Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

HANDBOK I KOMMUNAL KRISBEREDSKAP
4. RISKKATALOG

Elektromagnetiska hot

Handbok i kommunal krisberedskap – 4. Riskkatalog – Elektromagnetiska hot

Det här kapitlet är en del av publikationsserien *Handbok i kommunal krisberedskap* där fler kapitel finns.

© Myndigheten för samhällsskydd och beredskap (MSB)
Produktion: Advant

Publikationsnummer: MSB2029 - november 2022

Innehåll

Elektromagnetiska hot **4**
Om riskområdet 4
Kort om konsekvenser 6
Osäkerhetsbedömning 8
Utveckling och trender 8
Exempel på inträffade händelser 8
Löpande riskbedömningar 9
Ansvar och roller 9
Mer information om riskområdet 12

Elektromagnetiska hot

Som stöd till riskkatalogen finns en användarguide som beskriver syftet med riskkatalogen och förklaringar till den information som finns i respektive kapitel. MSB kommer att komplettera riskkatalogen med ett dokument av generell karaktär som är relevant för flera olika riskområden.

Om riskområdet

Elektromagnetiska hot (EM-hot) utgörs av elektriska och/eller magnetiska fält som är tillräckligt starka för att kunna påverka elektriska/elektroniska apparater och system. Det civila samhället är beroende av ett flertal system som innehåller elektronisk utrustning för bland annat styrning, kontroll, övervakning, och kommunikation. Dessa kan påverkas av elektromagnetiska hot, antingen av naturligt förekommande fenomen eller som genereras av människor oavsiktligt, exempelvis av elektromagnetiska fält skapat av felaktigt fungerande utrustning, eller avsiktligt, genom angrepp med exempelvis störsändare eller vapen som avger elektromagnetiska pulser.

Avsiktliga elektromagnetiska hot kan beskrivas som generering av skadlig elektromagnetisk energi i syfte att införa brus eller signaler som har tillräckligt hög nivå för att störa eller skada elektriska och elektroniska system. Potentiella antagonister som kan tänkas använda sig av elektromagnetiska vapen för att uppnå olika syften varierar mellan allt från 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. Avsiktlig elektromagnetisk påverkan genom nyttjande av dessa vapen brukar sammanfattas under benämningen avsiktlig elektromagnetisk interferens (Intentional Electromagnetic Interference (IEMI)). Även teknikintresserade som konstruerar och testar enkla störkällor kan påverka och störa elektronisk utrustning både avsiktligt och oavsiktligt.

I militära konflikter används begreppet telekrigsangrepp för att beskriva när elektromagnetisk energi används för att nedsätta eller förstöra motståndarens systemfunktioner och stridsförmåga. FOI har mer information om telekrig på sin webbplats. Genom att nyttja telekrigsystem kan en antagonist vinna fördelar avseende möjligheten att upptäcka, positionera, analysera, blockera eller vilseleda sin motståndares radio- eller radarsystem.

Läs mer

MSB har samlat relevant information och fördjupningsmaterial på sin webbplats. Som fördjupningsmaterialet finns en introduktion till elektromagnetiska hot som är avsedd att användas som bakgrundsmaterial för risk- och sårbarhetsanalyser (RSA) som innefattar elektromagnetiska hot mot samhällsviktig infrastruktur. Det finns också två vägledningar, en med metodik och stödjande underlag för att genomföra en risk- och sårbarhetsanalys avseende elektromagnetiska hot, och en för hur en organisation kan hantera en pågående incident med elektromagnetiska hot och vilka åtgärder som kan vidtas för att förhindra liknande incidenter.

→ Elektromagnetiska hot (msb.se)

Till ovan nämnda introduktion finns också ett faktablad som syftar till att kort presentera vad avsiktliga elektromagnetiska hot är och hur antagonistiska aktörer skulle kunna använda dessa vid attacker mot anläggningar och system.

→ Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur (msb.se)

Totalförsvarets forskningsinstitut (FOI) har på uppdrag av MSB redovisat två pilotstudier av elektromagnetiska hot mot samhällsviktig verksamhet i samband med höjd beredskap. Studien ska vara vägledande för organisationer som avser att genomföra en risk- och sårbarhetsanalys rörande elektromagnetiska hot mot sin verksamhet.

→ Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur (msb.se)

FOI har mer information om telekrig på sin webbplats.

→ Telekrig (foi.se)

→ Antagonistiska elektromagnetiska hot mot det civila försvaret (foi.se)

Kort om konsekvenser

Incidenter till följd av elektromagnetiska hot kan till exempel yttra sig som störningar i trådlös kommunikation mellan it-system, i mobiltelefonsystem, eller att datorer och annan elektronik beter sig felaktigt eller helt slutar fungera. Konsekvenserna av ett elektromagnetiskt hot är i de flesta fall avgränsade till ett begränsat geografiskt område eller till vissa funktioner. Svagare elektromagnetiska hot åstadkommer störningar som pågår under den tid som störfälten genereras, medan kraftigare elektromagnetiska hot kan åstadkomma fysisk skada som kvarstår i elektroniken efter att hotet har upphört.

Elektromagnetiska hot kan vara elektromagnetiska vågor eller fält som varierar i styrka och/eller riktning, mer eller mindre snabbt. Om störningarnas frekvens ligger inom det frekvensområde som apparaten använder (till exempel 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 elektromagnetiska hoten kan till och med påverka och skada utrustning som är avslagen eller förrådsställd.

Vid ett elektromagnetiskt angrepp genererar en antagonist avsiktligt elektromagnetisk strålning i syfte att störa, vilseleda eller förstöra elektronisk utrustning. Källan som genererar det störande fältet utgör då ett elektromagnetiskt hot för den påverkade utrustningen. Kraftiga elektromagnetiska fält kan generera så kraftiga strömmar i den apparat som utsatts att komponenter i apparaten bränns sönder, vilket leder till permanent fysisk skada. 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.

Högfrekventa elektromagnetiska pulser genereras av för syftet byggd utrustning, även kallade High Power Microwave (HPM). Militära HPM-vapen är mycket kraftfulla och kan förstöra oskyddad elektronisk utrustning på flera kilometers avstånd. Denna typ av vapen är dock mycket komplicerade och dyra konstruktioner. Sannolikt har inte kriminella eller terrororganisationer tillgång till dem, däremot syns ett ökande intresse på internet och sociala medier för enklare konstruktioner med kortare räckvidd som då kan störa utrustning på några tiotals meter. Detta är en av anledningarna till varför det är viktigt att säkerställa att en antagonist inte kan parkera sin bil precis i närheten av det som ska skyddas. Fysiskt avstånd är också en skyddsmekanism för HPM.

Elsäkerhetsverket och Försvarsmakten redovisade i december år 2020 en utredning av elektromagnetiska störningar på totalförsvarets verksamheter.[1] Inom ramen för uppdraget analyserades bland annat att risken för att elektromagnetiska störningar påtagligt kan försvåra tillkomsten eller nyttjandet av totalförsvarets anläggningar eller på annat sätt vara oförenliga med riksintresset för totalförsvaret. Försvarets materielverk (FMV), FOI och Elsäkerhetsverket genomförde mätningar och analyser av solcellsanläggningar, elvägar och trådlös laddning av elfordon och klarlade att dessa oavsiktligt kan störa militära frekvenser, flygradio, Rakel, mobiltelefoni, signalspaning, tv samt riks- och lokalradio. Dessa typer av störningar kan försvåra verksamheten för totalförsvarets anläggningar, men kan även ha negativa effekter på civila flygplatser, räddningstjänst och samhället i stort.

Läs mer

→ Solceller kan störa ut flygradio, Rakel, radio och signalspaning (forsvarsmakten.se)

1. Finansdepartementet. (2020). *Uppdrag till Elsäkerhetsverket och Försvarsmakten att utreda elektromagnetiska störningar på totalförsvarets verksamheter*. Fi2020/02994/SPN.

Punktvisa elektromagnetiska angrepp kan slå ut samhällsviktig verksamhet som flera länder är beroende av (exempelvis elproduktion och -distribution) medan angrepp som täcker stora geografiska områden kan drabba flera länder. Ett exempel på gränsöverskridande konsekvenser är störsändningar som stör ut mottagningen av Global Navigation Satellite System (GNSS) över stora arealer vilket tvingar flygplan och fartyg till att förlita sig på alternativ navigerings- och positioneringsmetod. En variant av detta är så kallad spoofing, där i stället för att överrösta satellitsignalerna med brus genereras en egen starkare signal i syfte att lura fartyg eller flygplan att räkna ut en felaktig position. Även väldigt små störsändare (till exempel sådana som kan drivas av ett fordons cigarettändaruttag eller USB-port) kan enkelt störa ut Global Positioning System (GPS) inom ett begränsat geografiskt område. Kompakta störsändare för mobiltelefoni, men med en begränsad geografisk störning, går att exempelvis beställa på internet.

Läs mer

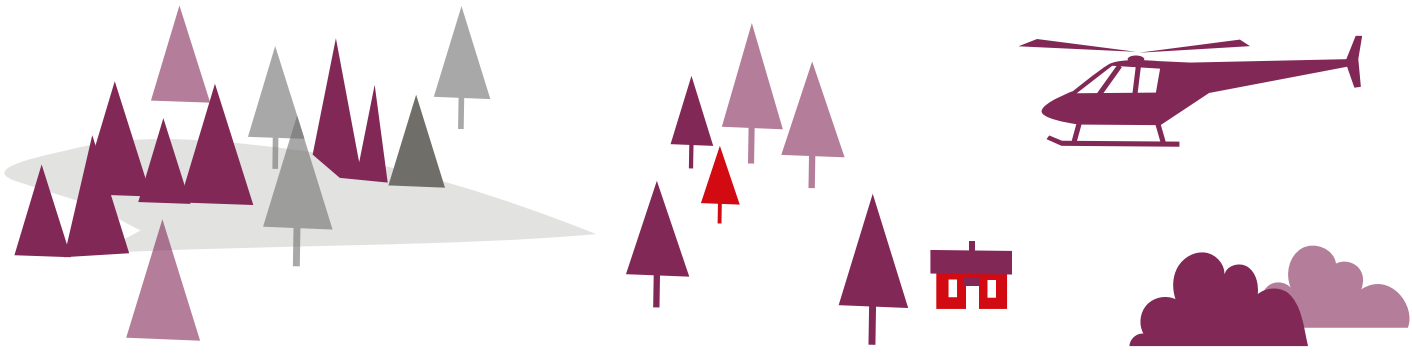
Som komplement till vägledningen för hur en pågående incident med elektromagnetiska hot kan hanteras och vilka åtgärder som kan vidtas för att förhindra liknande incidenter redogör detta FOI Memo för ett antal generella åtgärdspunkter före, under och efter en incident för att underlätta analys av förloppet och eventuell identifiering av förövare.

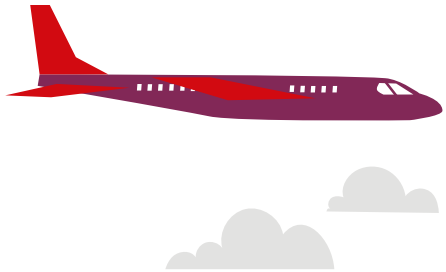
→ Incidenthantering av elektromagnetiska hot mot samhällsviktiga tjänster (msb.se)

I materialet nedan finns två tabeller som visar störavstånd för kommersiella störsändare och verkansavstånd för mikrovågsvapen.

→ Elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur – Störsändare och mikrovågsvapen (msb.se)

Förstudien innehåller exempelscenarier som illustrerar spännvidden bland tänkbara elektromagnetiska hot. Konsekvensbeskrivningarna i scenarierna illustrerar hur och under hur lång tid den skyddsvärda utrustningen påverkas negativt av det elektromagnetiska hotet, vilka återställningsåtgärder som behövs, samt tänkbara följdeffekter. Notera dock att det är respektive myndighet, region, kommun, et cetera som bäst kan avgöra de samhälleliga konsekvenserna av en genomförd elektromagnetisk attack mot egna system. Detaljerna i dessa exempelscenarier är inte slutgiltiga utan ska endast ses som exempel. Tänkbara variationer kan fås för olika antagonister, situationer eller samtidig förekomst av andra typer av attacker. Förstudie om risk- och sårbarhetsanalys avseende elektromagnetiska hot mot samhällsviktig infrastruktur (msb.se)





Osäkerhetsbedömning

Elektromagnetiska hot är att anse som relativt nya företeelser, kunskap om hoten är därmed relativt låg i jämförelse med andra hot. Det kan vara svårt att upptäcka ett elektromagnetiskt hot överhuvudtaget och det är i allmänhet svårt att identifiera och härleda exempel på incidenter. Låg medvetandegrad och okunskap gör det mer sannolikt att det tar ett tag innan en verksamhet uppmärksammar och kan konstatera att det rör sig om ett avsiktligt elektromagnetisk angrepp, snarare än till exempel en oavsiktlig driftstörning eller mjukvaruproblem. Elektromagnetiska hot konvergerar dessutom med och slår mot samma förmågor som cyberhot. Skillnaden är primärt att där den ena påverkar mjukvaran påverkar den andra hårdvaran som mjukvaran körs på (eller den trådlösa kommunikationen mellan it-system), och kan till skillnad mot (de flesta) mjukvaruattacker ge bestående men i form av förstörd utrustning.

Utveckling och trender

Det finns svårigheter med att bedöma en framtida utveckling inom riskområdet men ett par trender går att skönja. På internet finns redan idag såväl instruktioner för att bygga HPM-vapen som ett stort utbud av färdiga störsändare att köpa. Tillgängligheten på såväl information som produkter kommer sannolikt att öka. Sårbarheten för elektromagnetiska angrepp ökar då alltfler tjänster och produkter är beroende av trådlös kommunikation, exempelvis införande av 5G och utveckling av sakernas internet.

Exempel på inträffade händelser

Incidenter med GPS spoofing har skett i farvatten utanför Kina, där fartygen med vilseledande sändningar luras att tro att de befinner sig på annan position. Liknande har även skett i Svarta havet liksom i Nordkalotten, vilket lett till att norska och finska flygplan fått fel position, och i Mellanöstern runt Syrien som bland annat under veckolånga perioder drabbat flygplan som startar eller landar i på flygplatsen Ben Gurion (Israel) och i Larnaca (Cypern).

En telefonväxel i Ryssland slutade fungera till följd av en direktinjektion av spänning in i en telefonledning. Omkring 200 000 abonnenter tappade telefonförbindelse under en dag.[2]

Under sent 1980-tal exploderade en gasledning i Holland. En fartygsradar (i hamnen Den Helder) cirka 1.5 kilometer från styrsystemet (SCADA) fick det att öppna och stänga en ventil i samma takt som radarns svepperiod (6–12 varv per minut (RPM)) vilket ledde till tryckökning, läckage och slutligen explosion.[3]

Läs mer

FOI har på uppdrag av MSB genomfört en studie i syfte att utgöra ett stöd i arbetet med att höja det nationella medvetandet om elektromagnetiska hot mot cyberfysiska system. En del i denna studie var att inventera exempel på incidenter i Sverige.

→ NCS3 – Elektromagnetiska hot mot trådlösa system (msb.se)

MSB beskriver på sin webbplats vad cyberfysiska system är. De förklaras som datorbaserade system för interaktion med maskiner, fordon och annan utrustning, inklusive sensorer som kan inhämta data från omgivningen. I underlaget lyfts bland annat fram hur dessa kan styras.

→ Säkerhet i cyberfysiska system (msb.se)

2. Oakes, Benjamin Donald. (2017). *Risk Analysis of Intentional Electromagnetic Interference on Critical Infrastructures*, s. 3. Licentiate Thesis in Risk and Safety KTH Royal Institute of Technology Stockholm, Sweden. ISBN 978-91-7729-321-7.

3. US Department of Defence. (2005). *The Threat of Radio Frequency Weapons to Critical Infrastructure Facilities*, s. 7. Hämtad 2022-07-15: https://www.hsdl.org/?abstract&did=459435.

Löpande riskbedömningar

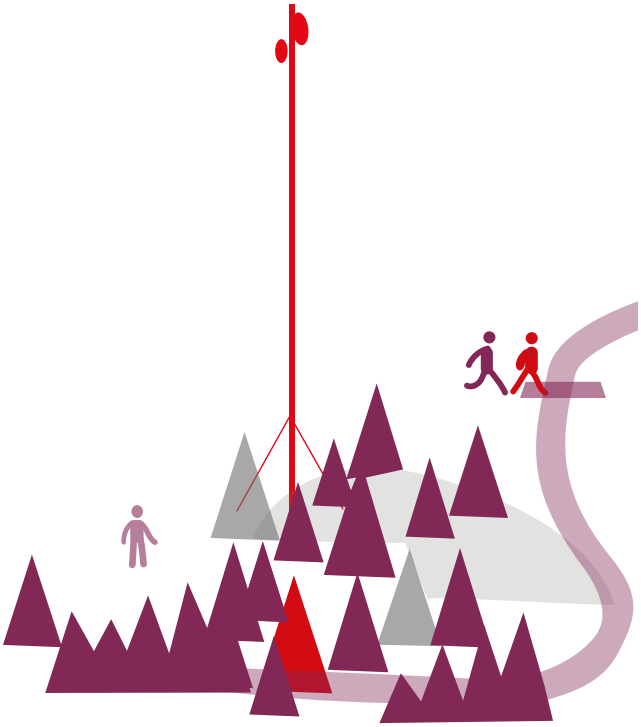
Centrala Beredningsgruppen Elektromagnetiska Hot (CBG EM-hot) är ett forum för informationsspridning och samverkan om elektromagnetiska effekter mellan statliga myndigheter och bolag. Forumet bedömer och värderar elektromagnetiska hot och dess konsekvenser på samhällsviktiga system och anläggningar samt utarbetar rekommendationer och råd. Forumets fokusområden innefattar elektromagnetisk puls, High Power Microwaves och andra elektromagnetiska hot, bland annat störsändare.

Läs mer

→ Centrala Beredningsgruppen Elektromagnetiska Hot (CBG EM-hot): forum för informationsspridning och samverkan om EM effekter (msb.se)

Se även

→ Handbok i kommunal krisberedskap – Åska och blixtnedslag (msb.se)



Ansvar och roller

Ansvaret för att förebygga, förbereda och hantera konsekvenserna på viktiga samhällsfunktioner av elektromagnetiska hot faller på ansvariga för respektive verksamhet som kan drabbas. Det innebär att ett stort antal aktörer på lokal, regional och nationell nivå har olika ansvar, roller och funktioner i händelse av elektromagnetiska hot. Nedan beskrivs övergripande några av de aktörer som kan komma att bli involverade i händelse av elektromagnetiska hot.

Läs mer

Om din organisation råkat ut för en incident eller störning vilken påverkar funktion hos för samhället viktiga system ska detta rapporteras till relevant myndighet. Genom rapportering kan berörda myndigheter stödja hantering av störning, samt upprätta en lägesbild kring såväl it-incidenter som störningar orsakade av elektromagnetiska fenomen.

→ Elektromagnetiska hot – Information om kontaktytor för incidentrapportering (msb.se)

Elsäkerhetsverket

Elsäkerhetsverkets uppdrag är att arbeta för hög elsäkerhet och för att elektriska utrustningar inte ska störa varandra. De ska förebygga skador orsakade av elektricitet på person och egendom samt störningar på radiokommunikation och näringsverksamhet inom området elektromagnetisk kompatibilitet. Elsäkerhetsverket utreder störningar orsakade av elektrisk utrustning.

Fortifikationsverket

Skydd mot avsiktliga elektromagnetiska hot kan bland annat bestå av att skydda elektriska ledare med transientskydd och filter, genom att skapa avstånd från säkerhetshotet eller att avskärma skyddsvärda system från elektromagnetiska signaler. Fortifikationsverket publicerar vägledningar hur system tekniskt kan skyddas mot elektromagnetiska hot. Vägledningarna beställs direkt av Fortifikationsverket.

Kommunen

Kommunerna har ett ansvar för att minska riskerna för störningar i sin kommunikations- och it-utrustning (till exempel datahallar). Om det ändå inträffar störningar bör kommunen ha lösningar för reservsamband (såsom till exempel Rakel och kortvågsradio) för att upprätthålla bland annat intern kommunikation, krisledning och kriskommunikation. Kommunen bör även ha nödrutiner för att upprätthålla verksamhetskritiska it-resurser (såsom patientjournaler). Olika verksamheter bör även bedöma var det är viktigt att säkerställa snabb service och tillgång till reservdelar.

Se även

→ Handbok i kommunal krisberedskap – Elektroniska kommunikationer (msb.se)

→ Handbok i kommunal krisberedskap – it (msb.se)

Myndigheten för samhällsskydd och beredskap

MSB är huvudman för Centrala Beredningsgruppen Elektromagnetiska Hot. MSB:s uppgifter inom informationssäkerhet, cybersäkerhet och säkra kommunikationer är bland annat att ansvara för utveckling och förvaltning av säkra kommunikationer, vara råd- och stödgivande i informationssäkerhetsarbetet och hantera samt förebygga it-incidenter vilket inkluderar elektromagnetiska hot.

Läs mer

→ Incidentrapportering för leverantörer av samhällsviktiga tjänster (msb.se)

→ It-incidentrapportering för statliga myndigheter (msb.se)

→ Frivillig incidentrapportering (msb.se)

MSB stödjer utveckling av ledningsplatser genom rådgivning och delfinansiering. Ledningsplatsen bör ges skydd mot elektromagnetiska störningar och hot som exempelvis störsändare, elektromagnetisk puls från kärnvapen (EMP) och mikrovågsvapen (HPM). MSB har tagit fram vägledning för ledningsplatser som innehåller information för att bygga säkra installationer.

Läs mer

→ Vägledning för ledningsplatser (msb.se)

Polismyndigheten

Polismyndigheten hanterar akuta situationer vid pågående antagonistiska handlingar såsom elektromagnetiska hot.

Post- och telestyrelsen

PTS bevakar områdena elektronisk kommunikation och post i Sverige. Begreppet elektronisk kommunikation rymmer telekommunikationer, it och radio. PTS utreder störningar i telefoni och radiokommunikation.

Säkerhetspolisen

Säkerhetspolisen utövar tillsyn över säkerhetsskyddet hos ett flertal myndigheter enligt säkerhetsskyddsförordningen (SFS 2021:955). Försvarsmakten är tillsynsmyndighet för vissa verksamheter. Dessutom har ett antal länsstyrelser och sektorsmyndigheter ett tillsynsansvar för regioner, kommuner och enskilda verksamheter.

Säkerhetspolisen inriktar själv sin tillsynsverksamhet och prioriterar då de mest skyddsvärda verksamheterna i samhället. Det innebär att kontrollerna främst är inriktade på de verksamheter där konsekvenserna av en antagonistisk handling eller röjande av säkerhetsskyddsklassificerade uppgifter skulle vara allvarligast för Sverige som nation. Efter tillsynen sammanställer Säkerhetspolisen en rapport med brister i säkerhetsskyddet som verksamhetsutövaren behöver åtgärda.

Säkerhetspolisen ger också löpande vägledning till de mest skyddsvärda verksamheterna för att förbättra säkerhetsskyddet i samhället.

Säkerhetspolisen tillhandahåller relevant hotinformation till de tillsynsmyndigheter som har ett särskilt tillsynsansvar för olika samhällssektorer, och i vissa fall direkt till de verksamhetsutövare som står direkt under Säkerhetspolisens tillsyn. Vidare tillhandahåller Säkerhetspolisen, såvida det inte i enskilt fall bedöms olämpligt, beskrivningar av dimensionerande antagonistiska förmågor (DAF) till verksamhetsutövare. DAF utgör ett underlag för att långsiktigt dimensionera säkerhetsskyddet, främst i fråga om fysisk säkerhet men även skydd mot röjande signaler (RÖS).

Läs mer

→ Säkerhetsskydd (sakerhetspolisen.se)

→ Vägledningar säkerhetsskydd (sakerhetspolisen.se)

Mer information om riskområdet

MSB har tagit fram en webbkurs som ger en introduktion till elektromagnetiska hot i syfte att sprida kunskap och medvetenhet till berörda aktörer inom området och öka medvetenheten hos de som ansvarar för system som kan påverkas. Webbkursen ger förutsättningar att bli medveten om elektromagnetiska hot samt tänkbara konsekvenser av angrepp. Vidare finns även råd och stöd för hur organisationer kan arbeta för att skydda sin verksamhet mot elektromagnetiska hot.

→ Elektromagnetiska hot – en introduktion (msb.se)

MSB har publicerat ett faktablad på engelska som omnämner ett par exempel på riskreducerande åtgärder.

→ Recent activities in Sweden to counter antagonistic electromagnetic threats: The electromagnetic threat (msb.se)

Förklaringar till olika begrepp

Bakvägskoppling

Den elektromagnetiska strålningen tar sig in i en utrustning via skarvar i ett apparathölje eller via komponenter som inte är avsedda att ta emot elektromagnetisk energi, till exempel genom att strålningen inducerar kraftiga strömmar i kablar eller kretskortsbanor, et cetera.

Elektromagnetisk interferens (EMI)

En apparat stör en annan, oftast oavsiktligt.

Elektromagnetisk kompatibilitet (EMC)

Ett tillstånd där olika utrustningar kan fungera tillsammans utan att påverka varandra negativt eller störa varandra. Elektromagnetisk kompatibilitet är ett kvalitetsbegrepp precis som driftsäkerhet, prestanda eller andra krav som ställs på en produkt. Elektromagnetisk kompatibilitet är ett krav reglerat i lag (1992:1512) om elektromagnetisk kompatibilitet med tillhörande förordning (2016:363) om elektromagnetisk kompatibilitet och föreskrifter (2016:3) om elektromagnetisk kompatibilitet från Elsäkerhetsverket.

Elektromagnetisk puls (EMP)

Avser oftast den bredbandiga energirika radiopuls som kan genereras vid en kärnvapendetonation. Pulser som genereras med ”vanlig” utrustning brukar vanligtvis benämnas som High Power Microwave (HPM).[4]

Det finns både konstgjord och naturlig EMP, olika skyddskomponenter krävs beroende på vad skyddet avser.

Konstgjord EMP

- **NEMP** – kärnvapen detonation (Nuclear EMP)
  - **LEMP** – kärnvapen detonation på låg höjd (Low altitude EMP)
  - **HEMP** – kärnvapen detonation på hög höjd (High altitude EMP)
  - **NNEMP** – syntetisk EMP (Non-Nuclear EMP), att genererar en EMP-puls på annat sätt än via kärnvapendetonation.

Naturlig EMP

- **LEMP** – EMP skapad av blixtar (Lightning induced EMP)
- **CME** – solstormar (Coronal mass ejection)

Elektrostatisk urladdning (ESD)

Elektriskt överslag på grund av stor spänningsskillnad mellan två föremål eller dylikt.

Framvägskoppling

Den elektromagnetiska strålningen tar sig in i en utrustning via antenner eller andra sensorer som är avsedda att ta emot elektromagnetisk energi från omgivningen.

Högeffekts mikrovågor eller högfrekventa elektromagnetiska pulser (HPM)

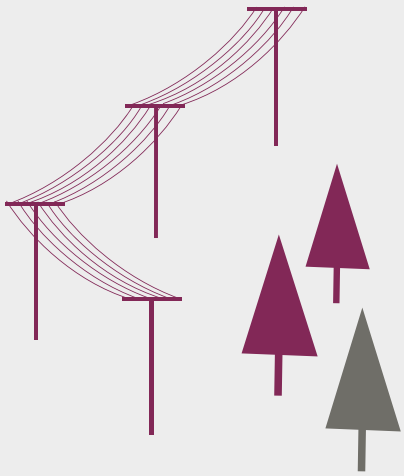
Radiostrålning som oftast består av korta pulser med hög effekt. Kan användas för att påverka eller skada elektronik på avstånd genom att inducera spänningar/strömmar i ledare eller andra komponenter.

Intentional Electromagnetic Interference (IEMI)

Avsiktlig elektromagnetisk påverkan som utförs av en antagonist.

Vilseledning, så kallad spoofing

Sändning av förfalskade positions- och tidssignaler, så kallad spoofing med syftet att få en eller flera GNSS-mottagare att beräkna en felaktig positions- eller tidsuppgift. Då tror användaren sig vara på ett annat ställe än var han eller hon verkligen är, eller det kan betyda att ett datasystem som använder en tidssignal fungerar fel.



4. Notera att det finns viss begreppsförvirring kring termen elektromagnetisk puls (EMP). EMP har kommit att bli synonym med den (de) mycket kraftiga radiopulser som genereras vid en kärnvapendetonation på hög höjd och som kan påverka/förstöra oskyddad elektronik över mycket stora geografiska områden. Pulser som genereras med ”vanlig” utrustning brukar vanligtvis benämnas som High Power Microwave (HPM).

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

Sveriges Kommuner och Regioner

© Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB2029 - november 2022