Myndigheten för samhällsskydd och beredskap

FOI

Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur

Bildkälla: MSBs bildarkiv

Bildkälla: Stefan Holm/Mostphotos/Trafikverkets bildarkiv

Faktaruta

Redovisande rapport om genomförandet av huvudstudie RSA EM-hot. Arbetet har genomförts på uppdrag av och med stöd av MSB.

2017

Totalförsvarets forskningsinstitut, FOI

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

Många samhällsviktiga verksamheter förlitar sig idag på elektroniska system och trådlösa kommunikationssystem. Eftersom dessa kan vara mycket känsliga för elektromagnetisk (EM) påverkan, utgör avsiktliga EM-störningar ett reellt hot mot samhällsviktig verksamhet. Denna rapport redovisar arbetet med två pilotstudier för risk- och sårbarhetsanalyser av två olika elektronikberoende samhällsviktiga verksamheter utsatta för EM-hot i samband med höjd beredskap.
I arbetet har typscenarier med realistiska EM-hot anpassats till analyserade samhällsviktiga verksamheter. Rapporten beskriver även arbete med framtagning av ett medvetandehöjande utbildningsmaterial inom området avsiktliga EM-hot.

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

Publikationsnummer MSB1179 – februari 2018
ISBN 978-91-7383-804-7

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

Förord

Denna rapport sammanfattar genomfört arbetet inom Huvudstudie Risk- och Sårbarhetsanalys Elektromagnetiska Hot (RSA EM-hot) under hösten 2017. Huvudstudien, som baserades på resultatet av en förstudie RSA EM-hot som FOI genomförde hösten 2016, innefattade vidareutveckling av metodiken för RSA EM-hot, genomförande av två pilotstudier hos två olika statliga aktörer, samt framtagning av ett vägledande material för organisationer som avser att genomföra en RSA rörande EM-hot mot sin verksamhet. Dessutom har ett medvetandehöjande utbildningsmaterial om EM-hot tagits fram för att kunna användas som underlag för informationsspridning om avsiktliga EM-hot.

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

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

Innehållsförteckning

Sammanfattning

Två genomförda pilotstudier av hur en RSA för EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur kan effektueras har visat att det finns några aspekter som är speciella just för elektromagnetisk påverkan. Det rör främst förståelsen av vad som kan vara ett EM-hot och hur detta kan uppträda vid en antagonistisk attack på samhällsviktig verksamhet och kritisk infrastruktur. För att hantera detta behövs det ett framtaget realistiskt hotscenario, anpassat till den studerade samhällsviktiga verksamheten, med användning av EM-hot som en del i ett mera omfattande angrepp. För att åstadkomma detta behövs ett förmöte mellan samhällsaktör och experter på EM-hot, som kan anpassa scenariot till den studerade verksamheten.

Bland viktiga slutsatser som framkommit är att det kan behövas flera olika kompetenser för att bedöma effekterna av en EM-attack på samhällsviktig verksamhet och kritisk infrastruktur, dels eftersom dessa kan vara komplexa och beroende av andra system, dels eftersom konsekvenserna av en störning kan gå utanför rent tekniska och behöva bedömas av beslutsfattare, entreprenörer, operativa användare, etc.

Det finns flera olika antagonister som kan tänkas använda EM-hot på olika sätt och med olika syften. Gemensamt för de flesta är att EM-hot kan användas tillsammans med andra typer av hot för att uppnå vissa syften. EM-hot kan nyttjas för att forcera larm och säkerhetssystem, för att förhindra betalningar, för att skära av kommunikation mellan en sambandscentral och enheter ute på fältet, eller för att stoppa flödet i samhällsinfrastruktur, som t.ex. trafiken.

En RSA för EM-hot ska kunna göras som en del av en övergripande RSA för en samhällsviktig verksamhet, men kan kräva expertstöd för genomförandet.

Det medvetandehöjande utbildningsmaterialet och vägledningen för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot finns publicerade som separata skrifter.

1. Inledning

1.1 Bakgrund

Det civila samhällets krishanteringsförmåga är beroende av ett flertal system som innehåller elektronisk utrustning för styrning, kontroll, övervakning, kommunikation, etc. Dessa kan utsättas för angrepp med olika typer av antagonistiska elektromagnetiska hot (EM-hot), som exempelvis kraftiga störsändare eller vapen som avger elektromagnetiska pulser. Kunskapen i det svenska samhället om dessa relativt nya hot är betydligt mindre än kunskaper om t.ex. vad en översvämning eller kravaller innebär och vilka konsekvenser dessa kan få.

Under 2016 genomförde FOI på uppdrag av MSB en förstudie om risk- och sårbarhetsanalys (RSA) avseende elektromagnetiska hot mot samhällsviktig verksamhet [1]. Arbetet innefattade framtagning av tre olika typscenarier med EM-hot samt en struktur för hur en samhällsaktör med ansvar för ett samhällsviktigt system skulle kunna genomföra en RSA avseende EM-hot.

Under förstudien genomfördes möten med samverkansområdena teknisk infrastruktur (SOTI), transporter (SOTP) och ekonomisk säkerhet (SOES), där statliga myndigheter, landsting, länsstyrelser och kommuner medverkar. Det framkom att det finns ett behov att sprida information om EM-hot, exempelvis genom en utbildningsinsats. Informationen kan behöva spridas till aktörerna inom samverkansområdena, men också till branschorganisationer där privata aktörer kan ingå. Flera aktörer uttalade ett stort behov av stöd för att kunna bedöma konsekvenserna av EM-hot och information om lämpligheten och robustheten hos olika kommunikations-system som används för en viss tjänst. Flera aktörer efterfrågade också att hotscenarierna anpassades speciellt mot deras verksamhet.

I förstudiens slutrapport presenterades ett förslag på hur en huvudstudie RSA EM-hot skulle kunna genomföras, bestående av följande delar:

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

Efter diskussioner mellan MSB och FOI under våren 2017 delades den fortsatta verksamheten upp i två projekt, ett för genomförande av pilotstudie med metodutveckling och framtagning av en vägledning för de organisationer som avser att genomföra en RSA avseende antagonistiska EM-hot, och ett projekt för framtagning av ett anpassat medvetandehöjande utbildningsmaterial om avsiktliga EM-hot. Dessa projekt har pågått parallellt under hösten 2017 och genomförts i dialog med MSB och med centrala beredningsgruppen elektromagnetiska hot (CBG EM-hot).

1.2 Syfte

En pilotstudie skall genomföras med en eller flera aktörer som är villiga att genomföra en RSA mot EM-hot i dialog med FOI. I pilotstudien ingår att ett av hotscenarierna som togs fram i förstudien förfinas och anpassas mot aktören. Vidare behöver viktig verksamhet och de system verksamheten baseras på identifieras. Alla beroenden till system som kan drabbas behöver identifieras, samt de skydd eller den resiliens som finns inbyggd behöver identifieras (riskidentifiering). Därefter görs en riskanalys där man identifierar vad som kan hända, sannolikheten för det och vilka konsekvenserna blir.

Baserat på detta underlag genomförs en riskutvärdering, följt av en ny riskutvärdering baserat på några olika åtgärdsförslag. I metodutvecklingen anpassas dialogmaterialet, och genom en utvärdering av vad som fungerar och inte fungerar vidareutvecklas processen för RSA:n.

Efter att pilotstudien har genomförts kan RSA:er för andra aktörer genomföras med avsevärt mindre insats eftersom metoden då har anpassats och kunskap har införskaffats om vilken typ av experter som kan bidra med information om aktörernas system.

Genomförandet av huvudstudien och erfarenheter från pilotstudierna presenteras i denna rapport, medan själva RSA-metodiken redovisas i en separat vägledning för dem som avser genomföra en RSA EM-hot.

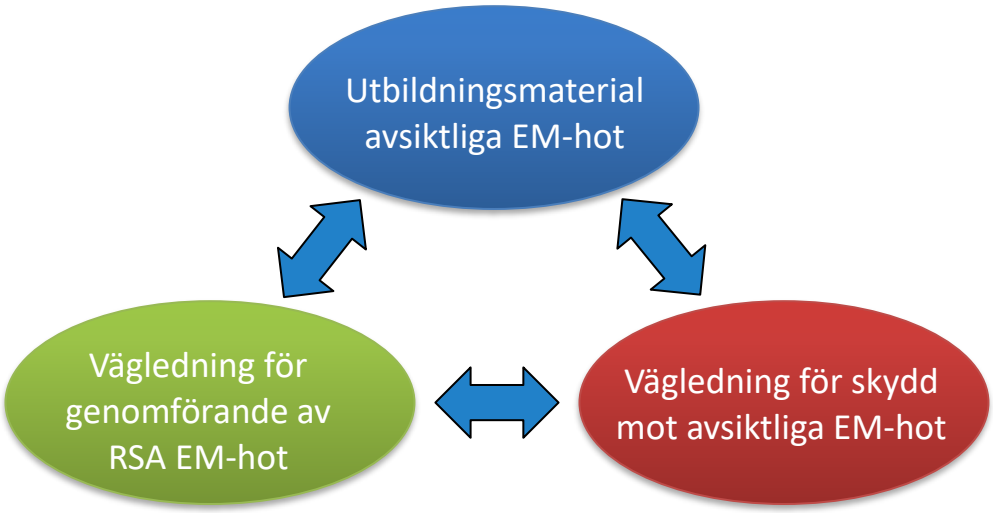
För att kunna genomföra en RSA för EM-hot krävs kunskap om hur EM-hot kan se ut och användas. Det medvetandehöjande utbildningsmaterial som tagits fram parallellt med utvecklingen av RSA-metodik för EM-hot är avsett att kunna användas för självstudier eller vid lärarledd undervisning inför genomförandet av en RSA EM-hot.

Utvecklingen av ett utbildningsmaterial om EM-hot skall fokuseras på omarbetning av befintligt forskningsmaterial samt produktion av skriftlig dokumentation i syfte att kunna användas av civila aktörer för att identifiera och skydda sig mot EM-hot. Syftet är att läsaren/publiken skall få förståelse för vad avsiktliga EM-hot innebär, vilka typer av EM-hot som kan finnas mot samhällsviktig verksamhet, och till viss del möjliga/typiska verksamhets-konsekvenser av dessa hot.

Fortifikationsverket har tidigare på uppdrag av MSB tagit fram en *Vägledning för skydd mot avsiktliga EM-hot* [2] som beskriver möjliga skyddsåtgärder mot avsiktliga EM-störningar och andra antagonistiska EM-hot, vilket utgör ett viktigt komplement till föreliggande arbete.

Utbildningsmaterialet avses leda till medvetandehöjande om och förståelse av olika EM-hot och möjliga konsekvenser, vilket leder till korrekt nyttjande av RSA-materialet, som i sin tur ger möjlighet att på ett strukturerat sätt kunna identifiera och prioritera sårbarheter, medan Fortifikationsverkets vägledning för skydd mot avsiktliga EM-hot visar hur man kan åtgärda de sårbarheter som identifierats i den samhällsviktiga infrastrukturen.

De tre delarna *Vägledning för skydd mot avsiktliga EM-hot*, *Vägledning för RSA avseende antagonistiska EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur* och *Introduktion till avsiktliga EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur* är avsedda att kunna användas tillsammans och komplettera varandra (jfr. Figur 1). Utbildningsmaterial och Vägledning för risk-och sårbarhetsanalys finns publicerade som separata skrifter [3,4]. Till utbildningsmaterialet hör dessutom en PowerPoint-presentation.



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

2. RSA EM-hot

En risk- och sårbarhetsanalys (RSA) avseende elektromagnetiska hot är inte tänkt att vara en fristående process hos en samhällsaktör utan ska utgöra en del av en övergripande RSA som innefattar alla tänkbara typer av hot som den studerade verksamheten skulle kunna utsättas för. Detta för att man ska kunna analysera och sammanväga alla risker och prioritera mellan åtgärder för att minimera de risker som bedöms utgöra de allvarligaste hoten mot verksamheten, oavsett ursprung.

Dessutom är det ofta så att ett angrepp med ett EM-hot kan ske i kombination med andra typer av angrepp eller antagonistiska aktioner, t.ex. där EM-hotet används för att störa ut ett säkerhets- eller kommunikationssystem medan angriparen utför en attack med andra medel eller tar sig in på ett förbjudet område.

Ett vanligt sätt att genomföra en RSA är att man först försöker identifiera alla möjliga händelser som skulle kunna påverka den studerade verksamheten och sedan gör en bedömning av sannolikheten för att en viss typ av händelse skulle kunna inträffa och en bedömning av vilka konsekvenser denna händelse skulle kunna få. Sannolikhet och konsekvens uttrycks i numeriska termer, exempelvis i hur ofta händelsen skulle kunna inträffa (en gång på tio år, dagligen, etc.) och vilken ekonomisk skada som händelsen uppskattas orsaka (t.ex. kostnaden för att ersätta en anläggning eller kostnaden för produktionsbortfall), alternativt hur många människor som skulle drabbas av händelsen (antal sjuka eller förlorade människoliv).

Risken för en viss händelse anges därefter som produkten av sannolikheten för och konsekvenserna av händelsen i fråga. Därefter rangordnas riskerna för alla olika typer av händelser från högst till lägst risk. Vanligen beslutar man sig för att åtgärda de högsta riskerna, men man kan också välja att förebygga en händelse med mycket låg sannolikhet och låg risk om dess konsekvenser anses oacceptabla för samhället.

2.1 Förstudien

Det finns flera mer eller mindre likartade metoder för att genomföra en risk- och sårbarhetsanalys för en verksamhet. I förstudien om RSA avseende EM-hot [1] behandlades flera varianter, bland annat FORSA-modellens arbetsblock [5].

Arbetet med att utforma RSA-metodik för EM-hot ansluter sig till MSB:s ”Vägledning för Risk- och sårbarhetsanalyser” [6] och till standarden SS-ISO 31000:2009 ”Riskhantering - Principer och riktlinjer” [7], som erbjuder en utvecklad terminologi för de olika delarna inom riskhantering, vilket är den övergripande termen för allt arbete med risker i en verksamhet, samt delar upp riskhanteringen i följande processteg:

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

  } Riskbedömning

- Förmågebedömning
- Sårbarhetsanalys

  } Sårbarhetsbedömning

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

Här utgör riskanalys och sårbarhetsanalys delar av riskbedömning respektive sårbarhetsbedömning. I andra framställningar kanske man inte skiljer mellan analys och bedömning och inte gör en lika tydlig uppdelning i processteg.

2.2 Huvudstudien

Tyngdpunkten för pilotstudierna av RSA EM-hot har legat på de första fyra processtegen i riskhanteringen eftersom svårigheterna har befunnits ligga i beskrivning av EM-hot och hur de kan uppträda i relevanta hotscenarier. Sårbarhetsbedömningen har behandlats i diskussionerna, medan slutsatser och utformning av eventuella åtgärder i stor utsträckning har lämnats åt de deltagande samhällsaktörerna som har ansvaret för respektive verksamhet.

2.3 Medvetandehöjande utbildningsmaterial

För att kunna genomföra en vederhäftig risk- och sårbarhetsanalys avseende elektromagnetiska hot behövs grundläggande kunskaper om vilka EM-hot som finns idag, vilka effekter de kan ha på elektronisk utrustning samt vilken inverkan som olika typer av skydd, t.ex. ett omgivande plåtskåp, kan ha.

Även en kvalificerad elektroingenjör som arbetar med utbyggnad och underhåll ett elektronikbaserat samhällsviktigt system kan ha svårt att inse vilka EM-hot som skulle kunna användas av en illasinnad individ eller grupp för att påverka det skyddsvärda systemet och vilken elektromagnetisk miljö som dessa EM-hot kan åstadkomma vid den elektroniska utrustningen. Detta beror bland annat på att de senaste decenniernas snabba utveckling inom elektronikområdet har gjort det enklare att få tillgång till avancerade störsändare eller anordningar som genererar elektromagnetiska pulser med förmåga att påverka elektronisk utrustning. Information om hur man själv kan bygga störsändare sprids i stor omfattning via internet samtidigt som man i flera större länder tar fram kraftigare elektromagnetiska vapen för militär användning.

För att stödja dem som ska genomföra RSA:er avseende EM-hot har FOI parallellt med vidareutveckling av metodiken för RSA EM-hot även tagit fram ett medvetandehöjande utbildningsmaterial som skulle kunna användas för självstudier eller i olika utbildningar som ges för personal med system- eller ledningsansvar.

3. Utveckling av material från förstudien

Huvudstudien bygger på material som tags fram inom förstudie RSA EM-hot, bland annat scenarier och RSA-metodik.

3.1 Scenarier för avsiktliga EM-hot

Under förstudien [1] togs det fram tre grundläggande hotscenarier som avsåg att täcka in flera tänkbara situationer där EM-hot kan komma att användas mot samhällsviktig verksamhet som är beroende av elektronisk utrustning. Variationsrikedomen i hur ett avsiktligt EM-hot kan vara utformat är stor. Dels kan antagonisten vara del av en militär styrka från främmande makt, en terroristgrupp, en kriminell gruppering, missnöjda individer eller studenter som experimenterar med generering av elektromagnetiska pulser. De fysiska EM-hoten kan vara kommersiella störsändare, hemmabyggda anordningar baserade på mikrovågsugns- eller radarmagnetroner, eller militärt utvecklade mikrovågsvapen med verkansavstånd på uppemot 1 km eller mer. Syftet med en avsiktlig EM-attack kan variera från att skapa tillfälliga störningar eller kaos i samhället till att möjliggöra ett inbrott, en terroristattack eller en militär intervention.

Av särskilt intresse är situationer i den s.k. gråzonen mellan krig och fred [8], ofta benämnd skymningsläge. Vid ett ökande antal sabotage, subversiva angrepp eller rena terrorhandlingar där man inte med säkerhet kan identifiera vem som ligger bakom kan det råda stor osäkerhet om vart utvecklingen är på väg. I sådana lägen kan regeringen förbereda ett beslut eller redan ha beslutat att införa höjd beredskap.

För vart och ett av huvudstudiens pilotfall har ett av typscenarierna valts som utgångspunkt och anpassats till den studerade verksamheten.

3.1.1 Typscenario 1

Scenariobeskrivning

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

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

utan att detta behöver lyftas. Utifrån ser det ut som en vanlig lastbil som används för privata transporter.

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

Konsekvensbeskrivning

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

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

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

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

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

3.1.2 Typscenario 2

Scenariobeskrivning

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

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

Varje störsändare väger några kilo och utplaceras tillsammans med batteri i väskor av många olika typer på ett trettiotal platser i varje stad. Strategiska

platser är dels offentliga platser där mycket människor rör sig och är vana att kunna använda trådlösa tjänster samt regeringskansli, polisstationer och andra områden där samhällsviktiga tjänster störs ut.

Konsekvensbeskrivning

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

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

3.1.3 Typscenario 3

Scenariobeskrivning

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

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

Konsekvensbeskrivning

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

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

3.2 RSA-metodik

Den under förstudien framtagna metodiken för att genomföra en RSA avseende EM-hot rekommenderade en anpassning av hotscenarierna till något av de typfall som FOI tagit fram [9, 10]. Dessa utgörs av:

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

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

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

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

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

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

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

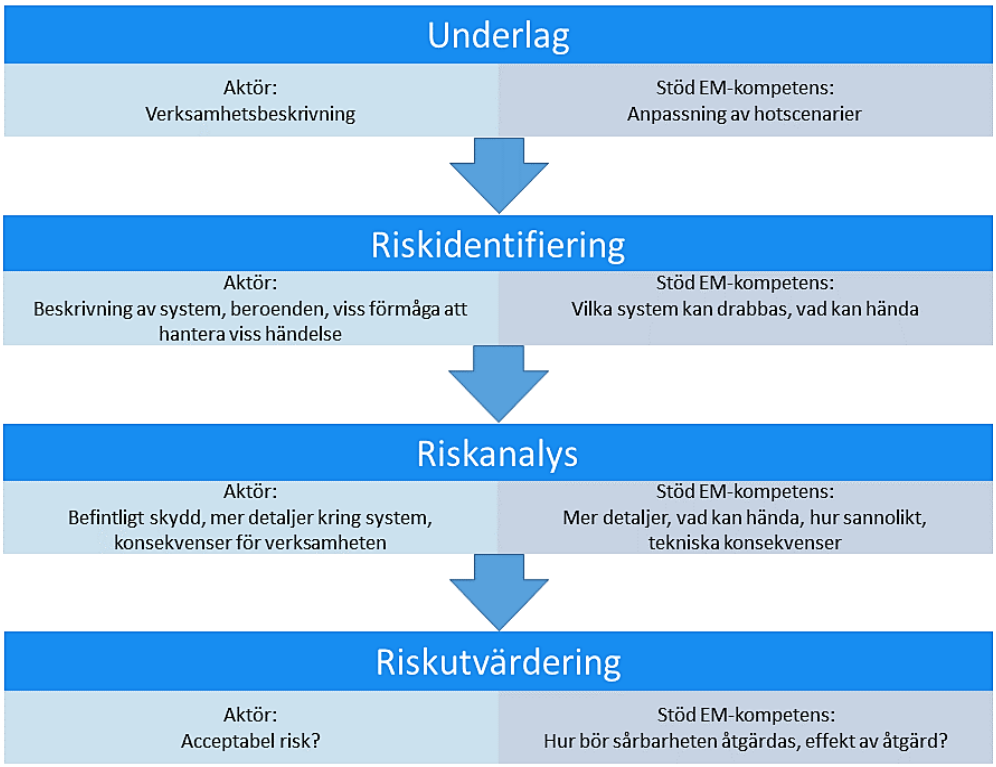
  Typfallet beskriver ett begränsat väpnat angrepp med fjärrstridsmedel mot militära mål och civil infrastruktur, i syfte att kraftigt begränsa Sveriges politiska vilja och militära förmåga att agera. Angreppet följs upp med landstigning och luftlandsättning mot begränsade områden.

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

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

I arbetet med EM-hot mot civil infrastruktur har fokus legat på hotscenarier som inträffar i lägen som ligger under typfall 1, 2 och 5.

Eftersom tekniska system och trådlös kommunikation kan påverkas kraftigt av EM-hot är det systemkunskap, beroenden mellan system och verksamhetens beroende av elektroniska stödsystem som behövs i en RSA avseende EM-hot. Figur 2 ger en vägledning om vilka frågeställningar som kan behöva penetreras i en sådan RSA. Förstudien rekommenderade dessutom att pilotstudien skulle genomföras i dialogform. Dessa riktlinjer har legat till grund för utformningen av de två pilotstudierna inom huvudstudien RSA EM-hot.



Figur 2. Förslag på hur deltagare med olika kompetenser kan delta i processstegen i en RSA. [1]

4. Genomförda pilotstudier

Under hösten 2017 har två pilotstudier genomförts i dialogform för att testa anpassning av hotscenarier till en specifik verksamhet och för att undersöka vilka personer/kompetenser som kan behöva delta i en RSA avseende EM-hot. Resultaten från pilotstudierna har använts för metodutveckling och utformning av det vägledande materialet

Lämpliga kontaktpersoner inom flera olika offentliga verksamheter har i början av projektet förmedlats av MSB och genom CBG EM-hot. Bland de kontaktade verksamheterna har två verksamheter av olika karaktär haft möjlighet att medverka och har valts ut för pilotstudierna. Den ena verksamheten är ett trådlöst kommunikationssystem som är gemensamt för många samhälls-aktörer, medan den andra verksamheten utgörs av ett landsomfattande kollektivt transportsystem som är beroende av ett flertal interagerande elektriska eller elektroniska stödsystem med varierande teknologisk ålder och robusthet.

Varje pilotstudie har delats upp i tre olika tillfällen, med någon eller några veckor mellan varje, enligt följande:

- Förberedande möte
- Genomförande av RSA
- Kompletterings- och avstämningsmöte

Det förberedande mötet har haft syftet att presentera arbetet med utveckling av RSA-metodik för EM-hot för deltagarna samt att samla information om den verksamhet som är föremål för pilotstudien. Förstudiens tre typscenarier har diskuterats och en preliminär bedömning av relevans och aktualitet har gjorts. En viktig diskussionspunkt har varit att ge deltagarna från FOI tillräckligt mycket information om de system som verksamheten är beroende av, hur de hänger samman med andra system, fysisk placering och förekomsten av eventuella barriärer som kan verka dämpande på elektromagnetisk strålning. Dessutom har man identifierat personer från den studerade verksamheten som bör vara med vid genomförandet av RSA:n.

Inför genomförandet av RSA:n har FOI valt ett typscenario och vidareutvecklat detta så att det blir mera relevant för den studerade verksamheten. Scenariot har beskrivit en omvärldssituation där den studerade verksamheten är en bland flera samhällsviktiga verksamheter som utsätts för en större attack, som inte enbart omfattar EM-hot. Beskrivningen av EM-attacken har satts in i ett större händelseförlopp som kan förväntas orsaka stora störningar i flera olika samhällsfunktioner. Beskrivningen av EM-attacken har gjorts så konkret som varit möjligt. Detta innebär bland annat att peka ut specifika delsystem eller komponenter som utsätts för en attack med ett specifikt EM-hot. I båda pilotstudierna har såväl störsändare som mikrovågsvapen använts mot olika delar i de studerade verksamheterna.

Ett syfte med att göra ett mera komplext scenario med flera samtidiga EM-attacker mot olika delsystem som del av en bredare attack på samhället har varit att försöka åstadkomma en stor belastning på såväl de elektroniska systemen som på personal som hanterar dessa. Avsikten har varit att få fram svagheter och beroenden som kanske inte skulle uppmärksammats vid ett mera begränsat scenario.

Den studerade verksamheten har under tiden fram till genomförandet av RSA:n haft möjlighet att ta fram ytterligare relevant information om de tekniska system som skulle beröras vid den tilltänkta EM-attacken.

För båda pilotstudierna användes följande arbetsgång:

1. Inledning
2. Hotscenario
3. Riskidentifiering – Tekniska konsekvenser
4. Riskanalys – Verksamhetskonsekvenser
5. Riskutvärdering
6. Sårbarhetsreducerande åtgärder
7. Avslutande utvärdering av metoden

Vid genomförandet av RSA:n presenterades först det anpassade scenariot för deltagarna från den studerade verksamheten. Därefter genomfördes ett pass med riskidentifiering innefattande diskussioner om de tekniska konsekvenser som de valda EM-angreppen skulle kunna få på olika delsystem. I den vidare riskanalysen försökte deltagarna uppskatta konsekvenserna för den skyddsvärda verksamheten om de tekniska systemen helt eller delvis skulle tappa funktion. En kvalitativ riskutvärdering syftade till att uppskatta vilka risker som kunde accepteras och vilka som borde/kunde prioriteras. En kortare diskussion om möjliga sårbarhetsreducerande åtgärder fullföljde RSA:n. Mötena avslutades med en gemensam utvärdering av metoden för att identifiera vad som kunde ha gjorts annorlunda och om något underlag saknades.

Genomförandet av de båda RSA:erna dokumenterades av FOI och slutsatser beträffande RSA-metodiken sammanställdes. Information som framkommit om eventuella sårbarheter i de studerade verksamheterna behandlas inte vidare av FOI utan lämnas att tas om hand av de studerade verksamheterna, som beslutar om sekretessnivå och eventuella åtgärder.

Vid det tredje mötet för komplettering och avstämning diskuterades resultaten från genomförandet och delar av innehållet i ett utkast till denna rapport, några kompletteringar gjordes och genomförandet diskuterades. Resonemangen kring sannolikhets- och konsekvensbedömningar utvecklades (se avsnitt 5.5 nedan). Detta möte hade främst syftet att stämma av erfarenheterna av metoden för genomförandet och i mindre mån själva resultaten, som identifierade svagheter eller möjliga åtgärder.

4.1 RAKEL-kommunikation (MSB)

”RAKEL[1] är ett kommunikationssystem för trygg och säker kommunikation mellan medarbetare inom samhällsviktiga verksamheter. Systemet har en unikt hög driftsäkerhet, täckning i hela Sverige och används av fler än 500 organisationer” [11].

”Rakel bygger på digital Tetrateknik som är en europeisk teknisk standard som används på flera håll i världen i verksamheter med särskilt höga krav på säkerhet och robusthet. Det är byggt för att klara tuffa väderförhållanden. Nätet har överlägsen täckning och klarar extremt hög belastning. Vid elavbrott finns reservkraft för upp till sju dagar” [11].

”MSB driver, utvecklar och stödjer användning av Rakel tillsammans med användarna. Teracom hanterar drift, underhåll och kundsupport på uppdrag av MSB. Det är MSB som godkänner organisationer som vill ansluta sig till systemet” [11].

Det anpassade EM-hotscenariot för Rakel-systemet innefattar ett antal terroristceller som genomför aktioner med sprängdåd, skjutningar samt störning av media och allmänna kommunikationer. Regeringen anser situationen vara mycket allvarlig och inför höjd beredskap (skärpt beredskap) samt förbereder allmän mobilisering.

Elektromagnetiska angrepp riktas direkt mot basstationer för Rakel och mot användarterminaler för att isolera blåljuspersonal som kallats till ett område med pågående upplopp. Syftet är att reducera myndigheternas förmåga att ingripa vid en större terroristaktion som genomförs på en annan plats. Flera Rakel-basstationer i området kring uppploppet angrips med egenhändigt konstruerade mobila mikrovågsvapen som på under hundra meters håll genererar kraftiga elektromagnetiska pulser som kan störa eller förstöra elektronik.

Samtidigt används kraftiga kommersiellt tillgängliga störsändare för att störa ut användarterminaler inom uppploppsområdet. Både störsändare och strålkällor hanteras av antagonisterna och kan avlägsnas vid lämpligt tillfälle, vilket försvårar forensiska undersökningar. Det blir svårt att bevisa vad Rakel utsatts för, att detta var avsiktligt och vem som genomfört attackerna.

En diskussionspunkt vid pilotstudien var om angreppet kan slå ut all Rakel-kommunikation hos de enheter som befinner sig inom uppploppsområdet. Frågor som behandlades var om man vid driftledningscentralen direkt upptäcker om en basstation eller en enskild terminal är utstörd och omedelbart kan vidta åtgärder, dvs. hur snabbt man blir medveten om att det är ett EM-angrepp som pågår. En relevant fråga var om användarna när de tappar kontakten med centralen kan finna andra möjligheter att kommunicera med denna, t.ex. med egna mobiltelefoner. Andra relaterade frågeställningar var hur snabbt driftpersonal kan vara på plats, hur snabbt det kan gå att återställa basstationer i det drabbade området, om reservdelar finns tillgängliga och vilka möjligheter det kan finna att pejla in störsändare och omhänderta dessa.

[1] akronym för RAdioKommunikation för Effektiv Ledning

Av särskilt intresse är vilka skyldigheter underhållsleverantörer enligt avtal har att agera i situationer liknande den beskrivna vid höjd beredskap.

Skyddsåtgärder i form av skalskydd och transientskydd diskuterades. Eftersom Rakel är ett kommunicerande elektroniskt system och kommunikations-frekvenserna är kända kan en EM-attack anpassas till dessa. Dessutom finns en risk att angrepp med störsändare mot andra elektroniska system skulle kunna störa Rakelfrekvenser som en sidoeffekt.

Tidsförloppet vid en EM-attack kan vara väsentligt. Ett angrepp av den beskrivna typen kräver att någon rekognoscerat platsen i förväg och identifierat objekt som angreppet ska riktas mot. Detta kan ske dagar eller veckor i förväg. När man väl konstaterat att Rakel utsatts för en incident i form av ett EM-angrepp kan en chef behöva fatta beslut om att kalla in extra personal för att hantera situationen. Sedan är det kritiskt att kunna hantera pågående störning så snabbt som möjligt, t.ex. få hjälp att pejla in störsändare, och snabbt få tillgång till reservdelar till komponenter som kan ha skadats under angreppet.

4.2 Järnvägens signalsystem (Trafikverket)

Järnvägens signalsystem består av ett flertal autonoma delsystem med var sin specifika uppgift. Järnvägskorsningar och växlar styrs av genomtänkta kontroll- och säkerhetssystem. Undersystemen utgör tillsammans en driftplats, t.ex. en järnvägsstation, som kan fungera autonomt även om dessa vid normal drift samverkar med intilliggande driftplatsers säkerhetssystem. [12]

Driftplatser levererar data till och övervakas av fjärrtågklarerare i en trafik-central i någon större tätort. Den genomsyrande principen i signalsystemet är att om något oväntat händer eller något fel upptäcks så ska trafiken stoppas på det berörda banavsnittet. Detta syftar till att undvika olyckor, men innebär också att järnvägstrafiken kan störas av många olika påverkansformer.

Järnvägen har system för automatisk tågkontroll (ATC) som kan bromsa och stoppa tåg som kör för fort eller passerar en röd signal. Kommunikationen går via fast placerade sändare i eller intill rälsen, s.k. baliser. Järnvägsnätet har även ett eget mobiltelefonliknande kommunikationssystem (GSM-R) för kontakt mellan tågklarerare vid ledningscentraler och tågförare ute på banan. GSM-R är en del av ett nytt sameuropeiskt säkerhetssystem för tågtrafik, kallat ERTMS[2], som är på gång att införas i Sverige.

Det anpassade EM-hotscenariot för det svenska järnvägsnätet beskriver en annalkande militär konflikt i Östersjöområdet vilket föranleder regeringen att förbereda allmän mobilisering. För att försvåra denna mobilisering utför antagonistiska grupper aktioner på många platser i landet med störning av kommunikationer, data- och mobiltelefontrafik, flyg, väg- och spårtrafik, TV, radio och tidningar. Det är mycket svårt att peka ut vem som ligger bakom störningarna.

[2] akronym för European Railway Traffic Management System

Speciellt för att försvåra transport av personal till mobiliseringsplatser utsätter antagonistiska grupper driftplatser i östra Sverige för angrepp med EM-hot, dels bestående av kraftiga kontinuerliga störsändare för GSM och GSM-R banden, dels av mikrovågsvapen som ger korta EM-pulser med mycket hög toppeffekt som fysiskt kan förstöra elektronik.

Kommersiella störsändare parkerar inom några tiotal meter från GSM-R-masten vid de attackerade driftplatserna medan grupper med insmugglade mikrovågsvapen kör runt till olika driftplatser och utsätter ställverkselektronik för bestrålning med kraftiga mikrovågspulser.

Det kan konstateras att vilken effekt som EM-attackerna får beror bland annat på vilka delsystem som finns vid respektive driftplats. Vissa sträckor kanske bara kontrolleras via GSM-R medan andra även har ATC och baliser[3]. Om en driftledningscentral angrips kan konsekvenserna bli annorlunda än om man ger sig på en driftplats eller elförsörjningsenheter för ett banavsnitt.

Bland frågor som berördes var vilken redundans det finns i GSM-R-systemet om en basstation skulle slås ut, gränssnitt mellan olika säkerhetssystem, placering och utformning av delsystem vid olika driftplatser, möjligheter att ersätta ett bortfallet GSM-R-nät med GSM, 3G eller 4G, samt hur snabbt kommunikationssystem och ställverkslogik kan återställas efter en störning i funktionen. En intressant aspekt är tillgången på kompetent personal som i händelse av helt funktionsbortfall skulle klara av att ge tåg körorder för att kunna upprätthålla en begränsad tågtrafik.

Eftersom det finns flera trafikaktörer som använder järnvägsnätet uppstod frågan om prioriteringar mellan olika tåg efter en driftstörning. Det visade sig att trafikaktörerna själva prioriterar mellan sina egna tåg vid en störning, men att Trafikverket inte utan vidare kan prioritera mellan olika trafikaktörers tåg.

En viktig fråga är hur säkert det är för reparatörer att gå in i en högspännings-anläggning efter att denna utsatts för ett EM-angrepp som kan ha satt vissa säkerhetssystem ur spel.

Skyddsåtgärder i form av skalskydd och transientskydd diskuterades. För att detektera extern påverkan via elektromagnetiska fält kunde varnare för EM-hot placeras ut på kritiska platser. En liknande teknik är de störkännare som finns på flera håll för att detektera variationer i spänning och ström på järnvägens elförsörjningssystem.

Av betydelse för hanteringen av en störning i järnvägsnätet är vilket ansvar inhyrda entreprenörer och underentreprenörer har. Exempelvis sker driften av GSM-R i Trafikverkets regi, medan underhållet sköts av en entreprenör.

[3] En balis är en fyrkantig platta mellan rälerna i spåret som sänder information om bansträckan och tillåten hastighet till passerande tåg.

5. Erfarenheter och slutsatser

5.1 Förmöte och avslutande avstämning

Att hålla ett förmöte mellan aktör (Rakelgruppen/MSB resp. Trafikverket) och experter på EM-hot (FOI) var mycket betydelsefullt för att kunna anpassa ett typscenario till den verksamhet som analyseras. Kunskap om verksamheten är väsentlig för att kunna bedöma vilka EM-hot som är relevanta för olika system och för att värdera vilka effekter ett EM-angrepp kan få.

Båda verksamheterna som deltog i pilotstudien är relativt komplexa med flera olika enheter eller delsystem distribuerade över ett stort geografiskt område. Samma typ av utrustning kan vara placerad på olika platser i ett utrymme (apparatskåp, serverhall, etc.) och ha olika grad av omgivande skydd på olika platser i landet. Detta innebär att effekterna av en EM-attack kan skilja sig något mellan olika platser som valts för angreppet.

Ett förmöte bedöms också vara viktigt för den systemansvariga aktören. Även om personal som deltar i en RSA är tekniskt kvalificerad så är kunskaperna om hur dagens EM-hot ser ut och verkar inte lika kända. Förmötet ger deltagarna möjlighet att tänka igenom möjlig påverkan på egna system från de typhot som diskuteras under förmötet.

Ett avstämningsmöte efter genomförd RSA är värdefullt för att stämma av resultaten från genomförandemötet och ge deltagarna tillfälle att komplettera den genomförda RSA:n. I pilotstudierna medförde detta avslutande möte dessutom möjligheter att reflektera över arbetsmetodiken.

5.2 Användning av scenariobeskrivningar

En scenariobaserad risk- och sårbarhetsanalys i en vidare samhällskontext uppfattades vid båda pilotstudierna som underlättande för att förstå hur ett EM-angrepp kan användas för att uppnå vissa syften och hur olika EM-hot kan se ut. En kommentar från en person som tidigare deltagit i RSA:er för sin verksamhet där man fått som uppgift att genom brainstorming identifiera risker utryckte att det scenariobaserade angreppssättet underlättade mycket när man ska identifiera konkreta EM-hot och hotsituationer.

EM-hot är relativt nytillkomna hot, jämfört med t.ex. åska och sprängdåd, och riktas direkt mot elektronisk apparatur. Detta gör att även kvalificerade driftsingenjörer och systemansvariga som förstår utrustningen väl kan ha svårt att föreställa sig hur ett EM-angrepp skulle påverka den egna utrustningen och vilka konsekvenser olika störningar kan få. För att integrera EM-hot i en RSA som omfattar alla hot mot en samhällsviktig verksamhet kan det därför underlätta att vid inledningen av analysen presentera ett genomtänkt scenario, där EM-angrepp utgör en del i en större samhällsstörning.

5.3 Medverkan av olika kompetenser

Under båda pilotstudierna uppstod situationer där ytterligare stöd av en operativ användare hade kunnat föra analysen ännu längre. Detta för att svara på frågor om hur en trafikplanerare planerar om järnvägstrafik när en driftplats är ur funktion eller hur en polis på fältet skulle agera i en situation när Rakel-kommunikationen inte fungerar.

Eftersom EM-hot är av teknisk natur och slår mot tekniska system är teknik-specialister nödvändiga. Men för att få med alla aspekter av hur EM-angrepp kan påverka en samhällsviktig verksamhet bör man eftersträva deltagande av såväl ansvarig chef, operatör, underhållspersonal som användarrepresentant.

Exempel på medverkande som kan bidra med olika aspekter på ett samhällsviktigt systems resiliens med avseende på EM-angrepp och vilka konsekvenser en partiell eller total systemblockering kan ge, samt beslut om åtgärder och alternativa handlingssätt, kan till exempel återfinnas bland:

- Beslutsfattande chefer
- Driftsansvariga
- Säkerhetsansvariga
- Underhållspersonal
- Inhyrda konsulter, underentreprenörer, etc.
- Operativa användare på fältet
- Personal från andra verksamheter som är beroende av att det studerade tekniska systemet fungerar.

Alla dessa kanske inte behöver vara med under hela RSA:n men kan finnas tillgängliga för att kunna bidra med specifik information när det uppstår ett behov av sådan. Observera att antalet deltagare bör begränsas för att RSA:n ska vara effektiv och smidig. Ungefär fyra till sju deltagare kan vara optimalt.

5.4 Ansvarsområden och ansvarsförhållanden

Vid båda pilotstudierna uppstod osäkerheter vad gäller underhållsleverantörers ansvar och behörighet vid krissituationer med höjd beredskap, liknande dem i de anpassade scenarierna. Entreprenörers ansvar under normala förhållanden regleras via skrivna avtal som ger dessa tillträde till delar av olika anläggningar och möjlighet att utföra specificerade underhållsåtgärder.

I en extraordinär situation under höjd beredskap kanske dessa avtal inte räcker till för att kunna upprätthålla en viss servicenivå. Särskilt viktig är tillgång till kvalificerad underhållspersonal hos en entreprenör om dess anställda har krigsplaceringar med andra uppgifter eller på annan plats. Dessa förhållanden som bör studeras vidare och kanske bli föremål för förtydliganden i skrivna underhållsavtal.

5.5 Osäkerheter och riskkvantifiering

För att i riskutvärderingen kunna prioritera mellan åtgärdande av olika risker behöver man i en komplett RSA kvantifiera dessa. Vid pilotstudierna åtföljdes inte riskanalysen av en fullständig riskkvantifiering, där man sätter numeriska värden på sannolikheten för en viss händelse och på konsekvenserna av händelsen, eftersom detta är meningsfullt bara för jämförelser med alla olika typer av händelser. Med en definition av risken för en händelse som

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

brukar man uppskatta risken för att händelsen ska inträffa och sätta en prislapp på konsekvenserna. T.ex. kan risken för en viss typ av trafikolyckor baseras på frekvensen för tidigare händelser (antal olyckor/år) och konsekvensen uttryckas i ekonomiska kostnader eller påverkade människoliv (miljoner kronor för reparation; antal döda eller svårt skadade).

Om vi låter S beteckna sannolikheten för ett angrepp med EM-hot kan denna skrivas som

$$S = S_T \cdot S_A \cdot S_I$$

där

S_T är den teknologiska sannolikheten att EM-hotet skulle kunna realiseras och användas på beskrivet sätt

S_A är sannolikheten att en viss antagonist ska välja att använda sig av en EM-attack i det givna scenariot framför andra typer av medel

S_I är sannolikheten att antagonisten har tillräckligt mycket information om det skyddsvärda systemet för att angrepp med EM-hot ska lyckas

De i pilotstudien beskrivna EM-hoten är antingen störsändare som existerar och är kommersiellt tillgängliga redan idag eller system som är baserade på idag existerande teknologi och skulle kunna sättas samman av tillräckligt kvalificerade antagonister. Det senare anses rimligt eftersom spridningen av teknisk information via internet idag är stor och exempelvis terrorist-organisationer visat sig inte ha några problem att rekrytera kvalificerade ingenjörer. För kommersiellt tillgängliga störsändare kan man sätta $S_T = 1$, medan den teknologiska sannolikheten för olika typer av mikrovågsvapen är något mindre, dels eftersom dessa inte finns kommersiellt tillgängliga utan kräver specialiserad kunskap för konstruktion och användning, dels eftersom kraftfullare militära varianter troligen ännu inte finns ute på operativa förband.

Hittills har terroristorganisationer inte visat något större intresse för användning av EM-hot, eftersom dessa enbart verkar mot utrustning och inte mot människor. Det finns här inga historiska data att basera en bedömning på. Terrorism syftar vanligen till att sprida skräck och oro i befolkningen, vilket uppnås med bombdåd, skjutningar och knivdåd, medan utslagning av elektroniska system inte har samma effekt. En vanlig reaktion hos personal när ett system inte fungerar är att tro att det är problem med strömförsörjning eller mjukvarufel. Att sätta en siffra på S_A avseende terrorism är något som i dagsläget bör utföras av andra aktörer än de som deltagit i pilotstudierna.

För militärt bruk av EM-hotsystem bör sannolikheten S_A för användning sättas hög eftersom olika typer av telekrigföring eller störningar av elförsörjning och kommunikationer använts frekvent i samband med militära interventioner på senare år, inte minst för att temporärt störa ut civil samhällsviktig verksamhet och försvåra mobilisering etc.

För en invaderande militär styrka kan det vara av intresse att kunna använda existerande infrastruktur efter ett övertagande, vilket ofta är enklare efter en EM-attack än en attack med sprängmedel och skjutvapen. En attack med störsändare mot ett kommunikationssystem påverkar systemet bara så länge attacken pågår, medan verkan av en attack med mikrovågsvapen, förutom påverkan under attackfasen, även kan ha bestående effekter, dvs. verka förstörande. Detta kan kräva en återställnings- eller reparationsfas på några timmar till dagar beroende på tillgången till reservdelar.

Störsändare påverkar kommunikationssystem som utnyttjar de störda frekvenserna för trådlös kommunikation, medan en attack med mikrovågsvapen kan även påverka icke-kommunicerande elektroniska system. Såväl störsändare som mikrovågsvapen kan, förutom att slå mot ett avsett målsystem, även påverka andra elektroniska system i närheten.

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

Demonstranter och aktivister kan tänkas använda EM-hot för att störa samhällsfunktioner, vilket t.ex. Göteborgskravallerna visar [13]. En annan grupp som skulle kunna orsaka störningar i samhällsviktig verksamhet och kritisk infrastruktur är tekniknördar, t.ex. studerande vid tekniska högskolor som enbart av intresse tillverkat utrustning och testar dess verkan mot elektronisk apparatur bara för att ”det är coolt”. Den samhällsviktiga verksamheten skulle kunna vara målet, men kan också bli utsatt som en bieffekt när man testar verkan mot något annat objekt. Sannolikheten för detta är troligen låg men svår att bedöma. Vad gäller antagonistiska gruppers benägenhet att använda olika typer av medel skulle Polisen eller SÄPO kunna ha en aktuell lägesbild.

För att kunna bedöma sannolikheten att utsättas för ett EM-angrepp behövs tillförlitlig statistik för inträffade incidenter. Därför är det viktigt att alla upptäckta eller misstänkta störningar inrapporteras. Elsäkerhetsverket brukar utreda störningar orsakade av elektrisk utrustning [14], medan Post- och Telestyrelsen utreder störningar i radiokommunikation [15]. En svårighet är att konstatera om man utsatts för avsiktlig störning eller om det rör sig om fel på utrustningen eller naturliga störningar.

Den faktor som ansvarig systemförvaltare inom en samhällsviktig verksamhet själv kan påverka är tillgängligheten av information om det skyddsvärda

systemet. Exempelvis typen av ingående komponenter, arbetsfrekvenser, vilka skydd som installerats, placeringen av antenner och kontrollenheter, etc.

Ibland kan sådan information inte hemlighållas av hänsyn till användarnas behov (t.ex. kan arbetsfrekvenser behöva vara kända), men det kan ur skyddssynpunkt vara värdefullt att inte oreflekterat lämna ut all information om typ och placering av komponenter i ett system, förekomst av olika typer av skydd eller om förfaranden för att hantera olika typer av störningar i verksamheten. Dvs. den faktor som en systemansvarig aktör själv kan påverka är S_I, som bör hålls så låg som möjligt.

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

6. Medvetandehöjande utbildningsmaterial

För att sprida information om dagens antagonistiska EM-hot har FOI baserat på befintligt forskningsmaterial och annat tillgängligt öppet material tagit fram ett utbildningsmaterial avsett att användas vid lärarledda utbildningar och självstudier syftande till att höja medvetenheten om utformning och användning av avsiktliga EM-hot.

Utbildningsmaterialet består av tre delar:

- En rapport som kan användas som kurslitteratur eller läsas enskilt
- En PowerPoint-presentation baserad på rapporten
- En folder som sammanfattar materialet

Utbildningsmaterialet har följande huvudrubriker:

- Inledning
- Elektromagnetiska hot
- Exempel på hotkällor
- Elektromagnetisk attack mot kritisk infrastruktur
- Konsekvenser av EM-attack
- Enkelt exempel på en RSA
- Att skydda skyddsvärd samhällsviktig verksamhet och kritisk infrastruktur
- Slutord
- Bilaga: Avståndsberoenden

Materialet syftar till att ge en tillräcklig grund inom avsiktliga EM-hot för att de som inte är experter ska kunna tillgodogöra sig och använda sig av de vägledande dokument som tagits fram för att genomföra en RSA avseende antagonistiska EM-hot och besluta om adekvata skyddsåtgärder för att minska identifierade risker.

7. Slutord

Medvetenheten om idag existerande elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur är inte allmän kunskap, ens hos de tekniker som arbetar med dessa system. För att höja medvetenheten om antagonistiska EM-hot och möjliggöra relevanta åtgärder för att minska riskerna med dessa EM-hot har FOI tagit fram ett medvetandehöjande utbildningsmaterial som kan användas för självstudier eller som kursmaterial. En ökad medvetenhet om avsiktliga EM-hot utgör första steget mot att kunna hantera dessa.

Det är viktigt att tidigt kunna identifiera en avsiktlig störning och särskilja sådana från andra störningar som naturliga störningar, mjukvarufel eller utrustningsfel i hårdvaran. Monitorering av den elektromagnetiska miljön kring kritisk infrastruktur kan vara ett sätt att snabbt identifiera avsiktlig störning, samt lokalisera och neutralisera denna.

Två genomförda pilotstudier av hur en RSA för EM-hot mot samhällsviktig verksamhet och kritisk infrastruktur kan effektueras har visat att det finns några aspekter som är speciella just för elektromagnetisk påverkan. Det rör främst förståelsen av vad som kan vara ett EM-hot och hur detta kan uppträda vid en antagonistisk attack på samhällsviktig verksamhet. För att hantera detta behövs det ett framtaget realistiskt hotscenario, anpassat till den studerade samhällsviktiga verksamheten, med användning av EM-hot som en del i ett mera omfattande angrepp. För att åstadkomma detta behövs ett förmöte mellan samhällsaktör och experter på EM-hot, som kan anpassa scenariot till den studerade verksamheten.

Bland viktiga slutsatser som framkommit i de två pilotstudierna är att det behövs flera olika kompetenser för att bedöma effekterna av en EM-attack mot ett samhällsviktigt system, dels eftersom dessa kan vara mycket komplexa och beroende av andra system, dels eftersom konsekvenserna av en störning kan gå utanför rent tekniska och behöva bedömas av beslutsfattare, entreprenörer, operativa användare, etc.

Det finns flera olika antagonister som kan tänkas använda EM-hot på olika sätt och med olika syften. Gemensamt för de flesta är att EM-hot kan användas tillsammans med andra typer av hot för att uppnå vissa syften. EM-hot kan nyttjas för att forcera larm och säkerhetssystem, för att förhindra betalningar, för att skära av kommunikation mellan en sambandscentral och enheter ute på fältet, eller för att stoppa flödet i samhällsinfrastruktur, som t.ex. trafiken.

En RSA för EM-hot ska kunna göras som en del av en övergripande RSA för en samhällsviktig verksamhet, men det kan vid genomförandet krävas expertstöd beträffande EM-hot och deras möjliga användning.

Referenser

1. ”Förstudie om risk- och sårbarhetsanalys avseende EM-hot mot samhällsviktig infrastruktur”, Tomas Hurtig, Sten E Nyholm, Åsa Waern, Hampus Thorell, Kia Wiklundh, MSB1081 - mars 2017, ISBN 978-91-7383-733-0
2. ”Vägledning för skydd mot avsiktliga EM-hot”, Fortifikationsverket, 2017, ISBN 978-91-639-5650-8
3. ”Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, Tomas Hurtig, Sara Linder, Kia Wiklundh, Karina Fors, Sten E Nyholm, MSB1180 – februari 2018, ISBN 978-91-7383-805-4
4. ”Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur”, Kia Wiklundh, Sara Linder, Karina Fors, Tomas Hurtig, Sten E Nyholm, MSB1178 - februari 2018, ISBN 978-91-7383-803-0
5. 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.
6. ”Vägledning för Risk- och sårbarhetsanalyser”, Myndigheten för samhällsskydd och beredskap (MSB), MSB245 - april 2011, ISBN 978-91-7383-129-1.
7. ”Riskhantering - Principer och riktlinjer”, SIS Förlag AB, Svensk standard SS-ISO 31000:2009, publicerad 2010-03-30.
8. FM MSD16, Militärstrategisk doktrin för Sveriges militära försvar, 2016.
9. Fredrik Lindgren, ”Hotbildsunderlag i utvecklingen av civilt försvar”, FOI Memo 5089, 2014-10-14.
10. Daniel K Jonsson, ”Typfall 5: Utdragen och eskalerande gråzons-problematik, Komplettering av hotbildsunderlag i utvecklingen av civilt försvar”, FOI Memo 6338, 2018-01-31
11. MSB hemsida: https://www.msb.se/sv/Produkter--tjanster/Rakel/Om-Rakel/Vad-ar-Rakel/ (2017-11-22)
12. Jörgen Städje, ”Järnvägens signalsystem – principer och logik. Del 1”, IDG, https://www.idg.se/2.1085/1.591542/jarnvagens-signalsystem--principer-och-logik-del-1, 2014-11-16 (2017-11-22)
13. ”Göteborgskravallerna”, Wikipedia, https://sv.wikipedia.org/w/index.php?title=Göteborgskravallerna&oldid=42135410 (2017-11-22)

14. http://www.elsakerhetsverket.se/privatpersoner/EMC/Radiostorningar/ (2017-11-22)

15. https://radiostorning.pts.se/Home/index (2017-11-22)

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1179 - februari 2018 ISBN 978-91-7383-804-7