Myndigheten för samhällsskydd och beredskap

Förstudie om risk- och sårbarhetsanalys avseende EM-hot mot samhällsviktig verksamhet

Faktaruta

Förstudie om risk- och sårbarhetsanalys avseende elektromagnetiska hot mot samhällsviktig infrastruktur

2016

FOI

Tomas Hurtig, Sten E Nyholm, Åsa Waern, Hampus Thorell, Kia Wiklundh

Många samhällsviktiga funktioner förlitar sig idag på elektroniska system och trådlösa kommunikationssystem. Eftersom dessa är mycket känsliga för elektromagnetiska (EM) störningar, utgör EM-störningar ett hot mot samhällsviktig verksamhet. Denna förstudie utgör ett underlag för fortsatt arbete för att nyttjas vid risk- och sårbarhetsanalyser med EM-hot vid höjd beredskap. I arbetet har exempelscenarier som innehåller realistiska EM-hot och ett förslag på fortsatt arbete tagits fram.

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

Publikationsnummer MSB1081 – mars 2017
ISBN 978-91-7383-733-0

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

Förord

Denna rapport är framtagen av FOI på uppdrag av MSB, MSB 2016-2480.

Arbetet har utförts av FOI. Som komplement till underlaget har diskussioner genomförts med samverkansområdena Teknisk Infrastruktur, Transporter och Ekonomisk Säkerhet, samt med stöd av en referensgrupp bestående av representanter från MSB, FortV, FHS, FMV och FOI och centrala beredningsgruppen (CBG) mot elektromagnetiska (EM) hot.

Innehållsförteckning

Förord **3**
Innehållsförteckning **4**
Sammanfattning **6**
1. Introduktion **7**
1.1 Bakgrund 7
1.2 Syfte 7
1.3 Metod 8
1.4 Definitioner 9
2. EM-hot **11**
2.1 Typer av EM-störningar 11
2.1.1 Naturliga EM-störningar 11
2.1.2 Oavsiktliga EM-störningar 12
2.1.3 Avsiktliga EM-störningar 12
2.2 Exempel på EM-incidenter 14
2.2.1 Oavsiktliga EM-störningar 14
2.2.2 Avsiktliga EM-störningar 15
2.2.3 HPM 16
2.3 Klasser av EM-störningar 18
2.4 Konsekvenser av EM-hot i form av verkansavstånd 18
2.4.1 Avsiktlig störning mot trådlösa system 18
2.4.2 HPM 18
3. Riskhantering och RSA **21**
3.1 RSA – modeller allmänt 22
3.2 Processteg i RSA 22
3.3 Information i de olika processtegen 24
4. Gemensam hotbild **25**
4.1 Behovsanalys 25
4.2 Hotscenarier 27
4.3 Gråzonen mellan krig och fred 28
4.4 Exempelscenarier 30
4.4.1 Exempelscenario 1 30
4.4.2 Exempelscenario 2 31
4.4.3 Exempelscenario 3 32
5. Former för att genomföra en RSA **33**
5.1 Struktur för att organisera informationen 35
6. Slutsatser **38**
6.1 Diskussion 38

6.2 Förslag på organisation av huvudstudie 38
7. Referenser 40
8. Bilaga 1: Verkansavstånd HPM 42
9. Bilaga 2: Aktörer inom de olika samverkansområdena 44

Sammanfattning

Många samhällsviktiga funktioner förlitar sig idag på elektroniska system och trådlösa kommunikationssystem. Eftersom dessa är mycket känsliga för elektromagnetiska (EM) störningar, utgör EM-störningar ett hot mot samhällsviktiga verksamheter. 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 förstudie utgör ett underlag för fortsatt arbete för att nyttjas vid risk- och sårbarhetsanalyser med EM-hot vid höjd beredskap.

Förstudien behandlar de EM-hot som kan anses relevanta mot samhällsviktiga funktioner. Förstudien ger förslag på hur EM-hoten kan klassificeras och visar på vad som är väsentliga parametrar samt hur dessa kan struktureras. Tre exempel på hotscenarier presenteras. De tre hotscenarierna beskriver situationer som skulle kunna inträffa vid höjd beredskap eller i den s.k. gråzon som föregår höjd beredskap, men händelser i scenarierna kan även ske i ett normalläge exempelvis i ett kriminellt syfte. Grundscenarierna ska kunna nyttjas i kommande RSAer. Scenarierna utgörs av fyra delar (scenariobeskrivning, tekniska specifikationer, strålningsegenskaper och konsekvensbeskrivning) och är utvecklade för att kunna anpassas mot den verksamhet som är föremål för en RSA.

Förslag ges även på hur en RSA skulle kunna genomföras. Olika steg definieras, vilken typ av information och frågeställningar som behöver besvaras, samt vilken typ av kompetens som krävs för att genomföra en RSA presenteras. Förstudien utgör också ett underlag för den huvudstudie som föreslås. Förslaget består av en pilotstudie, där en RSA mot EM-hot genomförs i dialog med en aktör, samt av metodutveckling av hur RSAn bör genomföras.

1. Introduktion

1.1 Bakgrund

Kommuner, landsting, länsstyrelser och centrala myndigheter är skyldiga att sammanställa risk- och sårbarhetsanalyser (RSA) för att kartlägga sårbarheten i samhället och för att öka förmågan att hantera kriser. En RSA ger kunskap om hur vi kan förbereda oss inför och hantera kriser. Syftet med en RSA är att:

- ge beslutsunderlag för beslutsfattare och verksamhetsansvariga,
- ge underlag för information om samhällets risker till allmänheten och anställda,
- ge underlag för samhällsplanering, samt
- bidra till en riskbild för hela samhället.

En RSA ska identifiera samhällsviktig verksamhet och olika oönskade händelser, bedöma hur troligt det är att händelserna inträffar, bedöma de omedelbara negativa konsekvenserna, analysera verksamhetens sårbarheter samt bedöma förmågan att hantera olika påfrestningar.

Även samverkansområdena[1] har fått i uppgift att under 2016 påbörja en övergripande RSA som tillkommer vid höjd beredskap och civilt försvar inom sina respektive områden.

Centrala Beredningsgruppen (CBG) Elektromagnetiska Hot (EM-hot), som består av representanter för ett antal myndigheter, har i uppgift att sprida information inom EM-området till deltagande organisationer. Med EM-hot menas, i detta sammanhang, källor till elektromagnetisk strålning som kan skapa svåra störningar av samhällsviktiga funktioner som t.ex. teknisk infrastruktur. En deluppgift för CBG EM-hot är även att ta fram rekommendationer och råd för EM-skyddsåtgärder och utarbeta underlag för RSA. CBG EM-hot har gjort bedömningen att de RSAer som tidigare genomförts för samhällsviktig infrastruktur inte i tillräcklig grad omfattar EM-hot.

1.2 Syfte

Mot denna bakgrund har en förstudie genomförts med uppgiften att beskriva problemområdet kring EM-hot mot samhällsviktig verksamhet, hur en RSA kan genomföras samt med att utveckla grundscenarier att utgå från då en RSA ska genomföras.

---

[1] Samverkansområdenas uppgift finns angivna i bilaga till Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (krisberedskapsförordningen).

I förstudien har även ingått att ge förslag på hur en huvudstudie bör organiseras och genomföras, där huvudstudien ska behandla EM-hot och risker mot samhällsviktig verksamhet. Resultatet från förstudien ska kunna utgöra en grund för den RSA som kommer att genomföras inom samverkansområdena.

Det bör betonas att detta är en förstudie och ett relativt begränsat arbete, vars resultat kan användas som grund för vidare arbete. Resultatet från förstudien ska därför ses som ett underlag för huvudstudien, men underlaget kan också användas för att förklara relevansen och betydelsen av att beakta EM-hot mot samhällsviktiga funktioner och infrastruktur. Arbetet behandlar inte åtgärder och skydd mot EM-hot. För sådan information hänvisas läsaren exempelvis till [6].

Rapporten beskriver olika typer av EM-hot samt tre grundscenarier med EM-hot mot samhällsviktig verksamhet. Scenarierna beskriver situationer som kan inträffa vid höjd beredskap eller i den s.k. gråzon som föregår höjd beredskap, men händelser i scenarierna kan även ske i ett normalläge exempelvis i ett kriminellt syfte. Scenarierna utgörs av fyra delar, scenariobeskrivning, tekniska specifikationer, strålningsegenskaper och konsekvensbeskrivning. De tre exempel som tagits fram representerar en bredd av troliga situationer där EM-hot kan tänkas dyka upp, olika tillvägagångssätt av antagonister, olika grad av komplexitet hos EM-hotet samt olika grad av upptrappningen av beredskap. Grundscenarierna ska kunna nyttjas för kommande RSAer. Dock kan det finnas behov av att anpassas grundscenarierna något mot den verksamhet som är föremål för en RSA, eftersom system, hotbild och förutsättningar, exempelvis geografiskt, kan variera mycket mellan olika verksamheter. Det finns en fördel i att utgå från grundscenarier. Det möjliggör att flera aktörer som använder sig av samma grundscenarier kan jämföra resultat, detaljer kan diskuteras och eventuella förändringar av scenarierna kan nyttas av flera aktörer.

Rapporten ger också förslag på hur en RSA som involverar EM-hot kan genomföras. Förslag ges på former för genomförandet, vilken typ av kompetens som behövs, vilken information (information om EM-hot, verksamhetens system, hotbild) som behövs i de olika stegen av en RSA samt hantering av sekretess. Det poängteras exempelvis att teknisk expertis både om EM-hot och om verksamheternas system och deras inbördes beroenden är nödvändig vid genomförandet av flera av de olika stegen i en RSA. Förslaget ska användas som grund för det fortsatta arbetet där förslaget är att en pilotstudie genomförs och att utveckla metoden för genomförandet. Pilotstudien innebär att en RSA mot EM-hot genomförs i dialog med en aktör.

1.3 Metod

Arbetet har baserats på tidigare resultat som tagits fram på FOI, men också genom diskussioner med samverkansområdena Teknisk Infrastruktur (SOTI), Transporter (SOTP) och Ekonomisk Säkerhet (SOES). Projektet har också nyttjat styrning från CBG EM-hot och den referensgrupp som bildats för uppdraget. Referensgruppen har bestått av representanter från MSB, FortV, FHS, FMV och FOI. Anledning till att diskussioner har skett speciellt med SOTI, SOTP och SOES är att dessa bedömdes som viktigast att träffa. Detta

eftersom de ansågs ha ett stort beroende av elektronik, IT-utrustning, trådlös kommunikation och GPS, vilka alla är mycket sårbara för EM-källor.

Diskussioner med SOTI, SOTP och SOES har speciellt rört frågor kring:

- Hur hotscenarierna bör utformas, vilken information, detaljeringsgrad
- Former för att få fram information från experter på samverkansområdenas system, som behövs vid riskidentifieringen, riskbedömningen och beroenden

Diskussionerna har också gett förståelse för vilken verksamhet som finns inom de olika samverkansområdena och vilka system som kan anses vara kritiska för deras verksamhet.

1.4 Definitioner

Antagonist - Person som har för avsikt att orsaka negativa effekter eller skador, t.ex. på samhällskritiska funktioner 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 som en samhällsviktig verksamhet är beroende av. 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 EM-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 de fenomen som uppträder när elektromagnetisk strålning påverkar elektronisk utrustning.

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

Samhällsviktiga funktioner – En samhällsviktig verksamhet definieras som 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 [15].

Kritisk infrastruktur – Fysisk struktur vars funktionalitet bidrar till att säkerställa upprätthållandet av viktiga samhällsfunktioner [15].

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 av dem.

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

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

2. EM-hot

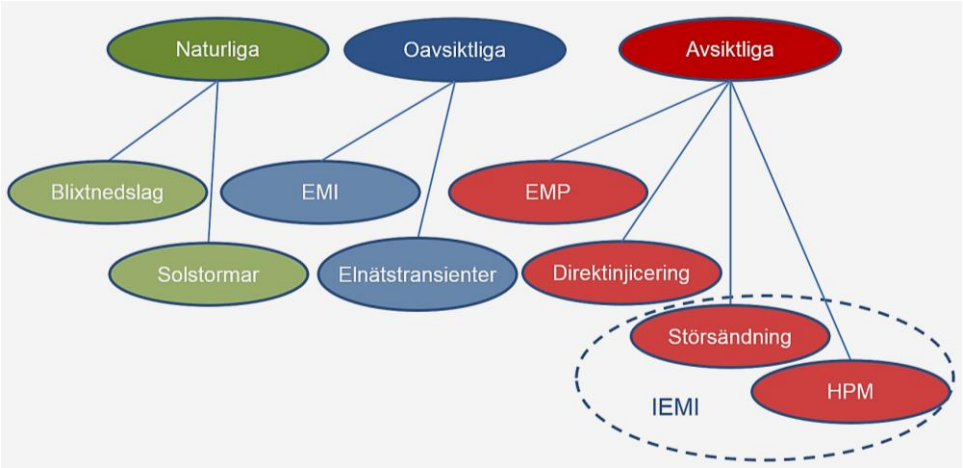
EM-hot kan på olika sätt störa eller helt slå ut tekniska system och infrastruktur antingen direkt eller indirekt. Direkt störning har, som begreppet antyder, direkt påverkan på kritiska funktioner medan indirekt störning avser följdverkningar på system, vilket exempelvis kan ske då GPS-mottagare störs så att felaktig eller ingen tid levereras, som får till följd att funktioner fallerar.

2.1 Typer av EM-störningar

Den totala bilden avseende EM-hot mot samhällsviktig infrastruktur består av ett antal specifika hot som har olika orsaker, olika karakteristika, olika verkan på olika infrastrukturobjekt samt kräver olika typer av skyddsåtgärder. En första indelning av EM-hot kan göras i naturliga hot, av människa skapade oavsiktliga hot och av människa skapade avsiktliga hot, Figur 1.

2.1.1 Naturliga EM-störningar

Exempel på naturligt förekommande hot är blixtnedslag direkt i eller i närhet av infrastrukturen och solstormar. Blixtströmmar kan vara kraftiga, toppvärdet ligger i medeltal på 30 kiloampere, men kan i vissa fall uppgå till några hundra kiloampere medan pulslängden kan vara upp till några tiotal millisekunder [1]. Frekvensinnehållet är oftast jämförelsevis lågt (upp till ca 10 kilohertz). En anläggning behöver inte utsättas för en direktträff vid blixtnedslag för att utsättas för påverkan. Blixtströmmen omges av ett kraftigt magnetfält som i närbelägna objekt, t.ex. elektriska ledningar, inducerar strömmar och spänningar som kan vara kraftiga och förstöra känsliga komponenter.



Figur 1. Indelning av EM-hot mot samhällsviktig infrastruktur.

Solstormar, s.k. rymdväder, genereras av utbrott i solens korona och består av elektriskt laddade partiklar som efter några dygn träffar jordens atmosfär och ger upphov till geomagnetiska störningar i jordens magnetosfär. Dessa störningar påverkar större geografiska områden och kan inducera kraftiga strömmar i större metalliska strukturer som kraftledningar, teleledningar, järnvägsräls, pipelines, m.m. Dessa geomagnetiskt inducerade strömmar (eng. Geomagnetically Induced Currents, GIC) genererar ofta synnerligen lågfrekvent störning, ofta långt under 1 Hz, som kan slå ut elektriska komponenter, t.ex. i transformatorstationer, öka korrosionen i pipelines, m.m. [2].

2.1.2 Oavsiktliga EM-störningar

All elektrisk utrustning genererar EM-fält i sin omgivning. Ofta är dessa helt försumbara, men kan ibland vara så kraftiga att de stör annan elektrisk utrustning i närheten, vilket benämns elektromagnetisk interferens (eng. ElectroMagnetic Interference, EMI). Det är speciellt mottagare för trådlösa kommunikationssystem som är känsliga för EMI eftersom denna utrustning är utvecklad för att ta emot EM-signaler. All kommersiell elektrisk utrustning måste uppfylla standarder och bestämmelser som kräver att utrustningen inte genererar EM-fält kraftigare än en viss angiven nivå. Utrustning som uppfyller dessa krav antas kunna samexistera med annan utrustning och sägs därför ha uppnått en viss grad av elektromagnetisk kompatibilitet (eng. ElectroMagnetic Compatibility, EMC). Det är inte ovanligt att utrustning strålar ut mer elektromagnetisk energi än vad som är tillåtet, t.ex. när någon komponent i utrustningen uppvisar en felfunktion. EMI kan uppträda vid såväl låga som höga frekvenser och störa kontinuerligt eller i form av transienta pulser [3,4,5]. I Sverige är det Elsäkerhetsverket som är tillsynsmyndighet för att säkerställa att lagar och förordningar uppfylls inom området EMC.

En annan oavsiktlig källa till EM-störningar utgörs av kortvariga transienter på lokala elnät. Sådana kan uppkomma t.ex. i samband med att en stamledning eller transformatorstation fallerar, som en följd av att en felaktig apparat inkopplats på nätet eller vid blixtnedslag.

2.1.3 Avsiktliga EM-störningar

Bland avsiktligt orsakade EM-hot kan vi särskilja användning av olika typer av störsändare, direktinjicering av kraftiga strömmar eller spänningar på elektriska ledningar eller signalkablar, generering av kraftiga mikrovågspulser (eng. High-Power Microwave, HPM), samt elektromagnetisk puls från kärnvapen (eng. ElectroMagnetic Pulse, EMP).

Störsändning är ett effektivt sätt att med måttlig energi under en längre tid störa ut funktionen hos en kommunicerande elektronisk utrustning. Det finns idag ett stort antal kommersiellt tillgängliga störsändare som kan störa ut GSM, Global Navigation Satellite System (GNSS[2])-system som exempelvis GPS, WiFi, tetra-baserade system som RAKEL och många andra frekvensband. De är därför enkla att införskaffa och till liten kostnad. I flera länder, exempelvis i

[2] GNSS är ett samlingsnamn för satellitbaserade navigations- och positionsbestämningssystem.

Sverige, är det olagligt att inneha och använda störsändare, men eftersom de säljs via internet är innehavet svårt att kontrollera. En oavsiktlig störningskälla är däremot inte olaglig att inneha även fast effekten kan bli densamma. En störsändare kan operera kontinuerligt under mycket lång tid, men den är möjlig att bestämma riktningen till (pejla in) och åtgärdas. Det är dock relativt svårt att pejla in en störsändare, speciellt i stadsmiljö eller om störsändaren är mobil. Efter att störsändaren stängts ned återtar den störda utrustningen oftast sin funktion.

Kraftiga mikrovågsgeneratorer, HPM-vapen, har utvecklats i flera länder men finns i de flesta fall inte tillgängliga för allmänheten. HPM-källor genererar kortvariga pulser av elektromagnetisk strålning med mycket hög toppeffekt som kan kopplas via ledningar eller kretskort i elektronisk utrustning och fysiskt förstöra halvledarkomponenter. HPM består av högfrekvent strålning (typiskt 100 megahertz - 10 gigahertz) med hög toppeffekt (upp till flera gigawatt) och med kort varaktighet (mellan tiotals pikosekunder upp till millisekund). HPM-vapen går inte att pejla in eftersom strålningen är kortvarig.

Militära HPM-vapen kräver nationella resurser för tillverkning och kan utgöra hot på upp till kilometeravstånd. Dessa kan sägas utgöra det tunga artilleriet inom telekrigföring. Något enklare HPM-generatorer kan konstrueras av kunniga ingenjörer genom att sätta samman kommersiellt tillgänglig utrustning, som radarantenner, med lämplig kraftförsörjning och styrelektronik, m.m. Dessa pulsade mikrovågsgeneratorer kan utgöra hot på några tiotal eller hundratals meters avstånd.

Användning av störsändare eller av HPM-generatorer brukar sammanfattas i begreppet avsiktlig elektromagnetisk störning (Intentional ElectroMagentic Interference, IEMI).

En elektromagnetisk puls från en kärnvapendetonation i atmosfären genererar en kraftig elektromagnetisk puls med räckvidd över ett mycket stort område, som en hel kontinent. Den kopplar i huvudsak till långa metalliska strukturer som kraftledningar, telefonledningar och järnvägsräls. I dessa genereras starka strömmar och spänningar som kan förstöra inkopplad utrustning. Frekvensinnehållet från en EMP kan se mycket olika ut beroende på var man befinner sig i förhållande till själva detonationen. I Sverige har man enats om en standardpuls att förhålla sig till när man utvärderar materiels tålighet mot EMP. Standardpulsen utgår ifrån ett så kallat åskådarscenario som innebär att själva detonationen sker utanför Svenskt territorium. Den har ett frekvensinnehåll som ligger under 100 megahertz, med maximum under 1 megahertz, och med fältstyrka på upp till 50 kilovolt per meter [6]. I jämförelse med geomagnetiskt inducerade strömmar är en EMP mycket mer kortvarig och har ett högre frekvensinnehåll vilket gör att den även kan koppla till något mindre strukturer.

Direktinjicering av kraftiga spännings- och strömpulser på el- eller telekablar i en byggnad kan förstöra anslutna datorer och annan elektronisk utrustning. En utrustning för direktinjicering kan bäras i en resväska eller liknande och anslutas till åtkomliga ledningar. Signalkablar som arbetar med låga

spänningar (någon eller några tiotal volt) är givetvis särskilt känsliga. Detta är anledningen till att man bör begränsa obehörig åtkomst till dessa, men även till eluttag, kabelstegar, etc. som kan finnas i entréer, receptioner m.m.

2.2 Exempel på EM-incidenter

2.2.1 Oavsiktliga EM-störningar

Det finns en rad incidenter där trådlösa system har störts ut av oavsiktliga störningar. Under 2011 utsattes kommunikationen mellan flygledartorn och flygplan av störningar vid inflygning till Trollhättans-Vänersborgs flygplats [23]. Störningarna kom från en reklamskylt som stod i närheten av flygplatsen, Figur 2. Reklamskylten orsakade problem för flygplan som flög över skylten på låg höjd (ett antal hundra meter) vid start och landning. Flygplatsen hörde dock inte informationssignalen på sin radio och det förklaras av att det är långt till flygplatsen, flera kilometer, och signalerna blir svagare med avståndet. I december 2011 fattade Elsäkerhetsverket beslut om användningsförbud av två reklamskyltar vid Trollhättans-Vänersborgs flygplats som utgjorde ett allvarligt hot mot flygsäkerheten. Störs radiokommunikationen kan anrop från flygplatsen eller från ett annat flygplan missas.

2014 anmälde en nätoperatör problem med radiostörningar på GSM-nätets upplänk vid Eriksbergs shoppingcenter i Västerås [24]. Störningarna uppträdde enbart på kvällen och försvann dagtid, se Figur 3. Orsaken till störningen mot basstationen var en strålkastare som kvällstid belyste en flagga vid ingången till shoppingcentrets entré.

Figur 2. Reklamskylt som störde ut flygledning på Trollhättan-Vänersborgs flygplats [23] Foto: Henrik Olsson, Elsäkerhetsverket.

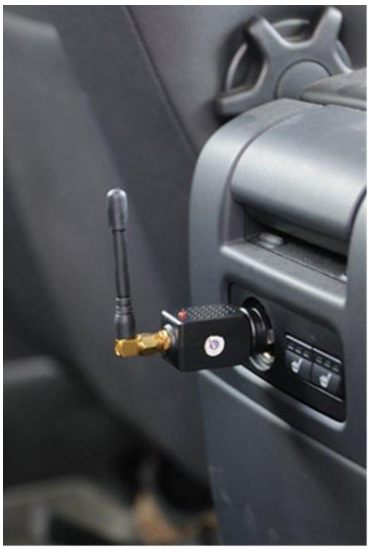
Figur 3. Flaggbelysning vid shoppingcenters entré som störde ut en basstation för GSM-nätet [24] Foto: Henrik Olsson, Elsäkerhetsverket.

2.2.2 Avsiktliga EM-störningar

Störsändning mot radiosystem har historiskt varit en rent militär förmåga där hotet kommit från fientliga utländska aktörer. Idag har den förmågan börjat sprida sig även till det civila samhället vilket innebär ett snabbt växande hot mot kritisk trådlös kommunikation för exempelvis polis, räddningstjänst, trådlösa larm- och övervakningssystem etc. Det är både kriminella grupperingar och aktivister som kan tänkas störa system för att hindra specifika funktioner eller tjänster (förbekämpning inför andra brott). Förmågan sprider sig i takt med att störutrustning är lättillgänglig och säljs mycket billigt via Internet. Där kan vi hitta både färdiga produkter och fullständiga beskrivningar av byggsatser för störsändare mot t ex tetrabaserade-, GPS-, GSM- och 3G-system, se Figur 4.

Det finns en rad rapporterade incidenter om aktiv störning mot civilsamhället, men mörkertalet antas kunna vara stort. Ett exempel på en händelse är i samband med Göteborgskravallerna vid EU-toppmötet 2001 då demonstranter utnyttjade sårbarheten i polisens radiosystem och lyckades störa radiotrafiken under insatsskedet. Störsändare används också av kriminella för att slå ut larm i samband med villainbrott [26]. Störsändaren slår ut den trådlösa kommunikationen, vilket gör att larmet som ska skickas från huset till villaägaren eller larmcentralen inte kommer fram.

Störning av GPS-mottagare i fordon har ökat som ett resultat av att GPS-mottagare installeras i vissa fordon för att kunna övervaka på vilket sätt fordonet används, till exempel vilken väg fordonet färdas. Denna typ av mottagare installeras ofta i lastbilar och andra fordon för yrkestrafik. Som en motreaktion på detta säljs GPS-störsändare som kan monteras i fordon av de som inte vill att deras rörelsemönster skall loggas [16]. 2013 dömdes en man i USA till böter på $32,000 efter att ha stört Newark-flygplatsens air traffic control (ATC) system. Mannen, som var yrkeschaufför, hade en GPS-



Figur 4. GPS-störsändare. Foto: Peter Johansson, FOI.

störutrustning i fordonet för att förhindra arbetsgivaren att följa hans rutt. Federal Communications Commission (FCC) fick indikationer från Federal Aviation Administration att det förekom störningar på väsentliga system på flygplatsen, varefter FCC satte upp ett monitoreringssystem för att kartlägga störningen. FCC fann att störningen kom från ett fordon som regelbundet passerade flygplatsen, vilket gjorde att GPS-mottagare som används för flygplatsens air traffic control system blockerades.

Generellt kan sägas att GPS är mycket enkelt att störa ut eftersom GPS-signalen har en låg effekt då den tas emot. Samtidigt förser GPS många system med kritisk information som position och tid.

2.2.3 HPM

Det finns ett fåtal inrapporterade incidenter där man vet eller har mycket goda indikationer på att kraftig mikrovågsstrålning använts i kriminellt syfte. Tyvärr är den senaste sammanställningen [17] redan ganska gammal (2011) och på grund av forensiska svårigheter kan mörkertalet vara betydande. Den sammanställning som hänvisas till här bygger i sin tur på [18-20], där de flesta av de inrapporterade incidenterna handlar om störning av GPS, GSM och stöldskyddssystem med hjälp av kommersiella eller hemmabyggda störsändare, och dessa tas inte upp här. Inrapporterade incidenter är:

1. I Japan använde kriminella en EMI-källa för att störa funktionen hos en dator i en spelmaskin i syfte att få den att ge vinst.

2. I S:t Petersburg använde en kriminell person en EMI-källa för att slå ut säkerhetssystemet i en juvelerarbutik. I rapporteringen från denna händelse nämndes att EMI-källan hade ungefär samma teknikniva som en vanlig mikrovågsugn.

3. I Ryssland använde, vad som beskrivs som en rebellrörelse, en EMI-källa för att slå ut säkerhetssystemet vid ett övervakat område i syfte att obemärkt kunna ta sig in på området.

4. I Nederländerna störde en angripare ut IT-nätverket vid en lokal bank efter att ha nekats ett lån i banken. Med hjälp av information från internet konstruerade personen en EMI-källa av portföljstorlek. Banken insåg inte att den utsatts för ett externt angrepp förrän förövaren greps.
5. I Moskva upphörde funktionen i en telefonväxel efter att den utsatts för direktinjicering av en elektrisk strömpuls genom en telefonledning med resultatet att 200000 människor blev utan telefon under en dag.

I exempel 5 har man inte använt mikrovågsstrålning utan direktinjicering vilket innebär att man har kunnat komma åt fysiska kablar. Gemensamt för exempel 1,2 och 4 är att man verkar ha använt fysiskt små strålkällor vilket innebär mycket begränsad räckvidd. Detta spelar dock liten roll då man har attackerat utrustning som man har kunnat komma mycket nära. I exempel 3 finns för lite information för att kunna avgöra storleken på utrustningen.

Då denna typ av störning inte nödvändigtvis riktar sig mot specifika kommunikationsband (i frekvens) utan kan koppla energi direkt in i elektronisk apparatur (även om den saknar radiofunktion) omfattas den inte automatiskt av lagen som förbjuder innehav av störsändare. Vanligtvis sänder denna typ av mikrovågsvapen (HPM) ut en serie av mycket korta pulser. Den korta tiden HPM-vapnet är aktivt gör att traditionell pejlutrustning är oanvändbar för att hitta källan.

Tabell 1. Sammanställning av EM-hot och vilken skada de kan orsaka.

EM-hot	**Kan skada:**	**Komplexitet/Realiserbarhet**
Avsiktlig störare –på GPS-systemets frekvensband	GPS-mottagare, stör ut position och tid	Låg/Kommersiell
		Hög/Militär
Avsiktlig störare – på det trådlösa kommunikationssystems frekvensband	Trådlöst kommunikationssystem, blockerar mottagning av den översända informationen	Låg/Kommersiell
		Hög/Militär
HPM	All form av elektronik, tillfällig till permanent skada	Låg/Kommersiell
		Medel/Ingenjörsmässig
		Hög/Militär

2.3 Klasser av EM-störningar

I Figur 1 visas flera olika typer av EM-störningar, vilka kan orsaka stor påverkan på system för samhällsviktig verksamhet. Då detta arbete är fokuserat på hotscenarier vid höjd beredskap (eller i den s.k. gråzon som föregår höjd beredskap) bedöms IEMI-källor vara mest relevanta som hot. Tabell 1 visar en sammanställning av de olika kategorierna samt vad de kan orsaka för skada.

2.4 Konsekvenser av EM-hot i form av verkansavstånd

2.4.1 Avsiktlig störning mot trådlösa system

Avsiktlig elektromagnetisk störning har som syfte att störa trådlösa tjänster som exempelvis tillhandahålls av mobiltelefonisystem, RAKEL, WiFi, och GPS. Risken för att en trådlösa 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. Det kan exempelvis uppstå genom skärmning av utrustning och effekten påverkas starkt av terrängen i kombination med hur upphöjd störsändaren är. Sammanfattningsvis är uteffekt, störsignalens frekvens, störsignalens bandbredd, antenn och antennplacering (antennhöjd) viktiga parametrar för hur väl störaren ska lyckas.

2.4.2 HPM

En HPM-källa sänder ut en serie korta pulser med mycket hög uteffekt och kan störa elektronisk utrustning över stora avstånd. För att åstadkomma förstörande verkan krävs dock mycket högre fältnivåer och verkansavstånden blir därigenom kortare. Med verkansavstånd menas det avstånd EM-källan får avsedd verkan. Exemplen i Tabell 2 till Tabell 4 utgår från tre olika HPM-system. De olika alternativen kräver helt olika kunskap och resurser för att kunna realiseras:

HPM-skåpbil (Militär utrustning)

Här antas ett system där de mest kritiska delarna (pulsaggregat, strålkälla och antenn) tillhandahålls av främmande makt men har anpassats till att kunna fungera i ett civilt scenario. Denna typ av utrustning kräver stora resurser för att realiseras.

HPM-skåpbil (Ingenjörsmässig)

Här antas att en eller flera kompetenta ingenjörer har konstruerat ett system utifrån vetenskapliga artiklar och annan öppen tillgänglig information. Att köpa delar och bygga ett dylikt system får ses som en rejäl investering så risken

att en enskild individ utan uppbackning av en organisation av någon typ bygger denna typ av strålkälla får ses som liten.

HPM-väska (kommersiell)

Det finns ett fåtal kommersiellt tillgängliga mycket kompakta HPM-system, så kallade HPM-väskor. De är av samma storlek som en normalstor resväska men förhållandevis tunga (~25 kg). Det är inte troligt att företagen som producerar dessa säljer dem till privatpersoner, men vartefter de sprids ökar även risken för att en eller flera kan hamna i orätta händer. Tekniken i dessa är dessutom inte så avancerad så det är fullt möjligt för en kompetent ingenjör att bygga ett liknande system, dock med något lägre prestanda.

Av informationen som visas i Tabell 2 till Tabell 4 framgår att verkan avtar hastigt med avstånd och detta beror på att en fördubbling av avståndet minskar effekten i målet med en faktor fyra (~$1/r^4$, där r anger avståndet). Att se till att en eventuell angripare inte kan komma för nära känslig utrustning är därför alltid en bra åtgärd. Att placera känslig utrustning en bit in i byggnader istället för nära fönster och entréer är också en relativt enkel metod som ger extra skydd, se Tabell 3. Slutligen visar Tabell 4 effekten av att se till att känslig elektronik är skärmad, d.v.s innesluten i metalliska skal som stänger ute det mesta av den inkommande strålningen från HPM-källan. Skärmning av elektronisk utrustning till den nivå som antagits (30 dB) är oftast inte så svårt om det görs hos tillverkaren som en del av designprocessen, det kan dock vara väsentligt svårare, och dyrare, att åstadkomma i efterhand. En alternativ presentation finns i Appendix.

Oskyddad civil elektronik

Tabell 2. Verkansavstånd för tre olika klasser av HPM-källor mot oskyddad civil elektronik.

Typ av källa	**Avstånd**			
	Enstaka meter	**15 meter**	**50 meter**	**500 meter**
HPM-skåpbil (Militär utrustning)	Ej relevant	Permanent fysisk skada	Permanent fysisk skada	Permanent fysisk skada
HPM-skåpbil (Ingenjörsmässig)	Ej relevant	Permanent fysisk skada	Störning [1,2]/ skada	Störning [1, 2]
HPM-väska (Kommersiell)	Permanent fysisk skada	Störning [1,2]	Risk för störning [1, 2]	Ingen verkan [3]

[1] Kan orsaka kvardröjande felfunktion

[2] Inombands framvägskoppling kan orsaka permanent skada på detta och större avstånd

[3] Inombands framvägskoppling kan ge störning på detta och större avstånd

Civil elektronik bakom skalskydd

Med skalskydd menas att utrustningen är en bit in i vanlig byggnad. Exempelvis ger ytterväggar av betong ungefärligen en dämpning på 10 dB dämpning, medan tegel ger en mycket liten dämpning.

Tabell 3. Verkansavstånd för tre olika klasser av HPM-källor mot civil elektronik bakom skalskydd.

Typ av källa	**Avstånd**			
	Enstaka meter	**15 meter**	**50 meter**	**500 meter**
HPM-skåpbil (Militär utrustning)	Ej relevant	Permanent fysisk skada	Permanent fysisk skada	Störning
HPM-skåpbil (Ingenjörsmässig)	Ej relevant	Störning[1, 2]/ skada	Störning[1, 2]	Risk för störning[1,2]
HPM-väska (Kommersiell)	Permanent fysisk skada	Störning[1, 2]	Ingen verkan[3]	Ingen verkan[3]

[1] Kan orsaka kvardröjande felfunktion

[2] Inombands framvägskoppling kan orsaka permanent skada på detta och större avstånd

[3] Inombands framvägskoppling kan ge störning på detta och större avstånd

Skärmad elektronik

För alternativet skärmad elektronik antar vi att ett visst extraarbete lagts ned på att skärma känslig elektronik, vilket antas ge 30 dB dämpning.

Tabell 4. Verkansavstånd för tre olika klasser av HPM-källor mot skärmad elektronik.

Typ av källa	**Avstånd**			
	Enstaka meter	**15 meter**	**50 meter**	**500 meter**
HPM-skåpbil (Militär utrustning)	Ej relevant	Permanent fysisk skada	Störning[1, 2]/ skada	Störning [1, 2]
HPM-skåpbil (Ingenjörsmässig)	Ej relevant	Störning[1, 2]/ skada	Ingen verkan[3]	Ingen verkan[3]
HPM-väska (kommersiell)	Störning [1, 2]	Ingen verkan[3]	Ingen verkan[3]	Ingen verkan[3]

[1] Kan orsaka kvardröjande felfunktion

[2] Inombands framvägskoppling kan orsaka permanent skada på detta och större avstånd

[3] Inombands framvägskoppling kan ge störning på detta och större avstånd

3. Riskhantering och RSA

Riskhantering, som är central för krisberedskapsarbetet, sker idag enligt ansvarsprincipen, d.v.s. hos respektive berörd samhällsaktör med utpekat ansvar. I riskhanteringsarbetet ingår RSA för identifierade potentiella extraordinära händelser. Syftet är att förbättra förmågan genom att arbeta förebyggande.

Riskhanteringsprocessen omfattar bland annat följande processteg [10]:

- Utgångspunkter – Roll och ansvarsområde, metod, perspektiv och avgränsningar
- Riskidentifiering
- Riskanalys
- Riskutvärdering

  } Riskbedömning

- Förmågebedömning
- Sårbarhetsanalys

  } Sårbarhetsbedömning

- Resultat och slutsatser, fortsatt arbete, åtgärder, planer mm

Utgångspunkter och riskbedömning ansluter sig till strukturen i ISO-standarden SS-ISO 31000:2009 ”Riskhantering - Principer och riktlinjer” [11], medan sårbarhetsbedömning innebär en fördjupad analys avseende den egna organisationens krishanteringsförmåga och möjliga konsekvenser.

Utgångspunkter syftar till att fastställa ramarna för det fortsatta arbetet, identifiera ansvarsområde och hur de efterföljande stegen i riskhanterings-processen ska genomföras. Detta steg kallas i SS-ISO 31000:2009 för ”Etablering av kontexten”.

Riskidentifiering syftar till att fastställa en uppsättning scenarier som innebär hot mot verksamheten, medan man vid *riskanalys* förfinar beskrivningen av riskscenarierna och försöker kvantifiera såväl sannolikheten för att ett visst scenario ska inträffa som vilka konsekvenser detta kan få.

I *riskutvärderingen* bedöms om en risk är acceptabel eller ej. Detta tillsammans med en bedömning av möjliga riskreducerande åtgärder utmynnar i en prioritering mellan olika risker och utgör underlag för beslut om åtgärder.

Förmågebedömning innebär en bedömning av den egna krishanterings-förmågan om ett visst scenario skulle inträffa, medan *sårbarhetsanalys*, som utgår från det skyddsvärda i verksamheten, innehåller en förfinad analys av riskscenariernas konsekvenser och syftar till att analysera hur allvarligt och omfattande ett specifikt scenario påverkar samhället eller organisationen.

3.1 RSA – modeller allmänt

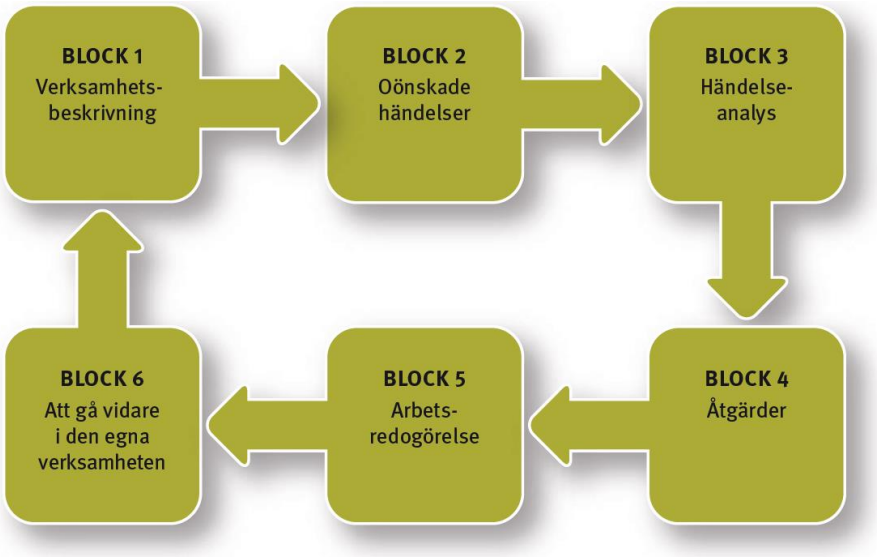
Att genomföra en RSA är många gånger ett omfattande arbete. Flera olika befattningshavare behöver vara inblandade och bidra med sin kompetens på sitt respektive område och för att få ett systematiskt arbetsflöde bör någon etablerad RSA-metod användas. En välkänd och ofta använd metod torde sannolikt vara mer mogen för användning än en ny oprövad.

Det finns ett flertal metoder och modeller för RSA och de flesta har en likartad struktur. Problemet med modellerna är att de är generella och därför inte heltäckande. För en RSA om EM-hot behöver modellerna kompletteras med en rad verktyg för att t.ex. kunna beräkna den elektromagnetiska vågutbredningen och den därmed förväntade intensiteten och yttäckningen av störsignalen. Vid omfattande analyser kan det även behövas stödverktyg för att värdera, vikta och prioritera delfunktioner eller delresultat samt att hantera beroenden mellan olika funktioner. Det kan vara en god idé att involvera utomstående som har gedigen kunskap om området som ska analyseras och som har erfarenhet av att genomföra RSA. För en RSA innefattande EM-hot behövs t.ex. kunskap om EMI.

2012 genomförde FOI en kartläggning av nationella och internationella RSA-modeller [14]. Bland annat studerades de svenska etablerade modellerna ROSA (ver 2003), MVA (ver 2002), IBERO (ver 2006) och FORSA (ver 2011). Samtliga modeller är utvecklade för att klara extraordinära händelser och alla ska klara de formella krav som ställs på en RSA, men då rapporten skrevs var det bara FORSA som följde MSBs vägledning och föreskrifter inom RSA. I rapporten studeras även den danska ROS-modellen samt finska BAS5. Rapportens jämförelse mellan modellerna ROSA, MVA, IBERO och FORSA gav att samtliga är generella och kan anpassas efter verksamhetens behov. Alla utom ROSA har ett systemperspektiv, FORSA och MVA utgår från det som är särskilt viktigt i verksamheten. Alla modeller förutom MVA bygger sin analys på olika oönskade händelser, eller olika scenarier. FORSA är den enda av de studerade modellerna som förespråkar osäkerhetsbedömningar till sannolikhets- och konsekvensbedömningarna. Den danska ROS-modellen tar sin utgångspunkt i checklistor och baseras huvudsakligen på strukturerad brainstorming och kvalitativa expertbedömningar. Användarna kan genomföra analyser utan att ha detaljerad teknisk eller statistisk information. Den finska modellen BAS5 påminner om ”klassiska” RSAer, men fokus läggs på att bedöma osäkerheten istället för sannolikheten för en viss händelse. Osäkerheten blir särskilt intressant vid avsiktliga handlingar, eftersom den då blir så pass stor att det är svårt att bedöma sannolikheten för händelsen.

3.2 Processteg i RSA

Ett sätt att bedriva arbetet med risk- och sårbarhetsanalyser beskrivs i FORSA-modellen, se Figur 5 [12].



Figur 5. FORSA-modellen för arbete med risk- och sårbarhetsanalyser [12].

Block 1, *verksamhetsbeskrivning*, syftar bl.a. till att identifiera roller och ansvarsområden, beskriva vilka verksamheter som organisationen bedriver och vilka prioriterade åtaganden som finns. Speciellt intressant är kritiska beroenden (t.ex. av elektronisk utrustning) som behövs för att bedriva samhällsviktig verksamhet och vilka resurser som kan disponeras för att motstå störningar.

Block 2, *oönskade händelser*, innehåller processtegen riskidentifiering och riskanalys. Här gäller det att uppskatta sannolikheter och identifiera konsekvenser av olika oönskade händelser som kan påverka verksamheten. I fallet EM-hot baseras dessa på de scenariobeskrivningar som tagits fram och modifierats för att passa just den specifika verksamhet som studeras.

Block 3, *händelseanalys*, innefattar processtegen riskutvärdering, förmågebedömning och sårbarhetsanalys samt syftar till att utreda krishanteringsförmågan vid en inträffad händelse (här en EM-attack) samt förmågan att upprätthålla prioriterade åtaganden.

Block 4, *åtgärder*, baseras på genomförda risk- och sårbarhetsbedömningar och handlar om att beskriva säkerhetsförbättrande åtgärder, vilka kan utgöra underlag för beslut om att genomföra sådana åtgärder.

Block 5, *arbetsredogörelse*, innebär att beskriva hur man genomfört RSA, vilka källor och metoder som använts, samt vilka personer som medverkat, för att ge mottagaren en möjlighet att bedöma tillförlitlighet.

Block 6, *att gå vidare i den egna verksamheten*, innebär att sprida resultaten av RSAn inom organisationen, att fatta beslut om och genomföra risk- och sårbarhetsreducerande åtgärder, samt senare analysera effekterna av dessa.

De olika processtegen i FORSA-modellen beskrivs utförligare i FOI-rapporten [12], där man bl.a. finner förslag på medverkande och metoder, ett antal vägledande frågeställningar, samt förslag på sätt att systematisera och presentera resultaten av en RSA.

3.3 Information i de olika processtegen

En förutsättning för att kunna genomföra en RSA avseende EM-hot mot samhällsviktig infrastruktur är att studien har tillgång till information om de elektriska/elektroniska system som förekommer inom den studerade verksamheten. Förmodligen utgörs dessa i flertalet fall av kommersiell utrustning (COTS), som normalt endast är tillräckligt skyddad för att uppfylla EMC-kraven enligt de standarder som gäller för elektronikbranschen och utrustning för civilt bruk avseende oavsiktliga EM-störningar. COTS-utrustning är oftast helt oskyddad för påverkan av de kraftigare EM-fält som förekommer vid avsiktlig störning eller förstöring (IEMI). Detta under förutsättning att utrustningen inte kompletterats med tilläggsskydd i form av avskärmande skal eller transientskydd på alla ledningar som löper till/från utrustningen. Civil utrustning är att betrakta som i princip oskyddad mot avsiktlig elektromagnetisk påverkan, till skillnad från militär elektronik, som ofta är speciellt utformad eller har flera tilläggsskydd för att kunna klara avsiktliga EM-störningar och -attacker.

Några av de viktigaste medverkande att få med i en RSA avseende EM-hot mot samhällsviktig infrastruktur är operatörer eller personal som har kunskap om de specifika elektronikberoende system som används inom samhällskritiska verksamheter och personer med överblick över hur dessa system används inom verksamheterna. För att kunna beskriva EM-hoten behövs medverkan av personer som arbetat med denna typ av hot i försvars- eller säkerhetssammanhang. Det är även tänkbart att det i vissa fall kan behöva genomföras laboratorieundersökningar av utvalda kritiska system för att kunna bedöma deras sårbarhet för IEMI, vilket innebär ett behov av utrustning och kompetens för sådana susceptibilitetsstudier.

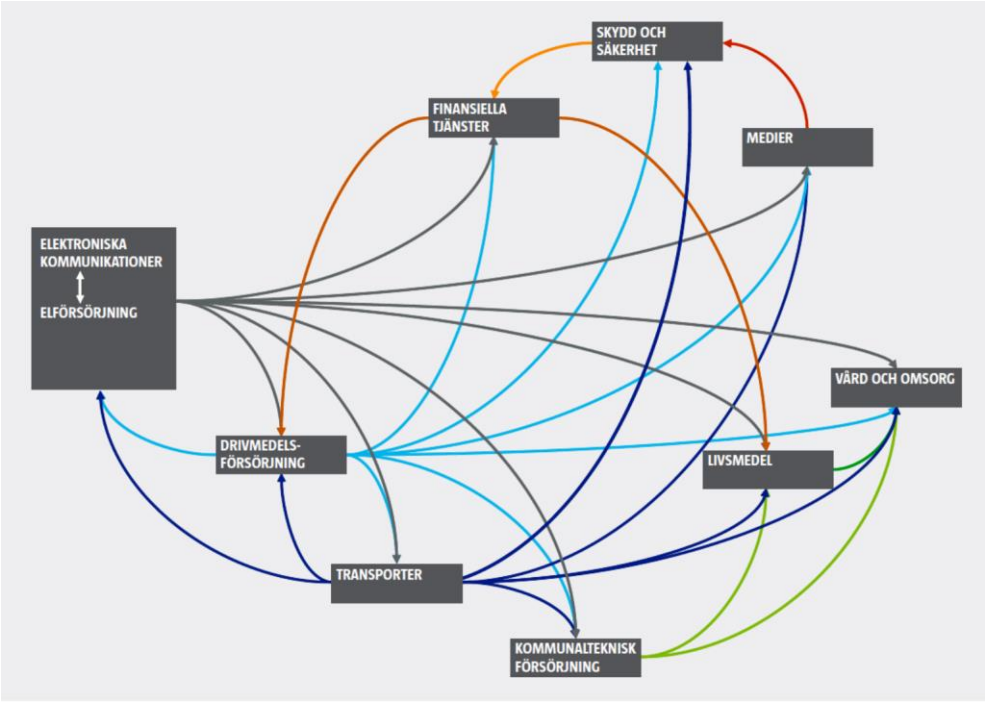
4. Gemensam hotbild

För att kunna identifiera potentiella extraordinära händelser används vanligtvis olika scenarier. Om samverkansområdena använder samma grundscenario som stomme ges förutsättningar att kunna jämföra resultaten. Det bör dock påpekas att grundscenarierna måste kompletteras med för varje organisation specifika detaljer för att de kritiska funktionerna lättare ska kunna upptäckas.

Detta kapitel fokuserar på de avsiktliga EM-hot (IEMI) mot samhällskritiska system som kan uppträda i fredstid, i ett skymningsläge eller som en del av en militär konflikt. De konkreta exempel som ges är just exempel för att illustrera några av de scenarier som kan uppkomma, men variationsrikedomen är tyvärr stor när det gäller denna typ av hot.

4.1 Behovsanalys

Vad som är relevanta EM-hotscenarier är starkt kopplat till den verksamhet som är kritisk i de olika samverkansområdena. Dock har elförsörjning och elektroniska kommunikationer i tidigare studier identifierats som nyckelfaktorer för att kunna bedriva många olika verksamheter inom ett flertal samhällssektorer, exempelvis i MSB-skriften ”Faller en - faller då alla?” [22], se Figur 6.



Figur 6. Översikt av sektorsvisa beroenden[22].

I [21] ges exempel på viktiga samhällsfunktioner för olika samhällssektorer, se Tabell 5. I tabellen har de samhällsfunktioner som direkt kan drabbas av EM-hot markerats med understrykning. Som kan ses i tabellen har i stort sett alla samhällssektorer viktig verksamhet som kan påverkas av EM-störningar.

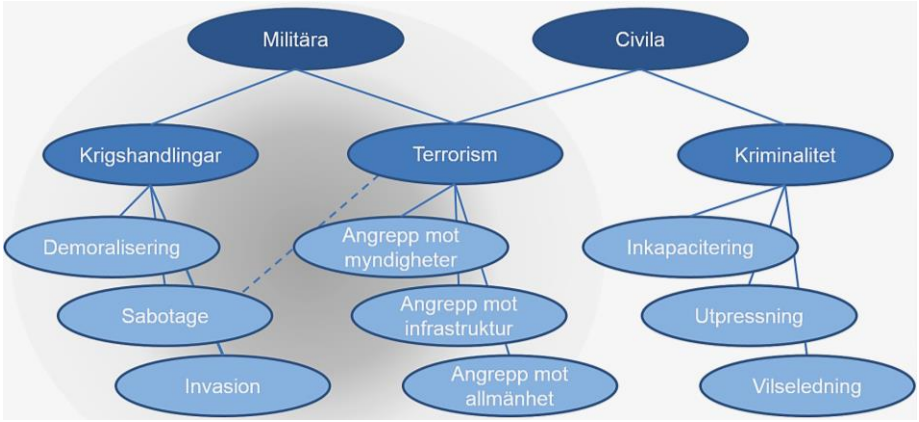
Tabell 5. Exempel på samhällsviktiga funktioner för olika samhällssektorer

Samhällssektor	**Exempel på viktiga samhällsfunktioner per samhällssektor**
Energiförsörjning	Produktion av el, distribution av el, produktion och distribution av fjärrvärme, produktion och distribution av bränslen och drivmedel m.m.
Finansiella tjänster	Betalningar, tillgång till kontanter, centrala betalningssystemet, värdepappershandel m.m.
Handel och industri	Bygg och entreprenadverksamheter, detaljhandel, tillverkningsindustri m.m.
Hälso- och sjukvård samt omsorg	Akutsjukvård, läkemedels- och materielförsörjning, omsorg om barn, funktionshindrade och äldre, primärvård, psykiatri, socialtjänst, smittskydd för djur och människor m.m.
Information och kommunikation	Telefoni (mobil och fast), internet, radiokommunikationer, distribution av post, produktion och distribution av dagstidningar, webbaserad information, sociala medier m.m.
Kommunalteknisk försörjning	Dricksvattenförsörjning, avloppshantering, renhållning, väghållning m.m.
Livsmedel	Distribution av livsmedel, primärproduktion av livsmedel, kontroll av livsmedel, tillverkning av livsmedel m.m.
Offentlig förvaltning, ledningsfunktioner och stödfunktioner	Lokal ledning, regional ledning, nationell ledning, diplomatisk och konsulär verksamhet m.m.
Skydd och säkerhet	Domstolsväsendet, åklagarverksamhet, militärt försvar, kriminalvård, kustbevakning, polis, räddningstjänst, alarmeringstjänst, tullkontroll, gränsskydd och immigrationskontroll, bevaknings- och säkerhetsverksamhet m.m.
Socialförsäkringar	Allmänna pensionssystemet, sjuk- och arbetslöshetsförsäkringen m.m.
Transporter	Flygtransport, järnvägstransport, sjötransport, vägtransport, kollektivtrafik m.m.

4.2 Hotscenarier

Man bör på något sätt strukturera mängden av möjliga scenarier innehållande avsiktliga EM-hot för att täcka in flera olika typer avseende aktörer, mål samt situationer (kontext). En möjlig klassificering, som dock inte är heltäckande, ges i Figur 7.

IEMI-hotsituationer kan delas in i Militära respektive Civila. Militära IEMI-hotsituationer (riktade mot militär förmåga) kan vara rena krigshandlingar eller av terrorkaraktär. Civila IEMI-hot (riktade mot civil förmåga) kan utgöras av terrorism eller av kriminella handlingar.



Figur 7. Klassificering av IEMI-hotsituationer.

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. Sabotage anses här utföras av kvalificerad militärt utbildad personal som opererar i landet, medan terrorhandlingar kan utföras av otränade sympatisörer. 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 angreppet.

IEMI-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 IEMI 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 (en explosion lockar till sig blåljusmyndigheternas insatspersonal, en elektronisk attack slår ut kommunikationssystemen i området så att insatspersonalen inte kan få vetskap om den egentliga kriminella handlingen, t.ex. ett 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) för att sedan flyttas till nästa plats för insats. 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.

För varje undernivå i Figur 7 kan man tänka sig ett scenario med störsändare eller med någon typ av HPM-generator.

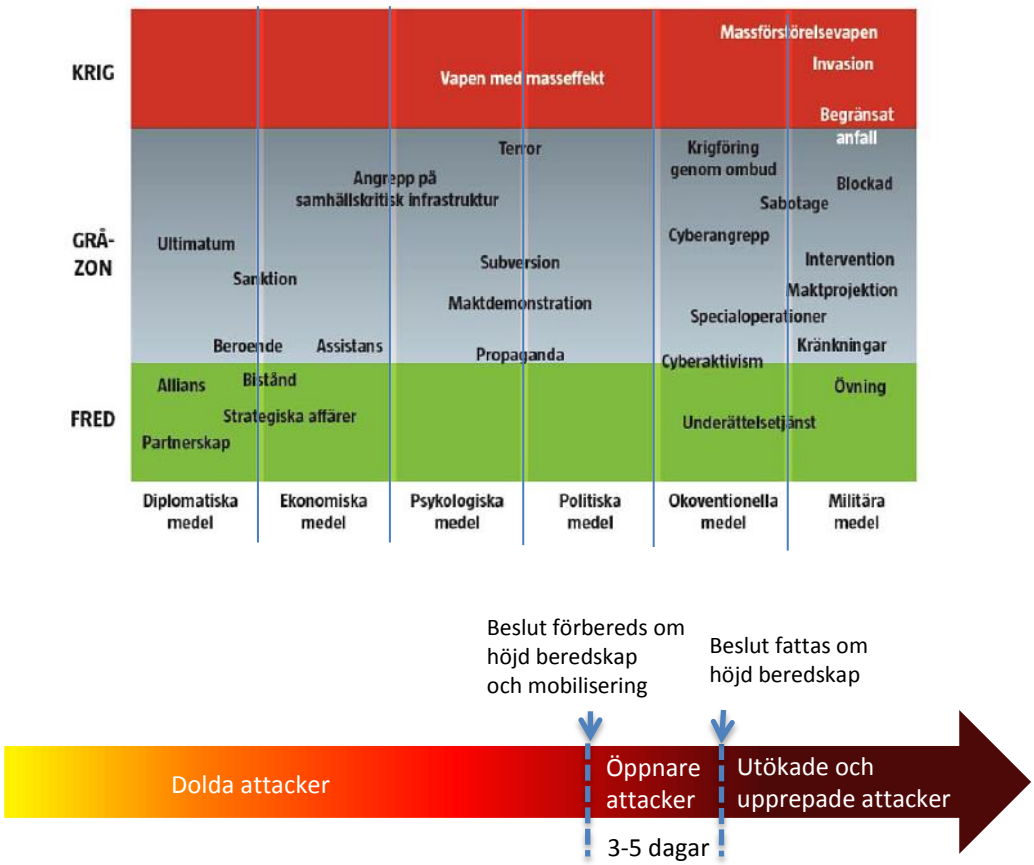
Ett annat sätt att klassificera EM-hot är om hotet uppträder som enda verkansform eller om det används tillsammans med andra verkansformer, t.ex. om antagonisterna slår ut elektronisk kommunikation för att uppnå en kraftigare samhällsstörning med en skjutvapenattack. Man kan även dela in EM-hot efter vilka frekvensband som berörs, om EM-hotet är pulsat eller kontinuerligt, hotkällans transporterbarhet eller efter andra fysikaliska parametrar.

4.3 Gråzonen mellan krig och fred

Eftersom ”försvarsmaktens möjligheter att verka i händelse av kris eller höjd beredskap är beroende av stöd från civila aktörer” (SOU2016:57 [77], s.52) kan en störning av civilsamhällets förmågor leda till konsekvenser för militära möjligheter att hävda Sveriges suveränitet. Regeringen skriver i en inriktningsproposition att ”Inom ramen för det civila försvaret bör berörda aktörer planera för att under höjd beredskap, inledningsvis under en kortare tid, kunna stödja Försvarsmakten” (Prop. 2014/15:109 [8], s.107).

En särskilt känslig fas är gråzonen mellan fredstida påfrestningar och en fullt utvecklad militär konflikt (det diffusa grå fältet i Figur 7). Denna situation benämns ofta skymningsläge och kan åtföljas av ett beslut att införa höjd beredskap. Exempelvis skulle det kunna inträffa ett antal till synes orelaterade terrorhandlingar som belastar de civila myndigheterna på skilda platser i Sverige samtidigt som det civila samhällets kommunikationssystem störs ut. När en främmande makt bedömer att det civila samhällets förmåga är tillräckligt försvagad skulle en militär intervention kunna inledas.

Figur 8, [25] visar exempel på olika aktiviteter som kan tänkas förekomma i den gråzon som ett skymningsläge utgör. EM-hot kan ingå i angrepp på samhällskritisk infrastruktur, subversion, terror, sabotage, specialoperationer eller tillsammans med ett cyberangrepp. Några typfall som ligger mellan skymningsläge och fullt krig med förutsättningar för civilförsvaret att stödja det militära försvaret redovisas i FOI-memot ”Hotbildsunderlag i utvecklingen av civilt försvar” [9]. Bilden visar också 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 [9].



Figur 8. Illustration av den s.k. gråzonen [25] samt möjliga tidsaspekter till det att beslut fattas om höjd beredskap [9].

Det kan vara värt att påpeka att ett incitament för en yttre angripare att använda elektromagnetiska verkansformer för att inkapacitera samhällsfunktioner är att det ofta kan vara lättare att återställa funktionaliteten i samhällssystemen efter en elektromagnetisk attack än efter användning av konventionella vapen och sprängmedel.

4.4 Exempelscenarier

I detta avsnitt presenteras några exempel på scenarier som ett sätt att karakterisera EM-hot. Ett fullständigt scenario utgörs av fyra delar:

- Scenariobeskrivning
- Tekniska specifikationer
- Strålningsegenskaper
- Konsekvensbeskrivning

Här återges endast tre scenario- och konsekvensbeskrivningar i syfte att illustrera spännvidden bland tänkbara EM-hot. Dessutom är de tekniska specifikationerna och strålningsegenskaperna utelämnade i denna rapport eftersom denna information 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 samhällskritisk 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 exempelscenarier 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.

4.4.1 Exempelscenario 1

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 samhällskritisk 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.

4.4.2 Exempelscenario 2

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 mobiltelefonband, RAKEL-bandet och GPS-navigationsband.

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.

4.4.3 Exempelscenario 3

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 exempel 1 och den kommersiella störsändaren i exempel 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.

5. Former för att genomföra en RSA

I en slutlig RSA måste organisationen (myndighet, landsting, länsstyrelse, kommun, ...) sammanväga RSAn avseende EM-hot med RSA för andra typer av hot (naturkatastrofer, oavsiktliga utsläpp av giftiga ämnen, terroristattacker med sprängmedel, m.m.) för att prioritera de åtgärder som har störst riskreducerande effekt sett till mängden av alla möjliga hotscenarier.

Något som kan tala för att det kan behövas en särskild RSA för EM-hot är att kunskapen om de avsiktliga EM-hoten (IEMI) är avsevärt mindre i det civila samhället jämfört med inom militär verksamhet. Här kan FOI bidra med underlag, exempel och stöd för att medvetandegöra ansvariga och operatörer inom samhällskritisk verksamhet om EM-hotens natur och möjliga konsekvenser.

EM-hot mot civila samhällssystem utgör främst hot mot elförsörjning, kommunikations- och informationssystem, som flertalet civila verksamheter idag är helt beroende av. Till exempel är så gott som alla andra energisystem, transporter, livsmedelsförsörjning, finansiella tjänster, medier, vård och omsorg, m.fl. beroende av tillgång till elektrisk energi från distributionsnätet [13], även om flera verksamheter har tillgång till reservkraft för en begränsad tid. Ett längre eller mera omfattande avbrott i elförsörjningen utgör ett hot mot alla samhällsviktiga funktioner. Detta talar för att en analys av EM-hot mot samhällsviktiga system bör göras i ett större perspektiv.

För att genomföra en RSA krävs kunskap om den aktuella verksamheten och om EM-hot. Projektet föreslår därför att en RSA mot EM-hot genomförs i dialogform, där flera olika kompetenser samverkar. Som underlag inför RSA:n behöver verksamheten beskrivas och systeminformation samlas. För att konkretisera hoten i syfte att underlätta sårbarhetsanalysen kan också hotscenarierna behöva anpassas speciellt för den aktuella verksamheten.

Hotscenarierna kan med fördel knytas mot något av de fyra typfall som FOI tidigare tagit fram och som är planerade att användas av några av samverkansområdena i deras kommande sårbarhetsanalyser [9]. Följande typfall redovisades:

- **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.

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

Då det i första hand är tekniska system och trådlös kommunikation som allvarligt kan påverkas av EM-hot är det främst systemkunskap, beroenden mellan system och hur verksamheten beror av elektroniska stödsystem som behövs då konsekvenserna ska bestämmas. Det är förslagsvis experter som exempelvis en teknisk systemansvarig och en verksamhetsansvarig, som behövs från verksamhetens sida. I vissa fall bör en säkerhetsansvarig också kunna bidra med underlag till riskanalysen.

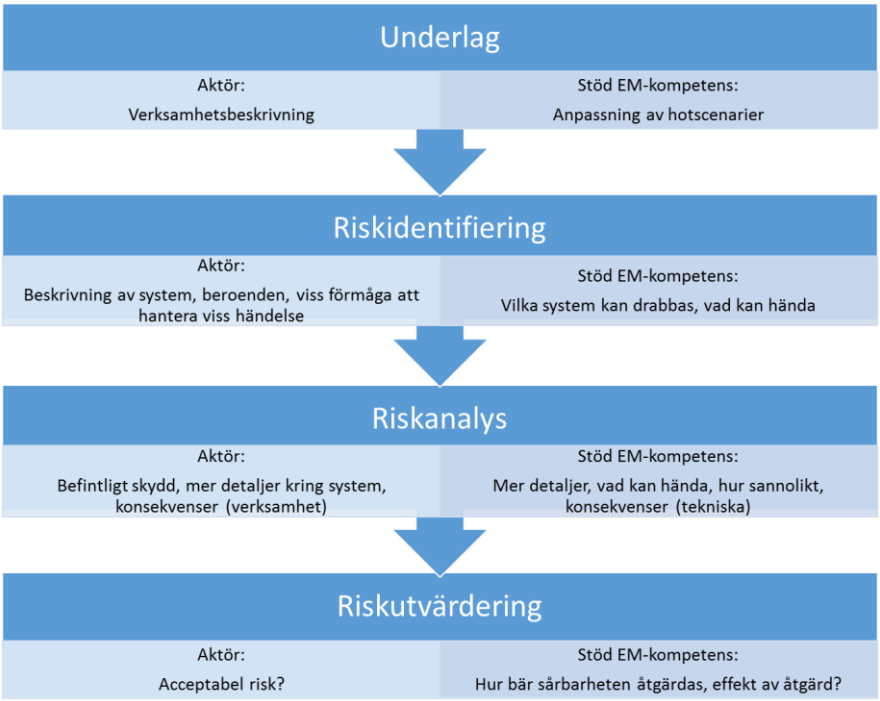
Det behövs också stöd kring hur EM-hot kan påverka system och verksamhet och hur åtgärder och skydd minskar riskerna. I Figur 9 presenteras exempel på frågeställningar som behöver besvaras.
Exempel på frågeställningar som behöver diskuteras genom dialog är:

- Vid riskidentifiering - Beskrivning av system som kopplar till samhällsviktig verksamhet. Beroenden eller viss förmåga att hantera viss händelse. Vilka system kan drabbas? Vad kan hända när de drabbas?

- Vid riskanalysen – Mer detaljerat, vad kan hända? Hur sannolikt är det? Vad blir konsekvenserna? Behöver också ta hänsyn till befintligt skydd och hur påverkar skyddet, redundansen eller hanteringen konsekvenserna?

- Riskutvärdering och ev riskhantering (i ett senare skede) – Hur bör sårbarheten eller risken åtgärdas, vad får det för effekt, med åtgärden, är då risken acceptabel?

Figuren visar också att olika typer av kompentenser behövs för att genomföra de olika stegen i en RSA.



Figur 9. Förslag på hur deltagare med olika kompetenser bör delta i RSAns olika processteg

Det är troligt att de anpassade hotscenarierna, system eller verksamheter som identifierats som kritiska, samt den slutgiltiga bedömningen kan utgöra känslig information. I en sådan situation kan ett sekretessavtal upprättas med den inblandade aktören avseende de delar som bedömts som känsliga.

5.1 Struktur för att organisera informationen

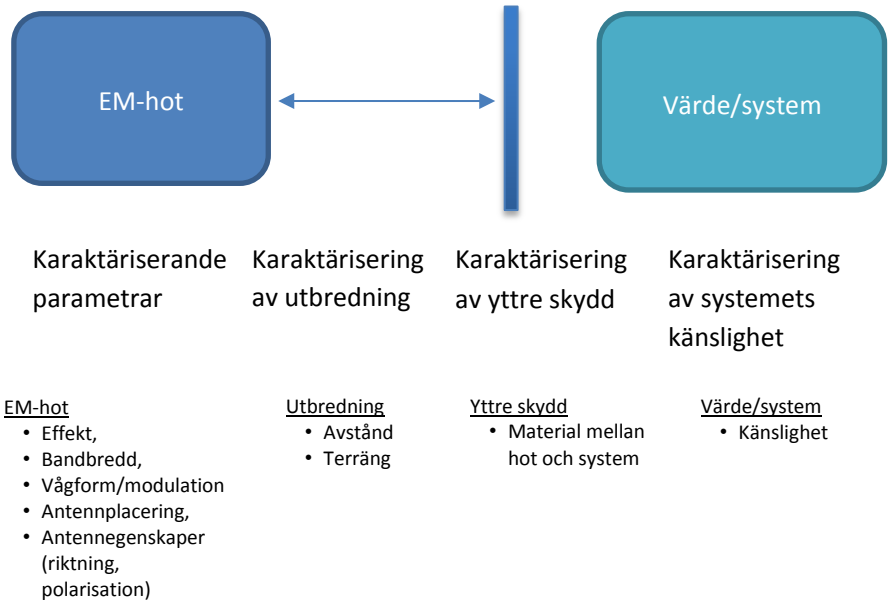
Det finns många olika scenarier som innefattar EM-hot mot samhällsviktig infrastruktur. Dels kan man variera vilken utrustning (hårdvara) som används, vilket syfte som angriparna har med attacken, vilka mål som utsätts för attacken, hur attacken går till, avstånd, varaktighet, m.m. Detta ger en stor uppsättning tänkbara scenarier, bland vilka man bör välja ut ett representativt antal som tillsammans spänner upp parameterrymden. Dessa kan organiseras i en katalog (lista) som tillsammans med en motsvarande lista över värden (elektrisk/elektroniska system inom samhällskritiska verksamheter) bildar en matris med alla kombinationer.

Ett EM-hot kan karakteriseras genom att beskriva EM-strålningens egenskaper på ett visst avstånd från det skyddsvärda objektet. Parametrar som frekvens, bandbredd, toppeffekt, polarisation, pulsform (för pulsade IEMI-källor) eller modulation (för kontinuerliga IEMI-källor) kan användas för att bestämma hur strålningen kopplar till elektronisk utrustning i olika målsystem.

Den tekniska påverkan som uppkommer bestäms i stor utsträckning av amplituden hos strålningen när den träffar målet. Eftersom elektromagnetisk

fältstyrka avtar i omvänd proportion till avståndet från källan[3] 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 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 de samhällskritiska system 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. I Figur 10 visas en enkel modell av de delar som är av betydelse för ett systems påverkan. Om värdet/systemet är ett trådlöst kommunikationssystem (en mottagare) finns vanligtvis inget yttre skydd. De beskrivande parametrarna är dock ungefärligen samma oavsett om EM-hotet utgörs av avsiktliga störning eller om det utgörs av HPM.



Figur 10. Modell av EM-hot och de delar som påverkar ett system.

[3] 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.

Svårare EM-hot utgörs av större och mera komplexa hotsystem som verkar på upp till kilometeravstånd och som kräver större resurser att tillverka, vilket endast stater eller större terroristorganisationer kan förfoga över. Dessa EM-hot innebär kraftigare verkan, långvarig funktion och repetitiv verkan mot flera olika mål. Eftersom dessa hotsystem är större är de också svårare att förflytta och kräver mera personal. Däremot kan enkla EM-hot tillverkas eller köpas i större mängd av enstaka personer som lätt transporterar dessa själva. Dock har dessa senare hotsystem kortare verkansavstånd, som ofta är av storleksordningen tiotals till hundratals meter.

För att få en hanterbar RSA bör man därför vid sidan av en utvald uppsättning typhot klassificera skyddsvärd elektronisk utrustning hos den studerade myndigheten i några förutbestämda klasser, t.ex. oskyddad kommunicerande elektronik, kommunicerande elektronik med transientskydd, kommunicerande elektronik med transientskydd och skalskydd, oskyddad icke-kommunicerande elektronik, icke-kommunicerande elektronik med transientskydd, samt icke-kommunicerande elektronik med transientskydd och skalskydd. Detta förenklar analysen om man dessutom i förväg bestämt graden av påverkan (tillfällig störning, störning som kräver operatörsingripande för återställning, permanent fysisk skada, etc.) vid några olika typavstånd så att man vid RSA:n direkt kan ange hur den elektroniska utrustningen påverkas för att sedan kunna bedöma sekundära effekter av dessa på den aktuella verksamheten.

6. Slutsatser

6.1 Diskussion

Vid mötena med samverkansområdena framkom att det är viktigt att sprida information om EM-hot, exempelvis genom en utbildningsinsats. Informationen kan behöva spridas till aktörerna inom samverkansområdena, kommuner och landsting, men också till branschorganisationer, där privata aktörer kan ingå. Flera av aktörerna uttalade ett stort behov av stöd för att kunna bedöma konsekvenserna av EM-hot och information om lämpligheten och robustheten hos olika kommunikationssystem som används för en viss tjänst. Flera aktörer efterfrågade också att hotscenarierna anpassades speciellt mot deras verksamhet.

Som framgår av sammanställningen av EM-hot finns en stor mängd av möjliga EM-källor som kan utgöra hot mot samhällsviktig verksamhet. Användningen av dessa kan bero på antagonisternas syften och på omvärldssituationen. Hur de kritiska systemen är utformade och skyddade har stor betydelse för om hotet ska anses som en stor risk i verksamheten. Hur stor risk en aktör kan tåla varierar också mellan olika aktörer och hur mycket pengar en aktör är beredd att lägga på skydd och åtgärder för att skydda systemen. Eftersom det finns så stora skillnader i förutsättningarna hos de representerade verksamheterna i samverkansområdena, kommer hot, hotscenarier, ingående kritiska system och beroenden samt konsekvenser av EM-hot att behöva analyseras, och i många fall anpassas, vid genomförandet av en RSA. Det innebär att flera av stegen i en RSA kommer att kräva specialkompetens. Det är speciellt kunskap om den aktuella verksamhetens kritiska system och beroenden, och kunskap om EM-hot, som krävs, för att bedöma påverkan och konsekvenser.

6.2 Förslag på organisation av huvudstudie

I förstudien har en grund tagits fram för att kunna genomföra RSA för olika aktörers verksamhet. Det behövs dock specifikt underlag då en skarp RSA ska genomföras. Det är speciellt information om aktörens verksamhet och de system som är väsentliga för dennes verksamhet som utgör viktigt underlag. Dessutom behövs en analys av hur de aktuella EM-hoten påverkar de identifierade kritiska systemen. Projektet föreslår därför att en RSA mot EM-hot genomförs i dialogform med flera kompetenser närvarande.

Vårt förslag är att huvudstudien består av följande delar:

- en pilotstudie där en RSA genomförs med en aktör,
- metodutveckling av den metod som delvis tas fram i förstudien och som vidareutvecklas i huvudstudien, samt
- utbildning i form av seminarium.

Pilotstudien genomförs med en aktör som är villig att genomföra en RSA mot EM-hot i dialog med oss. Förslag på aktör är Luftfartsverket eller Trafikverket. Deras intresse måste dock bekräftas och de behöver kunna delta med ett par experter, förslagsvis en systemansvarig och en verksamhetsansvarig. Eventuellt kan en säkerhetsansvarig också bidra.
I pilotstudien ingår typiskt att ett av hotscenarierna som togs fram i förstudien förfinas och anpassas mot aktören. Det kan t ex vara anpassning mot Luftfartsverket och vara en situation på Arlanda. Vidare behöver viktig verksamhet och de system verksamheten baseras på identifieras. Alla beroenden till system som kan drabbas behöver identifieras, samt de skydd eller den resiliens som finns inbyggda behöver identifieras (riskidentifiering). Därefter görs en riskanalys där vi identifierar risker, sannolikheten för händelserna och konsekvenserna av dessa. Baserat på detta underlag genomförs en riskutvärdering, följt av en ny riskutvärdering baserat på några olika åtgärdsförslag. Stöd vid utformning av åtgärder har efterfrågats vid diskussionerna med de olika samverkansområdena.

I metodutvecklingen anpassas dialogmaterialet, och genom en utvärdering av vad som fungerar och inte fungerar vidareutvecklas processen för RSA:n.

Aktiviteten utbildning tar vi med som förslag då det har framförts både i CBG EM-hot och vid mötet med SOTP. Det skulle kunna genomföras i form av några seminarier. Om en skrift ska tas fram tror vi att det kräver en större insats.

Efter att pilotstudien har genomförts kan RSA:er för andra aktörer genomföras med avsevärt mindre insats eftersom vi räknar med att metoden då har anpassats och att vi har bättre kännedom om vilken typ av experter som kan bidra med information om aktörernas system. Målet är då att en RSA kan genomföras med en aktör under ett par dagar, men det kan ta 2-3 veckor totalt för den bidragande aktören. Huvuddelen av tiden går åt till att införskaffa den information som behövs för RSA:n. För FOI blir tidsåtgången något mer då FOI behöver räkna på bl. a. konsekvenser och effekten av olika åtgärder.

7. Referenser

1. ”Åska och blixtdetektering”, Avdelningen för elektricitetslära, Uppsala Universitet, http://www.hvi.uu.se/ (2016-10-12).
2. M. Bäckström, ”Förstudie: Skydd mot elektromagnetiska risker. Geomagnetiskt inducerade strömmar (GIC)”, Combitech IK4-11:0092A, 2011-09-15.
3. International Electrotechnical Commission (IEC), http://www.iec.ch/emc/ (2016-10-13).
4. EUROPAPARLAMENTETS OCH RÅDETS DIREKTIV 2014/30/EU av den 26 februari 2014 om harmonisering av medlemsstaternas lagstiftning om elektromagnetisk kompatibilitet, http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32014L0030&from=EN (2016-10-13).
5. Elsäkerhetsverkets föreskrifter om elektromagnetisk kompatibilitet, ELSÄK-FS 2016:3, konsoliderad version 2016-04-20.
6. “Elektromagnetisk miljö användarhandbok, EMMA, Utgåva 2”, FMV:Materiel 21 840:44134/02, Försvarets bok- och blankettförråd, 2002.
7. “Säkerhet i en ny tid”, SOU 2016:57, Stockholm 2016, ISBN 978-91-38-24489-0.
8. ”Försvarspolitisk inriktning – Sveriges försvar 2016–2020”, Regeringens proposition 2014/15:109, 23 april 2015.
9. F. Lindgren, ”Hotbildsunderlag i utvecklingen av civilt försvar”, FOI Memo 5089, 2014-10-14.
10. ”Vägledning för Risk- och sårbarhetsanalyser”, Myndigheten för samhällsskydd och beredskap (MSB), MSB245 - april 2011, ISBN 978-91-7383-129-1.
11. ”Riskhantering - Principer och riktlinjer”, SIS Förlag AB, Svensk standard SS-ISO 31000:2009, publicerad 2010-03-30.
12. M. Winehav (red.), B. Nevhage (red.), J. Lusua, J Clausen Mork och R. Erdeniz, ”FOI:s modell för risk- och sårbarhetsanalys (FORSA)”, Totalförsvarets forskningsinstitut (FOI), FOI-R--3288--SE, ISBN 978-91-7056-128-3, 2011.
13. P. Wikman-Svahn, H. Carlsen, ”Energiomställningen och dess betydelse för samhällsskydd och beredskap”, FOI Memo 4572, 2013-09-25.
14. M. Winehav, L. Molin, E. Veibäck, P. Larsson, “Metod- och inventeringsstöd till sektorsövergripande risk- och sårbarhetsanalys”, Totalförsvarets forskningsinstitut (FOI), FOI-R—3516--SE, 2012.

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

16. P. Stenumgaard, Radiostörningar – ett växande hot, FOI-R—3494--SE, oktober 2012.

17. F. Sabath, “What can be learned from Documented Intentional Electromagnetic Interference (IEMI) Attacks”, presented at the International URSI XXX General Assembly, Istanbul, Turkey, 13-20 August 2011.

18. United States Department of Homeland Security, “The Threat of radio frequency weapons to critical infrastructure facilities”, TSWG and DTEO Publication, August 2003.

19. V. Fortov, Yu. Parfenov, L. Siniy and L. Zdoukhov, “Russian Research of intentional electromagnetic disturbances over the past ten years”, Proceedings of the AMEREM 2006, Albuquerque (NM, USA), July 2006.

20. R. Hoad and I. Sutherland, “The forensic utility on detecting disruptive electromagnetic interference”, Proceedings of the 6th European Conference on Information Warfare and Security (ECIW 2007), July 2007.

21. Vägledning för samhällsviktig verksamhet – Att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid, MSB620 – januari 2014.

22. Faller en - faller då alla?, MSB 2009.

23. Henrik Olsson, Reklamskyltars EMC-egenskaper, Risk för radiostörningar med LED, Elsäkerhetsverket, Dnr 12EV3659 2012-11-16.

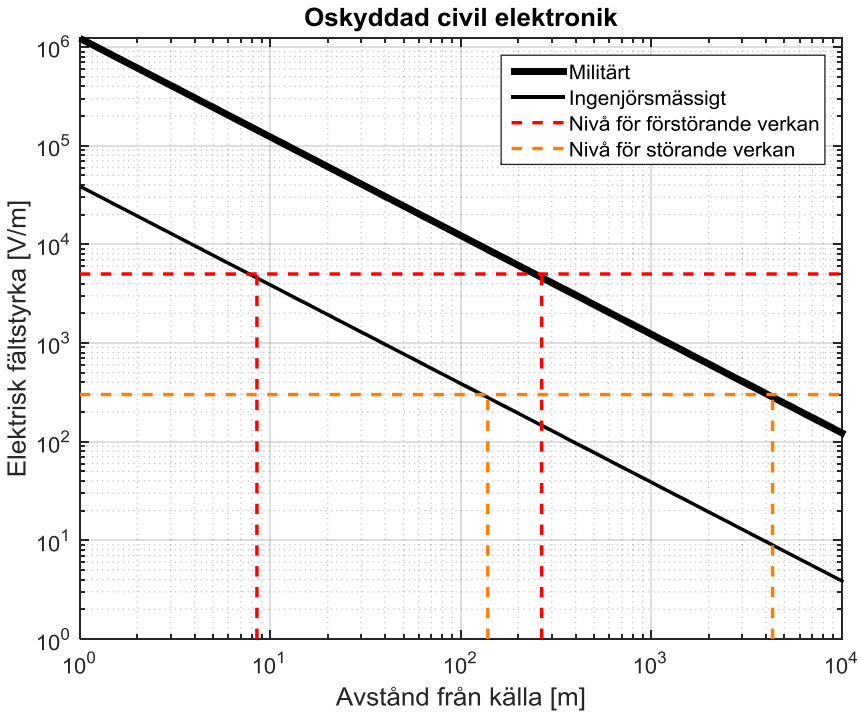
24. Henrik Olsson, ”Tillsynsbesök Eriksbergs shoppingcenter”, Elsäkerhetsverket, Dnr 14EV1335.

25. FM MSD16, Militärstrategisk doktrin för Sveriges militära försvar, 2016.

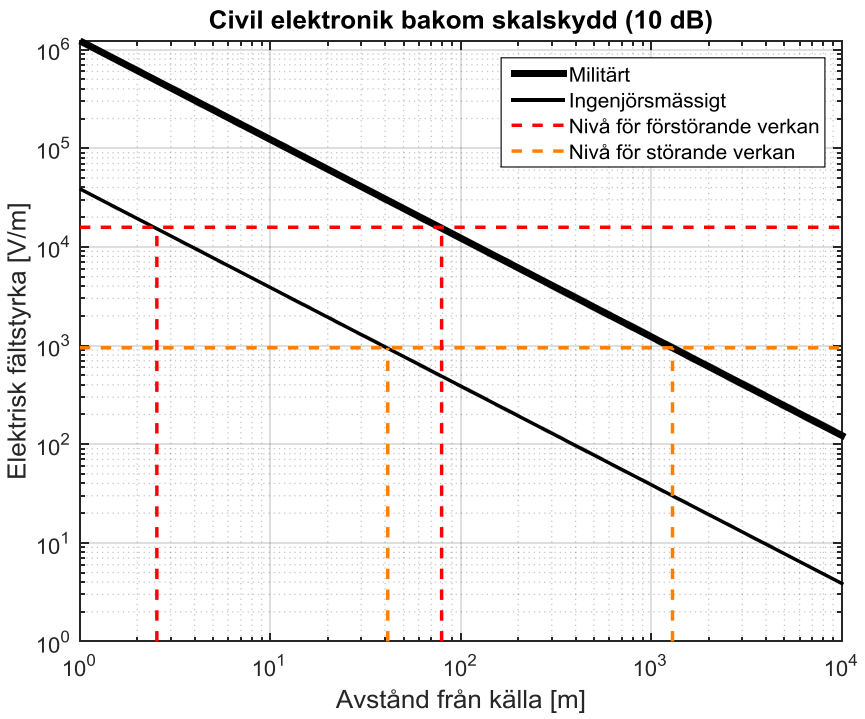
26. Tjuvarnas nya metod gör dyra larm värdelösa, Dagens Nyheter 22 augusti 2012.

8. Bilaga 1: Verkansavstånd HPM

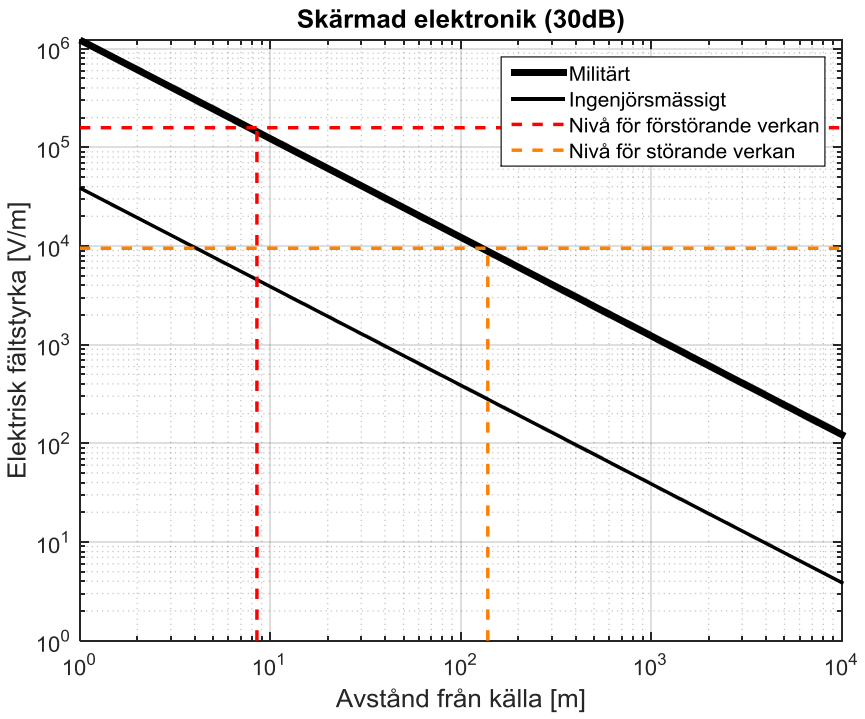
Som komplement till presentationen av verkansavstånd i avsnitt 2.4.2 för olika kategorier av HPM-källor visas i Figur 11-13 istället effekten av HPM-källor för ett varierbart avstånd.



Figur 11. Verkansavstånd för olika klasser av HPM-källor mot oskyddad civil elektronik.



Figur 12. Verkansavstånd för olika klasser av HPM-källor mot civil elektronik bakom skalskydd.



Figur 13. Verkansavstånd för olika klasser av HPM-källor mot skärmad elektronik.

9. Bilaga 2: Aktörer inom de olika samverkansområdena

Nedan listas de aktörer som medverkar i de olika samverkansområdena. De deltagande aktörerna är viktiga vid utformningen av relevanta hotscenarier och vid identifiering av samhällsviktig verksamhet.

- Ekonomisk säkerhet (SOES)
    - Arbetsförmedlingen
    - Finansinspektionen
    - Försäkringskassan
    - MSB
    - Pensionsmyndigheten
    - Riksgälden
    - Skatteverket
- Farliga ämnen (SOFÄ)
    - Folkhälsomyndigheten
    - Kustbevakningen
    - Livsmedelsverket
    - MSB
    - Polismyndigheten
    - Socialstyrelsen
    - Statens jordbruksverk
    - Statens veterinärmedicinska anstalt
    - Strålsäkerhetsmyndigheten
    - Säkerhetspolisen
    - Totalförsvarets forskningsinstitut (FOI)
    - Tullverket
- Geografiskt områdesansvar (SOGO)
    - Lantmäteriet
    - Länsstyrelserna (21 st)
    - MSB

- Skydd, undsättning och vård (SOSUV)
    - Kustbevakningen
    - Migrationsverket MSB
    - Polismyndigheten
    - Sjöfartsverket
    - SMHI
    - Socialstyrelsen
    - Transportstyrelsen
    - Tullverket
- Teknisk infrastruktur (SOTI)
    - Elsäkerhetsverket
    - Energimyndigheten
    - Fortifikationsverket
    - Försvarets radioanstalt
    - Livsmedelsverket
    - MSB
    - Post- och telestyrelsen
    - Svenska kraftnät
- Transporter (SOTP)
    - Energimyndigheten
    - LFV
    - MSB
    - Sjöfartsverket
    - Trafikverket
    - Transportstyrelsen

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1081 - mars 2017 ISBN 978-91-7383-733-0