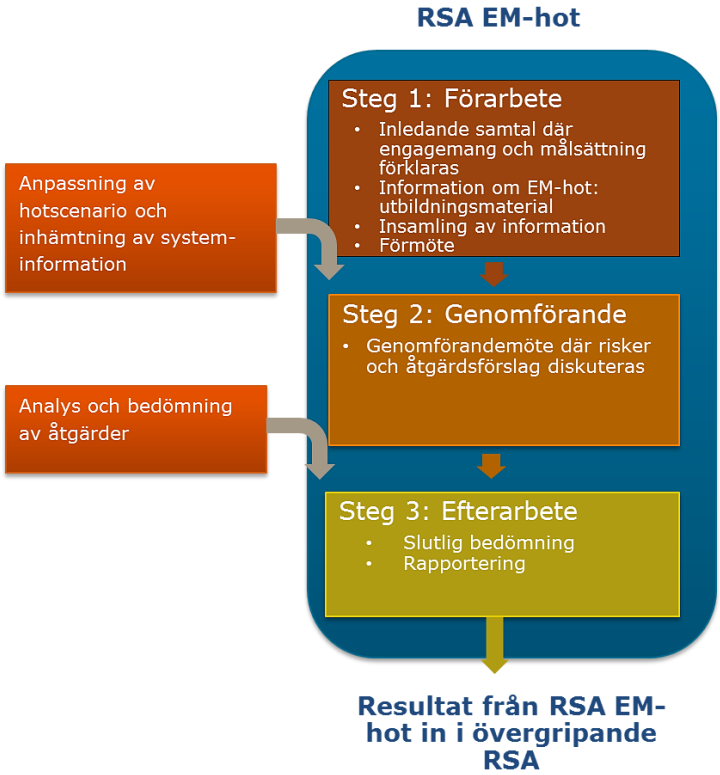
Myndigheten för samhällsskydd och beredskap

FOI

Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur



Faktaruta

Denna skrift avser att utgöra en vägledning för den som planerar att genomföra en risk- och sårbarhetsanalys (RSA) avseende avsiktliga elektromagnetiska hot (EM-hot) mot samhällsviktig verksamhet och kritisk infrastruktur.

Framtagning av denna vägledning har genomförts på uppdrag av och med stöd från MSB.

2017

Totalförsvarets forskningsinstitut, FOI

Kia Wiklundh, Sara Linder, Karina Fors, Tomas Hurtig, Sten E Nyholm

Många samhällsviktiga verksamheter förlitar sig idag på elektroniska system och trådlösa kommunikationssystem. Eftersom dessa kan vara mycket känsliga för elektromagnetisk (EM) påverkan, utgör avsiktliga EM-störningar ett reellt hot mot samhällsviktig verksamhet. Denna vägledning erbjuder ett metodstöd för genomförande av risk- och sårbarhetsanalyser (RSA:er) avseende EM-hot. Materialet beskriver hur man kan förbereda och genomföra en RSA EM-hot samt innehåller frågeställningar som kan användas för att identifiera sårbarheter i samhällsviktig verksamhet och kritisk infrastruktur.

MSB:s kontaktperson:
Gustav Söderlind, 010-240 42 57

Publikationsnummer MSB1178 - februari 2018
ISBN 978-91-7383-803-0

MSB har beställt och finansierat genomförandet av denna studierapport. Författarna är ensamma ansvariga för rapportens innehåll.

Förord

Denna vägledning är avsedd för de personer vid myndigheter, landsting, länsstyrelser och kommuner som avser att genomföra en risk- och sårbarhetsanalys (RSA) rörande avsiktliga elektromagnetiska hot (EM-hot) mot samhällsviktig verksamhet och kritisk infrastruktur. Vägledningen kan även användas av teknisk kompetens (konsulter) som bistår en organisation vid genomförandet av arbetet.

Eftersom avsiktliga EM-hot är av ren teknisk natur och slår mot tekniska apparater och system, ofta utan andra direkt märkbara effekter, kräver en sådan RSA tillgång till god teknisk systemkunskap. Dessutom behövs det kännedom om de nya EM-hot som utvecklats under de senaste åren och hur de skulle kunna användas. Denna typ av hot mot samhällsviktig verksamhet och kritisk infrastruktur har blivit allt mer uttalat med den ökande tillgången till kommersiella störsändare, men även informationsspridning om hur man konstruerar kraftiga elektromagnetiska pulskällor som på några tiotal meters avstånd kan störa, eller i vissa fall t.o.m. förstöra, elektronisk utrustning. Det är också känt att flera länder studerar och utvecklar vapen som kan avge kraftiga mikrovågspulser, som skulle kunna användas även mot civila system på kilometeravstånd vid en militär konfrontation.

Denna rapport är framtagen av FOI på uppdrag av MSB, MSB 2017-7212.

Arbetet har genomförts med stöd av en referensgrupp bestående av representanter från MSB, FortV, FHS, FMV och FOI samt Centrala Beredningsgruppen Elektromagnetiska hot (CBG EM-hot).

Innehållsförteckning

Förord **4**
Innehållsförteckning **5**
Sammanfattning **7**
1. Inledning **8**
1.1 Bakgrund 8
1.2 Syfte och målgrupp 9
1.3 Litteraturrekommendationer 10
1.4 Sekretess 11
1.5 Definitioner 12
2. Allmänt om risk och sårbarhetsanalys **16**
2.1 Komponenter i en RSA 16
2.1.1 Utgångspunkter 17
2.1.2 Riskidentifiering – Tekniska konsekvenser 18
2.1.3 Riskanalys – Verksamhetskonsekvenser 18
2.1.4 Riskutvärdering 19
2.1.5 Sårbarhetsbedömning 21
2.1.6 Riskbehandling 21
2.2 Kompetenser vid genomförande av en RSA avseende EM-hot 21
2.3 Hotscenarier 22
2.4 Dokumentation 26
3. EM-hot och påverkan på elektroniska system **27**
3.1 Faktorer som påverkar sannolikheten för en EM-attack 28
3.2 Faktorer som påverkar konsekvenserna av en EM-attack 30
3.2.1 Avsiktlig icke-förstörande störning 31
3.2.2 Avsiktlig förstörande störning 32
4. Praktiskt metodstöd för genomförande av RSA avseende avsiktliga EM-hot **34**
4.1 Översikt av arbetsgången 34
4.2 Förutsättningar 34
4.2.1 Roller – uppgifter och ansvar 34
4.2.2 Tid för genomförande 36
4.2.3 Hotnivå 36
4.3 Förarbete 36
4.4 Genomförande 38
4.5 Efterarbete 40
4.6 Kommentarer till processen 41
5. Slutord **44**

Referenser **45**
Bilaga 1: Hotscenarier **47**
Typfall med vidare kontext 47
Typscenarier 48
Typscenario 1 - Militär antagonist med insmugglat Mikrovågsvapen 49
Typscenario 2 - Terroristorganisation som använder kommersiella störsändare 50
Typscenario 3 - Terroristgrupp eller kriminellt gäng med hemmabyggd IEMI-källa 51
Bilaga 2: Mallar **52**
Förberedelser 53
Förarbete 54
Genomförande 56
Efterarbete 61

Sammanfattning

Vägledningen är tänkt att vara ett stöd vid risk- och sårbarhetsanalyser avseende antagonistiska EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur. Arbetet bör vara en del av en större RSA som omfattar alla möjliga risker för samhällsviktig verksamhet och kritisk infrastruktur. Däremot skiljer EM-hotet sig från många andra risker då risken beror på en antagonist som vill åstadkomma skada i ett system. Dessutom är EM-hotet ett tekniskt hot som verkar mot elektroniska system om vilka det kan behövas specialkunskap för att kunna bedöma vilken skada en antagonist kan åstadkomma.
Vägledningen ger metodstöd för genomförande av en RSA avseende EM-hot genom specificering av olika uppgifter, en indelning av arbetet i flera steg samt ett antal vägledande specifika frågeställningar som hjälp i varje steg. Det ges även exempel på hotscenarier och förslag på mallar för att strukturera arbetet och dokumentera resultaten.

1. Inledning

1.1 Bakgrund

Det åligger statliga myndigheter, landsting, länsstyrelser och kommuner att regelbundet genomföra risk- och sårbarhetsanalys (RSA) för sin verksamhet i syfte att kartlägga sårbarheter i samhällsviktig verksamhet och kritisk infrastruktur och för att öka förmågan att hantera många olika typer av kriser. Bland den stora mängden potentiella hot återfinns naturfenomen som åska, orkaner och översvämningar, oavsiktliga samhällsstörningar som olyckor och konstruktionsfel. Men det finns även avsiktliga hot som militära angrepp, terrorism och kriminalitet, där det finns en antagonist med onda avsikter. Denna vägledning fokuserar på antagonistiska elektromagnetiska (EM) hot.

Det som särskiljer avsiktliga elektromagnetiska hot från de flesta andra hot som samhället kan utsättas för är att de är relativt nytillkomna och att de flesta medborgare har tämligen vaga föreställningar om hur EM-hot kan se ut och uppträda i händerna på en antagonist. Dessa hot består av användning av störsändare eller mikrovågsvapen som kan störa eller förstöra elektronik på kortare eller längre avstånd.

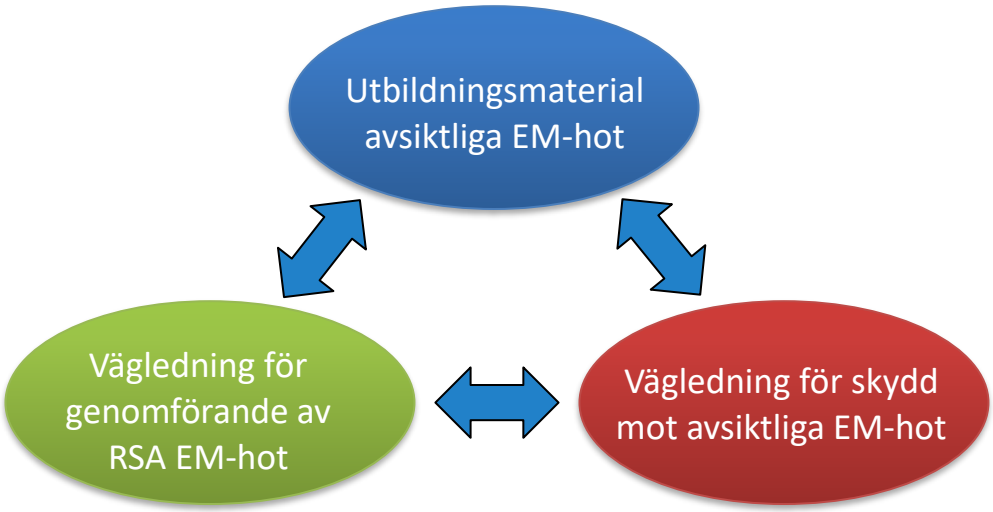
Det finns idag en stor flora av störsändare för de flesta frekvensband som idag används för trådlös kommunikation. Många störsändare säljs öppet på internet, även om det ofta anges att det kan förekomma lagliga restriktioner på innehav av sådana. Innehav och användning av störsändare är förbjudet i Sverige, men det finns risk för att någon olagligt inför utrustning som anskaffats utomlands.

Sedan 1960-talet har man i flera länder bedrivit forskning och utveckling av vapen som sänder iväg skurar av mikrovågor (eng. High-Power Microwave, HPM) för att på avstånd kunna förstöra fiendens elektroniska utrustning, som sensorer, datorer, kommunikationsutrustning, m.m. De senaste decennierna har man sett verkanstester av prototyper till mikrovågsvapen, samt koncept för montering av mikrovågsvapen på olika typer av plattformar. Dessa militära mikrovågsvapen kan avge mikrovågsstrålning i korta pulser med mycket hög toppeffekt som kan riktats mot utsedda målobjekt. Uppgifter har förekommit om verkansavstånd på hundratals meter och ibland flera kilometer, t.ex. som luftvärn för att skjuta ned drönare.

Teknikutvecklingen inom området har stimulerat elektronikintresserade ungdomar att själva bygga störsändare eller enkla mikrovågsvapen och lägga ut ritningar och instruktioner på internet. De har kunnat demonstrera verkan på många olika typer av vardagselektronik på korta avstånd, typiskt något tiotal meter. Även om avsikterna inte varit illasinnade utan man bara agerat av teknisk nyfikenhet, finns risken att sådana exempel inspirerar kriminella eller antagonistiska grupper som vill orsaka störningar i samhället för att uppnå sina syften.

Denna vägledning med metodstöd är ett resultat av ett MSB-finansierat uppdrag till FOI och baseras bland annat på två pilotstudier som gjordes under hösten 2017 och avrapporteras i ”Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur” [1].

Metodstödet utgör en del i ett större material med målsättningen att stödja och medvetandegöra verksamhetsansvariga om EM-hot mot samhällets kritiska infrastruktur samt anvisa principer för att kunna åtgärda brister. Förutom metodstödet finns också ett utbildningsmaterial kring EM-hot [2] samt en av Fortifikationsverket framtagen vägledning kring skydd mot avsiktliga EM-hot [3], se Figur 1.



Figur 1. Kompletterande material för arbete med EM-hot mot samhällsviktig verksamhet: ”Utbildningsmaterial avsiktliga EM-hot”, ”Vägledning för genomförande av RSA EM-hot” (föreliggande rapport) samt ”Vägledning för skydd mot avsiktliga EM-hot” (utgiven av Fortifikationsverket).

1.2 Syfte och målgrupp

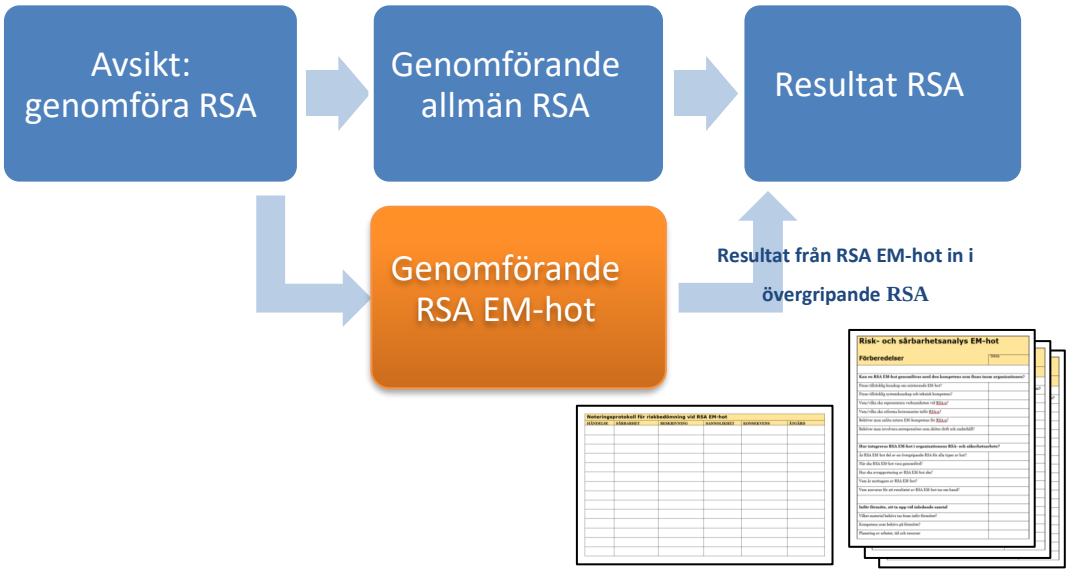
Denna vägledning är tänkt att användas vid genomförande av risk- och sårbarhetsanalyser avseende elektromagnetiska hot mot offentliga aktörers anläggningar och system som innehåller elektronisk utrustning som olika kommunikationssystem, datorer, styr- och kontrollsystem, säkerhetssystem, m.m. Utrustning som exempelvis kan ha betydande funktion i datorhallar, vattenverk, trafiksignalsystem, kommunikationsradiocentraler, sjukhus, m.fl.

Vägledningen syftar till att vara ett metodstöd vid genomförandet av RSA för EM-hot. Metodstödet är dock inte tänkt att utgöra en fullständig beskrivning av genomförandet av en RSA eller att ersätta etablerade metoder för RSA som MSB:s vägledning för risk- och sårbarhetsanalyser [4] och FORSA [5] , utan vara ett komplement till dessa. Metodstödet baseras på etablerade metoder för RSA-arbete, men denna vägledning är dock inte bunden till någon specifik metod utan är avsedd att kunna användas tillsammans med den aktuella metod

som verksamhetsägaren valt för genomförande av RSA. (exempelvis kvalitativa eller kvantitativa analysmetoder, se t.ex. [4], [5] eller [6]).

Vägledningen ska kunna användas som ett stöd främst under riskidentifiering, riskanalys och riskvärdering när man behandlar olika elektromagnetiska hot som den studerade verksamheten skulle kunna utsättas för. Den kan även utgöra ett bakgrundsmaterial för senare delar av RSA-processen, som sårbarhetsbedömning och riskbehandling, men dessa delar är mera verksamhetsspecifika och mindre generella till sin natur.

Avsikten är att resultaten från RSA-arbetet rörande EM-hot ska vara en del av och komplettera resultat framkomna från en övergripande RSA med ett mer generellt fokus, se Figur 2.



Figur 2. Resultaten från RSA med avseende på EM-hot bör ingå som del av verksamhetens övergripande RSA.

1.3 Litteraturrekommendationer

Det finns en del litteratur inom ämnena EM-hot samt risk- och sårbarhets-analyser som kan rekommenderas för att ge en bredare bild av området än vad som ingår i denna vägledning.

För att få en introduktion till EM-hot och vilka riskreducerande skyddsåtgärder som är möjliga kan man studera

- ”Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur” [2], (ger en översikt av kända EM-hot och hur de kan användas i antagonistiska syften), samt
- ”Vägledning Skydd mot avsiktliga EM-hot” [3], Fortifikationsverket, (ger råd och praktiska anvisningar för skyddsåtgärder mot EM-hot).

För anvisningar om hur en risk- och sårbarhetsanalys i offentlig verksamhet bör genomföras hänvisas till MSB:s publikationer:

- ”Vägledning för Risk- och sårbarhetsanalyser” [4],
- ”Myndigheten för samhällsskydd och beredskaps föreskrifter om landstings risk- och sårbarhetsanalyser” [7],
- ”Myndigheten för samhällsskydd och beredskaps föreskrifter om kommuners risk- och sårbarhetsanalyser” [8] samt
- ”Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser” [9].

Generella principer och riktlinjer för riskhanteringsprocessen ges i

- ”Riskhantering - Principer och riktlinjer”, Svensk Standard SS-ISO 31000:2009.[6]
- ”FOI:s modell för risk- och sårbarhetsanalys (FORSA)”, Totalförsvarets forskningsinstitut (FOI), FOI-R--3288--SE, 2011.[5]

Som fördjupad läsning om systematisk elmiljöverksamhet rekommenderas

- ”Elektromagnetisk miljö användarhandbok” (EMMA) Utgåva 2, Försvarets materielverk, 2002, M7773-000750.[10]

1.4 Sekretess

Vid genomförandet av RSA kan det finnas behov av en extern part som bidrar med kompetens om EM-hot. I dessa dialoger då sårbarheter identifieras och sammanställs kan informationen komma att omfattas av sekretess.

I 18 kap. 13 § offentlighets- och sekretesslagen (OSL) ges möjlighet att skydda uppgifter i upprättade risk- och sårbarhetsanalyser [11]. Det innebär att uppgifter som berör en myndighets[1] verksamhet och som består av risk- och sårbarhetsanalyser avseende fredstida krissituationer, planering och förberedelser inför sådana situationer, eller hantering av sådana situationer kan omfattas av sekretess.

Risk- och sårbarhetsanalyserna syftar till att minska samhällets sårbarhet, bl.a. genom att öka myndigheters förmåga att förutse och hantera krissituationer i fredstid och vid krig. För att uppgifterna inte ska kunna utnyttjas för angrepp mot myndigheter, enskilda eller samhället i stort, är det i viss utsträckning nödvändigt att begränsa insynen in denna verksamhet.

Även andra sekretessbestämmelser kan bli tillämpliga på uppgifter i risk- och sårbarhetsanalyser, t.ex. 15 kap. 2 § (Försvarssekretess), 18 kap. 8 § (Skydd av byggnader och anläggningar) och 9 § (Koder m.m.) i offentlighets- och sekretesslagen (OSL) [11].

Sekretessklassningen av verksamhetens system och sårbarheter sker av verksamhetsägaren. Verksamhetsägaren har ansvar att tillse att information om system och sårbarheter hanteras med vederbörlig sekretess, bl.a. med

[1] Vid tillämpning av OSL jämställs riksdag, beslutande kommunala församlingar, bolag där kommuner eller landsting utövar inflytande, etc. med myndigheter.

ledning av OSL, och avgör hur informationen ska hanteras i det vidare arbetet. Även EM-hotens utformning och scenarier kan omfattas av sekretess.

1.5 Definitioner

Antagonist - Person, grupp av personer eller organisatorisk enhet som har för avsikt att orsaka negativa effekter eller skador på en studerad verksamhet, t.ex. på samhällsviktig verksamhet eller utrustning.

Elektromagnetisk störning/interferens – Förekomst av elektromagnetisk strålning eller ledningsbunden elektrisk energi, antingen kontinuerligt eller i form av korta pulser, som har en oönskad negativ effekt på elektronisk utrustning. En elektromagnetisk störning kan antingen vara av tillfällig natur så länge störningen pågår eller innebära permanent funktionsnedsättning eller funktionsbortfall även efter att störningen upphört.

EM-hot – Betecknar i detta sammanhang elektromagnetiska störningar, både oavsiktliga och avsiktliga, som kan ge en svår negativ påverkan på en samhällsviktig funktion/värde.

EM-källa / EMI-källa - Naturfenomen eller apparat som avger elektromagnetisk strålning.

EMI - *Elektromagnetisk interferens*, sammanfattande benämning på fenomen som uppträder när elektromagnetisk strålning påverkar elektronisk utrustning.

GNSS – *Global Navigation Satellite Systems*, samlingsnamn för satellitbaserade navigations- och positionsbestämningssystem, som exempelvis *Global Positioning System,* GPS.

Gråzon - Ett läge eller en situation som ligger någonstans mellan två klart åtskilda väldefinierade situationer. Här använt speciellt i en situation när det är oklart om det råder fred eller krig. Jämför Skymningsläge.

HPM - mikrovågsvapen med hög toppeffekt (eng. High-Power Microwave). Se Mikrovågsvapen.

Händelse - Förekomst eller förändring av särskilda omständigheter, [6].

Höjd beredskap - Regeringen kan besluta om höjd beredskap för att stärka Sveriges försvarsförmåga vid krigsfara eller om det råder utomordentliga förhållanden pga. krig utanför Sverige. *Skärpt beredskap* kan införas vid extraordinära händelser t.ex. i en gråzon. *Högsta beredskap* råder om Sverige är i krig. Vid höjd beredskap ska statliga myndigheter, landsting och kommuner vidta de särskilda åtgärder som behövs för att under rådande förhållanden kunna fullgöra sina uppgifter i totalförsvaret [12].

IEMI - *Intentional EMI*, dvs. avsiktligt genererad elektromagnetisk interferens.

Intressent - Person eller organisation som kan påverka, påverkas av eller anser sig bli påverkad av ett beslut eller en aktivitet [6].

Konsekvens - Utfall från en händelse som påverkar målen [6].

Kritisk infrastruktur – Fysisk struktur vars funktionalitet bidrar till att säkerställa upprätthållandet av viktiga samhällsfunktioner [13].

Mikrovågsvapen – Utrustning som genererar kraftiga elektromagnetiska pulser med syfte att störa eller förstöra elektronisk utrustning, kan även benämnas HPM-vapen (High Power Microwave).

Resiliens - Förmåga att motstå och återhämta sig från störningar [13]. Jämför begreppet *stryktålighet* i Handbok verkansvärdring [14].

Risk - Osäkerhetens effekt på mål (ekonomi, hälsa, säkerhet, miljö). Risker karakteriseras ofta genom hänvisning till potentiella händelser och konsekvenser. Risker uttrycks ofta i termer av en kombination av en händelses konsekvenser relaterad till sannolikhet av förekomst [6].

Riskanalys - Process för att förstå riskens natur och avgöra risknivån [6]. Här görs en analys av de scenarion och riskkällor som identifierades i riskidentifieringen och ger svar på hur sannolik eller frekvent en händelse är och vilken konsekvens den medför givet att den inträffar. Innefattar inte att se till förmågeförändringens betydelse i ett större system

Riskbedömning - Övergripande process för riskidentifiering, riskanalys och riskutvärdering [6].

Riskbehandling - Process för att förändra risker, t.ex. eliminera riskkällan, förändra sannolikheten eller förändra konsekvenserna. Kan bestå av riskminskning, riskeliminering, riskförebyggande och riskreducering [6].

Riskidentifiering - Process för att (inom ett avgränsat system) upptäcka, kartlägga, känna igen och beskriva risker [6].

Riskkälla - Element som i sig självt eller i kombination har en inneboende potential att utgöra en risk [6].

Riskhantering - Samordnade aktiviteter för att styra och leda en organisation med avseende på risk [6]. Övergripande beteckning för hela arbetsprocessen med att identifiera, analysera och behandla risker.

Riskreducerande åtgärd - Åtgärd som avser att minska sannolikheten för eller konsekvensen av en identifierad risk. T.ex. konstruera ett skalskydd kring känslig elektronik.

Riskutvärdering - Process för att jämföra resultaten från riskanalysen med riskkriterierna för att avgöra om risken och/eller dess storlek är acceptabel eller godtagbar [6]. Här sammanförs data från riskanalysen för olika riskkällor och jämförs med varandra, vilket sedan blir ett underlag för sårbarhetsanalys och beslut om riskreducerande och/eller sårbarhetsreducerande åtgärder.

RSA - Risk- och sårbarhetsanalys.

Samhällsviktig verksamhet – En samhällsfunktion av sådan betydelse att ett bortfall av eller en svår störning i funktionen skulle innebära stor risk eller fara för befolkningens liv och hälsa, samhällets funktionalitet eller samhällets grundläggande värden [13].

Sannolikhet - Chans att något inträffar [6]. Kan baseras på frekvensen av hittills inträffade händelser, på uppskattningar eller gissningar. Sannolikheten kan vara kvantitativ eller kvalitativ och beskrivas i generella eller matematiska termer.

Susceptibilitet - En utrustnings mottaglighet eller känslighet för elektromagnetiska fält i omgivningen.

Skydd av samhällsviktig verksamhet – I det här samhanget avses alla de åtgärder, förebyggande, förberedande, avhjälpande och lärande, som bidrar till att värna/skydda verksamheten mot störningar och lindra konsekvenserna.

Skymningsläge - Ett tidsförlopp då ett samhällshot, yttre eller inre, kan observeras gå från hot till faktiska skadeeffekter. Används särskilt i ett läge då internationella väpnade konflikter är omedelbart förestående att spridas till eget territorium, men även i generellare betydelse då ett samhällshot håller på att materialiseras. [15]. Se Gråzon.

Störsändare - Radiosändare konstruerad med syfte att störa trådlösa kommunikationssystem.

Sårbarhetsanalys - Syftar till att detaljerat analysera hur allvarligt och omfattande en specifik händelse påverkar samhället eller den egna organisationen [4].

Sårbarhetsreducerande åtgärd - Åtgärd som avser att minska effekterna av en identifierad risk när den realiseras. T.ex. införa ett alternativt kommunikationssystem som kan användas när det studerade systemet blir utslaget.

Sällanhändelse - En händelse som inträffar sällan, dvs. frekvensen för denna typ av händelser är låg. Observera att sällanhändelser kan ha mycket svåra konsekvenser och därför ändå bör tas med i en RSA.

Totalförsvar - Verksamhet som behövs för att förbereda Sverige för krig; består av såväl militärt som civilt försvar. I krig utgörs totalförsvaret av all samhällsverksamhet som då ska bedrivas [12].

Transient - Ett svängningsförlopp av kort varaktighet, t.ex. en kort spänningspuls överlagrad den ordinarie nätspänningen.

Verksamhetsägare – Representant för verksamheten i genomförandet av en RSA.

Värde – Människor, material, materiel, information eller verksamhet som har väsentlig betydelse för ett företag eller en organisation.

2. Allmänt om risk och sårbarhetsanalys

2.1 Komponenter i en RSA

Syftet med risk- och sårbarhetsanalysarbetet är att öka medvetenheten och kunskapen hos beslutsfattare och verksamhetsansvariga om hot, risker och sårbarheter inom det egna verksamhetsområdet samt att skapa ett underlag för egen planering och prioritering av skyddsåtgärder.

RSA:er bör genomföras regelbundet för att följa upp effekten av genomförda riskreducerande och/eller sårbarhetsreducerande åtgärder samt för att inkorporera nytillkomna risker, som till exempel kan vara en följd av samhälls- och omvärldsutvecklingen eller en följd av förändringar i den egna verksamheten. En RSA kan genomföras med olika fokus beroende på verksamhetens karaktär och på omvärldsutvecklingen.

Riskhanteringsprocessen består av följande delar, se Figur 3 [4, 6]:

Utgångspunkter:

- Roll och ansvarsområde
- Metod, perspektiv och avgränsning

Riskbedömning

- Riskidentifiering
- Riskanalys
- Riskutvärdering

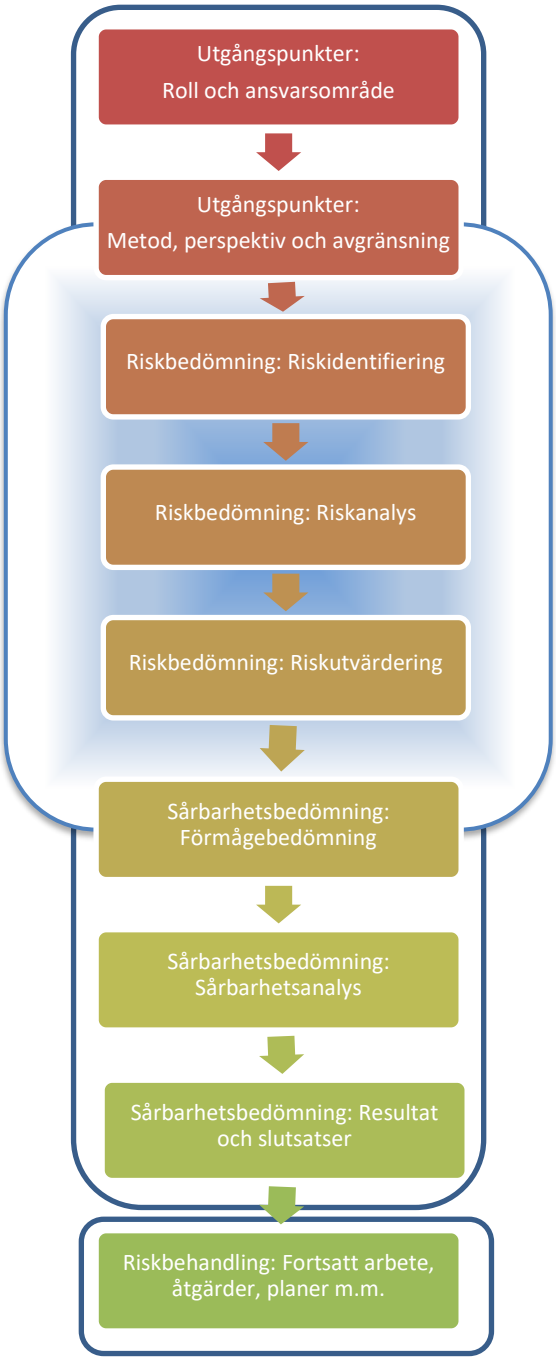
Sårbarhetsbedömning

- Förmågebedömning
- Sårbarhetsanalys
- Resultat och slutsatser

Riskbehandling

- Fortsatt arbete, åtgärder, planer m.m.

Det är främst i Riskbedömningen som teknisk kompetens krävs kring EM-hot och hur dessa påverkar system. Nedan beskrivs riskhanteringsprocessen i korta ordalag. Metoden som används i denna vägledning följer MSB:s beskrivning av risk- och sårbarhetsanalyser [4]. För fördjupning inom riskhantering hänvisas även till ISO-standarden [6]. Ett alternativt sätt att beskriva arbetsgången i en RSA ges i FORSA-modellen [5].



Figur 3. ***Schematisk bild av de olika stegen i RSA-arbetet.***

2.1.1 Utgångspunkter

I det inledande arbetet med risk- och sårbarhetsanalyser är det viktigt att bestämma och avgränsa analysens utgångspunkter. En viktig fråga är att avgöra vilket perspektiv som analysen ska ha och vilka lagar som därmed blir aktuella att förhålla sig till i risk- och sårbarhetsanalysen.

Att få med rätt kompetenser vid genomförandet av en RSA är också viktigt, framför allt för att kunna identifiera alla risker och sårbarheter samt för att korrekt bedöma konsekvenser och sannolikheter. Detta bestäms delvis av vilket perspektiv man anlägger och hur omfattande man väljer att göra en RSA.

Dessutom kan metoden behöva anpassas till den studerade verksamheten. Om denna är av teknisk natur behöver man ta fram tekniska beskrivningar. För att inte missa några risker kan man i sådana fall även behöva genomföra en inspektion av anläggningen som en del av RSA:n, då de platsspecifika förutsättningarna kan utgöra viktiga indata.

Det är också viktigt att bestämma vilken dimensionerande hotbild som ska betraktas i RSA-arbetet. Inriktningen kommer sedan att påverka de hotscenarier som kommer att användas, vilket i sin tur kommer att påverka vilka risker och sårbarheter som identifieras.

2.1.2 Riskidentifiering – Tekniska konsekvenser

Riskidentifiering handlar om att besvara frågan ”Vad kan hända?”, dvs. att upptäcka och identifiera alla risker som kan hota en verksamhet och att identifiera potentiella riskkällor.

Vid riskidentifiering behövs beskrivningar av den studerade verksamheten och dess betydelse för samhällsviktig verksamhet för att kunna avgöra vad som är risker. Beroenden mellan olika samhällsfunktioner eller förmåga att hantera olika händelser är viktiga i senare analysfaser för att fastställa vilka system som kan drabbas och vad som kan hända när de drabbas.

2.1.3 Riskanalys – Verksamhetskonsekvenser

Riskanalys går ut på att besvara frågorna ”Vad kan händelsen leda till ?”, ”Hur sannolikt är det?” och ”Vad blir konsekvenserna?”. Svaret på den första frågan har delvis besvarats i samband med riskidentifieringen. I analysfasen handlar det om att förfina beskrivningarna av hotscenarierna och bedöma hur troligt det är att vart och ett av de identifierade scenarierna inträffar. Därefter bedöms konsekvenserna av händelserna, kopplade till den valda värderingsmetod som analysen bygger på. I konsekvensbedömningen behöver man också ta hänsyn till hur befintligt skydd fungerar mot det aktuella hotet och hur skyddet, redundansen eller hanteringen av hotet påverkar konsekvenserna [4].

För att kunna jämföra olika risker och prioritera åtgärder av dem behöver de kvantifieras. En vanlig modell är att för varje risk bedöma sannolikheten att en händelse inträffar och konsekvenserna om den inträffar.

Dessa två storheter kan sedan användas på lite olika sätt för att jämföra olika risker med varandra. Ett sätt är att definiera risken för en händelse som

$$\text{Risk} = \text{Sannolikhet} \cdot \text{Konsekvens}.$$

Alternativt kan sannolikheten och konsekvensen bilda en riskmatris som fungerar som underlag för beslut.

Konsekvensen kan exempelvis bedömas i ekonomiska termer, exempelvis i form av kostnad för reparation, eller i antal skadade. Ofta används en skala 1-5 där 5 motsvarar de allvarligaste konsekvenserna. Även för sannolikheten kan man använda en femgradig skala, men ibland kan det vara relevant att ange den som en frekvens, dvs. hur många händelser av den typen som kan förväntas inträffa per år [4].

Sannolikheten för EM-hot bedöms ofta vara låg (en s.k. sällanhändelse), men samhällskonsekvenserna kan anses vara så stora att det ändå är motiverat att vidta motåtgärder.

I Tabell 1 visas ett exempel på hur de olika riskerna kan listas. Listan innehåller även exempel på åtgärder som tas fram under senare delar av riskhanteringen. I arbetet behöver både sårbarheter och EM-hot diskuteras för att slutligen erhålla en lista på händelser som kan få kännbara konsekvenser på verksamheten. I diskussionerna bör först varje EM-hot behandlas separat och om dessa uppträder i kombination kan även kombinationen av EM-hot behandlas som en händelse. För varje händelse bör också systemets sårbarhet beskrivas. Slutligen bör även sannolikheten och konsekvensen kvantifieras.

Tabell 1. Exempel på riskanalys av en rad händelser.

Händelse	**Sårbarhet (system eller förmåga)**	**Beskrivning**	**Sanno-likhet**	**Konsek-vens**	**Åtgärd**
Händelse 1 - Avsiktlig störning mot verksamhetens trådlösa kommunikations-system	Kommunikations-system för larmsamtal utstört	Den avsiktliga störningen stör helt ut utgående larm, vilket får förmågebortfall: - Övervakningscentralen får inte larm från operatör - Operatören kan inte larma.	1	4	Skaffa utrustning för att monitorera elektromagnetisk miljö.
Händelse 2- mikrovågsvapen som riktas mot driftcentral	Driftcentral obrukbar	Driftcentralen fungerar ej – elektroniken förstörd	1	5	Installera skalskydd.

2.1.4 Riskutvärdering

Riskutvärdering innebär att baserat på utfallet av riskanalysen och fastställda kriterier bedöma om en risk är acceptabel eller inte. Dessutom kan olika möjligheter att reducera risken (om sådana finns) inkluderas. Utvärderingen är ett lämpligt underlag för planering och genomförande av riskreducerande åtgärder, vilket är ett av syftena med risk- och sårbarhetsanalysen. Värderingen går ut på att väga fördelar mot nackdelar med de föreslagna åtgärderna och komma fram till om åtgärden bör genomföras eller inte. Utvärderingen bör utgå från den effekt som de föreslagna åtgärderna beräknas ha på risknivån, dvs. hur mycket de reducerar risken. Ett problem är dock att det ibland kan vara svårt att finna en riskreducerande effekt, vilket kan leda till beslut att en viss verksamhet inte ska bedrivas på ett visst sätt eller en viss plats. Åtgärderna kan sedan infogas i listan från riskanalysen, se exempel i Tabell 1.

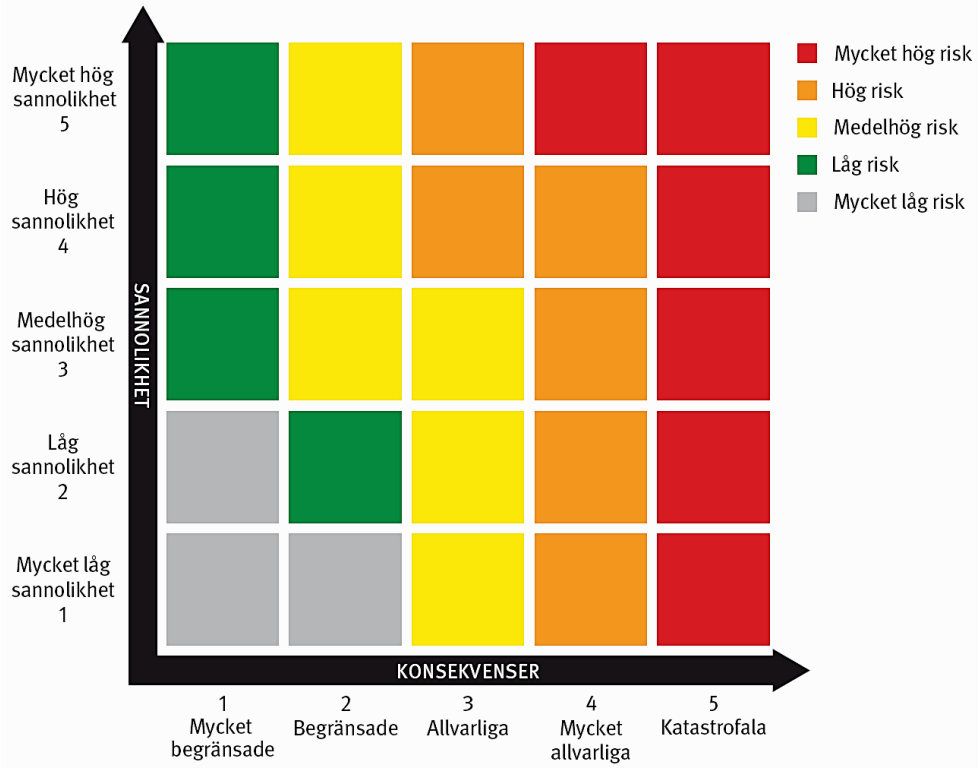
En riskmatris är ett vanligt verktyg som används vid riskutvärderingar. Den består av två sammanslagna skalor och används för en bedömning av hur troligt det är att ett specifikt riskscenario inträffar och vad konsekvenserna blir. Ett exempel på en riskmatris som kan användas i en RSA återges i Figur 4. Här

används femgradiga skalor för sannolikhet och konsekvens och man har klassat kombinationer av dessa i olika risknivåer [5].

Användning av en riskmatris är att föredra då det gäller sällanhändelser, som ofta är fallet då det rör EM-hot. Sårbarheter som orsakas av EM-hot tenderar att hamna långt ner åt höger i riskmatrisen, där sannolikheten är låg men konsekvenserna stora. Sällanhändelser med stora konsekvenser är ofta viktiga att särskilja från händelser med mycket hög sannolikhet och liten konsekvens, vilken hamnar i översta vänstra hörnet. Båda kan få samma riskvärde vid beräkning med den matematiska formeln *Risk* = *Sannolikhet* · *Konsekvens*, men sällanhändelser med stora konsekvenser är troligen viktigare att identifiera i en RSA. Ofta infogar man i riskanalysen en riskaversionsfaktor, som viktar riskuppskattningen så att mera allvarliga konsekvenser ges ett högre värde. Ett exempel på detta ses i Figur 4, där även katastrofala konsekvenser med låg sannolikhet givits ett mycket högt riskvärde.

Som alternativ till användande av riskmatriser finns *risktriangeln* [3], som definierar risken som en kombination av *Värde*, *Hot* och *Sårbarhet*, samt *riskkuben* [16], som byggs upp av utrustningens *Känslighet*, *Tillgänglighet* och *Konsekvens* av bortfall.

Riskutvärderingen är ett viktigt instrument för att i ett senare skede kunna prioritera vilka risker som bör åtgärdas och vilka åtgärder som ska vidtas [4].



Figur 4. ***Exempel på riskmatris för bedömning av risknivå [5].***

2.1.5 Sårbarhetsbedömning

Sårbarhetsbedömningen består dels av en förmågebedömning och dels av en sårbarhetsanalys. Förmågebedömningen utgör en bedömning av den egna organisationens krishanteringsförmåga och förmåga att motstå allvarliga störningar i samhällsviktig verksamhet, t.ex. resiliens hos samhällsviktiga tekniska system. Sårbarhetsanalysen studerar hur allvarligt och omfattande en specifik händelse påverkar samhället eller den egna organisationen. Sårbarhetsanalysen kan kombinera flera scenarier och syftar till att på ett fördjupat sätt identifiera sårbarheter och konsekvenser [4].

2.1.6 Riskbehandling

Riskbehandling innebär att välja riskreducerande åtgärder och implementera dessa. Detta innefattar att väga kostnaderna för åtgärderna mot de fördelar som uppnås. Riskbehandling är ofta en cyklisk process där man efter genomförda åtgärder utvärderar effekten, dvs. i princip genomför en förnyad RSA avseende den åtgärdade risken. Om denna inte nått en acceptabel nivå vidtar man ytterligare åtgärder samt utvärderar dessa, osv. [4].

2.2 Kompetenser vid genomförande av en RSA avseende EM-hot

För att genomföra en RSA krävs kunskap om såväl den aktuella verksamheten som om EM-hot. Eftersom EM-hot verkar mot tekniska system är det primärt teknisk systemkunskap som behövs för att bedöma de direkta fysiska effekterna, men även verksamhetskunskap och ledningsperspektiv är viktiga för att kunna bedöma konsekvenser och sekundäreffekter. Kompetens som kan beskriva hur åtgärder och skydd minskar risker är också värdefull.

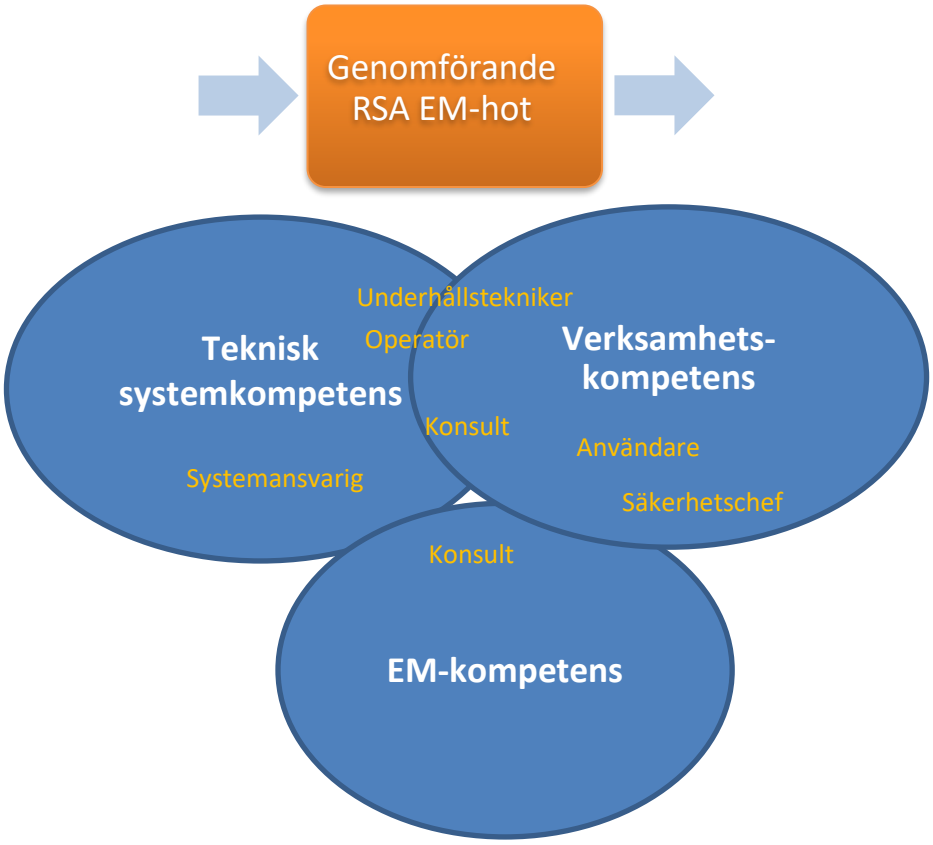
För att få med alla aspekter av hur en EM-attack kan påverka en samhällsviktig verksamhet bör man eftersträva deltagande av såväl ansvarig chef, operatör, underhållspersonal som användarrepresentant. Ibland kan det även vara fördelaktigt att ha med en systemanvändare, som kan beskriva hur man agerar vid ett funktionsbortfall, t.ex. försöker lösa sin uppgift med andra metoder. Även expertis med kunskap om EM-hot bör medverka för att utveckla hotscenarier och för att bedöma påverkan och konsekvenser av EM-hot mot kritiska system och för att analysera effekterna av olika åtgärder.

I Figur 5 presenteras olika typer av kompentenser som kan behövas för att genomföra de olika stegen i en RSA avseende EM-hot. Eftersom olika typer av expertis behövs är det därför lämpligt att genomföra en RSA avseende EM-hot i dialogform, där flera olika kompetenser samverkar. För att arbetet ska vara effektivt är det bra om antalet kan begränsas till omkring 4-7 deltagare. Alla deltagare behöver inte heller delta i alla RSA:ns skeden utan kan finnas tillgängliga vid vissa tillfällen för att svara på specifika frågor eller för att förbereda underlag inför genomförandet.

Som underlag inför genomförandet av RSA:n behöver verksamheten beskrivas tekniskt och funktionsmässigt och systeminformation samlas. För att

konkretisera hoten och beskriva dem som relevanta hot mot verksamheten kan hotscenarierna behöva anpassas till den aktuella verksamheten.

Ansvarsfördelningen mellan deltagarna i en RSA bör vara att verksamhets-ägaren ansvarar för genomförandet och uppföljningen, teknisk personal för teknisk systembeskrivning och bedömning av direktpåverkan på systemen, medan den tekniska kompetensen inom EM-hot ansvarar för att ta fram ett realistiskt hotscenario anpassat till verksamheten och att bistå med stöd om direkta verkansformer samt möjliga tekniska konsekvenser och skyddsåtgärder.

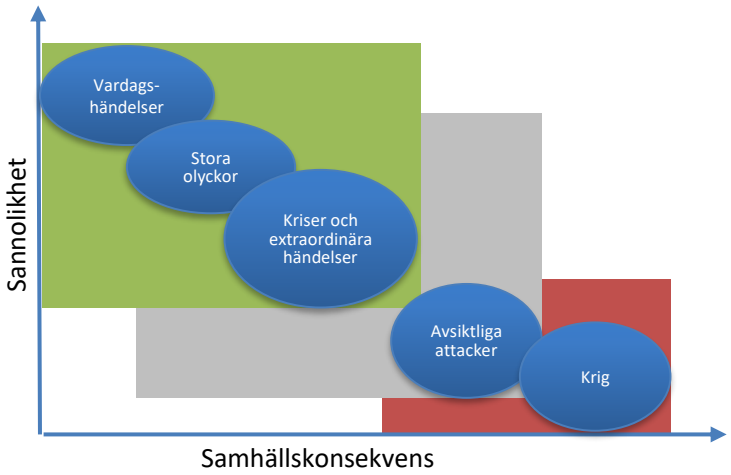


Figur 5. Förslag på hur deltagare med olika kompetenser kan delta i RSA rörande EM-hot.

2.3 Hotscenarier

I indelningen av arbetet bestäms vilken dimensionerande hotbild som RSA-arbetet bör inriktas mot. Inriktningen påverkar sedan vilken typ av händelser som kommer att beaktas. Det är dock viktigt att få med många olika typer av möjliga händelser och risker i en RSA, se Figur 6. Figuren beskriver olika händelsetyper som kan beaktas. Händelser i RSA:er utformas vanligtvis som vardagshändelser, stora olyckor, kriser och extraordinära händelser (den gröna regionen i figuren). Med ett förändrat hotläge och ökad risk för EM-hot har hotnivåerna kompletterats med högre hotnivåer (markerade med grå och röd region). Även om sannolikheten för en viss händelse är låg (en sällanhändelse) kan konsekvenserna vara så stora att det ändå är motiverat att vidta motåtgärder. Ett exempel är krig eller krigsfara, som kan ha genomgripande

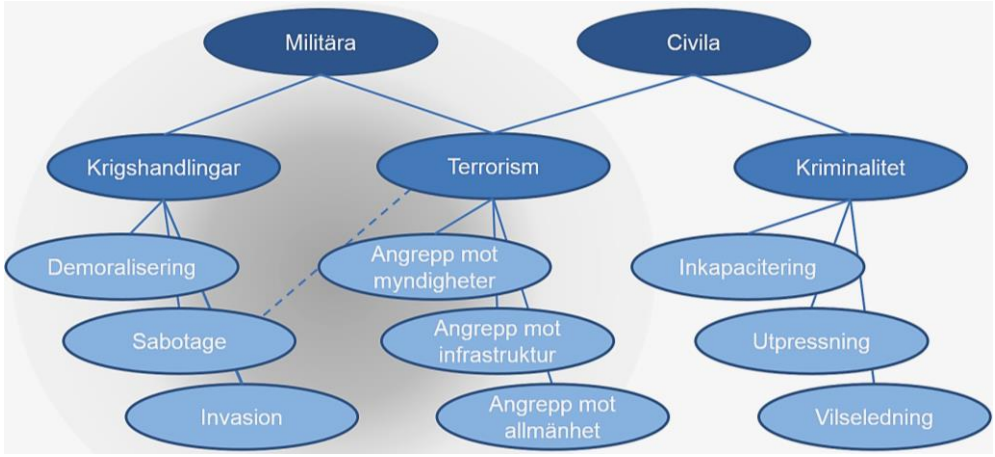
konsekvenser för hela samhället och alla dess verksamheter. Till exempel kan en förmågeförsvagning eller förmågeförlust som tidigare spelade en mindre roll nu bli kritisk. Vid fara för krig eller annan exceptionell samhällsstörning kan regeringen införa höjd beredskap, vilket innebär att samhällsaktörerna behöver vidta åtgärder för att kunna upprätthålla viktiga samhällsfunktioner. I denna kontext är en väl genomförd RSA viktig för verksamheten.



Figur 6. Schematisk bild av sannolikhet och samhällskonsekvens för några olika händelsetyper.

Riskidentifieringsprocessen kan genomföras på olika sätt, t.ex. genom en brainstormingsession där deltagarna själva får tänka ut vilka hot som kan finnas mot den egna verksamheten och vilka konsekvenser de kan få. Detta kan fungera i många fall där hoten är relativt kända. Om hotbilderna är mera oklara kan det vara bättre att experter på aktuella hotbilder sätter samman ett scenario där hoten uppträder. Hoten kan då kopplas till ett större skeende som inbegriper hela samhället och många olika samhällsfunktioner med direkta eller indirekta kopplingar till den i RSA:n studerade verksamheten.

Figur 7 visar en möjlig klassificering av några scenarier innehållande avsiktliga EM-hot. Uppdelningen är gjord avseende aktörer, mål samt situationer (kontext). Det är dock viktigt att notera att även om aktörerna och målen skiljer sig åt i de olika grenarna i strukturen, kan den fysiska händelsen, som består i att elektroniska system i verksamheten utsätts för strålning från ett EM-hot, ändå vara densamma och orsaka samma effekt på verksamheten. Anledningen till att en verksamhets elektroniska system störs med hjälp av en störsändare kan exempelvis vara att en militär aktör har ett militärt syfte eller att en kriminell person som avser att störa ut en kommunikationstjänst (t.ex. ett larm), som råkar sammanfalla med en viss verksamhets tekniska lösning.



Figur 7. En möjlig klassificering av scenarier innehållande avsiktliga EM-hot.

Krigshandlingar kan vara del av ett invasionsföretag, sabotagehandlingar som förberedelse inför en invasion (minska civila samhällets förmåga att stödja militärt motstånd), eller som psykologisk krigföring för att minska befolkningens förtroende för myndigheterna inför en intervention. Sabotage vid ett skymningsläge har mycket gemensamt med terrorism, som kan ha militära eller civila incitament. Även sabotage kan utföras militärt eller civilt och anses ofta syfta till att förstöra materiel, medan terrorism oftast syftar till att skapa oro och skräck hos befolkningen. Detta är ett exempel på att det finns en gråzon mellan krig och fred där det kan vara svårt att avgöra vem antagonisten är eller vad som är syftet med attacken.

EM-attacker vid invasion eller sabotage inför en invasion riktas främst mot operativa delar i totalförsvaret, ledningsfunktioner och informationskanaler till befolkningen, medan demoralisering främst slår mot civilbefolkningens trygghet och kan t.ex. innebära att privatpersoner inte kan få information eller nå myndigheter, larmcentraler, etc. och inte kan handla i affärer, bensinstationer, biljettautomater, m.m.

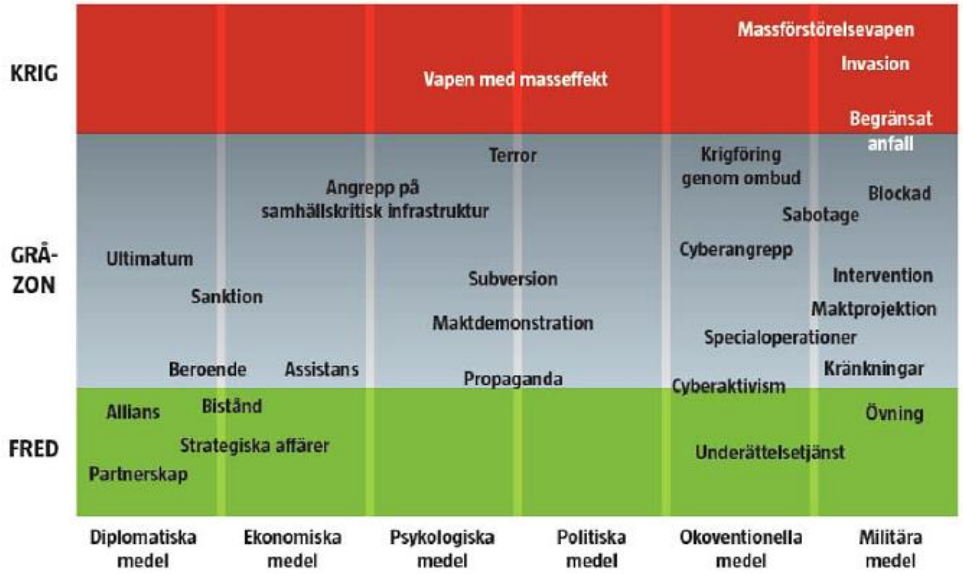
Terrorism kan inriktas mot myndighetsbyggnader, departement, etc. (ledningsfunktioner), mot förbindande infrastruktur (kraftledningar, vägar, telemaster, ...), eller direkt mot allmänheten i ett visst område (t.ex. slå ut alla informationskanaler inom ett geografiskt område).

Kriminell användning av EM-attacker kan förekomma genom inkapacitering (genom att slå ut t.ex. passagesystem, larmsystem eller radiokommunikation), som utpressning mot banker eller myndigheter (först en liten attack/störning som visar förmåga, sedan krav på pengar för att inte genomföra en större attack), eller som vilseledning (exempelvis en explosion som lockar till sig blåljusmyndigheternas insatspersonal följt av en elektronisk attack som slår ut kommunikationssystemen i området så att insatspersonalen inte kan få vetskap om den egentliga kriminella handlingen, t.ex. ett inbrott eller rån, som sker på en annan plats).

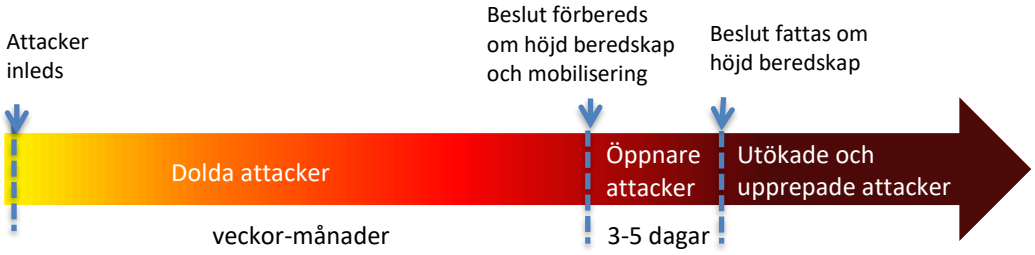
Samtliga situationer kan ha karaktären störning eller karaktären förstörelse av elektronisk utrustning, beroende på vilken utrustning som antagonisterna använder. Störning förutsätter långvarig funktion på en eller flera platser,

medan förstörelse kan åstadkommas under kort tid (sekunder-minuter). Störsändare kan pejlas in och lokaliseras, dock är detta relativt komplicerat och kan ta tid. Omhändertagandet kan dessutom försvåras pga. risken för apterade bomber. Att åtgärda förstörd elektronik kan innebära tidsödande felsökning och svårigheter att skaffa ersättningskomponenter.

Figur 8 illustrerar några händelser som kan uppträda i ett skymningsläge eller en så kallad gråzon, där samhället utsätts för olika strategiska medel som spänner mellan fred och krig. Dessa kan påverka förutsättningarna för civilförsvaret att stödja det militära försvaret. Figur 9 visar hur utvecklingen kan ske i tid från det att dolda attacker övergår till öppnare attacker och att beslut förbereds om höjd beredskap och mobilisering. Utvecklingen beskrivs i typfall 2 i FOI-memot ”Hotbildsunderlag i utvecklingen av civilt försvar” [17].



Figur 8. Illustration av den s.k. gråzonen mellan krig och fred [19].
Attacker med EM-hot kan tänkas uppträda som angrepp på kritisk infrastruktur, terror, subversion, maktdemonstration, krigföring genom ombud, sabotage, specialoperationer, eller kränkningar. EM-attacker kan ibland ha samma mål som cyberangrepp, men med användning av andra medel.



Figur 9. Illustration av möjliga tidsaspekter till det att beslut fattas om höjd beredskap.

Det kan vara bra om scenarierna som används har relativt stor spännvidd mellan olika typer av antagonister, använder olika typer av medel för påverkan och med olika avsikter. Hotscenarier kan användas för att hitta sårbarheter, men det är viktigt att man inte blir alltför låst av hotscenarierna. Exempelvis kan en terrorgruppering eller ensam galning göra samma sak men händelserna kan ha olika sannolikhet. Ett hotscenario ska användas som ett underlag för en diskussion för att identifiera risker. Diskussionen kan också fördjupa och modifiera ett hotscenario.

Bilaga 1 innehåller dels fem typfall som kan förekomma i samband med eller föranleda höjd beredskap, dels tre typscenarier med användning av EM-hot mot civil infrastruktur. Typscenarierna är avsedda att illustrera spännvidden i olika typer av antagonister, olika typer av EM-hot, samt olika typer av syften med attacken. Typscenarierna är endast exempel som skulle kunna användas som utgångspunkt i förarbetet i en RSA EM-hot och behöver anpassas till den specifika verksamhet som studeras i RSA:n.

2.4 Dokumentation

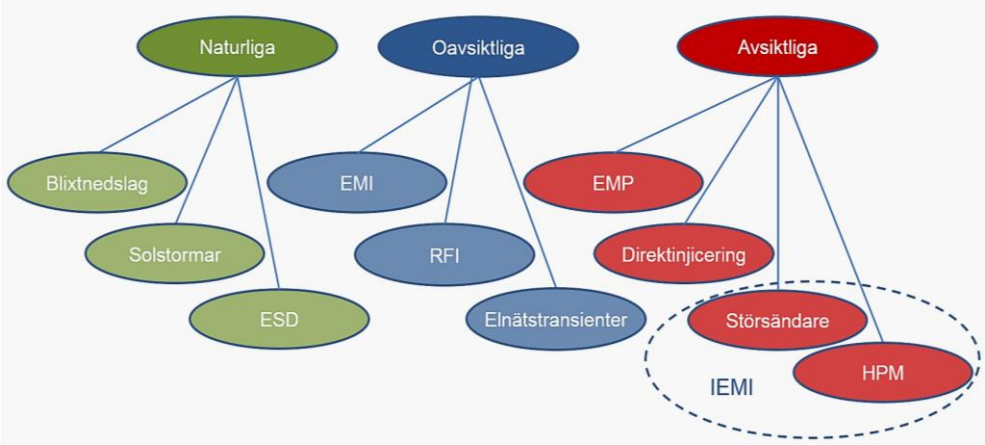
I samband med genomförandet är det viktigt att beskriva hur arbetet har genomförts och om det har lett till några avgränsningar. Det är alltså inte bara slutresultatet i form av identifierade risker och sårbarheter som är viktigt, utan också hur analysresultatet togs fram. Anledningen till att dokumentationen är viktig är att analysen ska kunna användas av andra än de som varit med vid genomförandet och att resultaten ska kunna infogas i organisationens övriga RSA-arbete. För att de identifierande riskerna ska kunna värderas mot andra risker framtagna i en övergripande RSA bör resultatet från en RSA för EM-hot sammanställas på ett sätt som passar en övergripande RSA.

Dokumentationen är också viktig då den genomförda risk- och sårbarhets-analysen ska uppdateras vid ett senare tillfälle. En noggrann dokumentation av varje steg i RSA:n leder till att efterföljande arbete (dvs. vidtagande av åtgärder, uppföljning av åtgärders resultat vid nästa RSA) blir lättare att genomföra. Även förändringar i genomförandet av framtida RSA:er underlättas.

3. EM-hot och påverkan på elektroniska system

I detta kapitel ges en kortfattad beskrivning av EM-hot och deras påverkan på elektroniska system, en utförligare beskrivning finns i [2].

Det finns många olika typer av EM-störningar som kan orsaka stor påverkan på system för samhällsviktig verksamhet. Det finns såväl naturliga som av människor orsakade oavsiktliga och avsiktliga EM-hot, se Figur 10.



Figur 10. Klassificering av EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur.

Naturliga EM-hot innefattar såväl blixtnedslag som solstormar och elektrostatiska urladdningar. Blixtnedslag genererar kraftiga strömmar i objekt närheten av nedslaget. Solstormar består av laddade partiklar som härstammar från solens korona och kan drabba en hel kontinent. Elektrostatisk urladdning (ESD) uppstår lätt vintertid inomhus, t.ex. om man bär plagg av syntetmaterial. Oavsiktliga EM-hot är elektromagnetisk interferens (EMI) som innebär att apparater stör andra apparater, medan radiofrekventa störningar (RFI) kan störa radiokommunikation. Elnätstransienter kan uppkomma vid kraftiga störningar på elnätet. Det finns även flera olika typer av avsiktliga EM-hot. Elektromagnetisk puls (EMP) från kärnvapen kopplar t.ex. till kraftledningar och kan förstöra ansluten utrustning. Direktinjicering innebär att någon leder in kraftiga strömpulser direkt på el- eller datakablar i en byggnad.

Denna vägledning fokuserar på genomförande av RSA för avsiktliga EM-hot (s.k. Intentional Electromagentic Interference, IEMI) i form av användning av störsändare och mikrovågsvapen (inom den streckade ovalen i Figur 10). De andra typerna av EM-hot beskrivs något mera utförligt i [20].

Tabell 2 visar en sammanställning av några olika varianter av EM-hot samt vilken typ av system de kan skada. De angivna EM-hoten är exempel på källor som är lämpliga då det finns ett avsiktligt uppsåt.

Tabell 2. Sammanställning av EM-hot och vilken skada de kan orsaka.

EM-hot	Kan skada	Att beakta
Avsiktlig störare – på GNSS-systems frekvensband	GNSS-mottagare, stör ut position och tid.	Många system har ett indirekt beroende till GNSS som tidtjänst. GNSS är mycket känsligt mot störning eftersom den mottagna signalen har mycket låg signaleffekt. Viktigt i bedömningen av sårbarheten är placeringen av GNSS-systemets antenn.
Avsiktlig störare – på trådlösa kommunikations-systems frekvensband	Trådlöst kommunikations system, blockerar mottagning av översänd information	Störning kan ske mot enskilda terminaler eller mot basstationer (då det gäller centraliserade nät som mobiltelefoni). Om störning sker mot enskilda terminaler slås bara dessa ut, medan om en basstation slås ut uppstår problem i hela cellen. Viktigt i bedömningen av sårbarheten är placeringen av kommunikationssystemets antenn.
Mikrovågsvapen, HPM	All form av elektronik och skadan kan vara antingen tillfällig eller permanent.	Skadan kan ske både om elektroniken är inkopplad till elektriskt nätverk, men kan även ske om elektroniken inte är inkopplad. Viktigt i bedömningen av sårbarheten är placeringen av elektroniken och det skalskydd som finns.

3.1 Faktorer som påverkar sannolikheten för en EM-attack

Sannolikheten för ett angrepp med EM-hot vara svår att bedöma men det kan underlätta att dela upp den i flera faktorer som

- den teknologiska sannolikheten att EM-hotet skulle kunna realiseras och användas på beskrivet sätt av en viss antagonist
- sannolikheten att en antagonist ska välja att använda sig av en EM-attack i det givna scenariot framför andra typer av medel

- är sannolikheten att antagonisten har tillräckligt mycket information om det skyddsvärda systemet för att en EM-attack ska lyckas.

Den teknologiska sannolikheten för olika typer av EM-hot skiljer sig åt, men kan ofta vara relativt hög. Ett exempel är kommersiella störsändare mot exempelvis GPS som finns att köpa på internet, där man kan ansätta en hög sannolikhet, eftersom teknisk utrustning finns att tillgå även om sådan inte är laglig att inneha. För olika typer av mikrovågsvapen är den teknologiska sannolikheten något mindre, dels eftersom dessa inte finns kommersiellt tillgängliga utan kräver specialiserad kunskap för konstruktion och användning, dels eftersom kraftfullare militära varianter troligen ännu inte finns ute på reguljära förband.

Sannolikheten att en viss antagonist ska välja en EM-attack kan vara svår att bedöma. Ofta används statistiskt underlag för att bedöma sannolikheter och för EM-attacker finns knapphändigt underlag för att bedöma sannolikheter, speciellt för en icke-militär antagonist. Hittills har terroristorganisationer inte visat något större intresse för användning av EM-hot, eftersom dessa enbart verkar mot utrustning och inte mot människor. Terrorism syftar vanligen till att sprida skräck och oro i befolkningen, vilket uppnås med bombdåd, skjutningar och knivdåd, medan utslagning av elektroniska system inte har samma effekt.

För militärt bruk av EM-hotsystem bör sannolikheten för användning S_A sättas hög eftersom olika typer av telekrigföring eller störningar av elförsörjning och kommunikationer använts frekvent i samband med militära konflikter under senare år, inte minst för att temporärt störa ut civila samhällssystem och försvåra mobilisering etc. För en invaderande militär styrka kan det vara av intresse att kunna använda existerande infrastruktur efter ett övertagande, vilket är möjligt efter en EM-attack. Vid störsändning påverkas infrastrukturen endast då störsändningen är aktiv medan efter en attack medmikrovågsvapen kan en återställnings/reparationsfas på några timmar till dagar behövas.

Det förekommer att kriminella använder störutrustning för att passivisera larm eller övervakningssystem för att kunna komma åt stöldbegärlig utrustning. Kunskapen om och benägenheten att använda andra typer av EM-hot är idag förmodligen låg eftersom detta kräver en speciell kompetens och möjligheter att färdigställa dessa. I dessa fall ligger sannolikheten S_A förmodligen någonstans mellan de för militärt bruk och terrorismanvändning.

Demonstranter och aktivister kan tänkas använda EM-hot för att störa samhällsfunktioner, vilket t.ex. visas av Göteborgskravallerna där störsändning användes mot polisens radiokommunikation [21, 22].

En annan grupp som skulle kunna orsaka störningar i samhällsviktig verksamhet och kritisk infrastruktur är tekniknördar, t.ex. studerande vid tekniska högskolor som enbart av intresse tillverkar utrustning och testar dess verkan mot elektronisk apparatur bara för att ”det är coolt”. Bland dessa grupper är det vanligt att information om hemmabyggda EM-källor läggs ut på internet, se t.ex. [23]. Den kritiska infrastrukturen skulle kunna vara målet, men kan också bli utsatt som en bieffekt när man testar verkan mot något

annat objekt. Sannolikheten för detta är troligen låg men svår att bedöma. Vad gäller antagonistiska gruppers benägenhet att använda olika typer av medel hänvisas till Polisen, SÄPO eller MUST för en aktuell lägesbild.

För att kunna bedöma sannolikheten att utsättas för en EM-attack behövs tillförlitlig statistik för inträffade incidenter. Därför är det viktigt att alla upptäckta eller misstänkta störningar inrapporteras. Elsäkerhetsverket brukar utreda störningar orsakade av elektrisk utrustning [24], medan Post- och Telestyrelsen utreder störningar i radiokommunikation [25]. En svårighet är att konstatera om man utsatts för avsiktlig störning eller om det rör sig om fel på utrustningen eller naturliga störningar. Bedömningen kompliceras av att en EM-attack kan vara en del i en större attack med flera olika medel.

Den faktor som ansvarig systemförvaltare inom en samhällsviktig verksamhet själv kan påverka är tillgängligheten av information om det skyddsvärda systemet. Det rör exempelvis typen av ingående komponenter, arbetsfrekvens, vilka skydd som installerats, placeringen av antenner och kontrollenheter, etc. Ibland kan sådan information inte hemlighållas av hänsyn till användarnas behov, men det kan ur skyddssynpunkt vara värdefullt att inte oreflekterat lämna ut all information om typ och placering av komponenter i ett system, förekomst av olika typer av skydd eller om förfaranden för att hantera olika typer av störningar i verksamheten. Det betyder att den faktor som en systemansvarig aktör själv kan påverka är S_I, som bör hålls så låg som möjligt.

3.2 Faktorer som påverkar konsekvenserna av en EM-attack

Figur 11 visar en sammanfattning av konsekvenser från oavsiktlig EM-störning, avsiktlig icke-förstörande EM-störning och slutligen förstörande EM-störning. Exempel på oavsiktlig störning är elektrisk utrustning som finns i närheten av kommunikationsmottagare och som på ett eller annat sätt stör mottagningen. Med avsiktlig icke-förstörande EM-störning och förstörande EM-störning avses främst avsiktliga störsändare respektive mikrovågsvapen. Oavsiktlig och avsiktlig icke-förstörande EM-störning stör typiskt trådlösa kommunikations-system, men då störningen stängs av kan kommunikationssystemet, eventuellt efter vissa procedurer, fortsätta att fungera. Skillnaden mellan oavsiktlig och avsiktlig icke-förstörande EM-störning är främst att oavsiktlig störning för det mesta har en lägre störningseffekt och att det inte finns ett avsiktligt uppsåt bakom. Förstörande EM-störning, med mikrovågsvapen, kan däremot förutom påverkan mot kommunikationssystem även påverka icke-kommunicerande elektronik och åstadkomma förstörande verkan. Generellt gäller att påverkan på de tekniska systemen beror bl.a. av källans placering (avståndet mellan källa och utsatt system, om det finns hinder mellan dessa samt från vilken riktning strålningen träffar det utsatta systemet), uteffekt och frekvensinnehåll.

Att sätta ett numeriskt värde på konsekvenserna av en EM-attack måste göras av systemansvarig aktör och förutsätter att man identifierat all påverkan som systemet utsätts för och såväl direkta som indirekta sekundäreffekter som kan uppträda, även sådant som påverkar verksamhet hos andra samhällsaktörer.

Nedan följer en sammanfattning av faktorer som påverkar effekten av avsiktlig icke-förstörande störning, som störsändare, och avsiktlig förstörande störnings, som mikrovågsvapen.

Figur 11 Schematisk bild över förhållandet mellan olika typer av elektromagnetiska störningar.

3.2.1 Avsiktlig icke-förstörande störning

Avsiktlig elektromagnetisk störning har som syfte att störa trådlösa tjänster som exempelvis tillhandahålls av mobiltelefonisystem, RAKEL, WiFi, och GPS. Risken för att en trådlös tjänst störs ut beror på en rad olika parametrar. Det avgörande för om den avsiktliga störningen lyckas är om störaren får ett effektövertag mot den önskade trådlösa tjänsten. En störsändare med högre uteffekt har en ökad chans att lyckas störa ut den trådlösa tjänsten. Dessutom spelar det stor roll hur utbredningsvägen ser ut mellan störsändarens antenn och målobjektet. Om störsändarens utsända effekt hindras av någon anledning minskar störeffekten vid målobjektet. Effekten påverkas starkt av terrängen i kombination med på vilken höjd över marken störsändaren finns, se Figur 12.

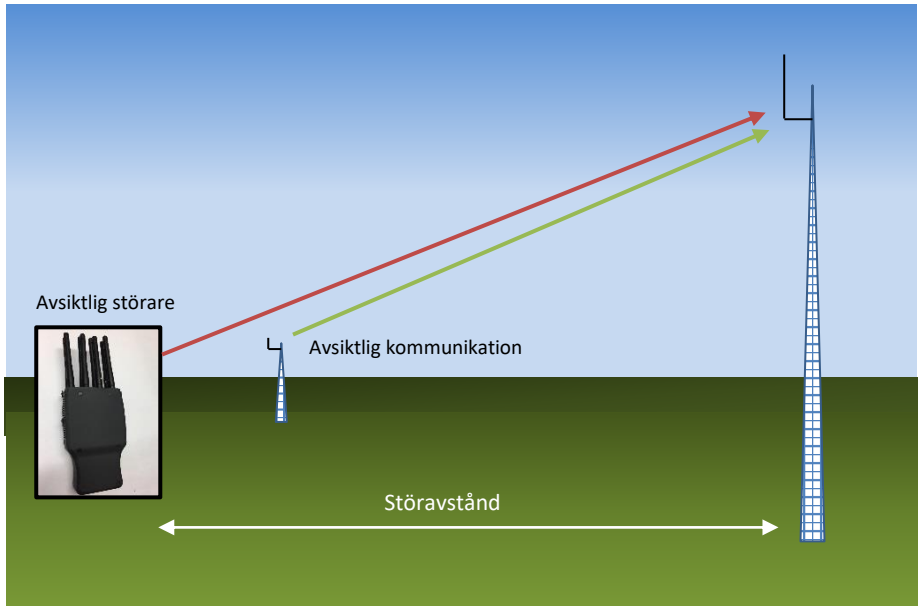
Faktorer som påverkar konsekvenserna av störsändning är:

- Störsändarens sändareffekt
- Riktantenn på störsändaren, dess antennförstärkning och riktning
- Fri sikt mellan störsändare och kommunikationssystemets antenn
- Avstånd mellan störsändare och kommunikationssystem
- Kommunikationsavstånd mellan olika enheter i kommunikationssystemet och om det använder riktantenner
- Kommunikationssystemets känslighet för störning

Ytterligare en förutsättning för att störsändaren ska kunna störa ut ett kommunikationssystem är att störsändarens effekt ligger inom frekvensbandet för kommunikationssystemet.

Olika trådlösa kommunikationssystem har olika känslighet för störning, där militära system är designade för att vara robusta mot EM-hot. Eftersom störsignalen tar sig in i kommunikationssystemet via antennen på samma sätt som kommunikationssystemet är det i regel svårt att i efterhand öka robusthet mot störsändning. Dock kan användning av riktantenner vara en åtgärd i vissa situationer.

Se ”Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur” [2] för exempel på störavstånd för olika typer av störsändare.



Figur 12 Schematisk bild över störsändare och kommunikationssystem.

3.2.2 Avsiktlig förstörande störning

Den tekniska påverkan som uppkommer till följd av en HPM-källa bestäms i stor utsträckning av amplituden hos strålningen när den träffar målet. Eftersom elektromagnetisk fältstyrka avtar i omvänd proportion till avståndet från källan[2] så innebär detta att avståndet mellan EM-hotsystemet och den skyddsvärda utrustningen är en väsentlig parameter i bedömningen av konsekvenser. Detta innebär även att en av de viktigaste skyddsåtgärder man kan vidta är att förhindra att potentiella antagonister kan komma nära det skyddsvärda objektet, t.ex. genom att spärra av ett större område runt objektet.

Andra sätt att dämpa EM-strålningens inträngning är att innesluta objektet i rum med tjocka väggar, gärna beklädda med metallplåt, och att installera

[2] Om avståndet fördubblas kommer fältstyrkan vid målet att halveras, om avståndet tiofaldigas kommer fältstyrkan att minska till en tiondel, osv. Notera dock att eftersom effekttätheten (energi per tids- och areaenhet) är proportionell mot kvadraten på fältstyrkan kommer effekttätheten att avta snabbare med ökande avstånd. En fördubbling av avståndet minskar effekttätheten med en faktor fyra, osv.

transientskydd på alla inkommande ledningar. Detta är dock inga triviala åtgärder utan måste utföras av kvalificerad personal med rätt utrustning.

När man har karakteriserat den strålning som genereras av ett specifikt EM-hot kan denna information matchas med susceptibiliteten (”känsligheten”) hos utrustningen i den kritiska infrastrukturen som man vill skydda.

Susceptibiliteten hos ett visst elektroniskt/elektriskt system kan mätas i laboratorieförsök eller uppskattas utifrån kända egenskaper hos apparater eller komponenter i liknande system.

Faktorerna som ökar påverkan från en HPM-källa liknar de för störsändare:

- HPM-källans sändareffekt
- Riktantenn på HPM-källan, dess antennvinst
- Fri sikt mellan HPM-källan och målet (kommunikationssystemets antenn, elektronik, kablage, etc.)
- Avstånd mellan HPM-källan och målet
- Målets (kommunikationssystemets antenn, elektronik, kablage, etc.) känslighet för störning. Målet kan vara designat med olika tålighet mot EM-hot.
- Skalskydd i form av inkapsling, transientskydd och filter samt korrekt genomförd zonindelning. Utformningen av byggnaden där målet är placerat kan ha stor påverkan.

För att åstadkomma förstörande verkan krävs mycket höga fältnivåer och verkansavstånden blir därigenom korta. Med verkansavstånd menas det avstånd EM-källan får avsedd verkan. Se ”Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur” [2] för verkansavstånd för olika typer av mikrovågsvapen och olika typer av målelektronik.

4. Praktiskt metodstöd för genomförande av RSA avseende avsiktliga EM-hot

4.1 Översikt av arbetsgången

Arbetet med att utföra en RSA där EM-hot beaktas kan med fördel delas upp i tre steg, där verksamhetsägare och teknisk kompetens kring EM-hot träffas och diskuterar, se Figur 13. Anledningen till uppdelningen i tre steg är att det kan krävas en viss arbetsinsats mellan de olika stegen. I detta kapitel beskrivs vad som bör genomföras i det olika stegen, vad som är underlag inför arbetet och vad som är syftet med varje steg. För att nå fram till det avsedda syftet i de olika stegen finns även förslag på diskussionsfrågor som ska ses som hjälpmedel för att nå fram till avsett resultat. Metodstödet finns beskrivet i detta kapitel samt i Bilaga 2.

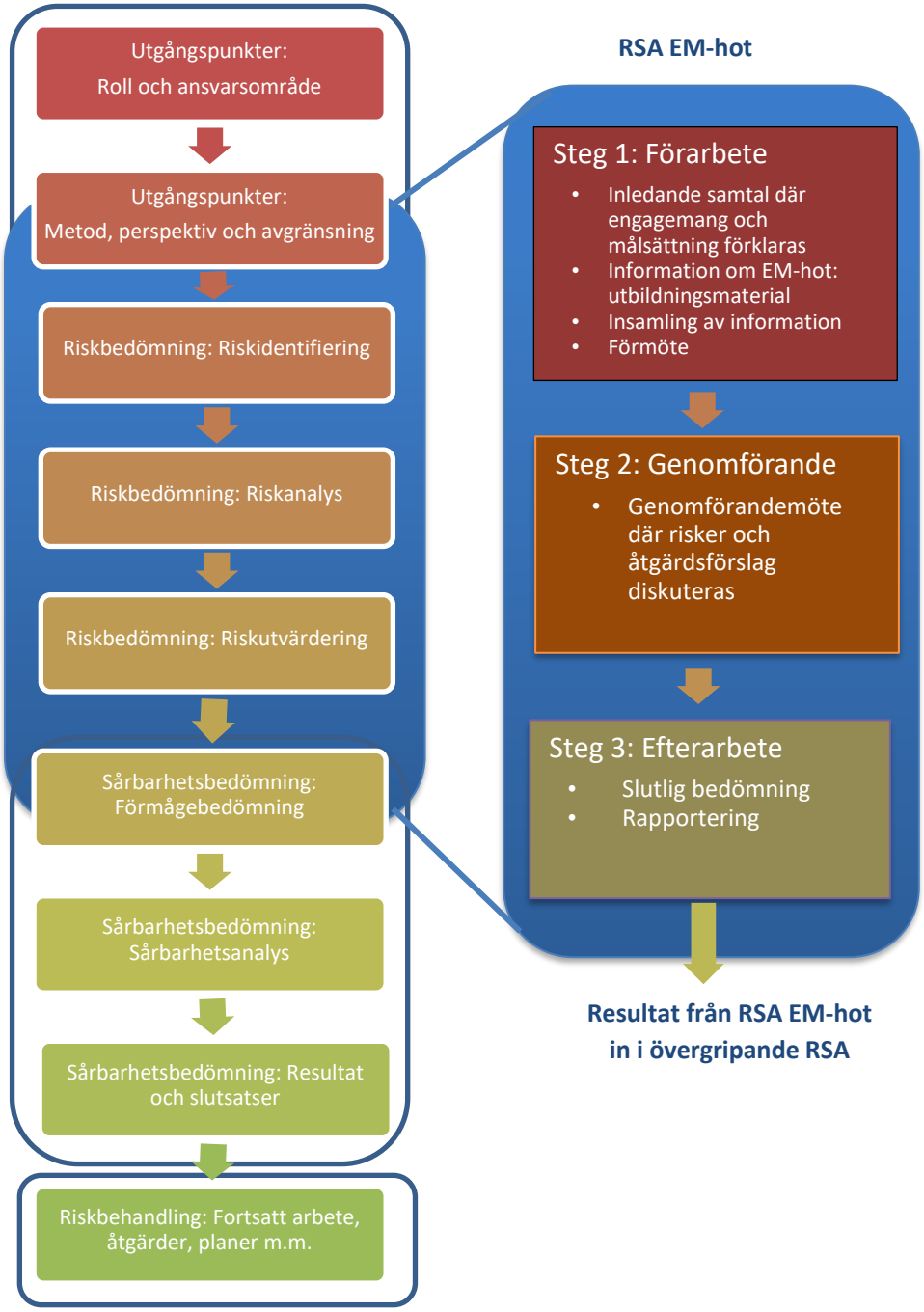
4.2 Förutsättningar

4.2.1 Roller – uppgifter och ansvar

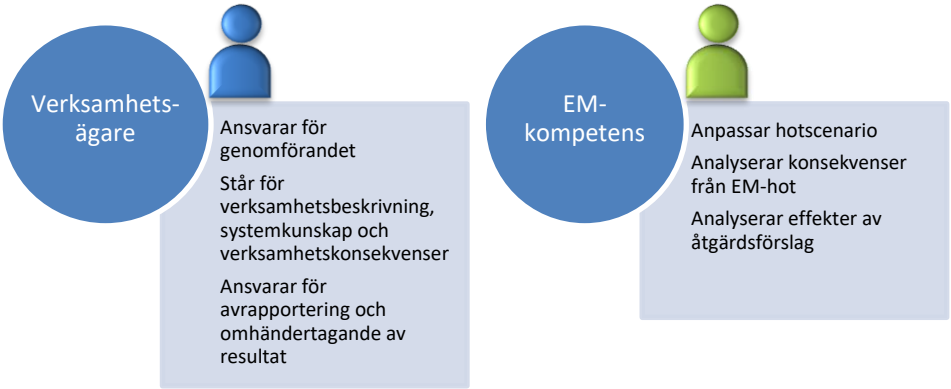
För att genomföra en RSA krävs att arbetet initieras av en verksamhets-företrädare eller verksamhetsägare. Det är verksamhetsägaren som formellt är ansvarig för att genomföra en RSA. Det är också verksamhetsägarna som vet hur resultaten bör beskrivas för att resultaten ska kunna inkluderas i verksamhetens övriga RSA-arbete.

Från verksamhetens sida är det främst systemkunskap, beroenden mellan system och hur verksamheten beror av elektroniska stödsystem som behövs vid genomförandet. Experter, exempelvis en tekniskt systemansvarig och en verksamhetsansvarig, från verksamheten är nödvändiga för RSA av EM-hot. Detta eftersom man i första hand behöver bedöma hur tekniska system och trådlös kommunikation kan påverkas av EM-hot.

I vissa fall kan även en säkerhetsansvarig eller en beslutsfattande chef bidra med underlag till riskanalysen. Med ett fokus på hur EM-hot kan påverka verksamheten krävs också stöd från personer med EM-kompetens, speciellt kunskap om existerande EM-hot, hur de används och verkar, se Figur 14. Om denna kompetens inte finns inom verksamheten kan extern expertis behöva anlitas. I det senare fallet bör sekretesshanteringen beaktas, se avsnitt 1.4.



Figur 13. Arbetets tre steg vid RSA avseende EM-hot.



Figur 14. Roller och ansvar.

4.2.2 Tid för genomförande

Erfarenheten är att RSA:n kan genomföras effektivt om rätt kompetens finns med vid de olika mötena. Detta är mycket väsentligt för genomförandet och om inte rätt kompetens är närvarande vid mötena kan fler möten krävas. Huvuddelen av förarbetet genomförs typiskt vid ett möte på några timmar, medan genomförandemötet kan ta en arbetsdag. Det är också viktigt att sprida ut de olika stegen i tid, eftersom det kan ta tid att genomföra informationsinhämtning och analyser som behövs mellan de olika stegen.

4.2.3 Hotnivå

Det är också viktigt att redan under förarbetet bestämma fokus för och vilken dimensionerande hotbild som RSA:n ska täcka. Om detta är bestämt i ett tidigt skede kan arbetet utföras mer effektivt. Hotnivån får sedan stark påverkan på det utvecklade hotscenariot.

Hotscenariot används som hjälpmedel för att diskutera fram risker och sårbarheter i några konkreta situationer. Under diskussionerna är även troligt att tankar väcks kring sårbarheter på andra platser eller i andra delar av systemet. Speciellt då komplexa system analyseras är det troligt att en rad olika sårbarheter framkommer, även sådana som inte direkt berörs av hotscenariot.

4.3 Förarbete

Syfte med förarbetet: Att förbereda både verksamhetsägare och EM-kompetens för arbetsgången och fastställa vilken typ av underlag som behövs, samt att ge EM-kompetensen en översiktlig bild av verksamheten och väsentliga system för verksamheten.

Arbetet startar med ett inledande samtal mellan verksamhetsägaren och EM-kompetensen, exempelvis via telefon. Syftet med det inledande samtalet är att diskutera hur EM-hot kan introduceras i en övergripande RSA och planera in ett förmöte. Verksamhetsägaren kan ge en översiktlig bild av verksamheten och ingående system. EM-kompetensen kan översiktligt beskriva EM-hot och konsekvenser, metoden för RSA EM-hot och hur hotscenarier används. Förutom att planera in ett förmöte bör man diskutera vilket underlag som

behövs inför mötet och vilken kompetens som behövs under RSA:n, framförallt från verksamhetssidan (se avsnitt 2.2).

Inför förmötet får verksamhetsägaren ett kortfattat utbildningsmaterial som förklarar effekter av EM-hot och om möjligt får EM-kompetensen en översiktlig beskrivning av verksamheten och ingående system.

Under förmötet bör följande delar avhandlas, några av dem kan typiskt vara presentationer förberedda av verksamhetsägare och EM-kompetens för att bygga en gemensam kompetensgrund inför RSA-arbetet.

- Verksamhetsbeskrivning och beskrivning av ingående system på översiktlig nivå – presentation av verksamhetsägare/systemexpert
- Allmän beskrivning av EM-hot och konsekvenser för olika typer av system och allmänt hotscenario – presentation av EM-kompetens
- Metoden för introduktion av EM-hot i RSA-arbetet och användandet av hotscenario – presentation av EM-kompetens
- Sekretess - nivå av sekretess för olika delar av RSA:n och hur känslig information ska hanteras
- Diskussion om sårbarheter och hotscenario – kan några sårbarheter redan nu pekas ut? Vilken hotnivå är relevant för verksamheten i ett hotscenario? Förslag på ytterligare frågeställningar finns i Bilaga 2. Genom att tidigt diskutera sårbarheter kan hotscenarier förberedas och göras mer specifika inför genomförandet.
- Fortsatt arbete
    - Boka in möte/möten för genomförande och efterarbete
    - Behövs annan/ytterligare kompetens vid genomförandet? Ytterligare kompetens kan också behöva införas under genomförandets gång varefter man ser nya problemställningar.
    - Material inför genomförandet?

Resultat av förarbete: EM-kompetensen får förståelse för den aktuella verksamheten. Verksamhetsägare med flera får förståelse för EM-hot och dess möjliga konsekvenser.

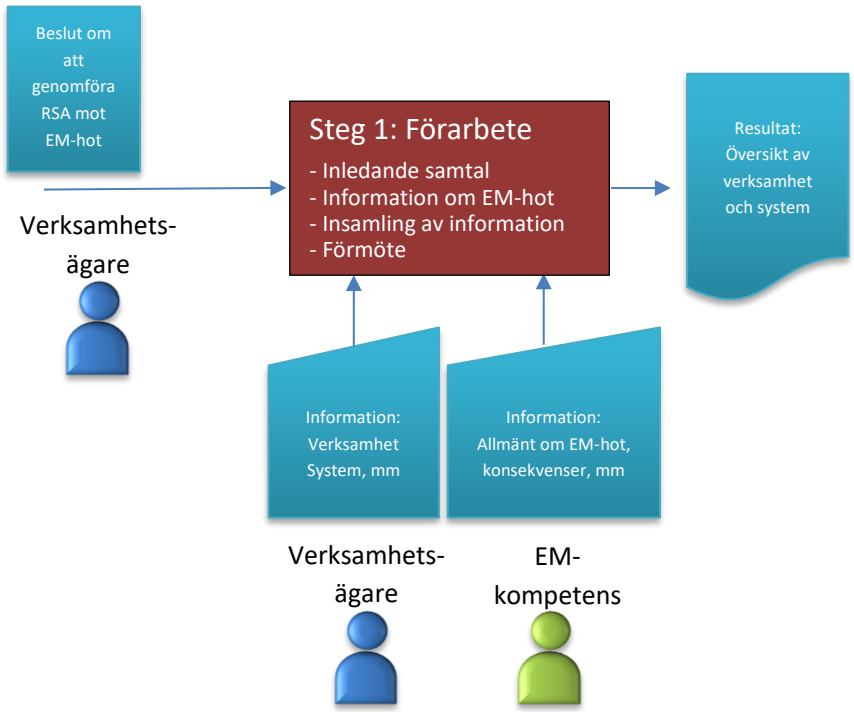
Dokumentation av förarbete: Mötesanteckningar, speciellt om systemspecifik utrustning och funktioner samt relevanta hotscenarier.

Arbete att utföras inför genomförandefasen: Efter förarbetet kan verksamhetsägaren bestämma vilken kompetens som behövs vid genomförandet samt ta fram ytterligare information om system som är relevanta för RSA-verksamheten.

EM-kompetensen har i uppgift att förbereda sig inför genomförandet genom att få förståelse för relevanta elektroniska system.

Baserat på informationen från förmötet utvecklar EM-kompetensen ett hotscenario baserat på en dimensionerande hotbild, och som är särskilt anpassat mot den aktuella verksamheten.

Figur 15 sammanfattar arbetsflödet under förarbetet.



Figur 15. In- och utdata för förarbetet.

4.4 Genomförande

Syfte med genomförandet: Att identifiera riskkällor, analysera risker och utvärdera konsekvenser av dessa.

Genomförandet består av ett eller, vid behov två, heldagsmöten där de inblandade genomför 1. Riskidentifiering, 2. Riskanalys och 3. Riskutvärdering. För de olika delmomenten finns i Bilaga 2 exempel på frågeställningar, vilka kan användas som stöd i diskussionerna. I Bilaga 2 finns även mallar som kan användas för anteckningar under arbetet. För att undvika att vissa delar missas är det bra med ett körschema med hålltider för de olika delmomenten.

Nedan följer de delmoment som ska behandlas:

- **Genomgång av verksamheten/systemen**
  Syfte: Ge en beskrivning av verksamheten och ingående system för analysen.

- **Genomgång av hotscenario**
  Syfte: Gå igenom hotscenariot som ligger till grund för diskussionerna. Leder naturligt till nästa punkt.

- **Riskidentifiering**
  Syfte: Identifiera risker och sårbarheter med hjälp av scenariot. Även risker som av någon anledning inte omfattas av scenariot, exempelvis annan plats eller annan antagonist, bör komma med. Hotscenariot bör ses som ett diskussionsunderlag inte en begränsning.
  Riskerna antecknas i noteringsprotokollet (i Bilaga 2). Eftersom hotsceneriet enbart används som hjälp för att identifiera risker i verksamheten ska i första hand varje EM-hot studeras för sig. Om kombinationen av flera EM-hot förvärrar situationen bör även ett sådant fall analyseras. Olika EM-hot kan riktas mot samma sårbarhet men bör noteras separat för att senare kunna bedöma olika sannolikheter mm för händelserna. Även de fall där kombinationer av EM-hot kan leda till förvärrande konsekvenser än för respektive EM-hot enskilt bör noteras separat.

- **Riskanalys**
  Syfte: Analysera varje risk genom att bedöma sannolikhet för att händelsen inträffar och dess konsekvenser vid inträffande. I första hand behöver sannolikheter och konsekvenser diskuteras och beskrivas och om möjligt sätts siffror för att kunna jämföra med andra risker.

- **Riskutvärdering**
  Syfte: Analys av hur riskerna förhåller sig till förmågeförluster för att ge underlag för en prioritering av vilka åtgärder som i första hand bör göras I detta sammanhang kan man behöva diskutera möjliga åtgärder för att reducera de olika riskerna och om möjligt använda en riskmatris för att jämföra olika risker. Förslag på åtgärder mot olika risker kan behöva bearbetas ytterligare under senare skeden i RSA:n innan beslut kan tas.

Kommentar om användning av hotscenario: Det är viktigt att hotscenariot utgör ett underlag för diskussion och inte begränsar riskidentifieringen. Genom diskussionerna kan hotscenariot komma att modifieras om det framkommer nya, värre hot eller om det upptäcks nya sårbarheter bland verksamhetskritiska system. Diskussionerna kan kräva omtag genom att man ifrågasätter vilka system som är kritiska för verksamheten.

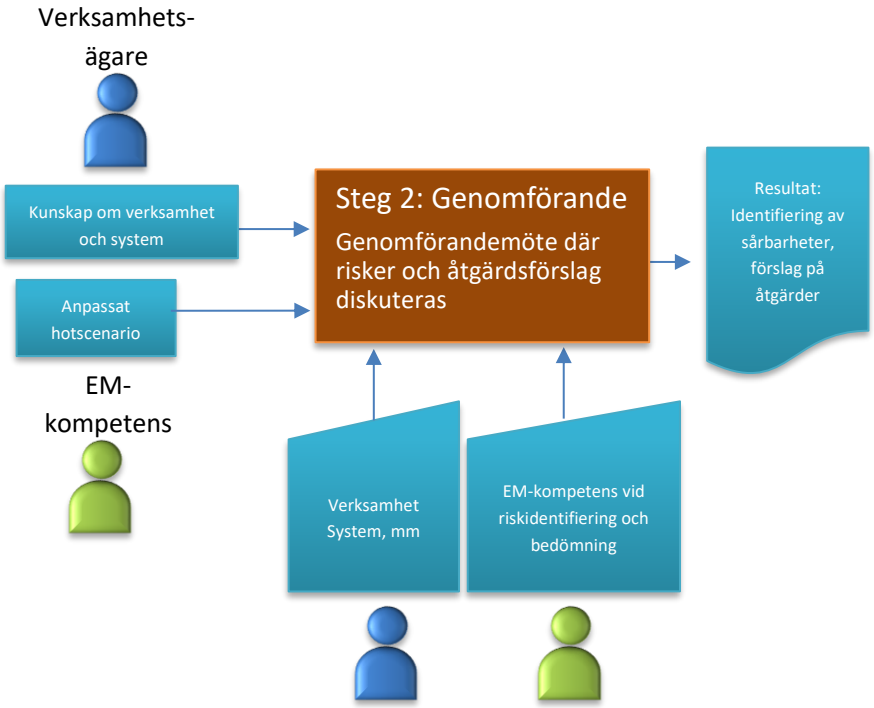
Resultat av genomförandet: Identifierade sårbarheter och en utvärdering av riskerna som finns i verksamheten.

Dokumentation av genomförandet: Mötesanteckningar, vilket inbegriper en beskrivning av kritiska system och hur dessa hänger ihop. Resultat i form av identifierade sårbarheter och konsekvenser exempelvis dokumenterade i mallar från Bilaga 2. Mallarna kan kompletteras med utförligare beskrivningar av analyserna för de olika händelserna. I riskutvärderingen ingår en diskussion om möjliga åtgärdsförslag. Arbetet delas upp mellan verksamhetsägaren och personer med EM-kompetens.

Uppgifter att utföras inför efterarbetet:
Inför efterarbetet gör EM-kompentensen en bedömning av effekten av olika åtgärdsförslag (kan kräva beräkningar).

Eventuellt kan ytterligare ett möte genomföras där arbetet inriktas helt mot riskreducerande åtgärder och en bedömning av tekniska effekter av föreslagna riskreducerande åtgärder på system och även konsekvenser för verksamheten.

Arbetsprocessen under genomförandefasen sammanfattas i Figur 16.



Figur 16. In- och utdata för genomförandeprocessen.

4.5 Efterarbete

Syfte med efterarbetet: Att sammanfatta de sårbarheter och åtgärdsförslag som framkommit i RSA:n. Resultaten ska vara formulerade på sådan form att de kan inkluderas i verksamhetens övriga RSA-arbete.

Efterarbetet består av en genomgång av identifierade sårbarheter som framkommit vid genomförandemötet samt att diskutera och bedöma de riskreducerande åtgärder som mer i detalj har analyserats av EM-kompetensen inför efterarbetsmötet.

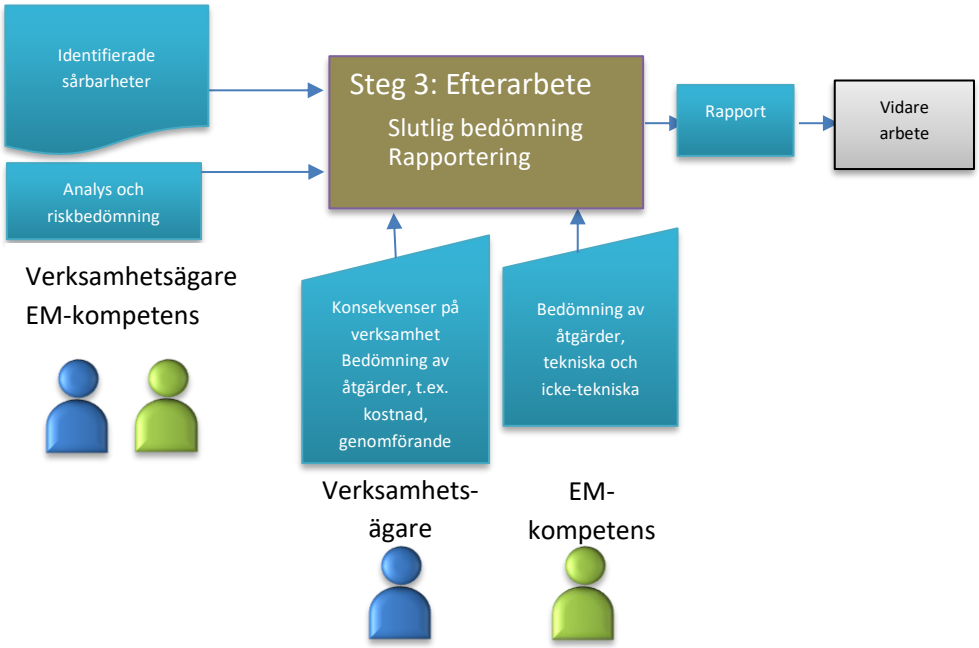
Resultatet ska vara i en sådan form att verksamhetsägaren sedan kan ta de identifierade sårbarheterna och åtgärdsförslagen för vidare arbete inom sin verksamhet. I detta arbete ska resultaten från RSA mot EM-hot inkluderas i verksamhetens övriga arbete med RSA.

Arbetet består av 1. Sårbarhetsbedömning och 2. Riskbehandling, se avsnitt 2.1.5 och 2.1.6. Dessa delar är sådant arbete som verksamhetsägaren själv kan bedriva inom sin egen organisation. I sårbarhetsbedömning gör verksamhets-ägaren en bedömning av den egna organisationens krishanteringsförmåga och förmåga att motstå allvarliga störningar i den egna verksamheten.

Sårbarhetsanalysen studerar hur allvarligt och omfattande en specifik händelse påverkar samhället eller den egna organisationen.

Resultat av efterarbetet: En dokumenterad sammanfattning av risker och sårbarheter s konkreta åtgärdsförslag för att minska riskerna med behandlade EM-hot.

Figur 17 sammanfattar arbetsflödet under efterarbetet.



Figur 17. In- och utdata för efterarbetet.

4.6 Kommentarer till processen

Genom att arbeta med ett eller flera hotscenarier blir hotet mot verksamheten mer konkret vilket underlättar processen med att hitta risker och sårbarheter. Scenarier är avsedda som underlag till arbetet och kan behöva uppdateras eller utvidgas om andra risker som inte täcks av scenariot kommer fram under arbetets gång eller om den dimensionerande hotbilden förändras.

Beroende på verksamheten som analyseras kan hotscenarier användas på lite olika sätt, antingen specifika för en speciell plats med de system som finns på platsen eller mer generella avseende en specifik typ av elektroniska system. I komplexa system med stor geografisk spridning kan det finnas flera platser med samma funktion men som även skiljer sig något åt. Samma generella hotscenario kan då användas för alla platser.

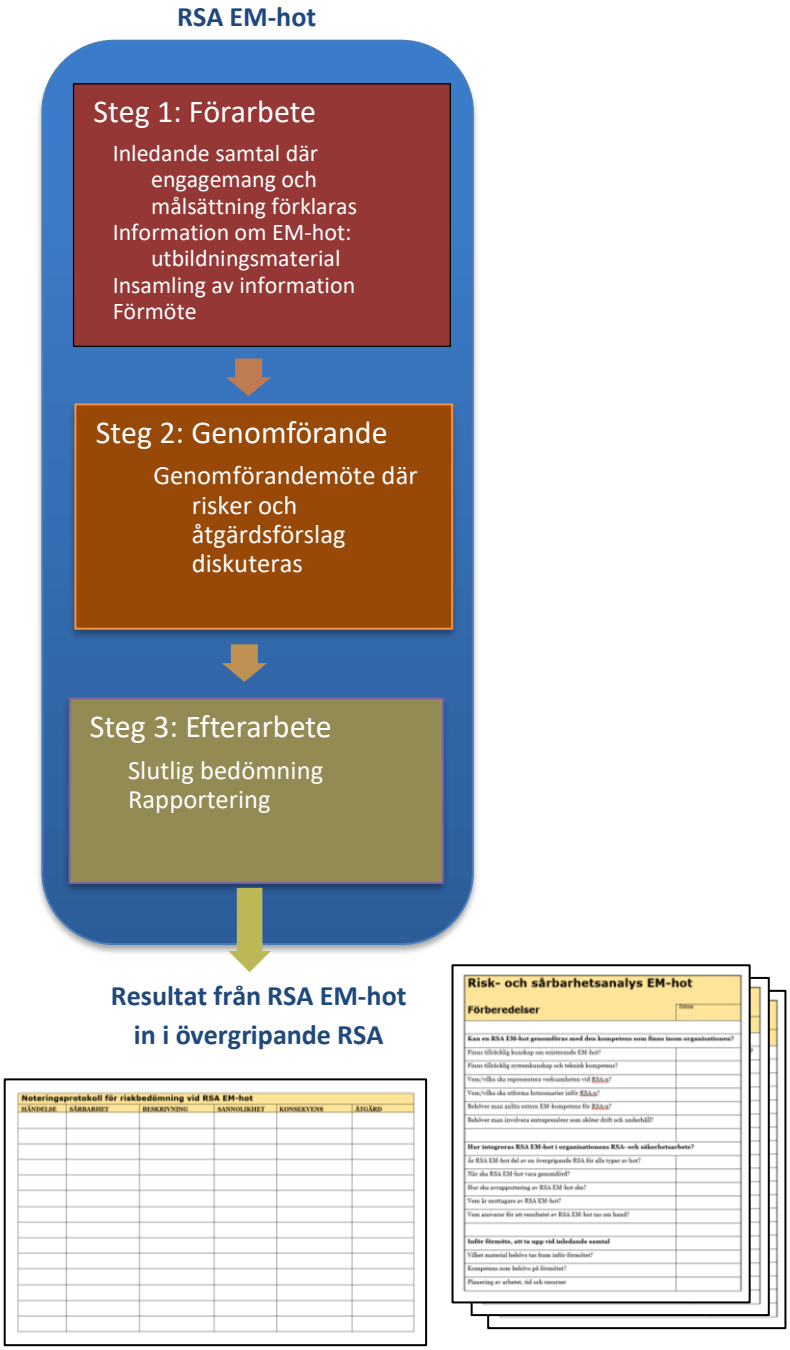
Hotscenariots viktigaste uppgift är att väcka tankar om sårbarheter i verksamheten och får inte styra arbetet så att sårbarheter missas för att de inte omfattas av scenariot. I hotscenariot är verksamheten som analyseras målet för en EM-attack, men det kan även finnas situationer där system påverkas av EM-attacker mot ett annat mål.

Exempelvis skulle det kunna vara system som använder mobiltelefonisystem för kommunikation, vilka påverkas av störning av mobiltelefonisystemet även om verksamheten i sig inte är det primära målet. Det finns även scenarier med olika angripare och som kan ha olika syften som resulterar i samma risker och konsekvenser för verksamheten.

Metoden för RSA avseende EM-hot som beskrivs ovan är indelad i steg som sker i tur och ordning men det kan ibland vara nödvändigt att iterera arbetet, antingen inom ett steg eller genom att ta omtag med föregående steg. Detta gäller speciellt då komplexa verksamheter analyseras och nya sårbarheter eller hot kommer fram under arbetets gång, både på de möten som genomförs och under arbetet som sker som för- eller efterarbete mellan möten. Speciellt attacker med mikrovågsvapen som kan ge konsekvenser för i princip alla elektroniska system är det naturligt att flera system i behov av analys framkommer under arbetets gång.

Metoden är uppdelad i flera steg som är tänkta att genomföras med ett visst uppehåll mellan de olika stegen. Mellan stegen genomför de olika parterna eget arbete för att sammanfatta föregående steg eller förbereda för nästa steg. Troligen är det även så att alla deltagare i RSA-processen gör nya erfarenheter under mötena, antingen om EM-hot eller om verksamheten. Även av den anledningen kan det vara fördelaktigt att ha processen något uppdelad i tiden så att parterna hinner fundera igenom konsekvenserna av det de lärt sig.

Metoden beskrivs översiktligt i Figur 18, där resultatet från en RSA avseende EM-hot i form av ifyllda mallar och anteckningar också visas. Resultatet från RSA-arbetet rörande EM-hot ska sedan kunna integreras i arbetet med verksamhetens övergripande RSA.



Figur 18. Arbetets tre steg vid RSA avseende EM-hot.

5. Slutord

Många samhällsviktig verksamheter förlitar sig idag på elektroniska system och trådlösa kommunikationssystem. Eftersom dessa kan vara mycket känsliga för elektromagnetisk (EM) påverkan, utgör avsiktliga EM-störningar ett reellt hot mot samhällsviktig verksamhet. I och med ett ökat beroende av elektroniska system och med en förändrad och skärpt hotbild i närområdet har hotet förstärkts. Samtidigt behandlar de risk- och sårbarhetsanalyser (RSA) som görs idag sällan eller aldrig denna typ av hot.

Denna vägledning erbjuder ett metodstöd vid genomförande av risk- och sårbarhetsanalyser avseende antagonistiska EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur. Arbetet med avsiktliga EM-hot bör vara en del av en större RSA som omfattar alla möjliga hot mot samhällsviktig verksamhet och kritisk infrastruktur. Dessutom utgör EM-hot tekniska hot som verkar mot elektroniska system och för vilka det kan behövas specialkunskap att bedöma vilken skada en antagonist kan åstadkomma.

Vägledningen beskriver en arbetsgång för RSA EM-hot och specificering av olika uppgifter. Materialet beskriver hur man kan förbereda och genomföra en RSA i olika steg samt innehåller specifika frågeställningar som kan användas för att identifiera sårbarheter i samhällsviktig verksamhet och kritisk infrastruktur. Det ges även exempel på hotscenarier och hur en systemansvarig aktör kan få stöd för ett riskreducerande arbete efter en genomförd RSA.

Referenser

1. ”Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, Sten E Nyholm, Tomas Hurtig, Sara Linder, Kia Wiklundh, Karina Fors, Myndigheten för samhällsskydd och beredskap (MSB), MSB1179 - februari 2018, ISBN 978-91-7383-804-7

2. ”Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, Tomas Hurtig, Sara Linder, Kia Wiklundh, Karina Fors, Sten E Nyholm, Myndigheten för samhällsskydd och beredskap (MSB), MSB1180 - februari 2018, ISBN 978-91-7383-805-4

3. ”Vägledning för skydd mot avsiktliga EM-hot”, Fortifikationsverket, 2017, ISBN 978-91-639-5650-8

4. ”Vägledning för Risk- och sårbarhetsanalyser”, Myndigheten för samhällsskydd och beredskap (MSB), MSB245 - april 2011, ISBN 978-91-7383-129-1.

5. ”FOI:s modell för risk- och sårbarhetsanalys (FORSA)”, Magnus Winehav (red.), Björn Nevhage (red.), Jens Lusua, Jonas Clausen Mork, Johan Lindgren, Robert Erdeniz, Totalförsvarets forskningsinstitut (FOI), FOI-R--3288--SE, 2011

6. ”Riskhantering - Principer och riktlinjer”, Svensk Standard, SS-ISO 31000:2009

7. ”Myndigheten för samhällsskydd och beredskaps föreskrifter om landstings risk- och sårbarhetsanalyser”, MSBFS 2015:4

8. ”Myndigheten för samhällsskydd och beredskaps föreskrifter om kommuners risk- och sårbarhetsanalyser”, MSBFS 2015:5

9. ”Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser”, MSBFS 2016:7

10. “Elektromagnetisk miljö användarhandbok, EMMA, Utgåva 2”, Försvarets materielverk, FMV:Materiel 21 840:44134/02, 2002, Försvarets bok- och blankettförråd, M7773-000750 (bok) samt M7773-000760 (CD).

11. Offentlighets- och sekretesslag 2009:400, Ändrad: t.o.m. SFS 2017:1012

12. Grundläggande begrepp och regelverk, del 2, MSB, pdf-presentation, https://www.msb.se/Upload/Utbildning_och_ovning/civilt%20f%C3%B6rsvar/Del%202%20Grundl%C3%A4ggande%20begrepp%20och%20regelverk_rev.pdf (2017-11-28)

13. ”Ett fungerande samhälle i en föränderlig värld - Nationell strategi för skydd av samhällsviktig verksamhet”, MSB266 - december 2011

14. Pernilla Magnusson, Mats Hartmann, Johan Gidholm och Rolf Jarlås: ”Handbok verkansvärdering”, FOI-R--4337--SE, 2016

15. Wiktionary, https://sv.wiktionary.org/wiki/skymningsl%C3%A4ge (2017-11-28)

16. Daniel Månsson, ”Intentional electromagnetic interference (IEMI). Susceptibility investigations and classifications of civilian systems and equipment”, Doktorsavhandling, Acta Universitatis Upsaliensis, Digital Comprehensive Summaries of Uppsala Dissertations from the Faculty of Science and Technology 549, 127 pp, 2008, ISBN 978-91-554-7272-6

17. Fredrik Lindgren, ”Hotbildsunderlag i utvecklingen av civilt försvar”, FOI Memo 5089, 2014-10-14

18. Daniel K Jonsson, ”Typfall 5: Utdragen och eskalerande gråzons-problematik, Komplettering av hotbildsunderlag i utvecklingen av civilt försvar”, FOI Memo 6338, 2018-01-31

19. FM MSD16, ”Militärstrategisk doktrin för Sveriges militära försvar”, 2016

20. ”Förstudie om risk- och sårbarhetsanalys avseende EM-hot mot samhällsviktig infrastruktur”, Tomas Hurtig, Sten E Nyholm, Åsa Waern, Hampus Thorell, Kia Wiklundh, Myndigheten för samhällsskydd och beredskap (MSB), MSB1081 - mars 2017, ISBN 978-91-7383-733-0

21. Peter Stenumgaard, ”EMC-kriminalitet – ett växande hot”, Electronic Environment, https://www.electronic.nu/2014/11/12/emc-kriminalitet-ett-vaxande-hot/ (2017-11-28)

22. ”Göteborgskravallerna”, Wikipedia, https://sv.wikipedia.org/wiki/G%C3%B6teborgskravallerna (2017-11-28)

23. “UHF microwave gun”, YouTube, https://www.youtube.com/watch?v=FIU8WZR9DNA (2017-11-28)

24. ”EMC - Elektromagnetisk kompatibilitet”, Elsäkerhetsverket, http://www.elsakerhetsverket.se/privatpersoner/EMC/ (2017-11-28)

25. ”Radiostörningar”, Post- och telestyrelsen, http://www.pts.se/sv/Bransch/Radio/Radiostorningar/ (2017-11-28)

Bilaga 1: Hotscenarier

Typfall med vidare kontext

Hotscenarierna kan med fördel knytas mot något av de fyra typfall som FOI tagit fram för att användas av några av samverkansområdena i deras kommande sårbarhetsanalyser. Följande typfall beskrivs [17, 18].

- **Typfall 1: Beredskapshöjning, mobilisering och transport till utgångsområden**

  Typfallet berör mobilisering och koncentrering av Försvarsmaktens krigsförband i ett läge där ett begränsat väpnat angrepp ännu inte inträffat, men kan vara förestående.

- **Typfall 2: Angrepp med fjärrstridsmedel m.m., huvudsakligen mot civila mål**

  Typfallet omfattar ett begränsat väpnat angrepp med fjärrstridsmedel mot civil infrastruktur, i syfte att påverka Sveriges vilja att agera i en pågående internationell kris.

- **Typfall 3: Angrepp med fjärrstridsmedel m.m., huvudsakligen mot militära mål**

  Typfallet omfattar ett begränsat väpnat angrepp med fjärrstridsmedel mot militära mål i syfte att begränsa Sveriges militära förmåga att agera i den aktuella krisen.

- **Typfall 4: Angrepp som omfattar landstigning och luftlandsättning mot viktiga områden i Sverige**

  Typfallet beskriver ett begränsat väpnat angrepp med fjärrstridsmedel mot militära mål och civil infrastruktur, i syfte att kraftigt begränsa Sveriges politiska vilja och militära förmåga att agera. Angreppet följs upp med landstigning och luftlandsättning mot begränsade områden.

- **Typfall 5: Utdragen och eskalerande gråzonsproblematik**

  Typfallet belyser ett eskalerat förlopp som skulle kunna leda mot ett så kallat skymningsläge, dvs. en konfliktsituation där nästa steg kan förväntas vara öppna stridshandlingar.

När händelseförloppen inleds förväntas ett allmänt fredstillstånd råda, utan några genomförda beredskapshöjningar.

För antagonistiska EM-hot mot samhällsviktig verksamhet i ett skymningsläge är det typfall 1 och typfall 2 som är relevanta, medan typfall 4 är en situation med intervention av främmande makt på svenskt territorium som kan väntas medföra direkta angrepp mot civil infrastruktur och typfall 5 beskriver ett förstadium till krigshandlingar.

Typscenarier

I detta avsnitt presenteras några exempel på scenarier som ett sätt att karakterisera EM-hot. Dessa typscenarier togs fram under förstudien för RSA EM-hot [20].

Ett fullständigt scenario utgörs av fyra delar:

- Scenariobeskrivning
- Tekniska specifikationer
- Strålningsegenskaper
- Konsekvensbeskrivning

Här återges tre scenario- och konsekvensbeskrivningar i syfte att illustrera spännvidden bland tänkbara EM-hot. De tekniska specifikationerna och strålningsegenskaperna är utelämnade eftersom denna information oftast är av känslig natur.

Scenariobeskrivningens syfte är att illustrera omständigheterna kring en situation där ett EM-hot kan tänkas dyka upp samt hur hotet kan användas. Beskrivningen kan innehålla en politisk eller samhällelig situation samt visa hur en antagonistisk grupp kan nyttja EM-hotet för att åstadkomma störningar av samhällsviktig verksamhet.

De tekniska specifikationerna visar på förekomsten av materiel som skulle kunna realisera EM-hotet. Dessa specifikationer ligger till grund för en uppskattning av strålningsparametrar, som i kvantitativa elektromagnetiska termer anger hotets dignitet för några relevanta avstånd. Parametrarna är användbara för att beräkna påverkan på en specifik skyddsvärd utrustning och kan användas som underlag för kravställning vid utformning av ett skydd av denna utrustning för att möta det givna EM-hotet.

Konsekvensbeskrivningen försöker illustrera hur och under hur lång tid den skyddsvärda utrustningen påverkas negativt av EM-hotet, vilka återställnings-åtgärder som behövs, samt tänkbara följdeffekter. Notera dock att det är respektive myndighet, landsting, kommun, etc. som bäst kan avgöra de samhälleliga konsekvenserna av en genomförd elektromagnetisk attack mot egna system.

Detaljerna i dessa typscenarier är inte slutgiltiga utan ska endast ses som exempel. Tänkbara variationer kan fås för olika antagonister, situationer eller samtidig förekomst av andra typer av attacker mot nationens förmåga.

Scenarierna behöver anpassas till den verksamhet som är föremål för en RSA. Detta innebär att man väljer ut specifika kritiska system i verksamheten som attackeras med ett relevant HPM-hot som kan ha verkan mot utrustningen, att det finns ett motiv för antagonistens agerande, dvs. ett mål man vill uppnå, samt att en lyckad attack leder till samhällskonsekvenser som inte är försumbara.

Typscenario 1 - Militär antagonist med insmugglat Mikrovågsvapen

Scenariobeskrivning

Efter ett par veckors incidenter mellan svenska och främmande makts militära flyg och fartyg i Östersjön förbereder regeringen ett beslut att införa höjd beredskap och mobilisera Försvarsmakten. I detta skymningsläge aktiveras ett tjugotal antagonistiska grupper med ca fyra personer i varje. De opererar i eller i närheten av de sju största svenska städerna.

Varje grupp har hyrt en lätt lastbil med kapell av elektromagnetiskt transparent material (tyg, plast, ...) och har på detta monterat en mikrovågskälla med pulsaggregat som laddas av ett dieseldrivet elverk. Elverket har köpts i handeln medan pulsaggregat och mikrovågskälla med hopfällbar reflektor har levererats i delar med gummibåtar från u-båtar utanför kusten. Utrustningen är monterad på lastbilens flak, antennen riktas åt sidan och strålar genom kapellet utan att detta behöver lyftas. Utifrån ser det ut som en vanlig lastbil som används för privata transporter.

Grupperna kör runt i sina tilldelade områden och stannar till utanför driftcentraler, kopplings- och transformatorstationer i eldistributionsnätet, större FM/TV-master, distributionscentraler för radio-, TV- och dataöverföring, myndighetsbyggnader, larmcentraler, kopplingsskåp för trafikljus, SJ:s biljettkontor, bensinstationer, banker, etc. Vid varje ställe stannar lastbilen till i några minuter och avfyrar en serie mikrovågspulser, med olika frekvens, som riktas mot elektronikinstallationer, datorer, antenner m.m. Avståndet mellan lastbil och målobjekt är några tiotal meter.

Konsekvensbeskrivning

Det tar en stund innan operatörer kan konstatera att man utsatts för en avsiktlig elektronisk attack och inte råkat ut för en vanlig driftstörning. Då har lastbilen hunnit försvinna och är på väg till nästa angreppspunkt.

Angreppet leder till att det utsatta objektet tappar kommunikationen med andra platser, att datorer slås ut och att larm- eller tillträdessystem kan upphöra att fungera, även efter att antagonisterna försvunnit och den EM-strålningen upphört.

Eftersom flera elektroniska komponenter i varje anläggning *förstörts* blir felsökningen tidsödande och det kan ta flera dagar att få tag på ersättnings-komponenter/apparater eftersom dessa måste beställas från leverantören.

Eftersom verksamheten inte kan fortsätta som normalt kommer organisationens krisplan att stresstestas. Finns redundanta systemlösningar som fungerar kan verksamheten återupptas så fort beslut om omkoppling kommer.

Är aktuell verksamhet av samhällsviktig natur måste allmänheten informeras. De vanliga informationskanalerna är dock sannolikt utslagna och det är svårt att få en klar bild över omfattningen på skadorna. Dessutom är det näst intill omöjligt att förklara hur situationen uppstått, vilket i sig kan oroa såväl personalen som medborgarna.

Typscenario 2 - Terroristorganisation som använder kommersiella störsändare

Scenariobeskrivning

Svenska regeringen har under en period offentligt kritiserat ett flertal organisationer som man anser genomför terrorhandlingar. Organisationerna har reagerat på regeringens utspel och hotat med vedergällning.

Vid detta tillfälle aktiveras ett tjugotal antagonistiska grupper med ca fyra personer i varje. De opererar i Stockholm, Malmö och Göteborg. Varje grupp har tillgång till en stor mängd enkla (kommersiella) störsändare som stör på frekvensband för mobiltelefoni, RAKEL och GPS.

Varje störsändare väger några kilo och utplaceras tillsammans med batteri i väskor av många olika typer på ett trettiotal platser i varje stad. Strategiska platser är dels offentliga platser där mycket människor rör sig och är vana att kunna använda trådlösa tjänster samt regeringskansli, polisstationer och andra områden där samhällsviktiga tjänster störs ut.

Konsekvensbeskrivning

Utrustning som kommunicerar på de störda frekvensbanden *störs ut* så länge störningen pågår, men kommer att återgå till normal funktion när störsändarna stängs av. Inga komponenter har skadats, men apparater kan behöva startas om för att fungera igen.

Sändarna kan hittas med pejlingsförfarande men då de är många och placerade i väskor kan man inte utesluta möjligheten att de är apterade med sprängladdningar, varför röjningsarbetet tar flera dagar i anspråk. Eftersom störsändarna är kommersiellt tillgängliga kan de inte kopplas direkt till en angripare.

Typscenario 3 - Terroristgrupp eller kriminellt gäng med hemmabyggd IEMI-källa

Scenariobeskrivning

En terroristgrupp har svårt att få tag på kemikalier för att tillverka explosivämnen eftersom i handeln förekommande peroxider m.m. innehåller tillsatsämnen som förstör tillverkningsprocessen och kontrollen av civila explosiva varor blivit striktare. De tillverkar istället en IEMI-källa av en marin radar med kraftaggregat. Radarantennen monteras vertikalt inuti en industridammsugare, där motor avlägsnats och metallskalet ersatts med ett gjutet plastskal. Även kraftförsörjning med PSU-enhet, bilbatteri och batteriladdare monteras in i skalet. Med en liten kontrollenhet kopplad till en mobiltelefon kan den konstruerade IEMI-källan göras fjärrstyrd och repetitiv.

Terroristgruppen klär ut sig till städare och tar med IEMI-källan till entrén av en myndighetsbyggnad, pluggar in elkabeln i städuttaget i entréhallen och riktar antennen mot reception och driftcentral, som drabbas av driftstörningar eller avbrott.

Konsekvensbeskrivning

Detta EM-hot utgör ett mellanting mellan den militära HPM-utrustningen i typscenario 1 och den kommersiella störsändaren i typscenario 2. Effekterna begränsas till utrustning som kan påverkas med frekvensen för den valda radarn, men är inte begränsad till enbart kommunicerande utrustning. Strålningen kan koppla in på kablar och ledningar på kretskort m.m., och vara ett hot även mot icke-kommunicerande utrustning.

Det finns en viss möjlighet att elektroniska komponenter kan förstöras permanent medan andra enbart störs under den tid bestrålningen pågår. Även om man drar ur den i vägguttaget inkopplade kabeln till ”dammsugaren” kan det ta en lång stund innan 12 V-batteriet är urladdat och strålningen upphör.

Bilaga 2: Mallar

Denna bilaga innehåller mallar med frågeformulär att använda vid en RSA avseende elektromagnetiska hot samt mallar för notering och bedömning av identifierade risker och sårbarheter. Dessa är avsedda att utgöra ett stöd för de som förbereder, genomför och sammanställer en RSA EM-hot.

Det är främst avsnittet riskidentifiering som är specifikt för EM-hot, medan andra delar av RSA:n ansluter sig närmare till en RSA för andra hottyper. Notera att vissa frågeställningar kan återkomma under olika faser i en RSA samt att beroende på verksamhetens natur kan även andra frågor vara aktuella.

Mallarna med frågor innehåller rutor för avprickning att man behandlat respektive frågeställning, medan utförligare beskrivningar kan behöva göras separat. Noteringsprotokollen har en rad för varje identifierad händelse, men även här kan det behövas utförligare dokumentation på separat papper. Dessutom bör man notera namn på deltagare och roller vid genomförandet.

Förberedelser

Underlag för att bestämma om man behöver anlita EM-extern kompetens för att beskriva EM-hot och möjlig verkan, samt hur en RSA EM-hot relaterar till organisationens övriga RSA-arbete.

Förarbete

Syftar till att etablera en gemensam syn på verksamhetens roll i samhället, samt bestämma vilka kompetenser som ska medverka och vad som behöver förberedas inför genomförandet av RSA EM-hot. Plats för genomförandet samt sekretess och tidsramar behandlas.

Genomförande

Innehåller vägledande frågor som avser att hjälpa till med identifiering av risker avseende EM-hot, analys av identifierade risker, samt en inledande riskutvärdering.

Noteringsprotokoll för riskbedömning

En mall för att fylla i identifierade händelser med en kort beskrivning, samt uppskattningar av sannolikhet och konsekvens för respektive händelse.

Efterarbete

Vägledande frågor för att tydliggöra vem som ansvarar för sammanställning av resultaten, identifierade risker, samt inledande sårbarhetsbedömning, riskbehandling samt åtgärdsförslag.

Noteringsprotokoll för sårbarhetsbedömning

En mall för att fylla i identifierade händelser med sårbarhetsbedömning, riskbehandling och åtgärdsförslag.

Risk- och sårbarhetsanalys EM-hot

Förberedelser

	Datum
Kan en RSA EM-hot genomföras med den kompetens som finns inom organisationen?	
Finns tillräcklig kunskap om existerande EM-hot?	
Finns tillräcklig systemkunskap och teknisk kompetens?	
Vem/vilka ska representera verksamheten vid RSA:n?	
Vem/vilka ska utforma hotscenarier inför RSA:n?	
Behöver man anlita extern EM-kompetens för RSA:n?	
Behöver man involvera entreprenörer som sköter drift och underhåll?	
Hur integreras RSA EM-hot i organisationens RSA- och säkerhetsarbete?	
Är RSA EM-hot del av en övergripande RSA för alla typer av hot?	
När ska RSA EM-hot vara genomförd?	
Hur ska avrapportering av RSA EM-hot ske?	
Vem är mottagare av RSA EM-hot?	
Vem ansvarar för att resultatet av RSA EM-hot tas om hand?	
Inför förmöte, att ta upp vid inledande samtal	
Vilket material behövs tas fram inför förmötet?	
Kompetens som behövs på förmötet?	
Planering av arbetet, tid och resurser	

Risk- och sårbarhetsanalys EM-hot

Förarbete

	Datum
Vilken roll spelar verksamheten i den nationella krisberedskapen?	
Vad är verksamhetens syfte?	
Vilka beroenden har denna verksamhet av andra verksamheter?	
Vilka andra verksamheter är beroende av denna verksamhet?	
Vilken typ av underlag behöver tas fram inför genomförandet av RSA EM-hot?	
Behöver verksamheten presenteras för de som står för EM-kompetens?	
Behöver EM-typhot presenteras för verksamheten?	
Vilka kompetenser/personer ska medverka vid genomförandet av RSA EM-hot?	
Behövs ytterligare verksamhetsföreträdare?	
Behövs ytterligare EM-kompetens?	
Behöver RSA:n genomföras på plats vid en anläggning eller verksamhetsplats?	
Finns möjlighet att inspektera utrustnings placering, skydd, etc.?	
Behövs särskilt tillstånd för besök vid anläggning?	
Vem arrangerar besöket?	
Begränsningar och villkor för RSA EM-hot	
Vilka sekretessnivåer och behörigheter gäller?	
När ska RSA EM-hot vara genomförd?	

Stödfrågor för att diskutera sårbarheter och hotnivå	
Finns några redan kända sårbarheter? Finns konkreta händelser att utgå ifrån? Vilka system är mest kritiska för verksamheten? Finns det system som andra system är beroende av? Finns det system utan redundans? Vad är det värsta som skulle kunna inträffa och kan det inträffa pga EM-hot?	
Beroende av trådlös kommunikation eller GNSS?	
Vilken hotnivå är viktig att täcka med ett hotscenario? Är det allmänna scenariot tillräckligt/för utmanande?	

Risk- och sårbarhetsanalys EM-hot

Genomförande

	Datum
RISKIDENTIFIERING	
Verksamhetsbeskrivning	
Vilka EM-typhot är mest relevanta för verksamheten? Vilka antagonister är troligast? Finns uttalade hotbilder mot verksamheten? Vilka EM-hot kan påverka verksamheten mest?	
Finns det i verksamheten system som om de slås ut kan orsaka regional eller nationell påverkan?	
Finns det system eller delsystem som inte har någon redundans? Vad blir konsekvensen om de slås ut?	
Hur känd är sårbarheten? (indirekt information om händelsens sannolikhet) Finns det kända brister, sårbarheter/information på internet eller i öppna publikationer som kan nyttjas av antagonist?	
Finns det system som är kritiska för verksamheten? Vad är förutsättningen för att systemen ska fungera? Vad kan hindra att systemen fungerar? Finns tillgång till reservdelar, strömförsörjning, bränsle till reservkraftaggregat?	
Finns risker som inte omfattas av scenariot? Sårbarheter hos andra system på samma plats? Finns samma typ av system på flera platser, skiljer situationerna sig åt? Vad händer om scenariot ändras något?	
Åtkomst och perimeterskydd	
Hur nära kan en antagonist komma det skyddsvärda systemet? Inom 10 m? Inom 10-50 m? Längre bort än 50 m? Längre bort än 100 m? Hur ser omgivningen ut? T.ex. öppet fält, skog, bebyggelse, …	
Finns det en allmän väg direkt utanför avspärrat område? T.ex. utanför staketet, fram till porten, etc.	
Var kan en avsiktlig störare placera sig? Har systemets antenn riktverkan och hur stor är den? På vilken höjd sitter antennen?	

Hur ser perimeterskyddet ut? T.ex. staket med taggtråd, byggnadsväggar, skyltar, patrullerande vakt, etc. Vad är väggarna gjorda av? T.ex. metall som skärmar av strålning, eller trä, betong, ...	
Finns det någon typ av skydd för systemet? T.ex. skalskydd kring viktig elektronik, transientskydd eller ingångsfilter på kablar och genomföringar, tillträdesskydd, etc.	
Finns tillträdesskydd? T.ex. passagesystem med kod, kameraövervakning, bevakning med vakt, etc.	
Bedrivs ett aktivt EMC-arbete med systemet?	
Upptäckt av hot och larmfunktion	
Hur upptäcks felet? Finns övervakningssystem?	
Hur snabbt upptäcks felet och hur snabbt kan felet åtgärdas? Tidsuppskattning?	
Finns det en larmfunktion som larmar om systemet blir utstört eller får nedsatt funktion?	
Finns det sensorer som övervakar den elektromagnetiska miljön, dvs. detekterar förhöjda nivåer av elektromagnetiska fält eller strålning? Kan dessa larma vid förhöjda nivåer? Kan dessa användas för forensiska analyser i efterhand för att utreda vad som har hänt?	
Åtgärdande av fel	
Finns det tillgång till servicepersonal som kan rycka in med kort varsel vid funktionsstörningar? Är dessa fast anställda i verksamheten, konsulter som sköter driften, eller inhyrda entreprenörer som kallas in vid behov?	
Finns reservdelar tillgängliga? Kan de ha påverkats vid en attack? Måste reservdelar beställas? Leveranstid?	
Vem kan vid behov beordra in extrapersonal eller servicepersonal? T.ex. chef, operatör, vakt, etc. Är denna person nåbar dygnet runt alla dagar?	

Konsekvenser och spridningseffekter	
Vad blir konsekvensen om fel uppkommer? Kan/måste man hantera felet manuellt? Vem kan åtgärda eventuella fel? Hur allvarlig är konsekvensen?	
Kan effekterna sprida sig i ett komplext system? Hur påverkas verksamheten om effekterna sprider sig?	
Om scenariot ändras något, vad händer då?	
RISKANALYS	
Hur sannolikt är det att någon ska kunna få tag på eller konstruera utrustningen för EM-hotet? Är EM-hotet kommersiellt tillgängligt? Kan EM-hotet konstrueras av någon med kunskaper och resurser? Finns beskrivningar av hotkonstruktioner på internet?	
Hur sannolikt är det att antagonisten ska välja att använda sig av EM-hotet? Finns det alternativa metoder? Har denna typ av antagonist använt EM-hot tidigare? Finns erfarenhetsdata eller statistiskt underlag?	
Hur sannolikt är det att antagonisten har tillräcklig information om det skyddsvärda systemet för att EM-attacken ska lyckas? T.ex. arbetsfrekvenser, placering, förekomst av fysiska skydd, åtgärder vid felfunktion, etc.	
Finns det allmänna sårbarheter som kan utnyttjas (högre sannolikhet)? Exempelvis beroende av trådlösa system eller GNSS?	
Hur omfattande blir de tekniska konsekvenserna resp. verksamhetskonsekvenserna vid användning av EM-hotet? Kan dessa kvantifieras i ekonomiska termer eller antal drabbade personer?	
Kan identifierade konsekvenser spridas till andra samhällsviktig verksamhet och kritisk infrastruktur eller andra samhällssektorer?	
Kan scenarierna modifieras eller förfinas för att hitta ytterligare sårbarheter eller ännu svårare konsekvenser?	
RISKUTVÄRDERING	
Vilka osäkerheter finns i bedömningen av de identifierade riskerna? Är bedömningen baserad på statistiskt underlag, erfarenhet eller rena gissningar?	
Hur långa avbrott kan man tillåta i systemets funktioner?	

Vilka riskreducerande åtgärder kan vidtas? T.ex. utökat perimeterskydd, extra skalskydd, transientskydd eller filter på kablar och signalingångar, larmfunktion för förhöjd EM-nivå, lagerhålla reservdelar eller reservsystem, etc. Vilka fördelar resp. nackdelar har varje föreslagen åtgärd? Kan de olika riskreducerande åtgärderna värderas?	
Kan de olika riskerna rangordnas i prioriteringsordning?	
Finns det identifierade risker som kan accepteras om de uppträder under en viss begränsad tid?	
Behövs ytterligare analyser av vissa identifierade risker med EM-hot?	

Noteringsprotokoll för riskbedömning vid RSA EM-hot					
HÄNDELSE	SÅRBARHET	BESKRIVNING	SANNOLIKHET	KONSEKVENS	ÅTGÄRD

Risk- och sårbarhetsanalys EM-hot

Efterarbete

	Datum
Vem ansvarar för att sammanställa resultatet av RSA EM-hot?	
Behövs medverkan av EM-kompetens i fortsättningen av RSA?	
Ska RSA EM-hot innehålla detaljerade förslag på åtgärder?	
Genomgång av riskutvärdering	
Finns det risker som inte behandlats i riskanalys och riskutvärdering?	
Vilka osäkerheter finns i bedömningen av de identifierade riskerna?	
Sårbarhetsbedömning	
Vilka förmågor bortfaller eller reduceras om EM-hotet realiseras?	
Hur länge sker bortfall eller reducering av förmågor?	
Hur kan förmågeförlust sprida sig till andra system eller verksamheter?	
Hur påverkas den nationella krisberedskapen vid bortfall av eller reducerad förmåga?	
Riskbehandling och åtgärdsförslag	
Vilka risker kan accepteras och vilka risker behöver åtgärdas?	
Finns risker som kan åtgärdas med utökat perimeterskydd?	
Finns risker som kan åtgärdas med utökat tillträdesskydd?	
Finns risker som kan åtgärdas med extra skalskydd?	
Finns risker som kan åtgärdas med transientskydd eller filter?	
Vilken kostnad innebär föreslagna åtgärder?	
Vilka risknivåer uppnås efter föreslagna åtgärder?	

Noteringsprotokoll för sårbarhetsbedömning vid RSA EM-hot			
HÄNDELSE	SÅRBARHETSBEDÖMNING	RISKBEHANDLING	ÅTGÄRDSFÖRSLAG

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1178 - februari 2018 ISBN 978-91-7383-803-0