

Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur



Faktaruta

Utbildningsmaterial för lärarledd handledning eller självstudier av avsiktliga elektromagnetiska hot mot det civila samhällets elektronikberoende system och infrastruktur.

2017

FOI

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

Många samhällsviktiga verksamheter 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 introduktion till EM-hot är avsedd att användas som bakgrundsmaterial för risk- och sårbarhetsanalyser som innefattar EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur, till exempel inför införande av eller vid höjd beredskap.

MSB:s kontaktperson:

Gustav Söderlind, 010-240 42 57

Publikationsnummer MSB1180 - februari 2018

ISBN 978-91-7383-805-4

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

Förord

Detta utbildningsmaterial syftar till att sprida kunskap om de avsiktliga elektromagnetiska hot som kan uppträda i dagens samhälle och orsaka störningar i olika samhällsviktiga verksamheter vid myndigheter, landsting, länsstyrelser, kommuner eller privata aktörer som tillhandahåller viktiga samhällstjänster. Avsiktliga elektromagnetiska hot kan uppträda när som helst, men kan bli särskilt signifikanta i kritiska lägen som exempelvis vid höjd beredskap.

Utbildningsmaterialet är avsett att användas för självstudier eller som grundläggande material vid en handledd utbildning om elektromagnetiska hot för beslutsfattare, verksamhets- och säkerhetsansvariga eller operatörer av samhällsviktiga verksamheter. Som komplement till det skrivna materialet finns ett presentationsmaterial och en folder om EM-hot.

För den som avser att genomföra risk- och sårbarhetsanalyser samt åtgärda eventuella upptäckta risker hänvisas till kompletterande material i form av ”Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, utgiven av MSB.

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

Framtagning av utbildningsmaterialet 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 Läsanvisningar	9
1.3 Introduktion till elektromagnetiska fält	10
1.4 Definitioner	13
2. Elektromagnetiska hot	14
2.1 Naturliga EM-hot	15
2.2 Oavsiktliga EM-hot	15
2.3 Avsiktliga EM-hot	18
2.4 Kopplingsvägar	19
3. Exempel på hotkällor	21
3.1 Störsändare	21
3.2 Mikrovågsvapen	23
4. Elektromagnetisk attack mot kritisk infrastruktur	26
4.1 Varför avsiktliga EM-hot?	26
4.2 EM-attack som del av ett större angrepp	26
4.3 Antagonister och syften	28
4.4 Tidsförlopp och varaktighet	29
4.5 Att bli medveten om ett EM-angrepp	30
5. Konsekvenser av EM-attack	32
5.1 Tekniska konsekvenser	32
5.1.1 Avsiktlig störning	32
5.1.2 Mikrovågsvapen	34
5.2 Verksamhetskonsekvenser	36
5.3 Sektorsvisa beroenden	39
6. Enkelt exempel på en RSA	40
7. Att skydda skyddsvärd samhällsviktig verksamhet och kritisk infrastruktur	42
7.1 Kommunikation	42
7.2 Elektroniska system	43
8. Slutord	44
Referenser	45
Bilaga: Avståndsberoenden	48
Störavstånd för avsiktlig störsändare	48

Verkansavstånd för HPM-vapen	49
------------------------------------	----

Sammanfattning

Elektronisk utrustning och trådlös kommunikation har blivit en alltmer integrerad del av vårt samhälles infrastruktur och det gör att den person, organisation eller stat som vill orsaka problem eller sprida förvirring och osäkerhet kan göra det genom att se till att utrustningen inte går att använda.

Hotkällor för avsiktlig elektromagnetisk verkan kan grovt indelas i störsändare som stör ut trådlös kommunikation eller satellitbaserade navigationssystem och mikrovågsvapen som sänder ut kortvariga, men mycket kraftiga, radio- eller mikrovågspulser och som kan störa eller till och med förstöra elektroniska system.

Första steget mot att kunna skydda samhällsviktig verksamhet och kritisk infrastruktur mot denna typ av nya avsiktliga hot är att bli medveten om deras existens och hur de skulle kunna användas av antagonister för att störa ut eller inkapacitera viktiga samhällssystem.

Gemensamt för alla avsiktliga EM-hot är att de bör ses som en del i ett större sammanhang. Kriminella kan störa ut ett villalarm för att förenkla själva stölden och en terrororganisation kan använda sig av störning för att försvåra ingripande från blåljusmyndigheterna. Under en militär operation eller i en gråzon innan öppen militär konflikt kan störsändare och mikrovågsvapen användas för att försvåra informationsspridning och försämra samhällets krisberedskap samt indirekt i befolkningen sprida osäkerhet och misstro mot myndigheternas förmåga.

1. Inledning

1.1 Bakgrund

I det moderna samhället används elektroniska apparater och system för att lagra och distribuera information, kommunicera via telefoni och internet, styra industriprocesser och serviceanläggningar som TV- och radioutsändningar, kraftverk, vattenverk, kommunikationscentraler, vägbelysning, trafiksignaler, trafikledning, inpasserings- och övervakningssystem, sjukvårdsutrustning, etc. Mindre radarsystem används för övervakning, för fartreglering i moderna bilar och inom en snar framtid i självkörande bilar. Utvecklingen av automatiserade elektronikberoende system har accelererat kraftigt de senaste decennierna. En tydlig trend är att elektroniken arbetar vid allt lägre spänningar och har blivit allt mer strömsnål. Trots detta har elektronikindustrin genom robustare konstruktioner förbättrat utrustningens motståndskraft mot naturliga och oavsiktliga elektromagnetiska störningar.

Parallellt med expansionen av elektroniskt kontrollerade system i samhället har det uppkommit möjligheter att avsiktligt störa dessa med elektriska och magnetiska fält. Militärt har telekrigområdet blivit ett av de centrala verktygen i konflikter runt om i världen. Detta inkluderar avlyssning av fiendens elektroniska kommunikation, generering av störande eller vilseledande signaler, samt olika skyddsåtgärder för att skydda egen utrustning. Störsändare har även kommit att användas civilt, t.ex. av polis för att ta ner drönare, men tyvärr också för kriminella syften, som att blockera villalarm vid inbrott.

Sedan andra världskriget har stormakterna kunnat generera kraftiga elektromagnetiska pulser som slår ut elektriska och elektroniska system över en hel kontinent genom att spränga en kärnvapenladdning i atmosfären. Denna teknologi befaras nu vara på väg att spridas till skurkstater och terroristorganisationer. Under 1960-talet startade forskning och utveckling av möjligheter att generera kraftiga elektromagnetiska pulser utan att använda kärnvapen. De senaste decennierna har sett en utveckling och test av utrustning som på några hundra meters avstånd fysiskt kan förstöra fiendens elektronik.

Idag säljs kommersiella störsändare via internet medan glada amatörer på samma informationskanal diskuterar och lägger ut information om hur man själv kan bygga utrustning som stör eller förstör elektronik på några tiotals meters avstånd. Kunskapen om dessa möjligheter sprids samtidigt som man kan konstatera att det inte krävs några exotiska, svårhanterliga material eller industriell kapacitet för att konstruera utrustning som kan åsamka system som innehåller och styrs av elektronik stora störningar.

Denna skrift bygger enbart på öppet material och är bland annat baserad på delar av FOI:s mångåriga forskningsverksamhet och omvärldsanalyser inom områden som robust telekommunikation, störsändare, telekrig och elektromagnetiska vapen.

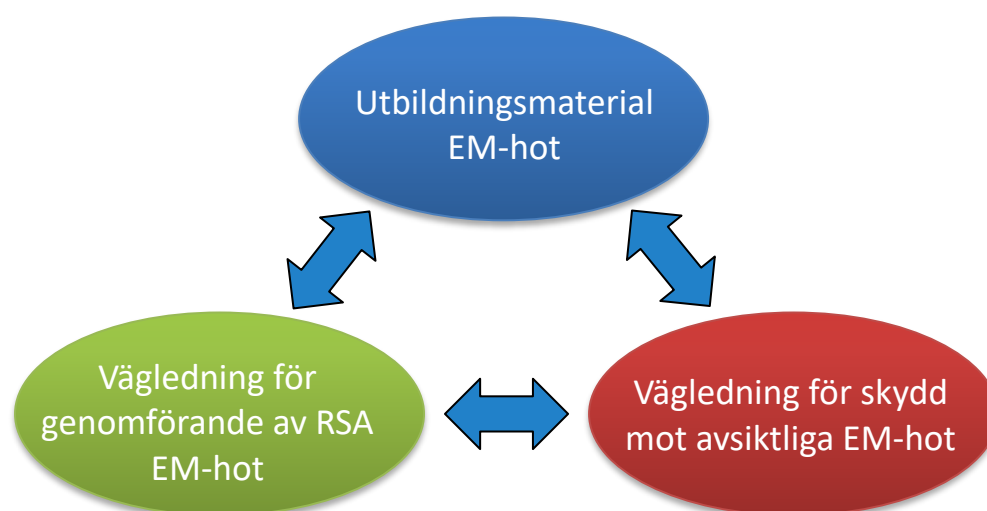
1.2 Läsanvisningar

Detta dokument syftar till att ge en kort introduktion till vad avsiktliga elektromagnetiska hot (EM-hot) är och hur de av antagonistiska grupper skulle kunna användas vid attacker mot offentliga aktörers anläggningar och system som innehåller kommunikationssystem, elektronisk utrustning, datorer, styr- och kontrollsystem, säkerhetssystem, m.m. Exempel kan vara datorhallar, vattenverk, trafiksignalsystem, kommunikationsradiosystem, sjukhus, m.fl.

Introduktionen är främst avsedd att användas av dem som planerar att genomföra risk- och sårbarhetsanalys (RSA) av kritisk infrastruktur. Syftet är att höja medvetenheten om att det finns avsiktliga elektromagnetiska hot som man behöver beakta i en risk- och sårbarhetsanalys som innefattar alla möjliga typer av hot, samt att i en RSA identifierade EM-hot kan behöva åtgärdas innan en allvarligare samhällsstörning inträffar. För den som så behöver finns i avsnitt 1.3 en kort introduktion till elektromagnetiska fält.

Detta dokument är ett resultat av ett MSB-finansierat uppdrag till FOI under hösten 2017 som avrapporteras i "Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur" [1]. Introduktionen kan utgöra kursmaterial vid en lärarledd utbildning inför en RSA-process, men kan även användas fristående för självstudier inom området avsiktliga EM-hot.

För att genomföra en RSA avseende EM-hot kan man använda "Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur" [2], som dels ger en allmän översikt av hur man kan genomföra en RSA och dels utgör ett praktiskt metodstöd med specifika frågeställningar vid varje steg i genomförandet. När det är dags att vidta riskreducerande skyddsåtgärder för identifierade EM-hot mot en verksamhet ger Fortifikationsverkets "Vägledning Skydd mot avsiktliga EM-hot" [3] råd och praktiska anvisningar för hur man kan gå tillväga, se Figur 1. Som fördjupad läsning om systematisk elmiljöverksamhet rekommenderas FMV:s "Elektromagnetisk miljö användarhandbok" (EMMA) [4].



Figur 1. Kompletterande material kring EM-hot:
Vägledning för genomförande av RSA EM-hot, Vägledning Skydd mot avsiktliga EM-hot (utgiven av Fortifikationsverket) samt detta Utbildningsmaterial EM-hot.

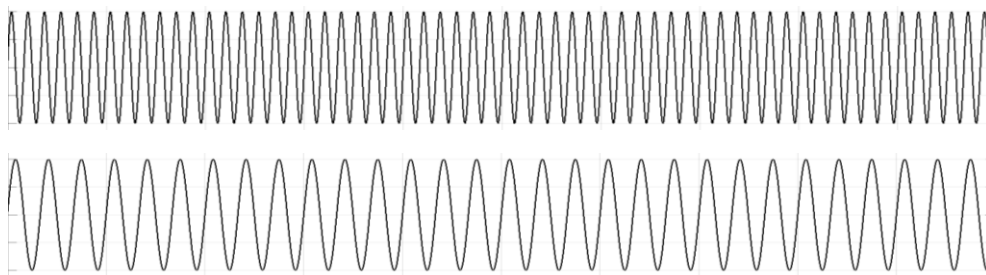
1.3 Introduktion till elektromagnetiska fält

Elektriska och magnetiska fält förekommer allmänt i vår vardag. Om man går omkring i syntetiska material kan man laddas upp med statisk elektricitet som urladdas i en elektrisk stöt t.ex. när man berör en vattenkran. Då har det mellan handen och kranen uppkommit ett elektriskt fält som sliter loss laddningar och flyttar dem för att utjämna fältet. Magneter kan användas i kompasser eftersom de känner av jordens magnetfält och vi använder ofta mobiltelefoner som både genererar elektromagnetiska fält och kan känna av elektromagnetiska fält från basstationer i närheten. I affärer används larmbågar för att kommunicera med s.k. RFID-taggar som fästs på varorna. Många passagesystem läser med elektromagnetiska fält av små elektroniska som är kretsar inbyggda i passerkort.

En uppladdad kropp omges av ett elektriskt fält, medan magneten omges av ett magnetfält. Att det finns ett fält betyder att andra föremål kan påverkas på avstånd av kroppen som alstrar fältet. Om ett elektriskt fält varierar i styrka bildas ett magnetfält och vice versa. Olika typer av elektromagnetisk strålning (som t.ex. radiovågor, mikrovågor, synligt ljus, och röntgenstrålning) utgörs av snabbt svängande kopplade elektriska och magnetiska fält.

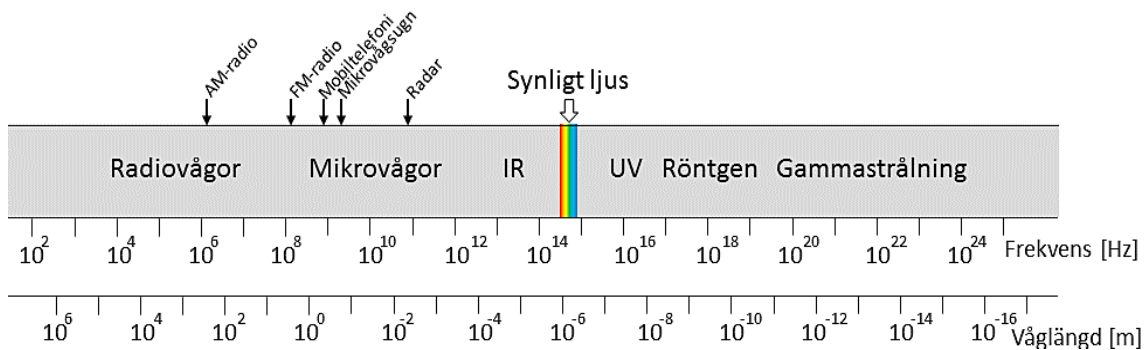
Hur många svängningar fälten gör per sekund, dvs. vilken frekvens fälten har, bestämmer typen av strålning, se Figur 2 och Figur 3. Till exempel brukar man kategorisera elektromagnetiska fält som svänger upp till en miljard gånger per sekund (1 GHz) som radiovågor medan de fält som svänger mellan 1 GHz och upp till 1 THz kallas för mikrovågor¹. Vid ännu högre frekvenser kallas det ljus, först infrarött ljus, sedan synligt ljus och till sist ultraviolett ljus när frekvensen succesivt ökar. Om inte annat sägs avses med elektromagnetisk våg i denna rapport en våg som svänger i frekvensintervallet för radio- eller mikrovågor.

Typiska frekvenser för FM-radio ligger i intervallet 88-108 MHz, för mobiltelefoner i intervallet 700-2600 MHz, medan mikrovågsugnar använder frekvensen 2,45 GHz för att hetta upp vattenmolekyler.



Figur 2. Två svängningar med olika frekvens. Den undre kurvan har halva frekvensen jämfört med den övre, men våglängden är dubbelt så stor i den undre kurvan som i den övre. Hastigheten för båda vågrörelserna är dock densamma.

¹ Grundenheten för frekvens är Hertz, förkortat Hz, som är en svängning per sekund. Prefixet G står för Giga, som betyder miljard, dvs. 1 000 000 000. Prefixet T står för Tera, som betyder biljon, dvs. 1 000 000 000 000.



Figur 3. Illustration av elektromagnetiska vågor av olika frekvens. Nästan all den elektroniska utrustning vi använder för kommunikation mellan människor, datorer och andra maskiner ligger i frekvensintervallet runt mobiltelefoni och mikrovågsugnar. T.ex. arbetar våra WiFi- och Bluetoothnätverk ofta vid samma frekvenser som mikrovågsugnar. IR = Infrarött, UV = Ultraviolett.

Elektromagnetiska fält påverkar de elektriska laddningarna i alla ledande eller halvledande objekt och kan sätta elektronerna i rörelse så att en elektrisk ström uppkommer i objekten. Om detta är avsikten kallar man objektet för en antenn, men effekten uppkommer i alla metalliska höljen, ledningar och komponenter. D.v.s. även objekt som inte är avsiktliga antenner kan mer eller mindre effektivt påverkas av elektromagnetiska fält i sin omgivning och ge upphov till inducerade strömmar. Dessa inducerade strömmar kan ta sig in i och påverka andra delar i apparaten, till exempel halvledarkomponenter som integrerade kretsar.

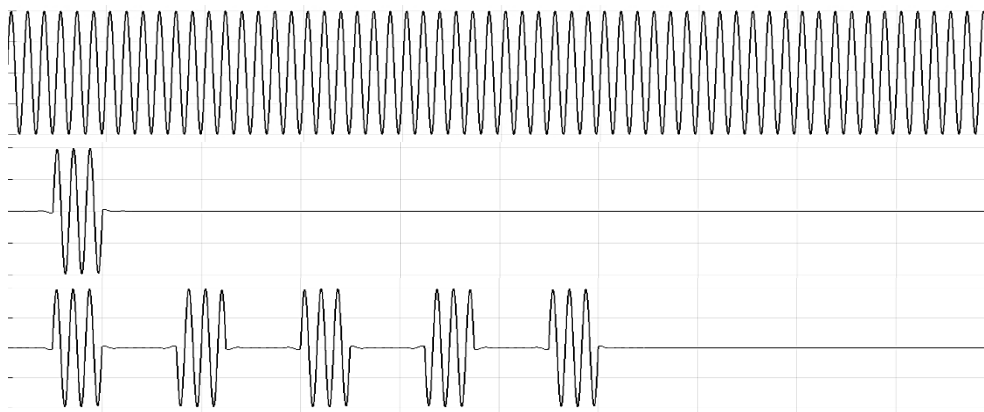
Att en apparat oavsiktligt påverkas av elektromagnetiska vågor i omgivningen kan leda till störningar i apparatens funktion, t.ex. brus eller funktionsbortfall. Detta gäller även för apparater utan antenner, dvs. sådana som inte är avsedda att reagera på omgivande elektromagnetiska fält. Elektromagnetiska fält kopplar givetvis lättast in på antenner som är konstruerade för att ta emot vågor av just den frekvensen, men även om vågorna är av en annan frekvens kan inkoppling ske.

Man brukar använda termen *framvägskoppling* när elektromagnetiska fält tar sig in via avsiktliga antenner, medan fält som tränger in genom kablar, flänsar, m.m., som inte är antenner, tar sig in i apparaten via *bakvägskoppling*. Framvägskoppling kan ske vid den frekvens som utrustningen arbetar och kallas då *inombands framvägskoppling*, eller vid en annan frekvens än den som utrustningen arbetar vid och kallas då *utombands framvägskoppling*.

När apparater störs av fält från andra apparater brukar man prata om *elektromagnetisk interferens* (eng. ElectroMagnetic Interference, EMI). För att förhindra detta finns industristandarder för hur apparater ska konstrueras så att de inte avger alltför kraftiga fält och så att de inte är alltför känsliga för omgivande fält. Teknikområdet *elektromagnetisk kompatibilitet* (eng. ElectroMagnetic Compatibility, EMC) går ut på att se till att olika typer av apparater ska kunna samexistera, t.ex. i ett hem, i en personbil, på ett kontor eller i en industrilokal.

Om någon antagonist avsiktligt genererar elektromagnetiska fält eller pulser för att störa apparater eller annan utrustning som används i en viss verksamhet brukar man kalla detta för *avsiktlig elektromagnetisk interferens* (eng. Intentional ElectroMagnetic Interference, IEMI). Källan som genererar det störande fältet utgör då ett *elektromagnetiskt hot* (EM-hot) för den påverkade utrustningen. Mycket kraftiga fält kan generera så kraftiga strömmar i den apparat som utsatts att halvledarkomponenter i apparaten bränns sönder, vilket leder till permanent fysisk skada.

Elektromagnetiska fält som kan påverka elektronisk utrustning kan innehålla en eller ett flertal frekvenser. Oscillationerna kan vara kontinuerliga, som från en störsändare, eller förekomma i korta pulser, som från ett mikrovågsvapen. Ibland kan de komma i pulsskurar med ett antal pulser i varje, se Figur 4.



Figur 4. Schematisk illustration av en kontinuerlig oscillation, en enstaka puls och en pulsskur med fem pulser.

För att bestämma styrkan i en elektromagnetisk svängning brukar man använda begreppen effekt och energi. Den elektromagnetiska effekten i en punkt är ett mått på hur kraftigt EM-fältet är vid en viss tidpunkt och beror av den momentana fältstyrkan. Effekt mäts i enheten watt (W), med multiplarna kilowatt (kW) och megawatt (MW). Den elektromagnetiska energin är ett mått på det samlade effektförflödet under ett visst tidsintervall, t.ex. under en kort strålningpuls. Energi mäts i Joule (J), eller ibland i kilowattimmar (kWh), megawattimmar (MWh), etc.²

Definitionerna av effekt och energi är här anpassade efter den situation vi studerar, nämligen elektromagnetisk strålning som riktas mot ett elektronikobjekt. Man kan använda en liknelse med bilkörning för att illustrera dessa begrepp: Trycket på gaspedalen i en bil bestämmer det momentana effektuttaget, dvs. energiförbrukningen, som är kopplad till bilens hastighet, medan mängden bensin i tanken bestämmer hur mycket energi som kan förbrukas, vilket bestämmer hur långt bilen kan köra.

² Prefixet k står för kilo som betyder tusen, dvs. 1 000.

Prefixet M står för Mega som betyder miljon, dvs. 1 000 000.

1.4 Definitioner

Antagonist - Person, grupp av personer eller organisatorisk enhet som har för avsikt att orsaka negativa effekter eller skador, 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 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-hot kan också syfta på utrustning som kan generera elektromagnetiska fält med sådan påverkan.

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.

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

Kritisk infrastruktur – Fysisk struktur vars funktionalitet bidrar till att säkerställa upprätthållandet av viktiga samhällsfunktioner [5].

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 [5].

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

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

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 en organisation.

2. Elektromagnetiska hot

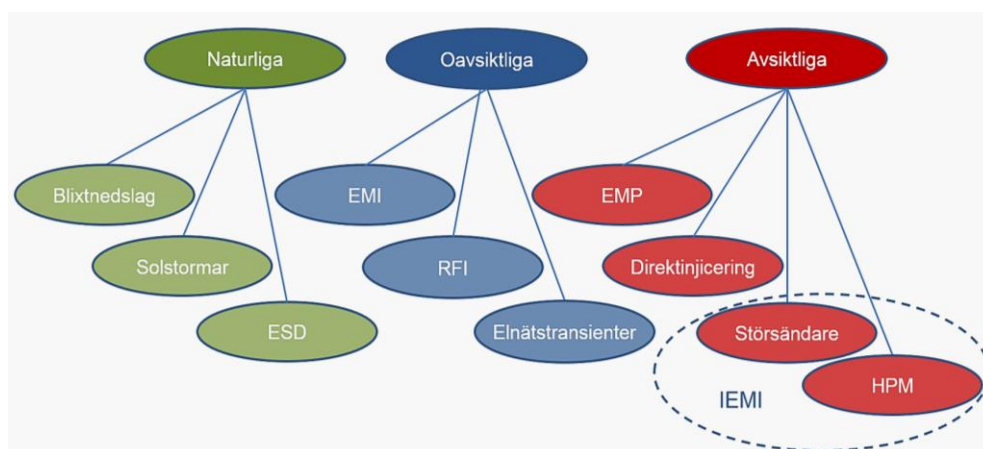
Många människor har någon gång råkat ut för störningar av mobiltelefon, radio eller dator under ett kraftigt åskväder eller när man befunnit sig i närheten av en transformatorstation eller annan elektrisk anläggning. Det som då händer är att störkällan alstrar elektromagnetiska fält som påverkar den egna apparatens funktion genom att inducera strömpulser i ledningar och komponenter.

Elektromagnetiska hot (EM-hot) utgörs av elektriska och/eller magnetiska fält som är tillräckligt starka för att kunna påverka elektriska/elektroniska apparater och system. EM-hot kan härröra från naturligt förekommande fenomen eller vara genererade av människor, antingen oavsiktligt eller med avsikt att åstadkomma störningar i verksamheten.

Svagare EM-hot åstadkommer störningar som pågår under den tid som störfälten genereras, medan kraftigare EM-hot kan åstadkomma fysisk skada som kvarstår i elektroniken efter att hotet har upphört.

EM-hot kan vara statiska elektromagnetiska fält eller fält som varierar i styrka och/eller riktning, mer eller mindre snabbt. Om störningarnas frekvens ligger inom det frekvensområde som apparaten använder (t.ex. FM-bandet för en radio) kan dessa lätt fångas upp av antennen och störa den ordinarie radiosignalen. Men även om störningarna inte har en frekvens som överensstämmer med någon av apparatens arbetsfrekvenser kan störningar ändå ta sig in och påverka apparatens funktion. De kraftigare EM-hoten kan till och med påverka och skada utrustning som är avslagen eller förrådsställd.

Figur 5 visar en indelning av elektromagnetiska hot i naturliga EM-hot, oavsiktliga EM-hot genererade av mänsklig aktivitet, samt avsiktliga EM-hot.



Figur 5. Indelning av EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur.

2.1 Naturliga EM-hot

Det är inte ovanligt att kraftiga åskväder leder till störningar på elektronisk utrustning, kommunikationer och elförsörjning. Vid direkträff av blixten i en ledning kan blixtrömmen följa ledningen och förstöra utrustning som är kopplad till denna eller orsaka brand. Blixtrömmen vid en urladdning mellan moln och mark är kraftig och kan ge upphov till en elektromagnetisk puls som påverkar elektronik på kilometeravstånd. Detta kan orsaka tillfälliga störningar eller permanent skada i utrustningen, se [6].

Solstormar, även kallat ”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. Störningarna påverkar stora geografiska områden och kan inducera kraftiga strömmar i större metalliska strukturer som kraftledningar, teleledningar, järnvägsräls, pipelines, m.m. Sådana *geomagnetiskt inducerade strömmar* (eng. Geomagnetically Induced Currents, GIC) genererar ofta synnerligen lågfrekvent störning, ofta under 1 Hz, som kan slå ut elektriska komponenter, t.ex. i transformatorstationer, öka korrosionen i pipelines, m.m. [7].

Elektrostatiska urladdningar (eng. Electrostatic Discharge, ESD) är en elektrisk urladdning av statisk elektricitet, t.ex. från en uppladdad människa, vilket kan skada elektronik.

2.2 Oavsiktliga EM-hot

Vi omges idag av allt fler apparater som innehåller elektronik som arbetar med svaga spänningar och strömstyrkor, vilket gör dem känsliga för externa elektromagnetiska fält. Även större anläggningar i offentlig eller privat regi omdisponerar allt fler funktioner till elektronisk kontroll och styrning. Detta leder till att apparater allt oftare riskerar att störa varandra.

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 brukar benämnas *elektromagnetisk interferens* (eng. ElectroMagnetic Interference, EMI). Speciellt kan radiomottagare utsättas för *radiofrekventa störningar* (eng. Radio Frequency Interference, RFI) eftersom dessa är utvecklade för att ta emot radiosignaler. Kortvariga transienter kan uppstå på elnät t.ex. när en stamledning eller transformator fallerar, som en följd av att en felaktig apparat inkopplats eller vid blixtnedslag.

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 händer att utrustning strålar ut mer elektromagnetisk energi än vad som är tillåtet, t.ex. när någon komponent i utrustningen gått sönder. EMI kan uppträda vid såväl låga som höga frekvenser och störa kontinuerligt eller i form av transienta pulser [8,9,10]. I Sverige är Elsäkerhetsverket tillsynsmyndighet för att säkerställa att lagar och förordningar uppfylls inom området EMC.

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 [11]. Störningarna kom från en reklamskylt som stod i närheten av flygplatsen, se Figur 6. Reklamskylten orsakade problem för flygplan som flög över skylten på låg höjd (ett antal hundra meter) vid start och landning. Flygplatsen hörde dock inte den störande signalen på sin radio vilket förklaras av att det är långt till flygplatsen, flera kilometer, och av att signalstyrkan minskar med avståndet.

I december 2011 fattade Elsäkerhetsverket beslut om användningsförbud för två reklamskyltar som utgjorde ett allvarligt hot mot flygsäkerheten vid flygplatsen. Om radiokommunikationen störs kan anrop från flygplatsen eller från ett annat flygplan missas, vilket kan leda till en allvarlig incident.

2014 anmälde en nätoperatör problem med radiostörningar på GSM-nätets upplänk vid Eriksbergs shoppingcenter i Västerås [12]. Störningarna uppträdde enbart på kvällen och försvann dagtid, se Figur 7. Orsaken till störningen mot basstationen var en strålkastare som kvällstid belyste en flagga vid ingången till shoppingcentrets entré.

I Japan används LED-lampor i stor utsträckning för att spara energi. LED-lampor är strömsnåla, vilket är en stor fördel ur miljöhänsen, däremot kan elektroniken i lamporna ge upphov till betydande störningar. Ett exempel är från 2010 då TV mottagningen försämrades på en gata där LED-lampor installerats [13].

Även i Sverige orsakar LED-lampor störningar, både störningar på elnätet och radiostörningar. Elsäkerhetsverket har vid en marknadskontroll belagt över hälften av de testade LED-lamporna med försäljningsförbud, vilket är en hög siffra [14]. LED-lampor som säljs i Sverige ska följa det regelverk som finns avseende egenskaper för att elektriska apparater ska fungera tillsammans, dvs. krav på elektromagnetisk kompatibilitet, EMC.



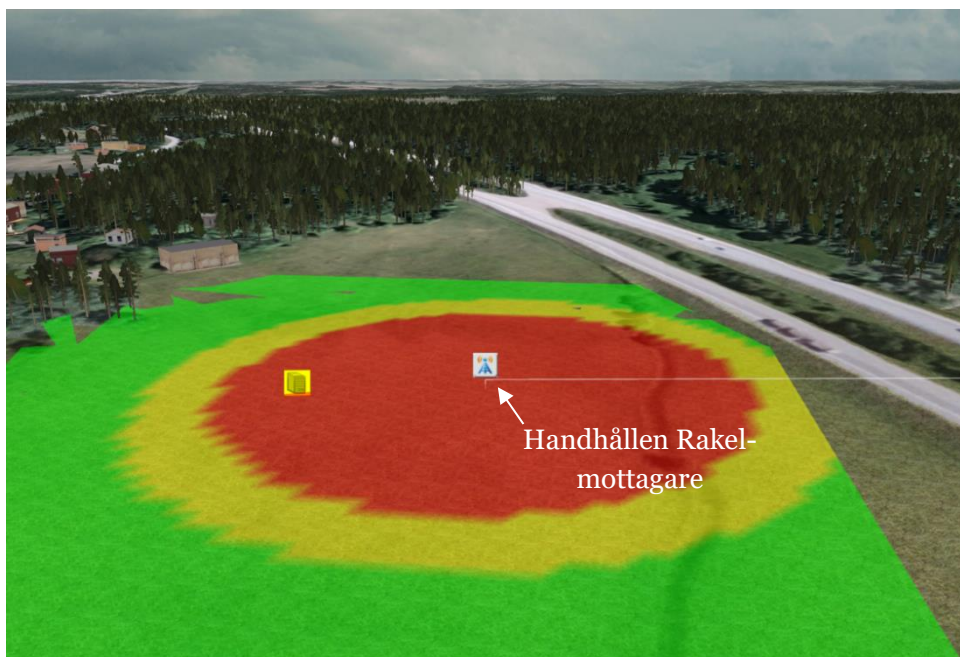
Figur 6. Reklamskylt som störde ut flygledning på Trollhättan-Vänersborgs flygplats [11] Foto: Henrik Olsson, Elsäkerhetsverket.



Figur 7. Flaggbelysning vid shoppingcenters entré som störde ut en basstation för GSM-nätet [12] Foto: Henrik Olsson, Elsäkerhetsverket.

Figur 8 visar ett exempel på ett område runt en handhållen Rakel-mottagare där man bör undvika att placera en datorutrustning. Även om datorn uppfyller regelverket för kommersiella utrustningar, kan kommunikationssystemet få en prestandaförsämring om Rakel-mottagaren tar emot en svag kommunikations-signal, dvs. befinner sig långt från en basstation. Exemplet visar att en oavsiktlig störningskälla kan få stora konsekvenser om den placeras i närheten av en radiomottagare.

Det faktum att man oavsiktligt och utan särskild kunskap kan råka använda en apparat som stör andra apparater visar att det är fullt möjligt att åstadkomma avsiktlig störning om man i något avseende optimerar funktionen hos den störande apparaten.



Figur 8. Exempel på område runt en handhållen Rakel-mottagare där annan utrustning kan störa kommunikationen [15].

2.3 Avsiktliga EM-hot

Det finns många potentiella antagonister som kan tänkas använda sig av elektromagnetiska hot för olika syften, alltifrån teknikintresserade studenter som själva konstruerar och testar enkla störkällor, via kriminella som vill slå ut larm eller andra säkerhetssystem vid inbrott, till terroristorganisationer och främmande makt som vill förlama det civila samhället vid en internationell konfrontation.

Om en antagonist genererar elektromagnetisk strålning i syfte att störa, vilseleda eller förstöra elektronisk utrustning kallar vi detta för ett avsiktligt EM-hot. I militära konflikter använder man begreppet telekrigsangrepp [16] för att beskriva när elektromagnetisk energi används för att nedsätta eller förstöra motståndarens systemfunktioner och stridsförmåga. Telekrigsangrepp har en lång militär historia där de första exemplen hänför sig till det rysk-japanska kriget 1904-1905 där både Ryssland och Japan använde sig av kraftiga störsändare för att försvåra motståndarens möjligheter till radiokommunikation.

Under stormakternas tidiga kärnvapenkapprustning gjordes ett flertal försök med kärnvapendetonationer högt upp i atmosfären. I juli 1962 utförde USA en atomvapensprängning, kallad Starfish prime [17], på 400 km höjd och i samband med denna observerades den första nukleära elektromagnetiska pulsen (eng. Nuclear ElectroMagnetic Pulse, NEMP). En tredjedel av alla satelliter i låga banor stördes och vissa av dem förstördes av den elektromagnetiska energin som frigjordes då detonationen accelererade elektroner högt upp i atmosfären. På denna tid var samhället ännu inte helt beroende av elektronisk apparatur och den som fanns byggde ofta på elektronrörsteknik som är relativt okänslig för elektromagnetiska pulser. Dagens samhälle ser naturligtvis helt annorlunda ut och en nukleär EMP skulle idag få förödande konsekvenser.

I efterdyningarna av stormakternas atomvapensprov och upptäckten av NEMP började forskning vars syfte var att generera kraftiga elektromagnetiska pulser utan kärnvapen och där energin, till skillnad från strålningen från en NEMP, kunde riktas mot ett specifikt mål. På detta sätt föddes forskningen kring mikrovågsvapen (eng. High-Power Microwave, HPM), även kallade radiofrekventa vapen (RF-vapen). Utvecklingen på detta område leds av Ryssland och USA men även länder som Kina och Indien satsar stora resurser på att ta fram effektiva HPM-vapen och i stort sett alla större nationer har någon typ av militärt HPM-vapenprogram.

Militära HPM-vapen är mycket kraftfulla och kan förstöra oskyddad elektronisk utrustning genom bakvägskoppling på upp till någon kilometers avstånd och genom framvägskoppling på flera kilometers avstånd. Denna typ av vapen är dock mycket komplicerade och dyra konstruktioner och det är knappast troligt att kriminella eller ens terroristorganisationer har tillgång till dem. Däremot syns på internet och sociala medier ett ökande intresse för enklare konstruktioner med kortare räckvidd, men som kan störa utrustning på några tiotals meter.

Vad gäller störsändare finns ett enormt utbud på internet både vad gäller färdiga utrustningar och tips för den som vill bygga själv. En störsändare behöver heller inte vara speciellt kraftfull, komplicerad eller dyr för att ha en räckvidd på några hundra meter i alla riktningar.

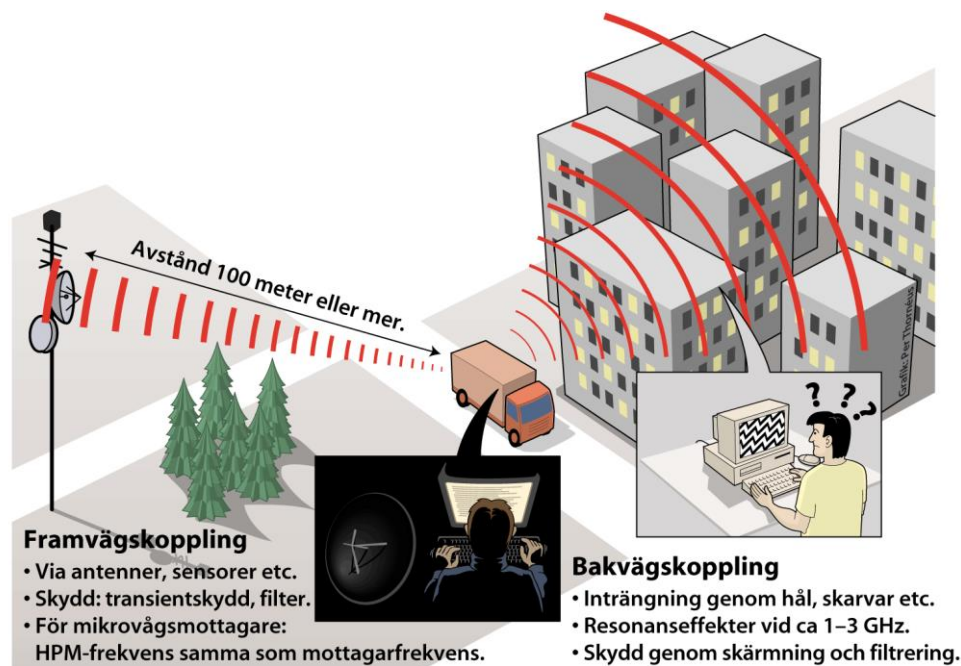
Gemensamt för alla avsiktliga EM-hot är att de bör ses som en del i ett större sammanhang. Kriminella kan störa ut ett villalarm för att förenkla själva stölden och en terrororganisation kan använda sig av störning för att försvåra ingripande från blåljusmyndigheterna. Under en militär operation eller i en gråzon innan öppen militär konflikt kan störning och HPM-vapen användas för att sprida osäkerhet och misstro i civilsamhället samt försvåra informations-spridning och därigenom försämra motståndarens beredskap. Undantaget från denna regel skulle vara rena "pojkestreck" där inga intentioner att skada finns men där konsekvenserna blir större än vad man avsett eller kunnat föreställa sig.

2.4 Kopplingsvägar

Det är brukligt att indela påverkan från EM-hot i tre olika kategorier med avseende på hur den elektromagnetiska energin kopplar in i de elektroniska system som störs eller förstörs, enligt nedan och illustrerat i Figur 9.

- *Framvägskoppling*
Innebär att elektromagnetisk energi kopplar in på en antenn som systemet använder för kommunikationsändamål. Framvägskoppling delas upp i två underkategorier.
 - *Inombands framvägskoppling*
Innebär att EM-hotet genererar strålning i det frekvensband som systemet använder för kommunikation.
 - *Utombands framvägskoppling*
Innebär att EM-hotet genererar strålning utanför det frekvensband som systemet använder för kommunikation.
- *Bakvägskoppling*
Innebär att den elektromagnetiska energin kopplar in direkt på kablar anslutna till systemet eller, via hål i skalet, direkt in på kretskort och internt kablage.

Kommunicerande system är känsligast för framvägskoppling, speciellt inombands framvägskoppling. För att störa eller förstöra system genom framvägskoppling behövs normalt sett mycket mindre energi än via bakvägskoppling. Skydd mot utombands framvägskoppling kan utgöras av filter som bara släpper igenom den frekvens som utrustningen är avsedd för. Skydd mot inombands framvägskoppling av HPM kan utgöras av transientskydd som hindrar alltför höga effekter att nå de känsliga komponenterna i mottagarenheten. Det hjälper dock inte mot störsändare.



Figur 9. Illustration av fram- och bakvägskoppling. Verkan genom inombands framvägskoppling kan ske på många kilometers håll medan verkan genom bakvägskoppling kräver högre effekt och därför sker på kortare avstånd.

På grund av rent geometriska effekter sker bakvägskoppling oftast mest effektivt i ett frekvensband mellan 1 och 3 GHz och bästa sättet att skydda utrustningen är att se till att den är väl skärmad, d.v.s. innesluten i metalliskt skal och att det sitter filter på in- och utgående kablar. Det kan vara svårt och kostsamt att skydda utrustning med filter och skärmning i efterhand men det är ofta relativt enkelt och mycket mindre kostsamt om sådana skydd finns med i kravställning när känsliga och kritiska system upphandlas.

Då effekttätheten hos den elektromagnetiska vågen avtar kvadratisk med avståndet, d.v.s. en fördubbling av avståndet minskar risken med en faktor fyra, är det alltid en god idé att se till att det inte vem som helst kan komma i närheten av verksamhetskritisk och känslig elektronisk utrustning.

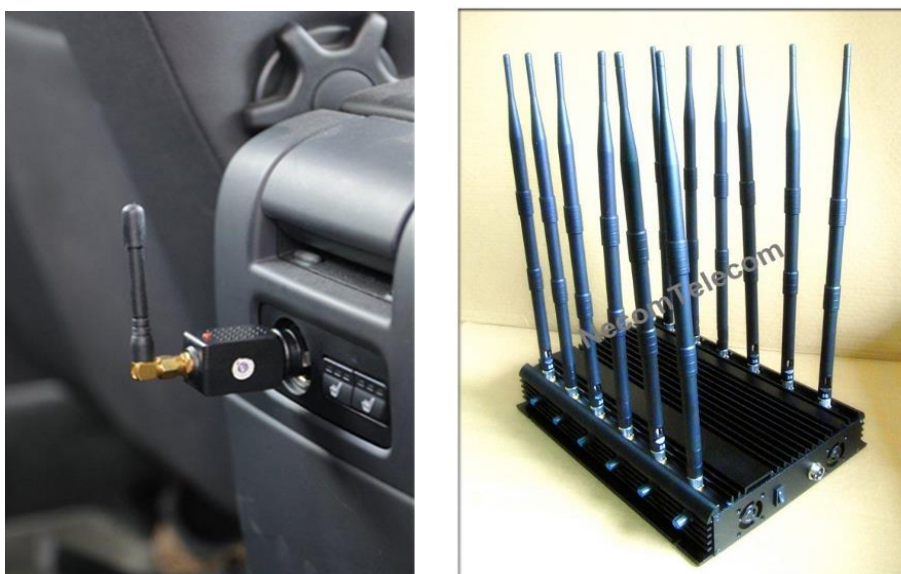
3. Exempel på hotkällor

Hotkällor för avsiktlig elektromagnetisk verkan kan grovt indelas i störsändare som stör ut trådlös kommunikation eller satellitbaserade navigeringssystem och i HPM-vapen som sänder ut kortvariga, men mycket kraftiga, radio eller mikrovågspulser och som kan störa eller till och med förstöra elektroniska system genom framvägs- och/eller bakvägskoppling.

3.1 Störsändare

Störsändare förekommer i många olika utföranden och för olika frekvensband och kan köpas över internet till priser som börjar på några få hundralappar. Oftast är dessa inriktade på att störa kommunikationssystem eller GNSS, men kan även vara byggda för att störa andra trådlösa system som exempelvis radar. Det sistnämnda förekommer framförallt militärt.

I Sverige är det förbjudet att inneha störsändare men det är i praktiken mycket svårt att hindra personer från att införskaffa dem. En typ av störsändare som blivit mycket populär är GPS-störare. Dessa används ofta i syfte att störa ut ett arbetsfordons position så att chauffören kan hindra centralen från att se var fordonet för tillfället befinner sig [18], se Figur 10. Figuren visar två olika typer av kommersiellt tillgängliga störsändare. Störsändaren till vänster är en GPS-störare som kostar några hundralappar och har en tänkt störradie på några meter för att lura fordonets inbyggda positionsrapportering. Den kan dock orsaka problem i omgivningen på mycket längre avstånd. Till höger visas en mycket mer kompetent och långräckviddig störsändare som kostar några tusenlappar och som kan störa blåljusmyndigheternas RAKEL-system, kommunikationsbanden GSM, WiFi, 3G och 4G på avstånd upp till 100 m.



Figur 10. Två olika typer av kommersiellt tillgängliga störsändare. Vänster: Liten GPS-störare. Höger: Multi-störsändare som stör flera olika kommunikationssystem. Foto: FOI och Wikimedia commons.

Att störa ut GPS och mobilkommunikation är belagt med grova böter men det är mycket svårt att hitta en störkälla som förflyttar sig och som dessutom bara är påslagen under någon eller några timmar per dygn.

En störsändare kan ha en störradie från några få meter (som i exemplet ovan) upp till många hundra meter och det finns gott om färdig utrustning att köpa. I en och samma enhet kan alltså den som vill få ett system som stör allt från blåljusmyndigheternas RAKEL-system till WiFi, GPS, GSM, 3G och 4G över några hundra meters radie [19], se exempel till vänster i Figur 11. En sådan utrustning får plats i en attachéväska, väger några kilo och kostar några tusenlappar. För den radiokunnige är det inte heller särskilt svårt att bygga en störsändare och det finns gott om konstruktionstips på nätet [20]. Det finns även militära störsändare med bättre förmåga till störsändning vilket innebär att de kan störa på längre avstånd. Till höger i Figur 11 visas exempel på militär störsändare med kraftig riktantenn.

Störsändare kan användas i rent kriminella syften t.ex. för att störa ut kommunikationen mellan en bilnyckel och billåset. Föraren tror att bilen låser sig när knappen på nyckeln trycks in men i verkligheten är signalen utstörd och bilen länsas på värdesaker när ägaren avlägsnat sig från parkeringen.

Ett allvarligare scenario är att störsändning används i samband med inbrott för att hindra villalarm att kommunicera med larmcentralen. Ett annat användningsområde är störsändning vid större lager av tjuvgods för att hindra GPS-spårning av exempelvis bilar, skotrar, båtmotorer och andra dyra varor som ofta är försedda med GPS-spårare.

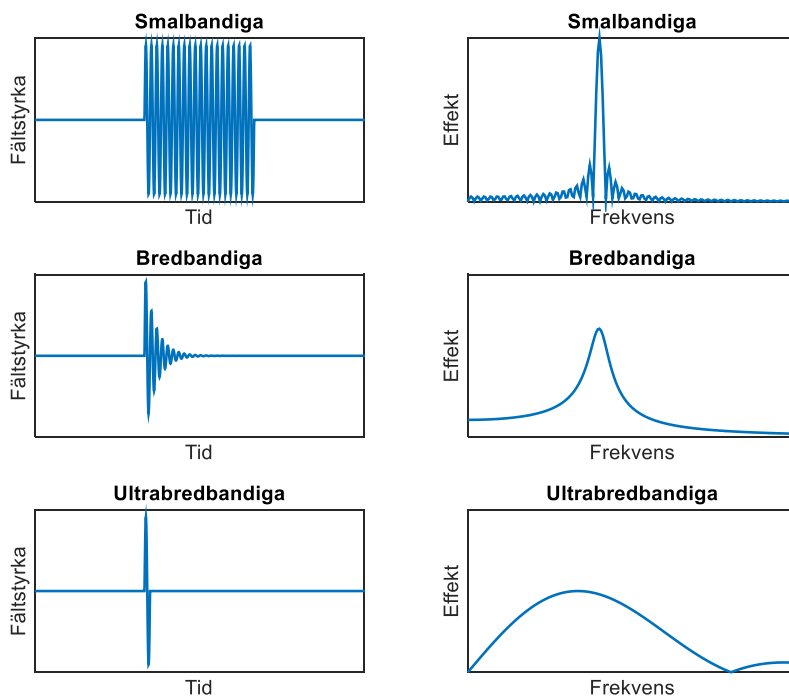


Figur 11. Olika typer av störsändare. Till vänster: en kommersiellt tillgänglig störsändare kapabel att störa flera kommersiella kommunikationssystem och GPS. Till höger: militär störsändare. Foto: FOI och FOI/FM.

3.2 Mikrovågsvapen

Mikrovågsvapen (även kallade RadioFrekvens-vapen, HPM-vapen; eng. High-Power Microwave, HPM) betecknar radio- och mikrovågssändare konstruerade i syfte att generera strålning med mycket hög toppeffekt i korta pulser. Om en typisk störsändare har en kontinuerlig uteffekt på upp till hundra watt så kan ett HPM-vapen ha en toppeffekt på flera miljoner watt (Megawatt, MW) och militära system kan i vissa fall generera toppeffekter på miljarder watt (Gigawatt, GW). Sådana system dels kan störa kommunicerande utrustning på mycket stora avstånd, upp till flera kilometer, men också störa eller förstöra elektronisk utrustning som inte kommunicerar via radio på kortare avstånd.

HPM-vapen brukar delas in i tre olika grupper efter hur frekvensinnehållet ser ut: smalbandiga, bredbandiga och ultrabredbandiga, se Figur 12. En smalbandig konstruktion genererar strålning med en enda frekvens medan bredbandiga och ultrabredbandiga källor genererar strålning över ett frekvensintervall. Smalbandiga HPM-vapen koncentrerar all energi i en frekvens och kan då, om frekvensen kopplar in effektivt orsaka förstörande verkan genom bakvägskoppling. Bredbandiga system sprider ut energin över ett stort frekvensintervall för att öka sannolikheten att inkoppling kan ske vid någon frekvens men det minskar sannolikheten för förstörande verkan genom bakvägskoppling. De kan dock vara mycket effektiva störare både genom bakvägskoppling och utombands framvägskoppling och, i vissa fall, orsaka förstörande verkan genom inombands framvägskoppling.



Figur 12. Schematiska pulsformer (elektrisk fältstyrka som funktion av tiden) och spektra (effektthet som funktion av frekvens) för tre huvudtyper av HPM-källa.

Ett HPM-vapens storlek skalar med uteffekten och därmed dess räckvidd, d.v.s. ett litet HPM-vapen har, i jämförelse, relativt kort räckvidd. HPM-väskan i Figur 13 kan störa elektronik som t.ex. datorer, datornätverk och kameror på

några tiotals meter och kan genom framvägsskoppling orsaka problem för kommuniserande utrustning på upp till några hundra meter. Den är dock inte kraftfull nog för att förstöra elektronisk utrustning på längre avstånd än enstaka meter. Den strålkälla som är monterad i en SUV till höger i Figur 13 är framtagen för att stoppa bilar på avstånd upp till 15 meter genom att störa ut den elektronik som styr tändsystemet i moderna bilar.



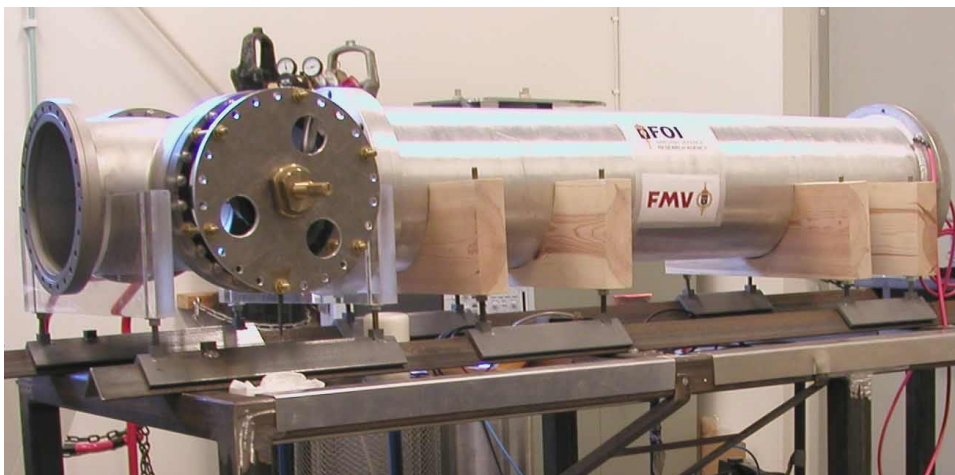
Figur 13. Två olika typer av bredbandiga HPM-vapen framtagna av Tyska Diehl Defence. Till vänster en kommersiellt tillgänglig utrustning som får plats i en resväska av kabintyp och till höger en utrustning framtagen för att stoppa bilar på upp till 15 m. Foto: FOI och Diehl Defence.

Ett annat system, monterat på ett biltak och designat för att störa ut drönare visas i Figur 14. Det ökande hotet från billiga men ändå ganska kvalificerade drönare mot t.ex. flygplatser, politiska sammankomster och fängelser har gjort att det finns ett hastigt ökande intresse för denna typ av HPM-vapen. De företag som saluför dessa mindre HPM-vapen riktar sig i huvudsak mot militär, blåljusmyndigheter och andra myndigheter med ansvar för fysisk säkerhet runt kritiska anläggningar som man vill skydda mot drönarhotet. Även om denna typ av vapen inte säljs till vem som helst så finns en risk att den ökade förekomsten gör att de sprids till kriminella och andra antagonister som kan använda dem till helt andra syften.



Figur 14. Utrustning designad för att störa ut små drönare av quadrokoptertyp. Enheten är batteridrivnen och allt som behövs finns i burken som sitter monterad på biltaket. Foto: Diehl Defence.

Flera länder utvecklar mikrovågsvapen för militär användning, men de flesta är fortfarande på forsknings- och utvecklingsstadiet. Ett exempel ges i Figur 15 som visar en mikrovågsgenerator som använts i FOI:s forskningsverksamhet. Den är cylindrisk och cirka 2 meter lång. Större delen av volymen och vikten består av en högspänningspulsgenerator som genererar korta spänningspulser på hundratal kilovolt för att driva strålkällan. Här ses strålkällan med en öppning till vänster, där man skulle kunna koppla på en antenn. Detta är ett ganska litet laboratoriesystem; på fler håll i världen finns det större mikrovågsgeneratorer som kan generera mycket kraftiga mikrovågspulser. Ryssland och USA utvecklar liknande system för att sättas på markfordon eller flygande plattformar.



Figur 15. Mikrovågsgenerator som använts för forskning vid FOI. Strålkällan utgör den vänstra fjärdedelen, medan resten är en högspänningspulsgenerator. Ett mikrovågsvapen baserat på denna teknologi skulle kunna placeras på ett fordon, fartyg eller i en robot. Foto: FOI.

4. Elektromagnetisk attack mot kritisk infrastruktur

4.1 Varför avsiktliga EM-hot?

Även om den ökade användningen av elektronisk apparatur för styrning, övervakning och kommunikation på många sätt gör vårt samhälle mer robust så utgör samhällets beroende av dessa funktioner en fara i händelse av funktionsbortfall. Vi litar helt enkelt på att de skall fungera och så länge de gör det har vi enormt stor nytta av de senaste årens utveckling inom t.ex. datorer, smartphones och trådlösa nätverk; och för det mesta fungerar det utmärkt. Problemet är att man hänger upp viktiga samhällsfunktioner på system som, även om vi bortser från cyberattacker, är mycket sårbara för EM-angrepp.

Elektronisk utrustning och trådlös kommunikation har blivit en alltmer integrerad del av vårt samhälles infrastruktur och det gör att den person, organisation eller stat som vill orsaka problem eller sprida förvirring och osäkerhet kan göra det genom att se till att utrustningen inte längre går att använda [21,22,23,24].

Denna sårbarhet är mycket enkel att utnyttja för kriminell aktivitet, terrorhandlingar och, kanske speciellt, av främmande makt i gråzonen mellan krig och fred där man vill sprida desinformation och osäkerhet som skadar civilsamhällets infrastruktur och tilltron till samhällets funktioner.

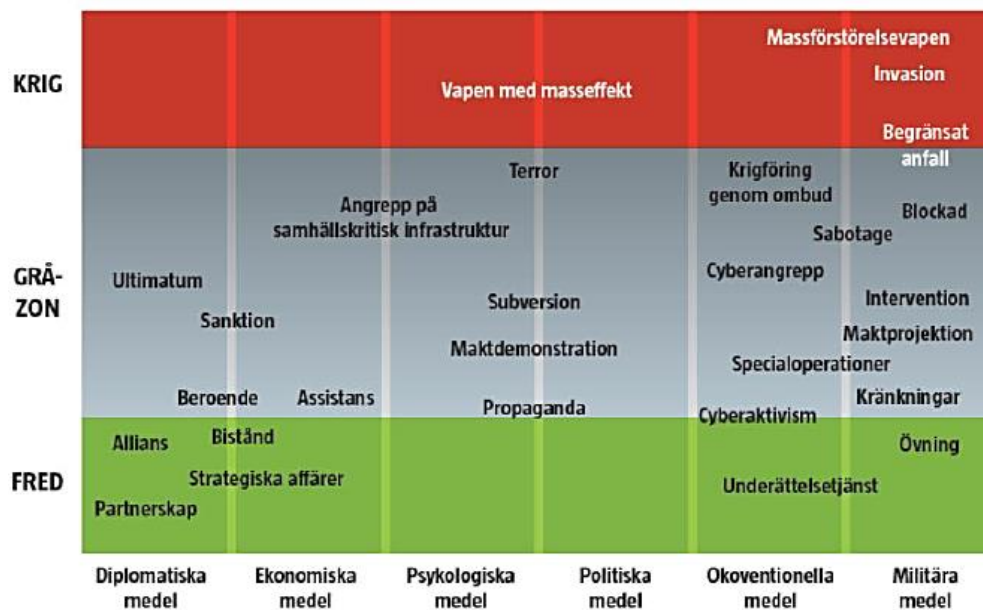
4.2 EM-attack som del av ett större angrepp

Ett typiskt scenario där samhällsviktig verksamhet och kritisk infrastruktur kan utsättas för angrepp med EM-hot är ett där det samtidigt förekommer andra typer av attacker, t.ex. med skjutvapen, bomber eller inbrottsverktyg. Alternativt kan en EM-attack vara förberedelse inför eller en del av ett invasionsföretag.

Med gråzon avses det läge som ofta uppstår i en konflikt mellan nationer långt innan militärt våld börjar användas och det vi kallar krig bryter ut, se Figur 16. I diagrammet sorterar elektromagnetiska hot under "Okonventionella medel" och kan utgöra angrepp på den samhällsviktiga infrastrukturen [25].

I gråzonen mellan krig och fred kan det vara av intresse för en annan nation att sprida osäkerhet i det civila samhället genom att störa eller förhindra användning av samhällsfunktioner. Militär materiel är kravställd och konstruerad för att kunna verka i en svår elektromagnetisk miljö men det är inte den elektroniska utrustning vi normalt förlitar oss på i olika civila samhällssystem. Det blir därför lätt för en kvalificerad motståndare att orsaka stora störningar i civilsamhället genom att göra åverkan på de

samhällsfunktioner som kräver avancerad elektronik, speciellt trådlös kommunikation.



Figur 16. Illustration av gråzonen mellan krig och fred och hur olika medel används i gråzonen.



Figur 17. Tekniska motiv för avsiktliga EM-hot är i huvudsak det moderna samhällets stora beroende av elektronisk apparatur och radiokommunikation. Det faktum att det inte finns legala krav på apparaturens tålighet utöver rena EMC-krav gör den sårbar för EM-attacker och det faktum att en antagonist ofta

kan komma ganska nära känsliga installationer gör i sin tur att det går att orsaka skada även med relativt okvalificerad utrustning.

Exempel på känsliga samhällssystem är:

- Datornätverk, elektroniska betalningssystem, informationssystem
- Medicinsk elektronik
- GPS för positions- och tidsbestämning
- Mobiltelefoni och kommunikationsradiosystem
- Radio och TV, tidningsproduktion
- Trafikövervakning och trafikreglering för väg-, spår- och flygtrafik

4.3 Antagonister och syften

Militärt angrepp

Militära motiv för att använda EM-hot för att störa ut eller förstöra civila eller militära system är att man behöver använda mindre väpnat våld för att uppnå sina mål. Dessutom är icke-fungerande samhällssystem en mycket viktig psykologisk faktor som snabbt demoraliserar motståndet vid en intervention. Att störa ordinarie radio- och TV-utsändningar och sända ut falsk eller vilseledande information är vanliga medel för att skapa oro och misstro. En annan fördel ur militärt perspektiv är att man efter reparation av eventuell skadad elektronik kan ta över och använda existerande infrastruktur. Telekrigföring eller användning av elektromagnetiska vapen mot civila mål har blivit en viktig del av den hybridkrigföring som förekommit på senare år för att destabilisera ett lands ledning och få befolkningen att tappa förtroendet för myndigheternas förmåga att kontrollera landet [26,27,28,29].

Det är mindre troligt att ett militärt angrepp eller en terroristattack skulle genomföras enbart med elektromagnetiska medel. Snarare skulle EM-hot nyttjas för att försvåra samhällets förmåga att fungera under en viss tidsperiod. Det skulle ge de antagonistiska krafterna möjlighet att ta kontrollen eller orsaka omfattande skada utan att möta mycket motstånd. Att EM-hot kommer att användas i framtida militära konflikter kan man vara helt säker på eftersom telekrig har fått en mycket viktig roll i alla moderna krigsmakter.

Kriminell användning

Kriminella ligor som i stor omfattning gör inbrott i villor och stjälar båtmotorer har på senare år använt sig av störsändare för GSM-bandet för att störa ut villa- och båtmotorlarm som använder sig av GSM för att skicka larm till ägaren via mobiltelefon [30,31]. Störsändarna gör att larmet inte kan skicka sms-meddelanden till ägaren när motorn flyttas och i vissa fall också att larmet tappar GPS-positioneringen.

Syftet med kriminell användning av EM-hot är att förhindra upptäckt och ostört kunna komma åt stöldbegärliga saker. En situation där EM-angrepp

skulle kunna vara det enda medlet är vid utpressning för att visa att man har sådan kompetens.

Terrorism

Terrorister kan använda en EM-attack som ett medel att försvåra polisens arbete och göra en attack med andra medel mera verkningsfull. Givetvis kan man tänka sig terrorister som stör ut kommunikationen i ett signalsystem bara för att orsaka trafikkaos, men då uppnår man bara irritation och inte den panik i befolkningen som terrorattacker på senare år verkar ha haft som huvudsyfte.

Aktivister mm

Aktivister, anarkister och andra som är missnöjda med samhällsutvecklingen kan använda EM-hot för att störa samhällsfunktioner. Ett exempel är de s.k. Göteborgskravallerna 2001, när polisens kommunikationssystem stördes ut av flera störsändare. [32].

Tekniknördar

De enda fall där man kan förvänta sig att en EM-attack är det enda medlet och syftet är teknikintresserade ungdomar eller anarkister som vill visa att de kan åstadkomma samhällsstörande effekter men inte avser att skada människor. Dessa risker ska inte förringas, men är samtidigt de EM-hot som bör vara lättast att skydda sig emot.

Kommentarer

Förutom ovanstående syften från olika typer av antagonister kan en verksamhet utsättas för angrepp utan att angreppet är direkt menat mot verksamheten. Påverkan kan ske som en följd effekt av ett angrepp eller genom att antagonisten utför en attack mot ett system som används av många olika verksamheter. Ett exempel är en antagonist som stör ut mobiltelefontrafik i en stad i syfte att påverka allmänheten. Om störningen slår mot ett relativt brett frekvensområde, skulle detta t.ex. kunna få till följd att även Trafikverkets kommunikation störs ut.

I de flesta exemplen ovan är användningen av EM-hot ett medel för att uppnå ett annat syfte, men gemensamt är att de utgör störningar av samhällets normala funktion eller den enskildes säkerhet. Skydd mot elektromagnetisk påverkan är därför viktigt för att upprätthålla samhällsfunktioner och bevara allmänhetens förtroende för rättsstaten.

4.4 Tidsförlopp och varaktighet

För att ett EM-angrepp ska ha möjlighet att lyckas behöver en antagonist känna till något om målet för angreppet, som t.ex. vilken typ av utrustning som målet utgör, vilka dess arbetsfrekvenser är, placeringen av antenner och ingångssteg, eventuella skydd som finns, hur nära man kan komma, och kanske också procedurer för hantering av störningar. Ju mera information som finns tillgänglig för en potentiell angripare desto större är sannolikheten att

angriparen väljer en EM-källa som kan verka effektivt mot målsystemet och en angreppsriktning som är effektiv. Förberedda angrepp föregås troligen av en rekognosceringsfas där antagonisten försöker hitta lämpligaste angreppspunkter och angreppsvägar, tidpunkter, m.m.

Ett angrepp där EM-hot används kan typiskt starta med att man med EM-angreppet sätter ett elektroniskt system ur funktion. Om det är flera målobjekt som angrips kan detta ske i sekvens genom att EM-hotet förflyttas mellan målen, eller om antagonisterna har tillräckligt med resurser, att angrepp sker samtidigt på flera platser med flera likadana eller olika EM-hot, beroende på målobjekt och tillgänglig kunskap om dessa.

EM-hotet kan i de flesta fall förväntas vara aktivt under den tid som det huvudsakliga angreppet pågår, för att sedan avlägsnas för att försvåra forensiska undersökningar och identifiering av vem som ligger bakom. När en EM-källa har stängts av finns det inte kvar någon strålning som kan detekteras. Utstörd kommunikation kan ofta återta normal funktion efter att ha varit utstörd, men ibland kan apparater behöva startas om för att kunna användas.

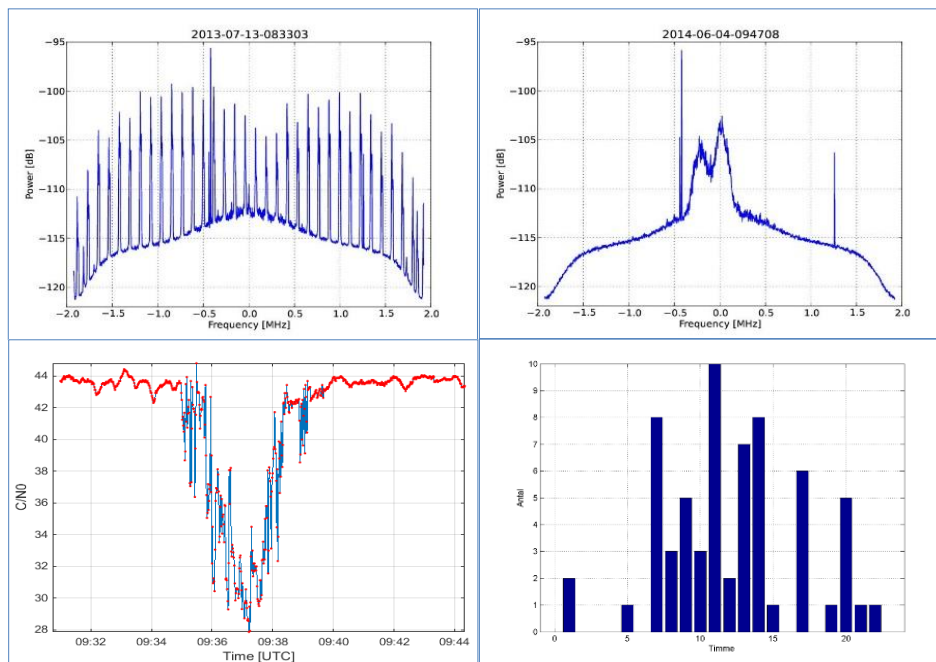
4.5 Att bli medveten om ett EM-angrepp

När utrustning utsätts för avsiktliga elektromagnetiska störningar eller förstörs av elektromagnetiska vapen upphör utrustningen att fungera normalt, vilket ofta kan missuppfattas som ett strömbrott, programvarufel eller att någon komponent i utrustningen spontant har gått sönder. Det kan ta flera minuter eller timmar innan man förstår att man är utsatt för ett avsiktligt angrepp, särskilt om man inte har utrustning som övervakar den elektromagnetiska miljön och kan larma vid förhöjda nivåer.

I Figur 18 visas ett exempel på resultat från ett detektionssystem som övervakar om frekvensspektrumet utsätts för elektromagnetiska störningar. Längst ner till höger visas antalet störningsincidenter på GPS-bandet vid olika klockslag. De två övre bilderna visar hur två olika störningssignaler kan se ut frekvensmässigt. Längst ner till vänster åskådliggörs hur funktionen försämras för en GPS-mottagare vid störning. Övervakningssystemet kan ge viktig information om detektionsstatistik, som exempelvis när på dygnet eller vilka veckodagar detektionerna har skett, se Figur 18. Resultaten från övervakningssystem är ofta mycket värdefulla för att kunna identifiera och åtgärda interferenskällor och minska risken att kritiska system störs ut. För att underlätta identifieringen av radiostörningarna gör detta system även en klassificering av varje detekterad interferens och en signatur av interferensen sparas.

Det är mycket svårt att i efterhand bevisa att det rört sig om ett avsiktligt angrepp eftersom strålningen inte lämnar några spår när den väl upphört. Om elektronik har skadats kan detta konstateras genom mikroskopisk undersökning av kretskort och komponenter, men det är mycket svårt att säkert fastställa om detta orsakats av avsiktligt genererad EM-strålning och

inte av en kortslutning. Endast med säkra observationer av förövarna eller om man får tag på EM-källorna kan detta göras.



Figur 18 Exempel på resultat ut från det FOI-utvecklade övervakningssystemet RF Oculus. De två övre bilderna visar exempel på hur två olika störsignaler kan se ut frekvensmässigt. Nere t.v. visas förhållandet mellan signal och störnivå. Nere t.h. visas förekomst av störincidenter under ett dygn.

5. Konsekvenser av EM-attack

5.1 Tekniska konsekvenser

5.1.1 Avsiktlig störning

Trådlösa kommunikationssystem är ofta känsliga för EM-störning eftersom de är avsedda att ta emot elektromagnetiska signaler. Exempel på trådlösa kommunikationssystem är mobiltelefonisystem, RAKEL, WiFi, och GPS. Effekterna av en störning kan visa sig på olika sätt. Vid kraftig störning så slutar det trådlösa systemet att fungera och ingen kommunikation kan ske. För GPS kan störning visa sig som en felaktig position, stor osäkerhet om positionen eller ingen positionsangivelse alls beroende på system. För kommunikationssystem kan effekterna av störningar även visa sig som en försämrad räckvidd för systemet eller ökade fördröjningar i systemet.

Risken för oavsiktliga störningar beror mycket på miljön som antennen till det trådlösa systemet placeras i. Risken för störningar ökar i komplexa miljöer med flera andra elektriska system, som exempelvis ombord på ambulanser där det finns flera system som skulle kunna ge upphov till störningar. Även i situationer där det finns andra sändande system ökar risken för störningar även om de inte använder samma frekvens. Ett exempel är att sändningar från LTE-system³ orsakade störningar i kommunikationen i GSM-R-systemet som används för järnvägstrafik. [33]

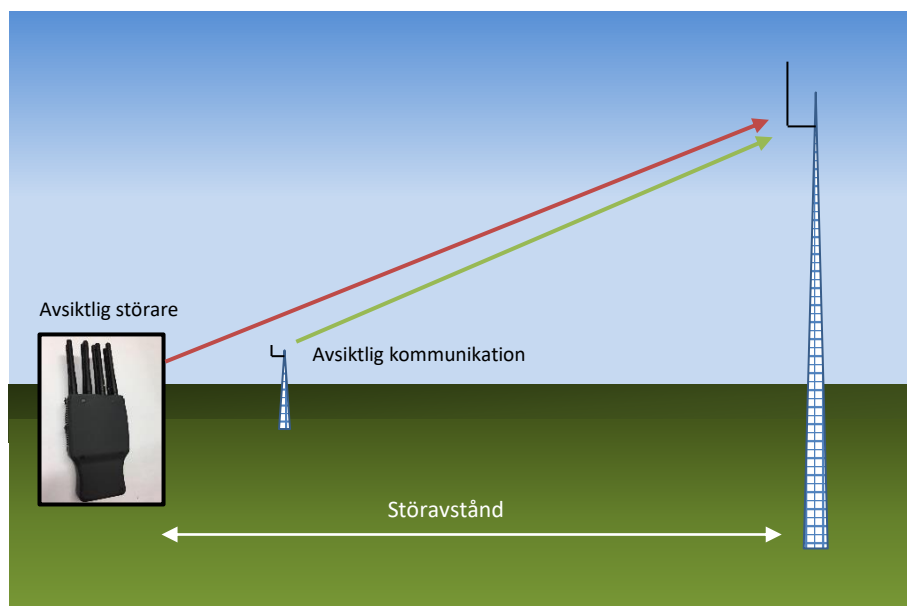
Risken för att en trådlös tjänst störs ut beror på en rad olika parametrar. Det avgörande för om den avsiktliga störningen lyckas är om störaren får ett effektovertag mot den önskade trådlösa tjänsten. En störsändare med högre uteffekt har en ökad chans att lyckas störa ut den trådlösa tjänsten. Dessutom 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, t.ex. genom skärmning av utrustning. Effekten påverkas starkt av terrängen i kombination med störsändarens höjd, se Figur 19.

Faktorer som ökar påverkan från en störsändare är:

- Anpassning av störsignalen till kommunikationssystemet
- Störsändarens sändareffekt
- Riktantenn på störsändaren, dess antennvinst
- Fri sikt mellan störsändare och kommunikationssystemets antenn
- Avstånd mellan störsändare och kommunikationssystemet
- Om störsändarens effekt riktas in mot kommunikationssystemets antennlob
- Kommunikationssystemets känslighet för störning (susceptibilitet)

³ LTE = Long Term Evolution; 4:e generationens mobiltelefonisystem (4G).

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



Figur 19 Schematisk bild över störsändare och kommunikationssystem.

Tabell 1 visar ungefärliga avstånd från vilken en avsiktlig störsändare kan påverka ett kommunikationssystem. Påverkansavstånden är dock starkt beroende av kommunikationsförhållandena för kommunikationssystemet och hur terrängen mellan störsändaren och kommunikationssystemets antenn ser ut. En annan viktig faktor är om störsändaren eller kommunikationssystemet använder riktantenn. Riktantennen gör att effekten förstärks i speciella riktningar och dämpas i övriga riktningar.

Tabellen ger även parametrar för några generella störsändare mot trådlösa kommunikationssystem. De tre första motsvarar störsändare som kan köpas på nätet, med lite olika funktionalitet och storlek. Störsändare kan även byggas av tekniskt kunniga med hjälp av generell hårdvara för radio och mjukvarublock som också finns tillgänglig och en effektförstärkare. En militär störsändare kan bland annat ha högre effekt och bättre riktverkan på antennen och kan därför uppnå större störavstånd.

Tabell 1 Parametrar för generiska störsändare.

Typ av störsändare	Effekt	Antenntyp (riktverkan)	Ungefärligt störavstånd
Handhållen	2 W	Rundstrålande (0 dB)	10 meter
Kommersiell	20 W	Rundstrålande (0 dB)	100 meter
Kommersiell, riktantenn	20 W	Riktantenn (15 dB)	500 meter
Tekniskt kunnig	100 W	Riktantenn (15 dB)	kilometer

Störavståndet varierar med typ av störsändare, se Bilaga: Avståndsberoenden. Speciellt det handhållna systemet kräver att störaren måste komma mycket nära antennen för att kunna störa. Om systemet har tillgång till högre uteffekt eller riktantenn kan störavståndet vara större. Det betyder att störsändaren kan placeras längre bort från kommunikationssystemet, men ändå störa ut systemet. För system byggt av tekniskt kunnig person kan störavstånd på hundratals meter åstadkommas.

5.1.2 Mikrovågsvapen

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 omvärd proportion till avståndet från källan⁴ 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 hos utrustningen i den samhällsviktiga verksamhet 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 i stor utsträckning de för störsändare:

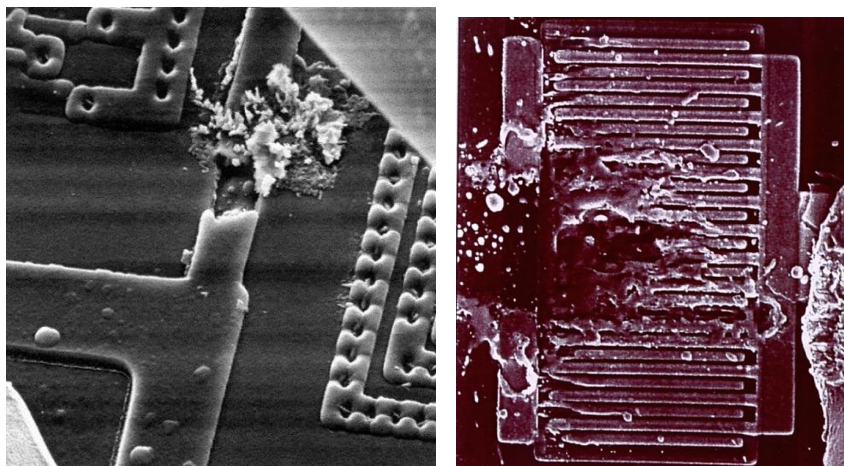
- HPM-källans sändareffekt
- HPM-källans grundfrekvens, bandbredd och pulsrepetitionsfrekvens
- Riktantenn på HPM-källan, dess antennvinst
- Fri sikt mellan HPM-källan och målet (kommunikationssystemets antenn, elektronik, kablage, etc.)
- Avstånd mellan HPM-källan och målet
- Målets (kommunikationssystemets antenn, elektronik, kablage, etc.) känslighet för störning. Målet kan vara designat med olika tålighet mot EM-hot.
- Skalskydd i form av inkapsling, zon-indelning. Utformning 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 största

⁴ 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 areeenhet) är proportionell mot kvadraten på fältstyrkan kommer effekttätheten att avta snabbare med ökande avstånd. En fördubbling av avståndet minskar effekttätheten med en faktor fyra.

avstånd där EM-källan får avsedd verkan. Se Bilagan för verkansavstånd för olika typer av HPM-vapen och olika typer av elektronik.

Kraftiga EM-fält som träffar elektriska ledningar, kretskort och elektroniska komponenter kan i dessa inducera strömpulser, som fysiskt förstör halvledare som transistorer och integrerade kretsar. Figur 20 visar två exempel på av strömpulser förstörd ledning och förstörd transistor.



Figur 20 Elektronmikroskopbilder av integrerade kretsar som förstörts av kraftiga strömpulser i kretsen. Foto: C. Afzelius, FMV Prov.

En grov uppskattning av verkansavstånd för tre olika typer av HPM-vapen återges i Tabell 2, nedan. Första raden ger verkansavstånd för ett militärt system litet nog att få plats i en skåpbil med flak och kapell. På nästa rad antas att systemet är mindre kvalificerat men konstruerat av någon med goda ingenjörsmässiga kunskaper och den nedersta raden anger verkansavstånd för en typ av väskmonterat HPM-vapen, jfr. Figur 13. Det är viktigt att poängtera att verkansavstånd är uppskattningar baserade på erfarenheter från provning av oskyddad elektronik och inte exakta data. Se bilagan.

Tabell 2. Verkansavstånd mot oskyddad civil utrustning. Redovisade verkansavstånd är baserade på erfarenhet från provning av icke-skyddad elektronik, bilar, datorer, nätverk, kommunikationsutrustning och dylikt.

Typ av källa	Avstånd			
	Enstaka meter	15 meter	50 meter	500 meter
HPM-vapen i skåpbil (Militär utrustning)	Ej relevant	Permanent fysisk skada	Permanent fysisk skada	Permanent fysisk skada
HPM-vapen i skåpbil (Ingenjörsmässigt)	Ej relevant	Permanent fysisk skada	Störning ^{1,2} /skada	Störning ^{1, 2}
HPM-vapen i väska (Kommersiellt)	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.

5.2 Verksamhetskonsekvenser

Man tänker kanske inte alltid på hur beroende vi i vardagen är av många olika samhällsfunktioner, men det brukar märkas tydligt när det uppstår störningar. Figur 21 visar exempel på samhällsviktiga verksamheter som är sårbara för EM-attack. Exempelvis kan en nedriven kontaktledning göra att tåg inte kan köra en viss bansträckning, med stora förseningar för ett flertal människor som följd. En sophämtarstrejk leder snabbt till sanitära problem i städerna, medan ett kraftigt åskväder kan slå ut elnätet i en hel landsända under flera dagar.



Figur 21 Exempel på verksamheter som är sårbara för EM-attack.

I Tabell 3 har några samhällsfunktioner som direkt kan drabbas av EM-hot markerats med understrykning. Tabellen bygger på kartläggningen som är framtagen i [34] och som kan ses i tabellen har i stort sett alla samhällssektorer viktig verksamhet som kan påverkas av EM-störningar.

En avsiktlig EM-attack kan vara riktad mot en specifik samhällsfunktion, t.ex. ett kommunikationssystem eller en transportnod, men kan få konsekvenser för andra verksamheter som helt eller delvis är beroende av den störda funktionen. Ibland uppträder konsekvenserna direkt, medan andra kanske blir märkbara först efter ett par dagar. Man brukar skilja mellan direkta och indirekta störningar av en verksamhet. Direkt störning har, som begreppet antyder, direkt påverkan på kritiska funktioner medan indirekt störning avser följdverkningar på system, vilka exempelvis kan uppkomma då en GPS-mottagare störs så att felaktig eller ingen tid levereras och får till följd att andra funktioner fallerar. Ett exempel är ekonomiska transaktioner, som är beroende av att kommunicerande servrar på olika platser använder samma tidsnormal.

Tabell 3. Exempel på samhällsviktiga verksamheter för olika samhällssektorer.

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

En specifik svårighet med EM-störningar av apparater eller elektronikberoende system är att operatörer oftast inte märker några andra effekter än att en funktion faller bort. Då är det naturligt att tänka att en "vanlig" naturlig eller oavsiktlig störning ligger bakom, som att en säkring löst ut av en transient på elnätet, t.ex. genererad av ett avlägset blixtnedslag, eller att det är ett konstruktionsfel eller programvarufel som är orsak till händelsen. Det kan ta flera minuter, timmar eller dagar innan ansvariga förstår att någon avsiktligt har åstadkommit störningen av verksamheten. Då kan EM-hotet vara borta och inte ha lämnat några andra spår än en felfungerande eller förstörd apparat.

Hur ska man kunna veta om ett visst system utsatts för ett EM-angrepp? Eftersom elektromagnetiska fält försvinner så fort som källan stängs av är det svårt att i efterhand kunna belägga att orsaken till störningen av verksamheten var ett avsiktligt genererat EM-hot. En forensisk analys blir svår att genomföra om det enda som finns är ett förstört kretskort i en dator eller om datorn efter EM-attacken har återtagit normal funktion.

Ett sätt att tidigt kunna identifiera att man utsatts för ett EM-angrepp är att för de viktigaste skyddsvärda elektroniska systemen inom en verksamhet ha ett varningssystem som hela tiden monitorerar den elektromagnetiska miljön, dvs. känner av elektromagnetiska strålningsfält, och larmar om systemet detekterar fältstyrkor över en viss nivå. Detta är möjligt och finns redan för att detektera störsändare som sänder kontinuerligt, men för att detektera pulser från HPM-vapen, som har mycket hög fältstyrka men mycket kort varaktighet, typiskt under en mikrosekund, finns det inte kommersiella system att tillgå. Detta beror på att de flesta detektionssystem för elektromagnetisk strålning är medelvärdesbildande över en viss tid.

För att minimera verksamhetskONSEKVENSERNA vid en EM-attack kan det vara bra att ha redundans i all samhällsviktig verksamhet och kritisk infrastruktur, så att bortfall av en systemenhet, t.ex. en mobilmast, kan ersättas av en annan i närheten, om än med reducerad kapacitet i det drabbade området, samt att, i möjligaste mån, använda kabelbunden kommunikation.

Att ha mobila system som kan placeras ut i ett område där utrustning har slagits ut kan vara ett alternativ för att upprätthålla viss funktion tills den ordinarie systemenheten har återställts eller reparerats.

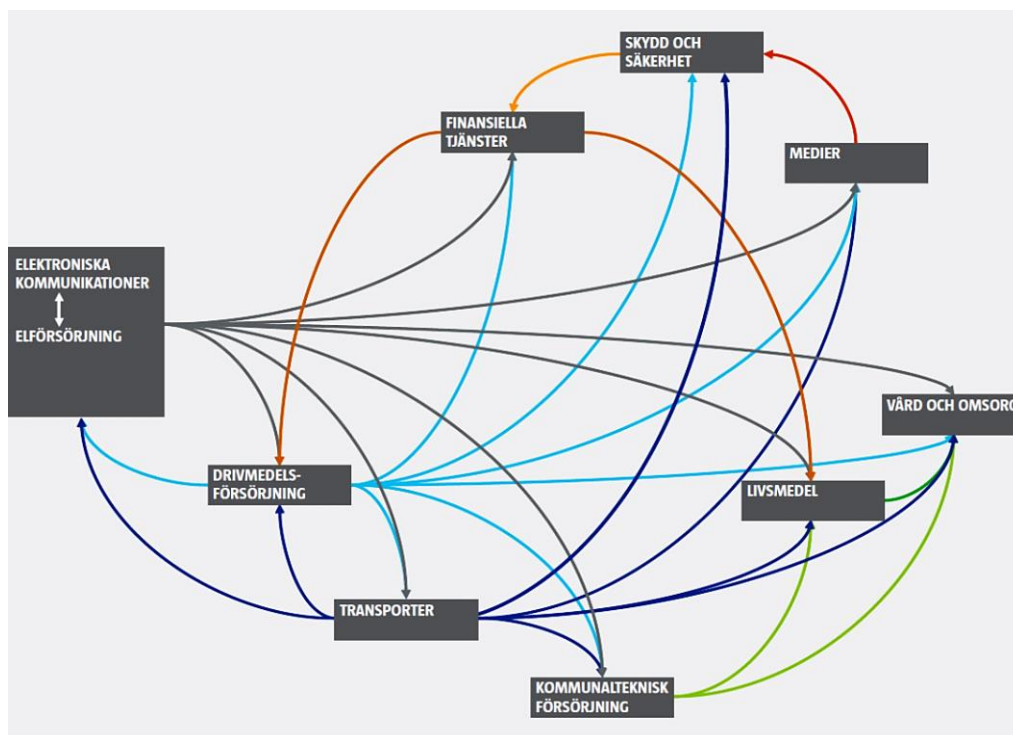
I de fall där utrustning har förstörts och komponenter måste ersättas är det viktigt att ha tillgång till reservkomponenter för att snabbt kunna återställa funktionen efter ett EM-angrepp. Reservdelar bör dock förvaras i förråd som inte enkelt kan utsättas för angrepp med EM-källor, eftersom även avstängd och förrådsställd elektronikutrustning kan skadas vid angrepp med kraftigare HPM-vapen.

5.3 Sektorsvisa beroenden

En särskild typ av konsekvenser är sådana som uppträder indirekt i helt andra system än det angripna. Sådana uppkommer oftast i kaskadeffekter, som när ett utslaget styr- och reglersystem i ett ställverk leder till att eldistributionen upphör inom ett visst geografiskt område, vilket i sin tur får konsekvenser för belysning, elektroniska passagesystem, trafikreglering, basstationer för mobil telefoni, m.m. Reservkraftförsörjning (batterier, dieselgeneratorer, ...) av dessa kan under en kortare period upprätthålla funktionen, men om funktionsbortfallet varar under en längre tid riskerar även reservkraften att upphöra.

Man bör vara särskilt uppmärksam på om en verksamhet är beroende av att ett visst kommunikationssystem fungerar eller om det är en verksamhet som inte kan upprätthållas vid ett avbrott i elförsörjningen. Speciellt gäller detta om det kritiska beroendet är av ett system som någon annan aktör hanterar, t.ex. inom en helt annan samhällssektor, eller om driften av detta sköts av en entreprenör.

Studier har visat att det moderna samhällets funktioner nästan undantagslöst är beroende av elektroniska kommunikationer och elförsörjning, dvs. praktiskt taget alla system är beroende av kontinuerlig tillgång på elektrisk energi för att driva datorer, kommunikations- och säkerhetssystem, och kommunikationssystem behövs för att hantera och distribuera samhällsresurser effektivt och rättvist [35, 36, 37]. Se Figur 22. I och med införandet av Internet of Things (IoT) kommer detta beroende att öka ytterligare inom en snar framtid.



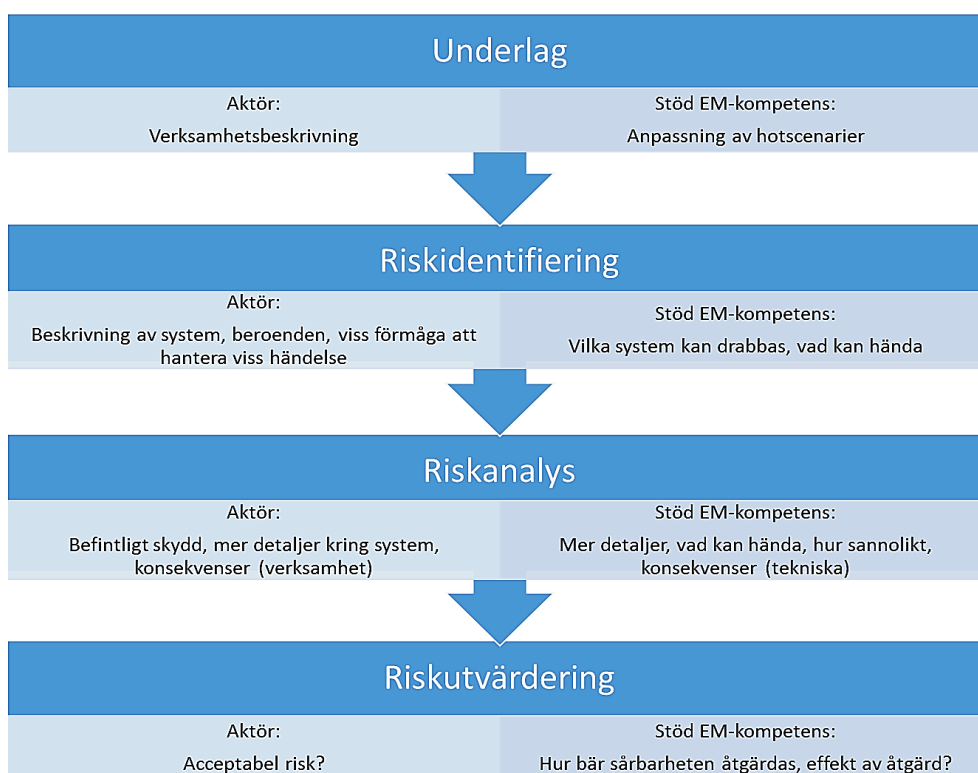
Figur 22. Illustration av beroenden mellan olika samhällssektorer. Notera det starka elberoendet. Bildkälla: "Faller en – faller då alla?", MSB [35].

6. Enkelt exempel på en RSA

En RSA avseende EM-hot kan ha följande huvudpunkter:

1. Presentation av hotscenario
2. Riskidentifiering – Tekniska konsekvenser
3. Riskanalys – Verksamhetskonsekvenser
4. Riskutvärdering
5. Sårbarhetsreducerande åtgärder

Eftersom avsiktliga EM-hot är av rent teknisk natur och slår mot tekniska apparater och system, ofta utan andra direkt märkbara effekter, kräver en sådan RSA tillgång till god teknisk systemkunskap. Det är alltså viktigt att ha med personal med goda tekniska systemkunskaper för att bedöma risker och konsekvenser. Det kan även vara bra att ha med personal som är beroende av att tekniska system fungerar för att få med användarperspektivet. Det kan dessutom behövas extern kunskap om aktuella EM-hot som kan uppträda, relevanta hotnivåer och ev. också förslag på möjliga skyddsåtgärder. Ett exempel på hur en systemansvarig samhällsaktör och ett externt stöd med EM-kompetens kan samverka i de olika stegen ges i Figur 23.



Figur 23. Förslag på hur deltagare med olika kompetenser kan delta i en RSA.

Eftersom en avsiktlig EM-attack inte är en slumpmässig händelse eller olycka kan det vara bra att arbeta utifrån ett hotscenario där en antagonist av någon anledning vill skada verksamheten. Där kan stödjande EM-kompetens bidra med en realistisk beskrivning av hur olika EM-hot skulle kunna användas i ett angrepp. För att hitta svagheter i en anläggning kan det många gånger vara bra att genomföra RSA:n på plats. Då kan man inspektera perimeterdistans och befintliga skalskydd, transientskydd, filter, etc.

Det kunde ibland vara önskvärt att kunna utsätta det analyserade systemet för skarpa tester med någon typ av störutrustning. Emellertid brukar man normalt inte göra provokationstester i samband med RSA:er. Det finns alltid en risk att man råkar störa andra verksamhetskritiska system än det man avser att testa. Dessutom är det i Sverige för de flesta aktörer inte tillåtet att inneha eller använda störsändare.

RSA:n leder vanligen fram till ett antal identifierade risker som i riskanalysen kvantifieras och rangordnas efter risknivå medan man i riskutvärderingen behandlar frågor om vilka risker som behöver prioriteras och vilka åtgärder som kan vara relevanta. Här kan stödjande EM-kompetens bidra med förslag på skärningsåtgärder och andra skyddsmetoder. Därefter är det upp till den systemansvariga aktören att hantera resultatet av RSA:n och gå vidare med sårbarhetsanalys samt vidta riskreducerande åtgärder.

En utförligare beskrivning av hur man kan genomföra en RSA avseende EM-hot och metodstöd med frågeformulär ges i "Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur" [2]. Mer generella aspekter på genomförande av en RSA finns i referenslistan [38,39,40, 41].

7. Att skydda skyddsvärd samhällsviktig verksamhet och kritisk infrastruktur

Det bästa och billigaste sättet att skydda kritisk utrustning är att kravställa den med avseende på EM-hot under anskaffningsförfarandet. Det är oftast mycket svårare och mer kostsamt att skydda redan befintliga system.

7.1 Kommunikation

Det bör eftersträvas att system som är vitala för verksamheten har en inbyggd resiliens och robusthet mot EM-hot. Detta kan realiseras genom redundans i systemet och att systemet är anpassat mot tillämpningen. Det gäller då speciellt störtålighet och funktionssäkerhet.

Att kunna byta frekvens vid störning eller att frekvenshoppa är ett skydd mot störningar på vissa frekvenser men kräver tillgång till ett större frekvensområde. För att minimera inverkan från andra oavsiktliga störningar bör man ha ett eget frekvensband.

En grundregel som minskar risken för störningar väsentligt är att inte använda sig av så kallade ISM-band (eng. Industrial, Scientific and Medical, ISM) för styrning och reglering av kritiska system. T.ex. ligger WiFi och Bluetooth på ett av ISM-banden (2,4 GHz) och dessa är lätta att störa ut då de använder mycket låg sändareffekt. Dessa kommunikationskanaler kan till och med störas ut av en mikrovågsugn, som använder den närliggande frekvensen 2,45 GHz för att värma mat. Om olicensierade frekvensband, som ISM-bandet, kan generellt sägas att på dessa band finns ingen garanti för att kommunikationen kommer att fungera.

Om det är möjligt att använda trådbunden kommunikation istället för t.ex. WiFi för kommunikation, styrning och reglering bör man göra det. Ytterligare ett steg mot att skydda kommunikation mellan enheter är att använda optofiber som är helt immun mot EM-hot. Behöver man ändå använda radiokommunikation mellan kritiska system kan man redan vid upphandling kravställa dessa med avseende på robusthet, störtålighet och redundans. Riktantenner på kommunikationssystemen gör att dessa behöver riktas in mot varandra och minskar störningskänsligheten då antennen inte i samma grad tar emot signaler som kommer från fel håll. Om det är möjligt med hänsyn till användningen bör man skydda information om vilka frekvenser ett visst system är beroende av.

En relativt enkel och genomförbar åtgärd är att kartlägga eller övervaka störningsmiljön för att upptäcka förekomsten av oavsiktlig eller avsiktlig störning. Det är viktigt att kommunikationssystemet redan initialt är dimensionerat för att erhålla en god tillgänglighet. Om systemet är väl

intrimmat och om oavsiktliga störningar är hanterade är systemet bättre rustat för att motstå avsiktligt störning.

7.2 Elektroniska system

Elektroniska system kan krävställas för att tåla en viss elektromagnetisk miljö och förses då med metalliska skal som skyddar elektroniken inuti genom att stoppa elektromagnetisk strålning från att nå innanför metallskalet. Även vanliga väggar i byggnader (betong, trä) ger en viss dämpning av elektromagnetisk strålning utifrån. Därför kan ett första steg vara att flytta känslig utrustning längre in i en byggnad så att den skyddas av flera väggar. Varje betongvägg ger ungefär samma riskreducering som att öka avståndet mellan hotet och den känsliga utrustningen med fyra gånger. Detta hjälper naturligtvis inte om vem som helst ändå kan komma nära eller till och med in i samma rum som den skyddsvärda utrustningen; därför kan det vara viktigt att begränsa tillgängligheten.

Nästa steg är att låta bygga ett skärmat rum dedicerat för kritisk elektronisk utrustning. Det finns ett flertal företag som tillhandahåller denna tjänst, som i princip går ut på att man bygger ett helt rum i plåt med dörrar som har elektromagnetiskt täta packningar så att rummet blir helt tätt mot elektromagnetisk strålning när dörrarna är stängda. Denna typ av skärmade rum kan också fås med speciella eluttag så att avsiktliga eller oavsiktliga störningar på elnätet inte kan skada utrustningen inuti det skärmade rummet.

Som redan nämnts avtar effekttätheten på elektromagnetiska strålning och därmed risken med kvadraten på avståndet så en fördubbling av avståndet mellan den kritiska utrustningen och en potentiell förövare/antagonist reducerar risken med en faktor fyra. Det är inte alltid enkelt att sätta upp staket eller andra perimeteravgränsningar runt anläggningar för att förhindra tillträde men i de fall detta går är det ofta mycket effektivt.

En mer omfattande genomgång av hur man kan gå till väga för att utvärdera och förbättra skydd mot EM-hot står att finna i Fortifikationsverkets publikation "Vägledning för skydd mot avsiktliga EM-hot" [3]. EMMA-handboken beskriver hur man kan arbeta systematiskt med elmiljöhot [4].

8. Slutord

Det är ingen trivial uppgift att skydda kritisk infrastruktur mot dagens moderna elektromagnetiska hot, särskilt inte om de används av en angripare med illvilliga avsikter. EM-attacker kan ses som en parallell till eller en förlängning av cyberattacker via internet, men där man inte bryr sig om att enbart korrumpiera information i samhällssystemen utan angriper hårdvaran som hanterar informationen, antingen genom att tillfälligt störa ut elektronikfunktioner eller genom att permanent förstöra elektroniska komponenter.

Det ständigt expanderande utbudet av störsändare som kan störa i allt fler frekvensband utgör ett allvarligt hot mot all verksamhet som är beroende av trådlös kommunikation. Att det är olagligt att importera, inneha och använda störsändare tycks inte avhålla kriminella eller aktivister från detta.

Utvecklingen av HPM-vapen för militärt bruk närmar sig tester på militära plattformar samtidigt som information sprids på internet om hur man kan bygga egna mikrovågskällor som kan störa eller förstöra elektronisk utrustning på kortare avstånd. Typiskt för HPM-källor är att de kan störa eller förstöra såväl kommunicerande som icke-kommunicerande elektronisk utrustning.

Första steget mot att kunna skydda samhällsviktig verksamhet och kritisk infrastruktur mot denna typ av nya avsiktliga hot är att bli medveten om deras existens och hur de skulle kunna användas av antagonister för att störa ut eller inkapacitera viktiga samhällssystem. Sedan behöver man genomföra en risk- och sårbarhetsanalys för egna kritiska system och åtgärda de risker som bedöms allvarliga. Det är dock viktigt att komma ihåg att risk- och sårbarhetsanalyser bör genomföras med vis regelbundenhet eftersom hoten och deras användning utvecklas.

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. ”Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, Myndigheten för samhällsskydd och beredskap (MSB), MSB1178 - februari 2018, ISBN 978-91-7383-803-0
3. ”Vägledning för skydd mot avsiktliga EM-hot”, Fortifikationsverket, 2017, ISBN 978-91-639-5650-8
4. ”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).
5. Ett fungerande samhälle i en föränderlig värld - Nationell strategi för skydd av samhällsviktig verksamhet, MSB266 - december 2011.
6. ”Åska och blixtdetektering”, Avdelningen för elektricitetslära, Uppsala Universitet, <http://www.hvi.uu.se/> (2017-12-18).
7. Mats Bäckström, ”Förstudie: Skydd mot elektromagnetiska risker. Geomagnetiskt inducerade strömmar (GIC)”, Combitech IK4-11:0092A, 2011-09-15.
8. International Electrotechnical Commission (IEC), <http://www.iec.ch/emc/> (2017-12-18).
9. 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/?qid=1516628345153&uri=CELEX:32014L0030> (2017-12-18)
10. Elsäkerhetsverkets föreskrifter om elektromagnetisk kompatibilitet, ELSÄK-FS 2016:3, konsoliderad version 2016-04-20.
11. Henrik Olsson, ”Reklamskyltars EMC-egenskaper, Risk för radiostörningar med LED”, Elsäkerhetsverket, Dnr 12EV3659 2012-11-16.
12. Henrik Olsson, ”Tillsynsbesök Eriksbergs shoppingcenter”, Elsäkerhetsverket, Dnr 14EV1335.

13. I. Wu, H. Ohta, K. Gotoh, S. Ishigami and Y. Matsumoto, "Characteristics of Radiation Noise from an LED Lamp and Its Effect on the BER Performance of an OFDM System for DTTB," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 56, no. 1, pp. 132-142, Feb. 2014.
14. <http://www.elsakerhetsverket.se/om-oss/press/nyheter/Forbjudna-LED-lampor/> (2017-12-18)
15. Rakel-störning, beräkning gjord vid FOI.
16. "Telekrig: Lärobok för Armén", Försvarsmakten 1997.
17. https://en.wikipedia.org/wiki/Starfish_Prime (2017-12-18)
18. Peter Stenumgaard, Radiostörningar – ett växande hot, FOI-R–3494--SE, oktober 2012.
19. <http://www.jammer4uk.com/> (2017-12-18)
20. http://diy.wikia.com/wiki/Cell_Phone_Jammer_DIY (2017-12-18)
21. Frank 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.
22. United States Department of Homeland Security, "The Threat of radio frequency weapons to critical infrastructure facilities", TSWG and DTEO Publication, August 2003.
23. 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.
24. Richard Hoad and Iain Sutherland, "The forensic utility on detecting disruptive electromagnetic interference", Proceedings of the 6th European Conference on Information Warfare and Security (ECIW 2007), July 2007.
25. FM MSD16, Militärstrategisk doktrin för Sveriges militära försvar, 2016.
26. "Russia's Hybrid War in Ukraine 'Is Working' ", Potomac foundation, February 26, 2015, <http://www.thepotomacfoundation.org/russias-hybrid-war-in-ukraine-is-working/> (2017-12-18)
27. "A Military Assessment of the Russian War in Ukarine", Stephen Blank, Testimony Presented to the Senate Foreign Relations Committee, Subcommittee on Europe and Regional Security Cooperation, March 4, 2015
28. "Russia's Hybrid War in Ukraine, Breaking the Enemy's Ability to Resist", FIIA report 43, Finnish Institute of International Affairs, 16 June 2015, ISBN 978-951-769-453-7, ISSN 2323-5454

29. Roger N. McDermott, "Russias Electronic Warfare Capabilities to 2015, Challenging NATO in the Electromagnetic Spectrum", International Centre for Defence and Security, Estonia, ISBN 978-9949-9972-0-6, 2017
30. "Tjuvarnas nya metod gör dyra larm värdelösa", Dagens Nyheter, 22 augusti 2012, <https://www.dn.se/nyheter/sverige/tjuvarnas-nya-metod-gor-dyra-larm-vardelosa/> (2017-12-18)
31. "Störningssändare slår ut villalarmen", Sveriges Television, 22 augusti 2012, <https://www.svt.se/nyheter/inrikes/storningssandare-slar-ut-villalarmen> (2017-12-18)
32. "Göteborgskravallerna", Wikipedia, 21 november 2017 kl. 21.22, <https://sv.wikipedia.org/w/index.php?title=Göteborgskravallerna&oldid=42135410> (2017-12-18)
33. "Riskanalys Mobiloperatörernas förändrade tekniska villkors påverkan på GSM-R", Trafikverket, TRV 2015/9709.
34. "Vägledning för samhällsviktig verksamhet – Att identifiera samhällsviktig verksamhet och kritiska beroenden samt bedöma acceptabel avbrottstid", MSB620 – januari 2014.
35. "Faller en - faller då alla?", MSB 0001-09, MSB 2009.
36. "Översiktlig risk- och sårbarhetsanalys över energisektorn i Sverige år 2012", Energimyndigheten, ER 2012:23, ISSN 1403-1892, november 2012.
37. Per Wikman-Svahn, Henrik Carlsen, "Energiomställningen och dess betydelse för samhällsskydd och beredskap", FOI Memo 4572, 2013-09-25.
38. "Vägledning för Risk- och sårbarhetsanalyser", Myndigheten för samhällsskydd och beredskap (MSB), MSB245 - april 2011, ISBN 978-91-7383-129-1.
39. "Riskhantering - Principer och riktlinjer", SIS Förlag AB, Svensk standard SS-ISO 31000:2009, publicerad 2010-03-30.
40. Magnus Winehav, Lena Molin, Ester Veibäck, Per Larsson, "Metod- och inventeringsstöd till sektorsövergripande risk- och sårbarhetsanalys", Totalförsvarets forskningsinstitut (FOI), FOI-R--3516--SE, 2012.
41. Magnus Winehav (red.), Björn Nevhage (red.), Jens Lusua, Jonas Clausen Mork, Johan Lindgren, Robert Erdeniz, "FOI:s modell för risk- och sårbarhetsanalys (FORSA)", Totalförsvarets forskningsinstitut (FOI), FOI-R--3288--SE, ISBN 978-91-7056-128-3, 2011.

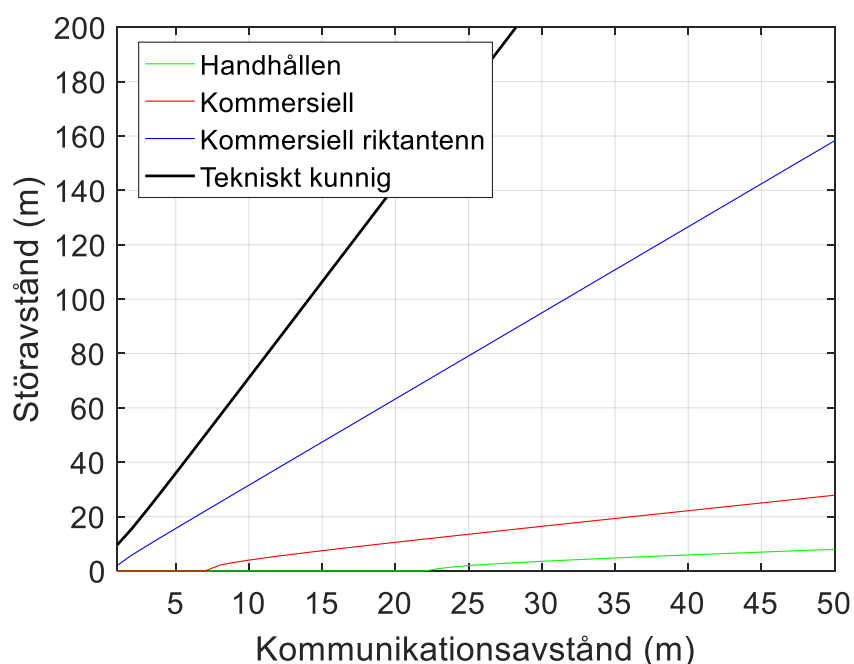
Bilaga: Avståndsberoenden

Störavstånd för avsiktlig störsändare

Vid störsändning mot ett kommunikationssystem är det flera ingående parametrar som avgör hur kommunikationssystemet påverkas. Några viktiga parametrar är avståndet mellan störare och radiomottagarens antenn, störarens uteffekt och antenn. Även kommunikationsavståndet har betydelse eftersom störsignalen måste överrösta kommunikationsavståndet, vilket är svårare för korta kommunikationsavstånd.

I Tabell 1, sidan 33, ges parametrar för några generella störsändare mot trådlösa kommunikationssystem. De tre första motsvarar störsändare som kan köpas på nätet, med lite olika funktionalitet och storlek. Störsändare kan även byggas av tekniskt kunniga med hjälp av generell hårdvara för radio och mjukvarublock som också finns tillgängliga och en effektförstärkare.

Figur 24 visar störavstånd för de olika störsändarna (som visas i Tabell 1) för olika kommunikationsavstånd. De olika systemens förmåga att störa ger olika avstånd och speciellt det handhållna systemet kräver att störaren måste komma mycket nära antennen för att kunna störa. Om systemet har tillgång till högre uteffekt eller riktantenn kan störavståndet vara större. Det betyder att störsändaren kan placera sig längre bort från kommunikationssystemet, men ändå störa ut systemet. För systemet byggt av en tekniskt kunnig person kan störavstånd på hundratals meter åstadkommas.



Figur 24. Störavstånd för olika typer av störsändare för olika kommunikationsavstånd.

Verkansavstånd för HPM-vapen

Nedan sammanfattas vilka verkansavstånd som kan förväntas från HPM-vapen med olika förmåga.

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 4 till Tabell 6 nedan framgår att verkan avtar hastigt med ökande avstånd och detta beror på att en fördubbling av avståndet minskar effekttätheten i målet med en faktor fyra ($\sim 1/r^4$, där r betecknar 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 i byggnader istället för nära fönster och entréer är också en relativt enkel metod som ger extra skydd, se Tabell 5. Slutligen visar Tabell 6 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.

Oskyddad civil elektronik

Tabell 4. 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 en vanlig byggnad.

Exempelvis ger ytterväggar av betong ungefärligen en dämpning på 10 dB dämpning, medan tegel ger en mycket liten dämpning.

Tabell 5. 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 6. Verkansavstånd för tre olika klasser av HPM-källor mot skärmad elektronik.

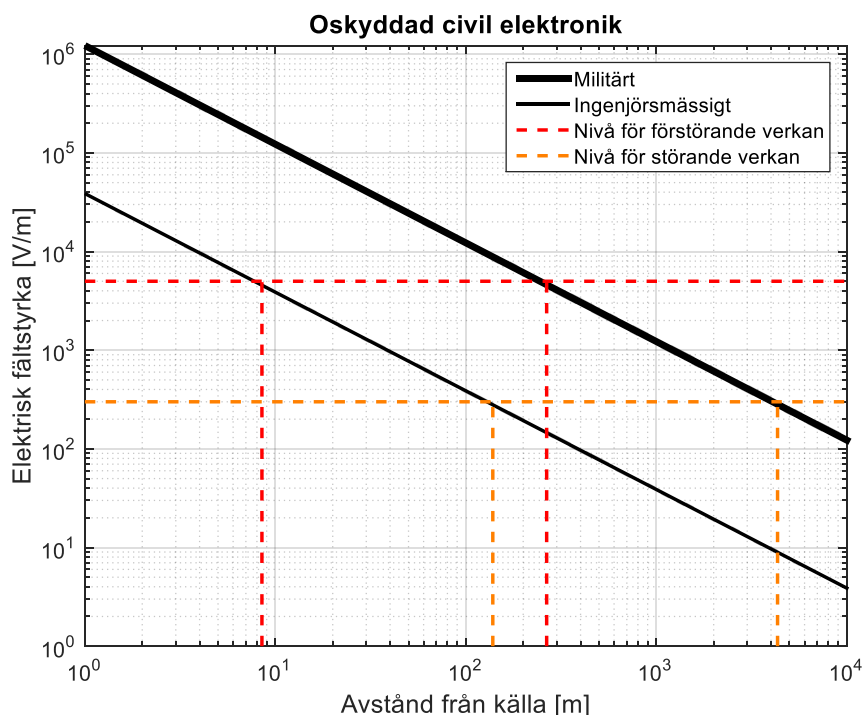
Typ av källa	Avstånd			
	Enstaka meter	15 meter	50 meter	500 meter
HPM-skåpbil (Militär utrustning)	Ej relevant	Permanent fysisk skada	Störning ^{1, 2/} skada	Störning ^{1, 2}
HPM-skåpbil (Ingenjörsmässig)	Ej relevant	Störning ^{1, 2/} skada	Ingen verkan ³	Ingen verkan ³
HPM-väska (kommersiell)	Störning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

¹ Kan orsaka kvardröjande felfunktion.

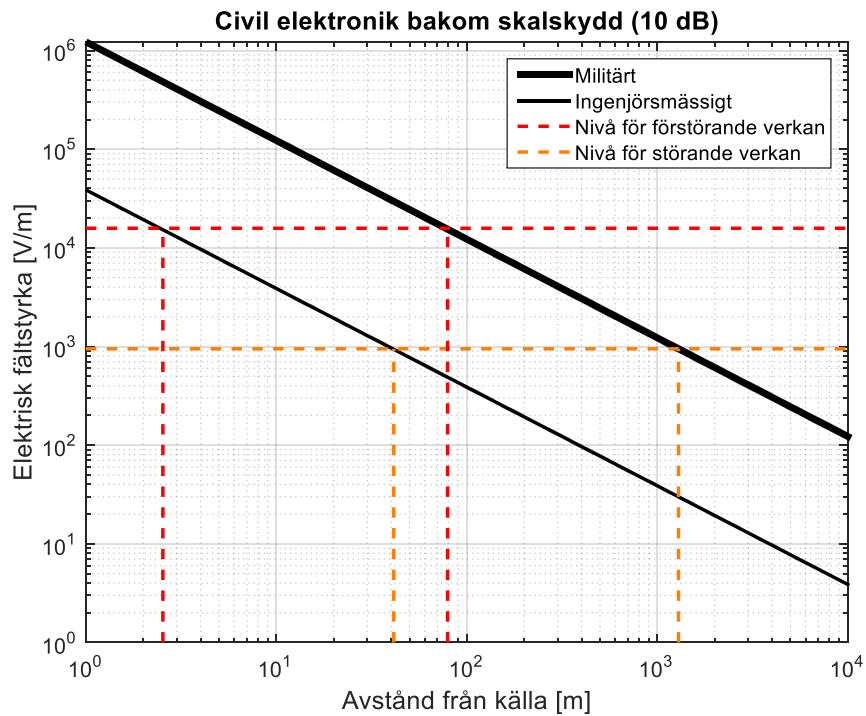
² Inombands framvägskoppling kan orsaka permanent skada på detta och större avstånd.

³ Inombands framvägskoppling kan ge störning på detta och större avstånd.

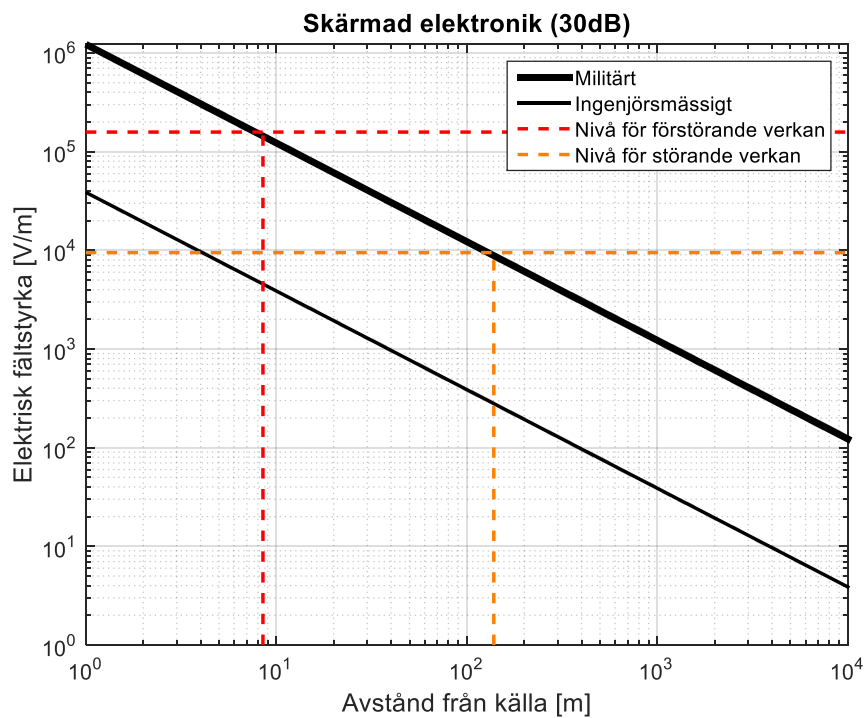
Som komplement till tabellerna med verkansavstånd för olika kategorier av HPM-källor visas i Figur 25 till Figur 27 nedan istället effekten av HPM-källor för ett varierbart avstånd.



Figur 25. Verkansavstånd för olika klasser av HPM-källor mot oskyddad civil elektronik.



Figur 26. Verkansavstånd för olika klasser av HPM-källor mot civil elektronik bakom skalskydd.



Figur 27. Verkansavstånd för olika klasser av HPM-källor mot skärmad elektronik.

Myndigheten för samhällsskydd och beredskap

651 81 Karlstad Tel 0771-240 240 www.msb.se

Publ.nr MSB1180 – februari 2018 ISBN 978-91-7383-805-4