säkerhetsskyddsklassificerade uppgifter upp till och med kvalificerat hemlig (KH).
SG Secret	Säkerhetsskyddsklassificerade uppgifter upp till och med hemlig (H).
SG Confidential	Säkerhetsskyddsklassificerade uppgifter upp till och med konfidentiell (K).
SG Restricted	Säkerhetsskyddsklassificerade uppgifter upp till och med begränsat hemlig (BH).
SG Trafikskydd	Inte godkänt för att skydda säkerhetsskyddsklassificerade uppgifter, men ger skydd mot trafikanalys, störsändning och falsksignalering.



Skyddar vi vår information?

Har vi identifierat informationens skyddsnivå genom informationsklassning och sett över vår aktörs möjligheter att hantera informationen?

Har vi valt rätt skyddsåtgärder som fungerar i den miljö och det beredskapsläge där människor ska arbeta?

Finns rätt förmåga hos oss? Har vår aktör kompetens, lokaler och utrustning för att hantera signalskydd?

Kapitel 5

Sambandssystemet och dess komponenter

5. Sambandssystemet och dess komponenter

I detta kapitel beskrivs hur ett sambandssystem är uppbyggt och hur olika tekniska och organisatoriska delar samverkar för att möjliggöra informationsöverföring. Kapitlet ger en gemensam begreppsgrund för sambandsmedel, gränssnitt, bärare och transmission, och visar hur dessa delar hänger ihop i praktiken. Genom att beskriva sambandssystemet uppifrån och ner blir det lättare att sätta förbindelsen i sitt sammanhang vid planering och genomförande av samband.

5.1 Vad är ett sambandssystem?

Ett sambandssystem utgör helheten som krävs för att informationsöverföring ska fungera. Ett sambandssystem består av sambandsmedel, regler och metodik samt personal med rätt kompetens och ansvar.

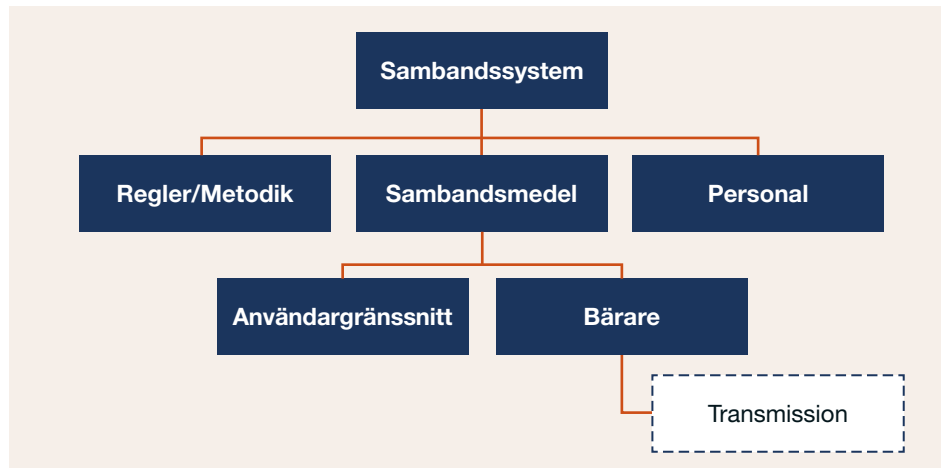
Sambandssystemet skapar därmed förutsättningar för att information kan överföras på ett tillförlitligt sätt, oavsett om det sker i vardagen, vid kriser eller vid höjd beredskap. Sambandsmedlet är den tekniska delen av systemet, medan regler, metodik och personal säkerställer att tekniken används på ett samordnat, säkert och effektivt sätt.

Vidare kan information som ska överföras delas in i olika informationstyper. Informationstyper beskriver formatet på informationen för att möjliggöra val av rätt sambandssystem (mer om detta i avsnitt 5.4).

Syftet med att beskriva sambandssystem och sambandsmedel på det här sättet är att både slutanvändare och sambandspersonal ska få den information som de behöver för att kunna planera och utföra uppgiften.

Figur 2 är en hierarkisk modell som visar att ett sambandssystem består av tre delar: Regler/Metodik, Sambandsmedel och Personal. Sambandsmedlen delas i sin tur upp i Användargränssnitt och Bärare. Transmission är en del av bäraren. Det illustrerar att sambandssystem omfattar både teknik, arbetssätt och människor.

Figur 2. Sambandssystemets komponenter – hierarkisk modell



5.2 Sambandsmedel – tekniken som används

Begreppet sambandsmedel beskriver den teknik som används för att överföra information. Ett sambandsmedel består av två huvudsakliga delar: ett **användargränssnitt** och en **bärare**. Dessa två delar fyller olika funktioner men är alltid beroende av varandra.

Hur sambandsmedlet är uppbyggt påverkar vilken information som kan överföras, hur snabbt överföringen sker och hur robust lösningen är vid störningar.

5.2.1 Användargränssnitt – det som användaren ser

I denna handbok används begreppet användargränssnitt för att beskriva den del av sambandsmedlet som användaren möter. Användargränssnittet är den kontakt-yta som används för att skapa, ta emot eller hantera information. Exempel på användargränssnitt är Webbaserat Informationssystem (WIS), meddelande-applikationer och e-postklienter.

Ett och samma användargränssnitt kan i vissa fall användas tillsammans med olika bärare. Det innebär att användaren kan uppleva sambandsmedlet på samma sätt, även om informationen i praktiken överförs via olika tekniska lösningar. Ett exempel är e-post, som kan överföras via internet, lokala nät eller radio.

Användargränssnittet

- kan bestå av mjukvara, hårdvara eller en kombination av båda
- beskriver vilken typ av mjuk- eller hårdvara användaren behöver för att kunna överföra information i sitt arbete
- avgör hur informationen presenteras och kan hanteras.

Valet av användargränssnitt är därmed gränssättande för vilken informationstyp som kan överföras och hur den kan struktureras.

5.2.2 Bärare – tekniken som överför informationen

Bäraren är den tekniska lösning som transporterar informationen mellan olika tekniska komponenter eller aktörer. Bäraren använder ett eller flera transmissionsmedel för att genomföra överföringen.

Valet av bärare har stor betydelse för sambandsmedlets robusthet, tillgänglighet och motståndskraft mot störningar. En bärare kan bestå av tekniska nät eller av fysisk överlämning av information. Exempel på bärare är Rakel-nätet, Swedish Government Secure Intranet (SGSI), internet samt fysisk överlämning genom ordonnans (läs mer om ordonnans i avsnitt 6.4.6).

5.2.3 Transmission – hur informationen tekniskt överförs

Transmission beskriver hur information överförs från en sändare till en eller flera mottagare. Överföringen sker antingen genom elektroniska, optiska eller akustiska impulser eller genom fysisk transport av information.

En bärare kan använda ett eller flera transmissionsmedel beroende på teknik, behov och förutsättningar. Valet av transmissionsmedel påverkar bland annat räckvidd, överföringshastighet, sårbarhet och möjligheten att skydda informationen.

Exempel på transmissionsmedel:

Radio använder elektromagnetiska vågor för att överföra information mellan olika platser. Olika frekvensområden ger olika överföringshastighet, räckvidd och känslighet för påverkan.

Radiolänk är en riktad radioförbindelse mellan två platser. Radiolänkstationer kan kopplas samman i nät och därigenom ge stor geografisk spridning.

Satellit – när information skickas från avsändaren till en satellit som i sin tur förmedlar signalen vidare till mottagaren.

Kabel kan bestå av metalledare eller optisk fiber och kopplar fysiskt ihop två system.

Ordonnans innebär att information överförs fysiskt av en person. Även vanlig post kan betraktas som en form av ordonnans. Ordonnanstjänsten beskrivs närmare i kapitel 6 Metoder.

5.3 Informationstyper

Information som överförs via sambandssystem delas in i olika informationstyper: tal, textmeddelande, video och data/filer. Dessa typer beskriver hur informationen uppfattas av användaren i sitt gränssnitt, och ligger till grund för valet av sambandssystem.

I moderna digitala system omvandlas all information till data vid överföring och återställs till rätt format i mottagarens gränssnitt. Samtidigt finns fortfarande analoga sambandssystem i drift, där informationen överförs direkt i sitt ursprungliga format – till exempel som ljud i en analog radio.

Valet av sambandssystem påverkas därför både av vilken informationstyp som ska överföras och av vilken teknik som används. När olika typer av sambandssystem används parallellt – till exempel digitala och analoga – behöver de vara interoperabla, så att informationen kan överföras och förstås oavsett systemtyp.

Tabell 6. Informationstyperna

Informationstyp	Definition	Exempel
Tal	Information som överförs i form av akustiskt ljud, framställt med rösten.	Telefonsamtal, radiosamtal
Text-meddelande	Information som överförs som ren text, utan inslag av andra format.	SMS, SDS, fax, dokument via ordonnans
Video	Information som överförs som rörliga bilder, med eller utan ljud, i realtid.	Möten via mötestjänster
Data/filer	Information som överförs digitalt i strukturerade filformat.	Information i WIS, e-post, transpondrar

5.4 Påverkansfaktorer – när sambandet inte fungerar som planerat

Alla faktorer som påverkar sambandet är inte avsiktliga. Sambandsförmågan kan även påverkas av naturliga fenomen, miljöförhållanden och tekniska beroenden som ligger utanför en aktörs direkta kontroll. Sådana påverkansfaktorer är ofta oavsiktliga, men kan ändå få betydande konsekvenser för informationsöverföring och ledning.

Dessa fenomen kan vara svåra att förutse exakt i tid och omfattning. Deras konsekvenser kan dock begränsas genom medvetna val av sambandslösningar, redundans och anpassade arbetssätt. Därför behöver påverkansfaktorerna beaktas vid val, utformning och användning av sambandssystem.

5.4.1 Väder och naturfenomen

Väderhändelser som stormar, kraftigt snöfall, värmeböljor, översvämningar och skogsbränder kan skada infrastruktur, slå ut elförsörjning eller begränsa tillgången till fysiska platser där sambandsutrustning är installerad. Sådana händelser kan påverka både trådlösa och trådbundna samband.

5.4.2 Solaktivitet och rymdväder

Kraftiga solstormar kan störa satellitkommunikation, GNSS-system och radiokommunikation. Detta kan påverka både positionering, tidsstämpling och sambandssystem som är beroende av rymdbaserad infrastruktur.

5.4.3 Tekniska fel och systemberoenden

Sambandssystem är ofta beroende av elförsörjning, datanätverk, kylning och andra stödsystem. Tekniska fel, överbelastning eller bristande redundans kan leda till avbrott även utan yttre påverkan. Ju mer integrerade och automatiserade systemen är, desto större kan följd effekterna bli vid ett fel.

5.4.4 Mänskliga fel

Felaktig hantering, bristande rutiner eller stress kan leda till att samband bryts, att fel kanal används eller att information inte når fram i tid. Ett exempel kan vara att inte ta hänsyn till terrängens inverkan på tekniken. Även dessa faktorer behöver beaktas som en del av hotbilden mot sambandet.

5.5 Exempel på ett sambandssystem

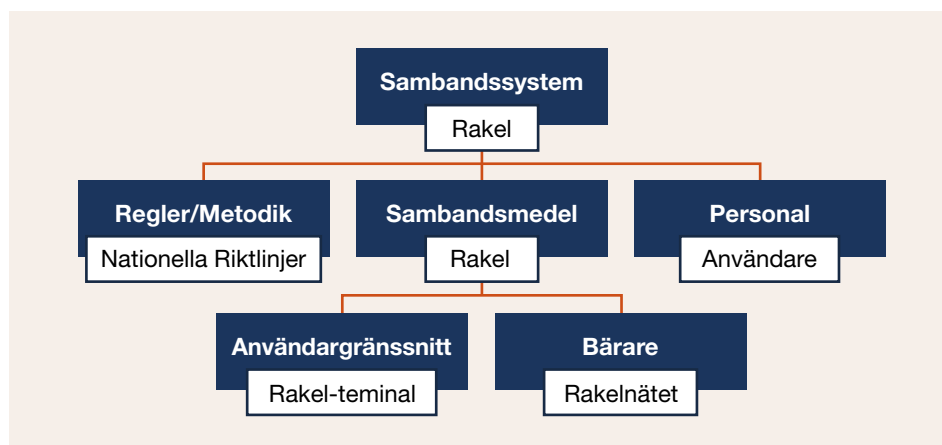
Rakel är ett exempel på ett komplett sambandssystem. Systemet består av sambandsmedlet Rakel, nationella regler och metodik samt utbildad personal, såsom användare och sambandsansvariga.

Sambandsmedlet Rakel består av gränssnittet Rakel-terminal och bäraren Rakel-nätet. Tillsammans med gemensamma riktlinjer och utbildning skapar detta förutsättningar för ledning och samverkan mellan olika aktörer.

Figur 3 är en förklaringsmodell som beskriver hierarkin i sambandssystemet Rakel:

- Sambandssystemet Rakel omfattar Regler/Metodik (Nationella riktlinjer), Sambandsmedel (Rakel), och Personal (Användare).
- Sambandsmedlet Rakel delas vidare in i Användargränssnitt (Rakelterminal) och Bärare (Rakelnät).

Figur 3. Sambandssystemet Rakel uppdelat enligt förklaringsmodellen (se figur 2)





Stödjer sambandet vår verksamhet?

Vilka människor och roller ska använda sambandet?

Vilket användargränssnitt behöver de för att kunna arbeta effektivt?

Vilka sambandsmedel är lämpliga i olika situationer

utifrån arbetssätt, miljö och belastning i just vår verksamhet?

Är sambandet anpassat till den information som ska överföras, med rätt skyddsnivå och format? Har vi säkerställt att mottagaren har tillgång till samma sambandslösning, rätt behörighet och tillräcklig kunskap för att ta emot informationen?

Har vår personal fått möjlighet att öva på sambandslösningen i realistiska situationer, så att sambandet fungerar även under stress och i påverkade lägen?

Kapitel 6

Metoder – så förmedlas information i praktiken

6. Metoder – så förmedlas information i praktiken

I detta kapitel beskrivs teknikoberoende metoder för att förmedla information inom och mellan aktörer. Metoderna kan användas oavsett sambandsmedel och behöver alltid anpassas till verksamhetens behov, tekniska lösningar och beredskapsläge. Metoderna skapar förutsägbarhet, effektivitet och spårbarhet i informationsöverföringen – både i vardagen och när förutsättningarna snabbt förändras.

6.1 Kontrollera att sambandet fungerar

För att kunna förmedla information tillförlitligt behöver sambandet kontrolleras innan det används i skarpt läge. Detta görs genom ett förbindelseprov.

Förbindelseprovet svarar på frågan: Går det att nå varandra just nu?

Ett förbindelseprov innebär att sambandet provas i praktiken för att säkerställa att informationsöverföringen fungerar som avsett. Provet omfattar både tekniska förutsättningar och hur sambandet fungerar i användning, till exempel att rätt kanal används, att anrop når fram, att information hörs eller förstås och att arbetssätt, format och rutiner fungerar.

I vardagligt språk används ibland begrepp som sambandsprov eller funktionellt prov. Ofta avser man då samma sak: att kontrollera att sambandet fungerar. För att skapa ett gemensamt och tydligt språkbruk är det bättre att använda begreppet förbindelseprov. Det samlar alla delar som behöver fungera – teknik, arbetssätt och rutiner – i ett och samma begrepp och gör det tydligare vad som faktiskt ska säkerställas.

Förbindelseprov kan genomföras när man upprättar samband, löpande under pågående verksamhet eller vid behov. Om det finns särskilda instruktioner för hur förbindelseprov ska genomföras för en viss sambandsväg eller ett visst sambandsmedel ska detta framgå av sambandsplanen.

6.1.1 Förbindelseprov – hur går det till?

Förbindelseprov kan genomföras på alla sambandsmedel.

Avsändaren testar sambandet genom att kontakta en mottagare på det aktuella sambandsmedlet. För att vara säker på att sambandet fyller den funktion som det är tänkt kan det, om situationen tillåter, vara bra att kontakten sker på det sätt som sambandet är tänkt att genomföras.

Exempel kan vara att skicka en stor fil, en kartbild i det format som kommer användas eller en videokonferens med det antal deltagare som är tänkt att använda sambandsvägen.

Sambandets kvalitet kontrolleras genom att fråga efter **HÖRBARHET**. Hörbarheten bedöms utifrån en fyrgradig skala.

Vid videosamtal kan **ÖVERFÖRINGSKVALITET** användas istället för **HÖRBARHET**.

Tabell 7. Bedömningsskala av hörbarhet vid talat samband

Uttryck (gradering)	Innebörd
God (5)	Ljudkvaliteten är klar och tydlig, meddelandet kan uppfattas utan ansträngning.
Godtagbar (3)	Ljudkvaliteten är tillfredsställande för att meddelandet ska kunna uppfattas och förstås.
Dålig (1)	Ljudkvaliteten är dålig, meddelanden kan inte uppfattas tillförlitligt.
Ohörbar (0)	Det går inte att höra meddelandet överhuvudtaget.

Källa: I huvudsak Handbok Samband telefonering, H Sb Tfn 2021, Försvarmakten, s 48 med anpassning.

6.2 Passning – när och hur vi är nåbara

Att ha passning innebär att omedelbart kunna ta emot, svara på och skicka information. Hur passningen sker beror på vilket sambandsmedel som används. Vilket passningsalternativ som krävs beror på verksamhetens behov och den aktuella situationen.

Passningsalternativen beskriver när eller hur ofta en aktör kan nås via ett visst sambandsmedel eller en viss sambandsväg. Passningsalternativen ska anges i sambandsplanen och anpassas utifrån läget av sambandsledaren. De anger därmed aktörens tillgänglighet över tid och skapar förutsättningar för gemensamt samband.

6.2.1 Passningsalternativ för tal och video

Vid talad informationsöverföring, till exempel via radio, telefon eller video, används ofta förutbestämda passningsalternativ. Dessa anger när aktören aktivt lyssnar och kan svara på anrop. Tabell 8 visar exempel på passningsalternativ för tal och video.

Tabell 8. Passningsalternativ för tal och video – exempel

Passningsalternativ	Innebär att aktören är:
Ständig passning (1)	Omedelbart tillgänglig.
Periodisk (2)	Omedelbart tillgänglig de fem första minuterna varje kvart.
Periodisk (3)	Omedelbart tillgänglig de fem första minuterna varje halvtimme.
Periodisk (4)	Omedelbart tillgänglig de fem första minuterna varje timme.

Källa: Handbok Samband grunder, H Sb G 2016, Försvarmakten med anpassning.

6.2.2 Passningsalternativ för text och data

Vid textbaserad informationsöverföring, till exempel e-post eller meddelandesystem, sker passning oftast genom regelbunden bevakning av inkorgar eller system.

Tabell 9. Passning för samband där text eller data överförs – exempel

Passningsalternativ	Innebär att aktören passar sambandsmedlet:
Ständig passning (S)	Kontinuerligt och kan ta del av information omedelbart.
Cyklisk passning (C X)	Minst var X minut.
Cyklisk passning mellan två klockslag (C X YY-ZZ)	Minst var X minut mellan klockslagen YY och ZZ.

6.3 Prioritering av information – när allt inte kan hanteras samtidigt

För att säkerställa att viktig och tidskritisk information når fram i tid används klassbeteckningar eller andra former av prioriteringsmarkeringar. Det blir särskilt viktigt i situationer där såväl mänsklig som teknisk kapacitet är begränsad. Det kan till exempel vara när mycket information överförs samtidigt eller när bandbredden är begränsad.

Syftet med klassbeteckningar är att

- göra det tydligt vad som ska hanteras först
- hjälpa mottagaren att förstå tidskraven
- minska risken att kritisk information försvinner i mängden.

Om ingen prioritet anges hanteras information enligt normal prioritet.

Klassbeteckningar som Z, O, P och R har sitt ursprung i Försvarmaktens arbetssätt och används där med fast betydelse. I civila sammanhang finns dock inget krav på att använda dessa beteckningar. Undvik därför att använda Försvarmaktens klassbeteckningar med någon annan innebörd, eftersom det riskerar att skapa förvirring vid samverkan.

Aktörer kan vid behov använda egna prioriteringsnivåer, men bör då välja andra benämningar. Det är avgörande att prioriteringen är tydlig, gemensamt förstådd och konsekvent använd.

Tabell 10. Klassbeteckningar och tidsgränser

Företrädesrätt	Klassbet.	Tidsgräns
Alarm	Z	Akut meddelande som ska sändas snarast, senast inom 10 minuter.
Brådskande	O	Viktigt meddelande som ska sändas senast inom 60 minuter.
Prioritet	P	Meddelandet som ska sändas senast inom 6 timmar.
Rutin	R	Standardnivå. Informationen ska sändas inom 24 timmar och måste vara framme senast nästa arbetsdags morgon.

Källa: Handbok Samband grunder, H Sb G 2016, Försvarmakten.

6.4 Sätt att överföra information

När förbindelse, prioritering och passning är på plats kan information förmedlas på olika sätt, beroende på situation och behov.

6.4.1 Signaldisciplin – att använda samband på rätt sätt

Signaldisciplin handlar om att använda sambandsmedel på ett korrekt, effektivt och säkert sätt. Det innebär att vi följer en gemensam terminologi, håller budskap korta och relevanta och använder överenskomna rutiner för exempelvis kvittens och kontaktvägar.

Signaldisciplin medverkar till att informationsöverföringen fungerar även när sambandsmiljön är störd eller påverkad. "Påverkad sambandsmiljö" innebär att system eller informationsflöden kan vara störda, överbelastade eller utsatta för påverkan.

Vad innebär signaldisciplin?

Signaldisciplin är en metod som innebär att

- använda fastställd terminologi och följa sambands- och signalskyddsrutiner
- genomföra informationsöverföring så kort och tydligt som omständigheterna medger
- enbart överföra den information som behövs för uppgiften.

6.4.2 Principen T2S2 (Tänk–Tryck–Sänd–Släpp)

För att hålla informationsöverföringen kort och relevant används principen T2S2 (Tänk–Tryck–Sänd–Släpp). Principen hjälper dig att förbereda budskapet, starta sändningen, förmedla informationen enligt överenskomna rutiner och avsluta. Den kan användas oavsett sambandsmedel.

Figur 4 visar ett flödesschema för modellen T2S2 (Tänk–Tryck–Sänd–Släpp):

- **Steg 1:** Tänk – Vad ska du förmedla?
- **Steg 2:** Tryck – Starta sändningen genom att trycka på knapp, slå på mikrofon eller liknande.
- **Steg 3:** Sänd – Förmedla informationen enligt överenskomna rutiner.
- **Steg 4:** Släpp – Avsluta sändningen genom att släppa knappen eller stänga av mikrofonen.

Figur 4. T2S2 (Tänk–Tryck–Sänd–Släpp)



6.4.3 Talad informationsöverföring via radio

Med talad informationsöverföring menas realtidsöverföring av information som talas mellan två eller flera parter.

För att talad informationsöverföring ska fungera väl i praktiken och minska risken för missförstånd behöver alla parter göra likadant. I följande avsnitt beskrivs därför metoder för talad informationsöverföring: struktur för samtal, adressering och tillrop, trafikuttryck samt återläsning.

Avsnittet behandlar metoder för talad informationsöverföring via radio där enbart en av deltagarna kan prata åt gången.

Struktur för talsamtal

Ett talsamtal via radio bör följa den fasta strukturen som beskrivs i detta avsnitt. Genom att använda samma ordning och uttryck skapas förutsägbarhet – även mellan aktörer som inte arbetar tillsammans till vardags. Grundstrukturen kan vid behov anpassas efter situationen.

Ett talsamtal delas normalt in i fem delar:

1. anrop
2. svar på anrop
3. informationsöverföring
4. kvittens
5. avslutning.

Tabell 11 visar ett praktiskt exempel på hur ett talsamtal via radio kan gå till.

Tabell 11. Talsamtal via radio – exempel

Samtalsdel	Anropare i detta exempel: Polisen	Mottagare i detta exempel: Jordbruksverket
Anrop	Jordbruksverket FRÅN Polisen, KOM.	
Svar på anrop		Jordbruksverket, KOM.
Informations- överföring	Vårt möte är flyttat till 1600, KOM.	
Kvittens		UPPFATTAT, KOM.
Avslutning	KLART SLUT	

Trafikuttryck – gemensamt språk för tydlighet och tempo

Trafikuttryck⁴ är standardiserade ord och uttryck som används i sammanhang där det är viktigt att vara tydlig och kortfattad. Trafikuttrycken används främst vid samband via radio, men kan i tillämpliga delar även användas vid tal via telefon eller video.

Tabell 12. Trafikuttryck

Uttryck	Uttrycket används
KOM	när du är färdig med din sändning och lämnar ordet till någon annan.
FRÅN	när du anger vem du är som sänder meddelandet.
SLUT-KOM	när du är klar med ditt meddelande och vill att mottagaren kvitterar och/eller avslutar samtalet.
KLART-SLUT	när du avslutar samtalet helt.
UPPFATTAT	när du bekräftar att du har tagit emot meddelandet.
REPETERA	när du behöver att hela eller delar av meddelandet sänds igen. Du kan använda FRÅN, INNAN eller MELLAN för att avgränsa vilken del av meddelandet du vill höra igen.
FEL	när du rättar en felsägning eller felsändning och omedelbart anger korrekt uppgift. När du rättar inleder du med SKA VARA.
VÄNTA	när du inte kan ta emot meddelandet just nu, men kommer att kunna göra det inom kort.
FÖRTUR⁵	när du behöver förmedla information med högre prioritet än pågående samtal.
MOTTAGNINGSBEVIS	när du behöver säkerställa att informationen har nått mottagaren inom mottagande aktör.
FRÅGAS	när du vill tydliggöra att ditt meddelande innehåller en fråga och att svar förväntas.
ÅTERLÄS	när du vill att mottagaren läser tillbaka meddelandet för att säkerställa att rätt information mottagits.

Källa: Handbok Samband telefonering, H Sb Tfn 2021, Försvarsmakten samt Vägledning i Rakel, MSB1452 – december 2019.

Not 4. Inom Försvarsmakten kallas dessa signaleringsuttryck.

Not 5. Inom Försvarsmakten används ALARM.

Adressering och anrop

Använd alltid principen ”Mottagaren FRÅN Avsändaren” vid adressering i talat samband. För extra tydlighet kan mottagarens namn eller anropssignal sägas två gånger vid anrop.

Vid etablerat samband kan adresseringen förkortas till enbart ”FRÅN avsändaren” alternativt till att inte adressera alls.

Normalt avslutas samtalet av den som initierat kontakten, om inget annat är överenskommet. Ett exempel på en överenskommelse är att ledningscentraler vanligen avslutar samtal.

Tabell 13. Adressering och anrop mellan två deltagare – exempel

Trafikverket	Kustbevakningen
Kustbevakningen FRÅN Trafikverket, KOM. (1)	
Kustbevakningen, KOM. (2)	
Här är mitt meddelande, KOM. (3)	
UPPFATTAT, SLUT KOM. (3)	
Från Trafikverket, KLART SLUT. (4)	

Förtydligande av exemplet i tabell 13:

1. Trafikverket använder först en fullständig adressering. Det är inte ovanligt att den första adressaten behöver repeteras.
2. Kustbevakningen svarar med förkortad adressering.
3. Ingen adressering under själva meddelandet och kvittensen.
4. Trafikverket avslutar samtalet med förenklad adressering.

Tabell 14. Adressering och anrop mellan fler deltagare – exempel

Trafikverket	Kustbevakningen	Polisen
Kustbevakningen, Polisen FRÅN Trafikverket, KOM. (1)		
Kustbevakningen, KOM. (2)		
Polisen, KOM (2)		
Här är mitt meddelande, KOM. (3)		
FRÅN Kustbevakningen. UPPFATTAT, KOM. (4)		
FRÅN Polisen, UPPFATTAT, KOM (4)		
Från Trafikverket, KLART SLUT.		

Förtydligande av exemplet i tabell 14:

1. Trafikverket ropar på Kustbevakningen och polisen med en fullständig adressering. Det är inte ovanligt att adressaterna behöver repeteras.
2. Både Kustbevakningen och polisen svarar med förkortad adressering.
3. Trafikverket använder sedan ingen adressering, då meddelandet ska gå till de båda mottagare som redan är uppropade.
4. Kustbevakningen och polisen använder förenklad adressering för att förtydliga vem av dem som uppfattat meddelandet.
5. Slutligen avslutar Trafikverket samtalet med förenklad adressering.

6.4.4 Återläsning – när korrekthet är kritisk

Återläsning (även kallat kollationering) används främst vid talad informationsöverföring när avsändaren behöver säkerställa att mottagaren har uppfattat informationen korrekt. Det gäller särskilt uppgifter där fel kan få konsekvenser, till exempel tider, platser, mängder, beslut eller ärendeidentifiering (till exempel diarienummer).

Vid återläsning läser mottagaren tillbaka hela eller delar av meddelandet som det har uppfattats. Avsändaren bekräftar därefter att återläsningen är korrekt eller rättar eventuella fel.

Mottagaren genomför återläsningen genom att inleda sitt svar med **JAG ÅTERLÄSER** och återger därefter informationen. Återläsning kan förkortas **ÅTL**.

Återläsning kan även användas vid andra informationstyper än tal, men behovet kan då ofta tillgodoses på andra sätt. För skriftlig informationsöverföring används någon form av mottagningsbevis eller spårbar kvittens istället för återläsning, särskilt när informationen redan finns dokumenterad i systemet.

Tabell 15. Återläsning – exempel

Trafikverket	Kustbevakningen
Kustbevakningen FRÅN Trafikverket, KOM.	
	Kustbevakningen, KOM.
ÅTERLÄS, bron stängs klockan 1900, SLUT KOM.	
	JAG ÅTERLÄSER, Bron stängs klockan 1900, KOM
RÄTT ÅTERLÄST, KLART SLUT.	

6.4.5 Viasignalering – när direkt samband saknas

Om två aktörer saknar möjlighet att upprätta direkt samband kan viasignalering (VIA) användas. Det innebär att information skickas via en tredje aktör som har samband med mottagaren.

Viasignalering förutsätter att

- det är tydligt vem som är avsedd mottagare
- alla inblandade känner till att viasignalering sker
- det finns en överenskommelse eller styrning som stödjer upplägget.



Viktigt vid sekretess och säkerhetsskydd

Viasignalering kan vara olämplig eller otillåten beroende på vilken information som överförs och vilka regelverk som gäller mellan aktörerna.

När information omfattas av sekretess eller säkerhetsskydd behöver aktören alltid göra en riskbedömning innan överföring. Riskbedömningen handlar bland annat om huruvida

- mellanhanden får ta del av innehållet (avsiktligt eller oavsiktligt)
- det krävs säkerhetsskyddsavtal eller annan styrning mellan aktörerna
- signalskydd krävs och kan tillämpas hela vägen.

Är ni osäkra? Avstå från viasignalering om ni är osäkra och använd istället en lösning som uppfyller kraven på skyddsnivå, eller inhämta stöd från berörd funktion – till exempel en funktion för informationssäkerhet, säkerhetsskydd eller signalskyddsorganisation.

6.4.6 Ordonnans – fysisk överföring av information

Ordonnans innebär att ett bud transporterar information fysiskt och överlämnar den till mottagande roll eller funktion. Ordonnans kan vara ett alternativ när andra sambandsmedel inte fungerar eller inte är lämpliga.

Den som transporterar informationen benämns ordonnans och ansvarar för att informationen förs från avsändare till mottagare enligt instruktioner.

I normalfallet överförs information i ett förseglat emballage och kvitteras av mottagaren. Om information förmedlas till flera aktörer under samma tur bör den förvaras separerad så att rätt information når rätt mottagare.

Ordonnansförbindelser finns i två former:

1. Fast ordonnans som upprättas med fasta ruttor och scheman för överföring av information. För att öka robustheten kan flera ruttor och scheman behövas, liksom alternativt fordonsslag.
2. Särskild ordonnans som används för en specifik informationsöverföring och levererar information direkt till en lämplig mötesplats. Den används särskilt när informationen är tidskritisk och inte kan invänta en fast ordonnans.

6.5 Spårbarhet

Spårbarhet innebär att det i efterhand går att följa vad som skickats, när, mellan vilka och hur det hanterats. Detta sker i huvudsak genom diarier, tidsnummer och loggar, alternativt genom en så kallad trafiklista samt kvittens och mottagningsbevis. Vid behov kan olika metoder kombineras.

6.5.1 Spårbarhet genom diarier, tidsnummer och loggar

Spårbarhet kan skapas genom diarienummer, tidsnummer eller systemloggar:

- **Diarienummer:** Använd det befintliga diarienumret om det finns ett sådant, annars kan man skapa ett nytt.
- **Tidsnummer:** Detta anges som datum och tid i form av dag + timme + minut (DDTTMM) – till exempel 221133, vilket betyder den tjugoförsta dagen i månaden klockan 11.33.
- **Systemloggar:** Vid datatrafik kan diarienummer sättas automatiskt av sambandssystemet, och spårbarhet kan även säkerställas genom systemloggar.

Om spårbarheten är oklar eller riskerar att gå förlorad behöver aktören införa en enkel rutin, till exempel genom att sätta ett diarienummer eller tidsnummer på meddelandet och säkerställa att relevant loggning är aktiverad i systemet.

6.5.2 Spårbarhet genom trafiklista

Trafiklistor utgör ett viktigt underlag vid incidenthantering eller vid en bedömning av vad som kan ha röjts, förvanskats eller gått förlorat. Därför behöver den innehålla tillräcklig information för att möjliggöra spårbarhet.

Följande uppgifter ska alltid vara med i en trafiklista:

1. **Datum och tid:** När genomfördes informationsöverföringen?
2. **Avsändare:** Vilken aktör, funktion eller roll skickade informationen?
3. **Mottagare:** Vilken aktör, funktion eller roll var avsedd mottagare?
4. **Ärendeidentifiering:** Det kan vara till exempel diarienummer, tidsnummer eller ärendemening, alternativt en kombination av dessa.

Trafiklistan kan kompletteras med följande:

- **Hantering** – vem som hanterat informationen.
- **Sambandsmedel** – vilket sambandsmedel som använts.
- **Åtgärd** – till exempel ”överlämnad till stabsexpedition”, ”vidarebefordrad” eller ”ingen åtgärd”.
- **Sekretessnivå eller klassificering** – säkerställ alltid att detta följer organisationens rutiner.
- **Klassbeteckning eller prioritering** – hur bråttom det är att meddelandet når mottagaren.

6.5.3 Kvittens och mottagningsbevis

Kvittens innebär att mottagande aktör har tagit emot informationen.

Mottagningsbevis (MBS) innebär att informationen nått fram till den roll eller funktion inom mottagande aktör som meddelandet är avsett för.

Exempel: Ett dokument skickas till en handläggare via registraturen. Ett autosvar kan innebära att dokumentet är kvitterat. När avsedd handläggare bekräftar att dokumentet har tagits emot och hanterats utgör detta ett mottagningsbevis.



? Fungerar våra metoder för informationsöverföring i praktiken?

Har vi tydliga och gemensamma arbetssätt för hur information ska förmedlas – i vardagen, vid kris och vid höjd beredskap?

Har vi kontrollerat att sambandet fungerar – både tekniskt och i praktiken?

Använder vi gemensamma trafikuttryck och strukturer som minskar risken för missförstånd, särskilt vid tidspress eller störd sambandsmiljö?

Har vi tydliga överenskommelser om passning – till exempel när och hur olika aktörer är nåbara – och stämmer dessa med verksamhetens behov?

Vet vi när kvittens räcker och när det krävs mottagningsbevis eller återläsning för att säkerställa att informationen nått fram korrekt?

Har vi rutiner för spårbarhet så att det i efterhand går att följa vad som skickats, när och mellan vilka aktörer – vid behov genom diarier, loggar eller trafiklista?

Är våra metoder kända, övade och anpassade till de som ska använda dem, så att informationsöverföringen fungerar även under stress och i påverkade lägen?

Kapitel 7

Organisation för sambandstjänst

7. Organisation för sambandstjänst

För att stödja samverkan och uppnå god interoperabilitet behöver varje aktör ha en funktion med tydligt ansvar för sambandstjänsten. Hur denna funktion organiseras varierar mellan aktörer, eftersom uppdrag, storlek och förutsättningar skiljer sig åt. Detta kapitel beskriver en rekommenderad miniminivå för hur aktörer ska organisera sin sambandsfunktion, oavsett beredskapsläge.



VIKTIGT!

Signalskyddsorganisation regleras i Försvarmaktens styrande dokument för signalskyddet. Se mer i kapitel 4 *Skydda informationen* i denna handbok.

7.1 Sambandsorganisation

Sambandsorganisationen ansvarar för att säkerställa att information kan överföras på ett tillförlitligt, samordnat och ändamålsenligt sätt – både inom den egna organisationen och i samverkan med andra aktörer.

Sambandsorganisationen behöver vara anpassningsbar för att stödja informationsförsörjningen både i ett normalläge och vid hantering av samhällsstörningar.

Oavsett organisationsform behöver vissa grundläggande funktioner och ansvar för samband alltid vara tillgodosedda. Detta avsnitt beskriver den gemensamma organisatoriska grund som krävs för att sambandet ska fungera, oavsett beredskapsläge.

7.1.1 Sambandsfunktion i ett normalläge

Sambandsarbetet behöver vara integrerat i den ordinarie organisationen och bemannas av personer som har ansvar för samband.

I ett normalläge behöver de administrativa funktionerna för samband vara tydligt utpekade och upprätthållas (se 7.4.1). Det gäller exempelvis ansvar för planering, förvaltning av sambandslösningar och samordning med andra aktörer. Funktioner som registratur och växel är exempel på sambandsfunktioner som alltid finns.

En tydlig ansvarsfördelning i vardagen skapar förutsättningar för att snabbt kunna skala upp sambandsorganisationen vid en samhällsstörning.

7.1.2 Sambandsfunktion vid hantering av samhällsstörningar

Vid hantering av samhällsstörningar organiserar många aktörer sitt ledningsstöd i form av en stab. I en sådan organisation behöver det alltid finnas en funktion med tydligt ansvar för samband.

För att underlätta samverkan mellan aktörer krävs inte bara teknisk kompatibilitet utan också organisatorisk samstämmighet. Gemensamma principer för hur staber organiseras och hur funktioner fördelas bidrar till ökad förståelse, effektivare samarbete och minskad risk för missförstånd.

I faktarutan beskrivs en vanligt förekommande stabsmodell och hur den kan användas som grund för organisatorisk interoperabilitet mellan aktörer.

Stabsmodell

Det är vanligt att använda den stabsmodell som NATO använder, benämnd Continental Staff System eller General Staff System. Modellen används i anpassad form av både civila och militära aktörer och bygger i grunden på ett antal funktionsområden som stödjer ledning och genomförande.

Modellen består i sin grundform av upp till nio funktioner. Benämningar, ansvar och arbetsuppgifter inom respektive funktion anpassas dock efter aktörens uppdrag, organisation och behov. Det är därför vanligt att vissa funktioner har ett mer inriktande och samordnande ansvar, medan det praktiska genomförandet sker i andra delar av organisationen eller i särskilda verksamhets- och stödfunktioner. Modellen ska därmed ses som ett ramverk, snarare än som en "fast mall".

I den här modellen benämns sambandsfunktionen med nummer 6.

7.2 Principer för sambandsorganisationens uppbyggnad

Detta avsnitt beskriver grundläggande principer för hur en sambandsorganisation kan organiseras och bemannas. Fokus ligger på funktion och ansvar – inte på formell organisationsstruktur eller enskilda befattningar.

I handboken används begreppet roll för att beskriva ett uppdrag eller en funktion som behöver utföras i sambandsorganisationen. En anställning reglerar den formella arbetsrelationen mellan en arbetsgivare och en individ. En roll beskriver däremot vilka arbetsuppgifter, vilket ansvar och vilka förväntningar som är knutna till en viss funktion i organisationen.

Hur rollerna organiseras, kombineras eller fördelas mellan olika delar av verksamheten kan variera mellan aktörer. En och samma person kan ha flera roller samtidigt, antingen som del av sin ordinarie tjänst eller som tillikauppgift. Roller som projektledare, mentor eller skyddsombud är exempel på funktioner som ofta utförs som tillikauppgifter.

Flera av de roller som beskrivs i detta kapitel kan i vardagen utgöra en mindre del av ordinarie arbetstid. Vid hantering av samhällsstörningar kan rollerna dock bli mer omfattande, särskilt när fler eller mer komplexa sambandslösningar används.

7.2.1 Bemanning, uthållighet och redundans

Hur sambandsorganisationen bemannas behöver anpassas till aktörens storlek, uppdrag och organisation. För att minska sårbarhet och personberoenden bör centrala roller inom sambandsorganisationen bemannas av fler än en person – särskilt vid långvariga eller resurskrävande händelser. I vissa fall kan underlydande organisatoriska sambandsfunktioner bidra till att upprätthålla centrala roller.

Samband och signalskydd är tätt integrerade delar av arbetet med säker informationsöverföring. De verkar sida vid sida och behöver vara samordnade i planering och genomförande. Signalskyddstjänsten är beroende av sambandstjänsten för att fungera, liksom sambandstjänsten behöver signalskydd för att skydda vissa delar av informationen som ska överföras.

Den funktion som ansvarar för aktörens ledningsplats kan ingå i sambandsorganisationen, men om ansvaret ligger hos en annan del av verksamheten behöver det finnas ett tydligt och fungerande samspel mellan ledningsplats och sambandsfunktion.

7.3 Roller, ansvar och nivåer inom sambandsorganisationen

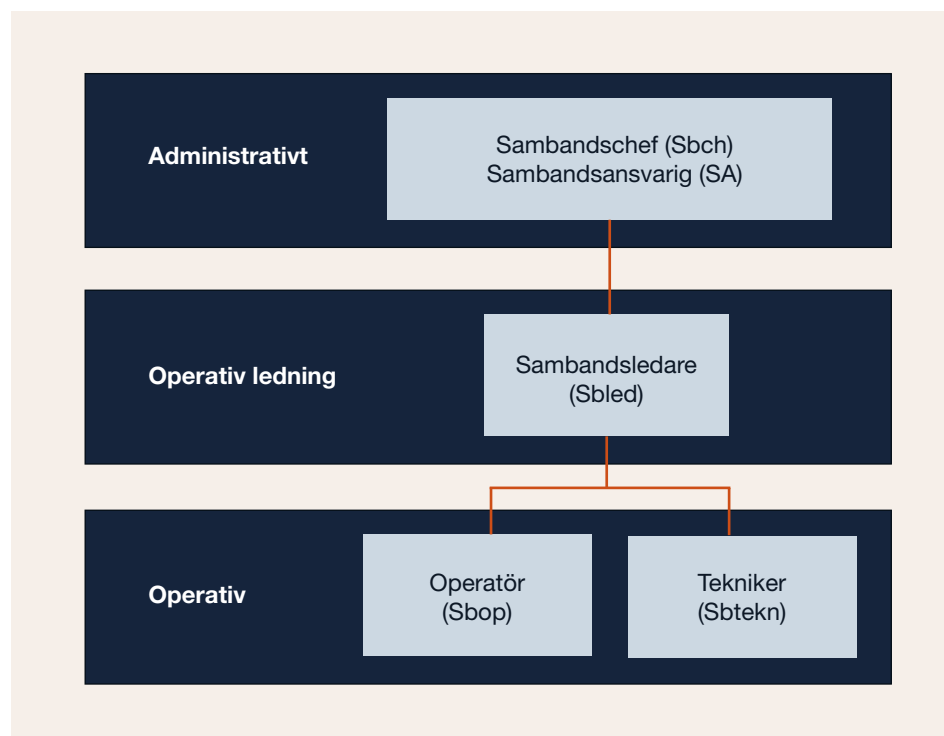
Det här avsnittet ger en översikt av grundläggande roller i sambandsorganisationen. Varje aktör kan naturligtvis utöka sin sambandsorganisation med fler roller utifrån sina behov och förutsättningar.

Roller inom sambandsorganisationen verkar på administrativ och operativ nivå och har olika fokus beroende på om arbetet avser planering, ledning eller genomförande (se tabell 14 och figur 5).

Tabell 16. Grundläggande roller i sambandsorganisationen

Roll	Ansvarsområde
Sambandschef (Sbch)	Ansvarar för aktörens sambandstjänst.
Sambandsansvarig (SA)	Ansvarar för en del av sambandsorganisationen.
Sambandsledare (Sbled)	Leder genomförandet av sambandstjänst.
Sambandsoperatör (Sbop)	Stödfunktion för användare av sambandsmedel, som bistår vid användning av sambandsmedel och genomför informationsöverföring enligt fastställda rutiner.
Sambandstekniker (Sbtekn)	Säkerställer sambandsmedlens tekniska funktion.

Figur 5. Nivåer inom sambandsorganisationen



Det här avsnittet tar upp tre nivåer inom sambandsorganisationen (se figur 5):

1. **På administrativ nivå** finns rollerna Sambandschef (Sbch) och Sambandsansvarig (SA).
2. **På operativ ledningsnivå** finns rollen Sambandsledare (Sbled) som leder det operativa arbetet och är länk mellan administrativ nivå och operativ nivå.
3. **På operativ nivå** finns rollerna Operatör (Sbop) och Tekniker (Sbtekn).

7.3.1 Administrativ nivå

Den administrativa nivån ansvarar för att sambandsorganisationen har de förutsättningar som krävs för att sambandstjänsten ska kunna planeras, upprätthållas och utvecklas över tid.

Arbetet på denna nivå omfattar planering, styrning och uppföljning av sambandsverksamheten, inklusive organisation, resurser, kompetens och tekniska lösningar.

På den administrativa nivån finns rollerna sambandschef och sambandsansvarig.

Sambandschef (Sbch)

Sambandschefen leder och samordnar aktörens sambandsorganisation på övergripande nivå. Rollen innebär ett strategiskt ansvar för att säkerställa att aktören har en fungerande och ändamålsenlig sambandsförmåga.

Uppdraget omfattar bland annat att fastställa inriktning för sambandstjänsten, säkerställa att organisationen, resurserna och kompetensen är tillräckliga samt att sambandsfrågor beaktas i aktörens övergripande planering.

Hur rollen är organisatoriskt placerad och om den är förenad med personansvar kan variera mellan aktörer.

Sambandsansvarig (SA)

Sambandsansvarig ansvarar för sambandsverksamheten inom ett utpekat ansvarsområde, till exempel ett geografiskt område, en process eller en del av organisationen.

Rollen har ett funktionellt ansvar med fokus på planering, förvaltning och tillämpning av sambandstjänst inom sitt ansvarsområde. Arbetet kan omfatta sambandsplanering, rutiner, teknisk utrustning och samverkan med andra aktörer.

Sambandsansvarig ansvarar främst för planering och uppföljning. Detta till skillnad från sambandschefen som har ett övergripande ansvar för hela sambandsorganisationen och sambandsledaren som leder genomförandet i en pågående situation.

Sambandsansvarig arbetsleds av sambandschefen.

7.3.2 Operativ nivå: Sambandsledning

Sambandsledning är avgörande för att sambandstjänsten ska fungera under själva genomförandet.

Sambandsledare (Sbled)

Sambandsledaren ansvarar för att leda sambandstjänsten under pågående verksamhet eller händelse i enlighet med fastställd inriktning och beslut.

Rollen omfattar att fördela sambandsresurser, följa sambandsläget, fatta beslut om anpassningar samt säkerställa att sambandet fungerar mellan berörda aktörer.

Vid ett aktörsgemensamt samband samverkar sambandsledarna med varandra för att säkerställa en fungerande informationsöverföring.

Sambandsledning kräver goda kunskaper om sambandsmetoder, tekniska lösningar och samverkansformer. Rollen bör därför, när så är möjligt, bemannas som en egen funktion och inte enbart som en tillikauppgift.

7.3.3 Operativ nivå: Genomförande

På den operativa nivån för genomförande finns två roller: sambandsoperatör och sambandstekniker.

Sambandsoperatör (SbOp)

Sambandsoperatören verkar nära verksamheten och är ofta den som i realtid använder sambandsmedlen eller stöttar dem som använder sambandsmedlen. Rollen är central för att säkerställa att information når rätt mottagare i rätt tid och i enlighet med fastställda rutiner, instruktioner och säkerhetskrav.

Sambandstekniker (SbTekn)

Sambandsteknikern ansvarar för att sambandsmedel och tekniska stödsystem fungerar på avsett sätt. Rollen kräver teknisk kompetens, både generellt och för de sambandssystem som används av aktören.

Uppdraget kan omfatta installation, konfigurerings, övervakning och felsökning av sambandslösningar samt tekniskt stöd vid upprättande och drift av ledningsplatser.

Hur rollen benämns och organiseras kan variera mellan aktörer. Det avgörande är att den tekniska kompetens som krävs för att upprätthålla sambandsförmågan finns tillgänglig.



? Fungerar vår organisation för sambandstjänst i praktiken?

Har vi tydligt beskrivit hur sambandstjänsten är organiserad i vår verksamhet – i vardagen, vid kris och vid höjd beredskap?

Är roller och ansvar för samband tydliga, kända och accepterade – från strategisk nivå till hantering vid genomförande?

Vet vi vem som har mandat att planera, upprätta, leda och förändra samband under pågående hantering?

Har vi säkerställt att sambandstjänsten är bemannad med rätt kompetens över tid – även vid längre händelser, hög belastning eller personalbortfall?

Finns det en tydlig koppling mellan sambandstjänsten och övrig lednings- och samverkansorganisation?

Har vi rutiner för samverkan med andra aktörers sambandsorganisationer, inklusive kontaktvägar, roller och ansvar vid gemensamma samband?

Är organisationen anpassad till våra faktiska sambandslösningar och metoder – inte tvärtom?

Kapitel 8

Sambandsplanering

8. Sambandsplanering

Detta kapitel är tänkt att användas praktiskt vid planering av samband – både i förväg och under pågående hantering. Resultatet av sambandsplaneringen är alltid någon form av sambandsplan, muntlig eller dokumenterad, som styr hur information faktiskt ska förmedlas.

8.1 Varför behövs sambandsplanering?

Sambandsplanering krävs för att säkerställa förmågan till informationsöverföring, oavsett beredskapsläge.

Sambandsplanering innebär att i förväg ta ställning till hur information ska delas för att uppgiften ska kunna lösas. Den ger ledningen ett underlag för beslut om sambandet och bör påbörjas snarast möjligt – så snart uppgiften blir känd. Detta innebär att aktören behöver ha tillgång till – och upprätthålla – både kapacitet och förmåga i relevanta sambandssystem.

Alla aktörer har ett eget ansvar för sin sambandsplanering. Den aktör som begär information, eller som leder och driver samverkan, ansvarar också för att besluta hur informationen ska delas, det vill säga att definiera och anvisa sambandsvägar.

Sambandsplaneringen ska möjliggöra en gemensam förmåga till ledning och samverkan, med stöd av de definitioner och metoder som beskrivs i denna handbok. Det krävs därmed en aktiv sambandsplanering både inom och mellan aktörer för att den samlade totalförsvarsförmågan ska fungera.

Den metod som beskrivs i detta kapitel återfinns i arbetssättet Sambandsplanering i ramverket Gemensamma grunder för ledning och samverkan, med vissa tillägg och anpassningar.

8.2 Sambandsplan – vad är det?

En sambandsplan är en beskrivning av metoder och tekniska system för informationsöverföring, utformad utifrån definierade behov. Sambandsplanen är ett verktyg för att säkerställa informationsförsörjning genom att strukturera och styra sambandet för exempelvis en händelse, en process, en aktör eller funktion.

Sambandsplanen kan tas fram som en del av förberedande planering eller som responsplanering i en pågående händelse. Resultatet av sambandsplaneringen är alltid någon form av sambandsplan – oavsett om den är enkel, muntlig eller dokumenterad i flera bilagor.

Sambandsplanen ska anpassas till den kontext som den ska stödja. Varje aktör avgör själv vilka delar som är relevanta utifrån den egna verksamheten.

En sambandsplan behöver dessutom löpande kunna anpassas till förändrade omständigheter. Planeringen bör alltid ta hänsyn till att det som planen ska stödja både kan växa och minska i omfattning. Därför är det viktigt ändringar av planen sker strukturerat och att det finns en ansvarig för varje sambandsplan.

8.3 Process för sambandsplanering

Processen för sambandsplanering som presenteras i det här kapitlet skapar förutsättningar och gemensamma grunder för att möjliggöra samplanering av samband mellan och inom aktörer. Syftet med processen för sambandsplanering är att på ett enkelt och strukturerat sätt omhänderta en aktörs behov av informationsöverföring.

Processen kan användas som stöd vid såväl förberedande planering som responsplanering, samt vid förmågeplanering och långsiktig förmågeutveckling.⁶ Den är tillämpbar i olika sammanhang, till exempel vid:

- övergripande sambandsplanering som beskriver den egna aktörens sambandsförmåga
- händelse- eller processspecifik planering, till exempel vid aktörsgemensam samverkan
- särskild rapportering.

Processen för sambandsplanering består av tre steg:

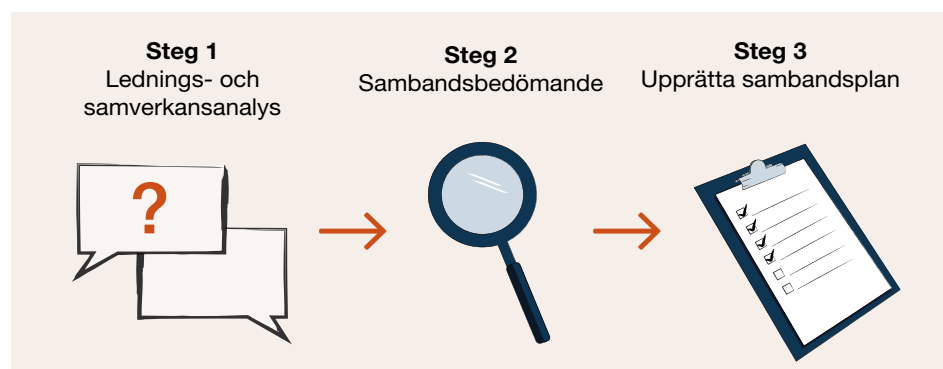
1. Lednings- och samverkansanalys
2. Sambandsbedömning – val av sambandssystem
3. Upprätta sambandsplan.

Det här avsnittet tar upp en processmodell i tre steg:

- **Steg 1:** Gör först analys av lednings- och samverkansbehov.
- **Steg 2:** Gör därefter bedömning och val av sambandssystem.
- **Steg 3:** Upprätta slutligen en sambandsplan.

Stegen följer i ordning från analys av behov, via val av sambandssystem, till färdig plan.

Figur 6. Processen för sambandsplanering.



Not 6. Planeringsformer inom det civila försvaret, MSB2594 – maj 2025.

8.3.1 Steg 1: Lednings- och samverkansanalys

Ett behov av informationsförsörjning skapar ett behov av informationsöverföring. För att kunna skapa en sambandsplan krävs en förståelse för aktörens behov av informationsförsörjning, vilket uppnås genom en lednings- och samverkansanalys.

Behovet av informationsförsörjning kan bland annat utgå från författningsstyrd rapportering, aktörsgemensam inriktning och samordning, interna behov och egen ledningsförmåga.

Frågor som stöd vid lednings- och samverkansanalys

- Vilka aktörer (interna som externa) ska dela information?
- Vilket syfte har informationsöverföringen?
- Är informationsöverföringen kritisk för aktörens uppdrag?
- Vilka informationstyper ska överföras – tal, textmeddelande, video eller data/filer?
- Vilka tidskrav har informationen? Hur ofta? Hur bråttom?
- Är informationen skyddsvärd eller säkerhetsskyddsklassificerad?

8.3.2 Steg 2: Sambandsbedömning – val av sambandssystem: Hur möter vi behoven?

Utifrån lednings- och samverkansanalysen väljs de sambandssystem som bäst möter behoven. Det är viktigt att bedöma för- och nackdelar med olika sambandssystem utifrån olika perspektiv (se faktaruta).

Perspektiv att beakta vid val av sambandssystem

- **Robusthet och resiliens:** Systemets förmåga att motstå störningar och återhämta sig efter avbrott.
- **Informationssäkerhet:** Systemets förmåga att upprätthålla informationens konfidentialitet, riktighet och tillgänglighet.
- **Tekniska och fysiska förutsättningar:** Geografisk och fysisk placering, tekniska systemegenskaper
- **Administrativa förutsättningar:** Krav på till exempel förvaltning och organisation för att upprätthålla systemet, krav på förvaring och fysiska krav för hantering av materiel och etableringstider.
- **Tillgängliga sambandssystem:** Vilka sambandssystem har den egna aktören tillgång till? Vilka sambandssystem har andra aktörer tillgång till?

Sambandsöversikt som stöd

En sambandsöversikt kan vara till stöd i sambandsplaneringen. En sambandsöversikt är en sammanställning av den tillgängliga förmågan och innehåller uppgifter om vilka sambandssystem som finns tillgängliga och vilka andra aktörer som kan nås på respektive sambandssystem. Sambandsöversikten är inte kopplad till ett behov eller sammanhang utan beskriver endast övergripande förutsättningar.

Tabell 17. Exempel på sambandsöversikt

System	E-post (Internet)	E-post (SGSI)	Telefoni (ATN)	WIS (Internet)	WIS (SGSI)	Rakel
Aktör A	X		X	X		
Aktör B	X	X	X	X	X	X
Aktör C	X	X	X	X	X	X
Aktör D	X		X	X		X
Aktör E	X	X	X	X	X	X
Aktör F	X	X	X	X	X	X
Aktör G	X		X	X		X
Aktör H	X		X	X		
Aktör I	X		X	X		X

Vid **responsplanering** måste planeringen utgå från de sambandssystem som är tillgängliga vid händelsen. Vid **förmågeplanering** kan analysen istället identifiera behov av ny förmåga genom nya sambandssystem.

Införande av nya system kräver god förberedande planering, både aktörsgemensamt och internt. Varje system behöver gå igenom aktörens godkännandeprocess för att säkerställa att det kan nyttjas inom ramen för infrastruktur, informationssäkerhet och (i förekommande fall) säkerhetsskydd.

Utöver en godkännandeprocess behöver aktören också säkerställa att man har den organisation och de lokaler som krävs för att omhänderta förvaltning, hantering och bemanning. Detta inkluderar även livscykelhantering, metoder och rutiner för användande samt utbildning, träning och övning.

Styrdokument att beakta

Vid sambandsplanering finns bland annat dessa styrdokument att ta hänsyn till:

- Myndigheten för samhällsskydd och beredskaps föreskrifter och allmänna råd (MSB FS 2025:4) om statliga myndigheters uppgifter inför och vid höjd beredskap.
- Nationella riktlinjer för samverkan i Rakel (MSB342 – reviderad december 2022).
- Nationella riktlinjer för samverkan och informationsdelning i WIS (MSB1146 – november 2017).
- Försvarsmaktens föreskrifter (FFS 2021:1) om signalskyddstjänsten.
- Myndigheten för samhällsskydd och beredskaps föreskrifter om civila myndigheters signalskyddsberedskap (MSB FS 2025:3).

8.3.3 Steg 3: Upprätta sambandsplan

I detta steg upprättas en sambandsplan. Sambandsplanen ska ge en tydlig struktur för hur information kan delas.

Sambandsplanen kan med fördel delas upp i internt samband (inom egen aktör) och det externa sambandet mellan olika aktörer. Sambandsplanen kan presenteras på olika sätt. Det viktiga är att sambandsplanen innehåller en beskrivning av

- den kontext som sambandet ska stödja
- vilka effekter som sambandet ska uppnå
- vilka sambandssystem och metoder som ska användas för att informationen ska kunna överföras
- hur sambandet leds och samordnas.

För att hantera olika behov av informationsöverföring delas sambandet upp i olika informationsbehov, till exempel inkallning, lägesrapportering, ledning eller samverkan mellan aktörer. Varje sådant behov behöver en tydlig och gemensam **sambandsväg** – alltså en beskrivning av hur informationen ska förmedlas i praktiken: vilka aktörer som deltar, vilka sambandsmedel som används, i vilken ordning och med vilka styrningar. Sambandsvägen omfattar även alternativ för redundans i händelse av att ordinarie sambandssystem har begränsad kapacitet eller är ur funktion.

Sambandsvägen kompletteras av en sambandsanvisning som beskriver sambandet på en övergripande nivå med sammanhang, syfte, inriktning och ansvar.

I den gemensamma grund som presenteras i det här kapitlet utgör sambandsanvisningen och beskrivningar av sambandsvägarna tillsammans en sambandsplan. Sambandsplanen kan sedan anpassas av enskilda aktörer.

PACE – en modell för kontinuitetshantering

PACE-modellen används för att reglera och strukturera sambandssystem i sambandsplanen. Syftet med PACE är att skapa redundans och förutsägbarhet redan i planeringen genom att beskriva hur man ska göra vid bortfall av ett eller flera sambandssystem.

Figur 7 visar hur sambandssystem prioriteras och struktureras i fyra nivåer med modellen PACE:

- **Primary (primär lösning):** Det primära sambandssystemet för att överföra informationen.
- **Alternate (alternativ lösning):** Detta är ett tillräckligt bra sambandssystem som kan användas som ett alternativ till det primära sambandssystemet.
- **Contingency (reservlösning):** Reservesambandssystemet används när de primära och alternativa sambandssystemen har begränsad kapacitet eller saknas helt.
- **Emergency (nödförfarande):** Nödsambandssystem används när samtliga andra sambandssystem är otillgängliga.

Figur 7. Visualisering av PACE-modellens fyra nivåer i syfte att prioritera och strukturera sambandssystemen i planeringen



Att använda sig av sambandssystem som är C eller E enligt PACE-modellen kan betyda att informationen behöver förändras på något sätt, till exempel att en kartbild behöver skickas i bildformat, att ett dokument behöver skrivas ut och överföras som ett fysiskt dokument eller att informationen behöver anpassas för att kunna skickas via tal.

Sambandsanvisning – från plan till genomförande

Sambandsanvisningen är en övergripande beskrivning av sambandet. För att sambandet ska kunna användas på ett samordnat och ändamålsenligt sätt behöver sambandsanvisningen alltid innehålla samma typ av information, oavsett struktur eller rubriksättning.

Följande delar behöver vara omhändertagna i sambandsanvisningen:

1. Sammanhang och förutsättningar

Sambandsanvisningen behöver tydliggöra i vilket sammanhang sambandet ska användas och vilka förutsättningar som påverkar informationsöverföringen. Exempel på frågor att besvara:

- Vad ska sambandet stödja?
- Vilka omständigheter påverkar informationsöverföringen – till exempel geografiskt läge, hotbild, beroenden till andra aktörer eller andra särskilda förutsättningar?

2. Effekt och syfte

Sambandsanvisningen behöver klargöra vad sambandet ska uppnå och vilket behov som styr användningen. Exempel på frågor att besvara:

- Vilken effekt ska informationsöverföringen bidra till?
- Vilket behov är styrande för sambandet i den aktuella situationen?
- Vad ska fungera bättre eller möjliggöras genom sambandet?
- Vilka informationstyper behöver kunna överföras för att uppnå syftet?

3. Inriktning och prioriteringar för sambandet

Sambandsanvisningen behöver ange hur sambandet övergripande ska användas och prioriteras. Inriktningen kan anpassas efter situation och aktörsgemensamma förutsättningar och kan uttryckas på olika sätt, till exempel genom ett inriktningsbeslut, ett Beslut i stort (BiS), en överenskommelse eller annan form av styrande vägledning. Exempel på frågor att besvara:

- Vilka ramar ska styra genomförandet?
- Vad ska prioriteras om allt inte kan hanteras samtidigt?

4. Genomförande

Sambandsanvisningen behöver beskriva hur sambandet ska bedrivas i praktiken. Själva beskrivningen av sambandsvägarna är därmed en del av genomförandet. Exempel på frågor att besvara:

- Hur och till vad ska sambandet användas operativt?
- Vilka sambandsmedel, talgrupper, frekvenser eller system ska användas?
- Hur ska passning, prioritering, kvittens och andra arbetssätt tillämpas?
- Hur ska informationsöverföringen fungera i praktiken, även vid störningar eller bortfall?

5. Ansvar, roller och mandat

Sambandsanvisningen behöver tydliggöra vem som gör vad – och med vilket mandat. Hur dessa delar rubriceras eller kombineras kan variera mellan aktörer. Det avgörande är att sambandsanvisningen ger ett tydligt och gemensamt handlingsstöd för dem som ska använda sambandet i praktiken. Exempel på frågor att besvara:

- Vem leder och anvisar sambandet?
- Hur är ansvar och roller fördelade under genomförandet?
- Vem har mandat att fatta beslut om förändringar eller anpassningar?
- Hur ska avvikelser, ändringar eller nya behov kommuniceras?

Beskrivning av sambandsvägar

En sambandsväg är ett sätt att strukturera informationsöverföring för ett specifikt informationsbehov. Den beskriver hur information ska förmedlas genom att tydliggöra vad som ska kommuniceras, vilka som deltar, vilka sambandsmedel som används (och i vilken ordning) samt vilka styrningar som gäller för genomförandet. Sambandsvägen svarar därmed på de frågor som behandlades under 4. Genomförande i föregående avsnitt.

En beskrivning av sambandsvägarna konkretiserar sambandsanvisningen och gör det tydligt hur informationsöverföringen ska fungera i praktiken. För att fungera som ett gemensamt operativt stöd ska varje sambandsväg alltid beskrivas med samma typer av information, oavsett om beskrivningen är muntlig eller dokumenterad.

Hur informationen struktureras kan variera mellan aktörer – till exempel i form av text eller tabell (se en variant i tabell 18). Det avgörande är att sambandsvägarna är så tydligt beskrivna att de kan användas, följas upp och vid behov anpassas under pågående verksamhet.

Tabell 18. Visualisering av sambandsvägar

Benämning	Användning	Aktörer	Informationstyp	P	A	C	E	Passning	Ledning
Lägesbild	Insamling och delning av lägesbilder	Aktör A, B, C	Data/filer/tal	E-post (Internet)	Telefon	Tal via radio	Ordonnans	3 h till 1 h innan lägesbilden sammanställs	Aktör A

Exempel: Sambandsvägen Lägesbild används för att dela information om aktuellt läge. I denna sambandsväg deltar aktörerna A, B och C:s ledningsfunktioner. Informationsöverföringen sker i första hand via e-post över internet, i andra hand via telefon, i tredje hand via radio och som sista utväg via ordonnans. Passning på telefon och radio gäller från tre timmar till en timme innan lägesbilden ska sammanställas. Aktör A ansvarar för sambandsvägen.

Följande information ska alltid finnas med i en beskrivning av sambandsvägar:

1. Benämning på sambandsvägen

Sambandsvägen behöver ha en tydlig och igenkännbar benämning som gör det enkelt att hänvisa till den i tal och skrift. Exempel: "Lägesbild område Y", "Ledning avdelning 2" eller "Samverkan Bron". Tydliggör följande:

- Vad ska sambandsvägen kallas?
- Är benämningen begriplig för alla berörda aktörer och funktioner?
- Går det att använda benämningen konsekvent i både planering och genomförande?

2. Syfte och användning

Beskrivningen behöver klargöra vad sambandsvägen används till och vilket informationsbehov den ska tillgodose. Exempel: "Delning av lägesbild", "Ledning från avdelningschef till underställda chefer" eller "Samverkan mellan aktörer vid Bron". Tydliggör följande:

- Vilken typ av information ska förmedlas via sambandsvägen?
- I vilket sammanhang ska sambandsvägen användas?
- Vad är det övergripande syftet med informationsöverföringen?

3. Aktörer och funktioner

Sambandsvägen behöver tydligt ange vilka som ingår i informationsöverföringen, det vill säga vilka aktörer, funktioner eller roller som ingår i sambandsvägen – både inom och utanför den egna organisationen. Exempel: "Aktör A, B och C", "Avdelningsledning 2 och enhetsledning 1–3" eller "Platschef hos respektive aktör". Tydliggör följande:

- Vilka aktörer deltar i sambandsvägen?
- Vilka funktioner eller roller representerar respektive aktör?

4. Sambandsmedel och deras inbördes ordning

Beskrivningen behöver ange vilka sambandsmedel som ska användas och i vilken ordning. Exempel: "WIS, yta X", "Chatt, grupp A2", "Radio, kanal 5" eller "Lägesbildssystem via internet". Tydliggör följande:

- Vilka sambandsmedel, talgrupper, frekvenser, kanaler eller motsvarande ska användas för informationsöverföringen?

5. Passning, tidsstyrning och prioritering

Sambandsvägen behöver beskriva hur tillgänglighet och tidskrav ska hanteras. Exempel: "Cyklisk, en gång per timme", "Första fem minuterna varje timme" eller "Ständig passning". Tydliggör följande:

- Hur ofta ska sambandsmedlet kontrolleras eller bevakas?
- När ska information förmedlas – vid behov, enligt schema eller vid särskilda tidpunkter?
- Har sambandsvägen någon särskild prioritet jämfört med andra?

6. Ansvar och ledning för sambandsvägen

Slutligen behöver det vara tydligt vem som ansvarar för eller leder sambandsvägen under genomförandet. Exempel: "Aktör B", "Sambandsansvarig Avd 2" eller "Sambandsledare, Aktör C". Tydliggör följande:

- Vem har ansvar för att sambandsvägen fungerar?
- Vem fattar beslut vid förändringar, avvikelser eller behov av anpassning?

8.4 Relaterade dokument

En sambandsplan kan behöva kompletteras med ytterligare dokument som samlar praktiska uppgifter, kontaktvägar eller särskilda instruktioner. Sådana dokument kopplas till sambandsplanen och utgör ett stöd i genomförandet.

8.4.1 Sambandskatalog

En sambandskatalog är en förteckning över relevanta kontaktuppgifter. Sambandskatalogen kan upprättas kopplat till en specifik sambandsplan eller som en mer generell förteckning över kontaktuppgifter.

Sambandskatalogen kan till exempel innehålla:

- telefonnummer
- Rakel-nummer och talgrupper
- e-postadresser
- postadresser
- nummer eller adresser till digitala konferensfunktioner.

Generellt sett bör sambandskatalogen innehålla kontaktuppgifter till funktioner och roller snarare än personer.

8.4.2 Ordonnansplan

En ordonnansplan beskriver hur informationsöverföring ska gå till när det av olika anledningar inte går att använda tekniska system. Planen kan innehålla information om platser, tider och metoder för överlämning av information.



? Är vår sambandsplan redo att tas i bruk?

Innan sambandsplanen tas i bruk kan följande frågor användas som en sista avstämning:

Har sambandsplanen förankrats hos de funktioner och aktörer som ska använda den? Finns det identifierade beroenden till andra planer, beslut eller aktörer som behöver beaktas i genomförandet?

Är sambandsplanen tillräckligt enkel för att kunna användas även under tidspress och störda förhållanden? Är sambandsplanen anpassad till den bemanning och kompetens som finns tillgänglig?

Finns alternativa lösningar om ordinarie bärare slås ut? Vet berörd personal *när* och *hur* bytet ska ske i praktiken?

Är ansvar och roller tydliga? Vet vi vem som leder sambandet? Vet berörda funktioner var sambandsplanen finns och hur de får tillgång till den?

Är sambandsplanen möjlig att öva, testa eller verifiera innan den behöver användas skarpt?

Är det tydligt hur och när sambandsplanen ska uppdateras eller justeras vid förändrade förutsättningar? Vem tar initiativ om sambandet inte fungerar som planerat?

Kapitel 9

Utbildning, träning och övning

9. Utbildning, träning och övning

Utbildning, träning och övning är grundförutsättningar för att samband ska fungera i praktiken. Sambandssystem består inte enbart av teknik, utan av människor, roller, rutiner och gemensamma arbetssätt. Utan tillräcklig kunskap och övning riskerar även väl fungerande teknik att användas fel, eller inte alls.

9.1 Skillnaden mellan utbildning, träning och övning

Utbildning, träning och övning kompletterar varandra och behöver kombineras över tid för att bygga och vidmakthålla förmåga. Utbildning ger kunskap, träning ger färdighet och övning prövar förmågan – tillsammans bygger de en robust och uthållig förmåga.

9.1.1 Utbildning

Utbildning syftar till att ge personalen kunskap och förståelse för samband, till exempel begrepp, roller, metoder, regelverk och system.

Utbildning är viktigt för att ge personalen kunskap om sambandets förutsättningar, begränsningar och regelverk, vilket är en förutsättning för korrekt och säker informationsöverföring.

9.1.2 Träning

Träning innebär att öva avgränsade moment i liten skala för att befästa färdigheter, till exempel att använda ett sambandsmedel, följa en anropsrutin eller byta sambandsväg.

Träning är viktigt för att befästa praktiska färdigheter och minska osäkerhet i enkla moment som annars riskerar att skapa onödiga störningar i sambandet. Sambandet fallerar ofta på grund av enkla handhavandefel.

9.1.3 Övning

Övning genomförs på organisationsnivå och prövar samband i ett sammanhang som liknar verkliga situationer. Övning mäter måluppfyllnad utifrån de mål som satts för övningen.

Övning är viktigt för att

- identifiera brister och beroenden som inte syns i planering eller dokumentation, men som får konsekvenser i skarpa lägen (utforskande övning)
- utveckla och verifiera organisationens samlade förmåga, inte bara individens kunskap (prövande övning).

9.1.4 Utvärdering och erfarenhetshantering

Det är centralt att såväl utbildning, träning som övning utvärderas och att erfarenheterna används för att utveckla förmågan. Utvärdering och erfarenhetshantering kräver både tid och resurser, men är väsentligt för att upprätthålla och stärka förmågan.

9.2 Befintliga utbildningar

I dagsläget finns fastställda utbildningar främst kopplade till specifika system och verktyg, till exempel Rakel och WIS. Dessa utbildningar fokuserar på systemanvändning och tillhandahålls av respektive systemägare eller ansvarig myndighet.

Inom signalskyddsområdet finns ett omfattande och etablerat utbildningsutbud. Utbildningar inom signalskydd genomförs inom ramen för Totalförsvarets signalskyddstjänst och återfinns i Totalförsvarets signalskyddsskolas (TSS) kurskatalog. Dessa utbildningar riktar sig till särskilda roller och funktioner och regleras av gällande styrning (se avsnitt 4.3).

9.3 Utveckling av utbildningar framåt

Myndigheten för civilt försvar planerar att vidareutveckla och samla utbildningsstöd inom området samband och sambandstjänst. Arbetet omfattar både innehåll, målgrupper och former för utbildning, till exempel grundläggande utbildning, fördjupning och stöd för övning.

Information om tillgängliga utbildningar, rekommenderade utbildningsvägar och framtida utbildningsinsatser kommer att samlas på en gemensam samlings-sida på mcf.se.



? Har vi rätt utbildning och övning för vårt samband?

Har berörd personal grundläggande kunskap om sambandets begrepp, principer och arbetssätt – utöver systemspecifik utbildning?

Har chefer och beslutsfattare tillräcklig förståelse för sambandets möjligheter, begränsningar och beroenden?

Har berörd personal utbildats och fått möjlighet att öva sina roller i sambandstjänsten, så att organisationen fungerar även under stress och i påverkade lägen?

Är utbildningen anpassad till specifika roller och funktioner inom sambandstjänsten?

Har vi övat samverkan och informationsöverföring tillsammans med andra aktörer – inte bara internt?

Fångar vi upp erfarenheter från utbildning och övning – och använder vi detta som underlag för att förbättra rutiner, planer och sambandslösningar?

Bokstaveringsalfabetet

Tabell 19. Bokstaveringsalfabetet på svenska och engelska

Bokstav	Svenska	Engelska
A	ADAM	ALFA
B	BERTIL	BRAVO
C	CAESAR	CHARLIE
D	DAVID	DELTA
E	ERIK	ECHO
F	FILIP	FOXTROT
G	GUSTAV	GOLF
H	HELGE	HOTEL
I	IVAR	INDIA
J	JOHAN	JULIETT
K	KALLE	KILO
L	LUDVIG	LIMA
M	MARTIN	MIKE
N	NIKLAS	NOVEMBER
O	OLOF	OSCAR
P	PETTER	PAPA
Q	QVINTUS	QUEBEC
R	RUDOLF	ROMEO
S	SIGURD	SIERRA
T	TORE	TANGO
U	URBAN	UNIFORM
V	VIKTOR	VICTOR
W	WILHELM	WHISKEY
X	XERXES	X-RAY
Y	YNGVE	YANKEE
Z	ZÄTA	ZULU
Å	ÅKE	ALFA ALFA
Ä	ÄRLIG	ALFA ECHO
Ö	ÖSTEN	OSCAR ECHO

Bokstavering sker på svenska om inget annat meddelas. Vid tillfällen då samverkan sker med utländska aktörer används internationell bokstavering.

Tabell 20. Uttal av siffror på svenska och engelska

Siffra	Svenska	Engelska
1	ETT	ONE
2	TVÅA	TWO
3	TREA	THREE
4	FYRA	FOUR
5	FEMMA	FIVE
6	SEXA	SIX
7	SJU	SEVEN
8	ÅTTA	EIGHT
9	NIA	NINER
0	NOLLA	ZERO



**Myndigheten
för civilt försvar**