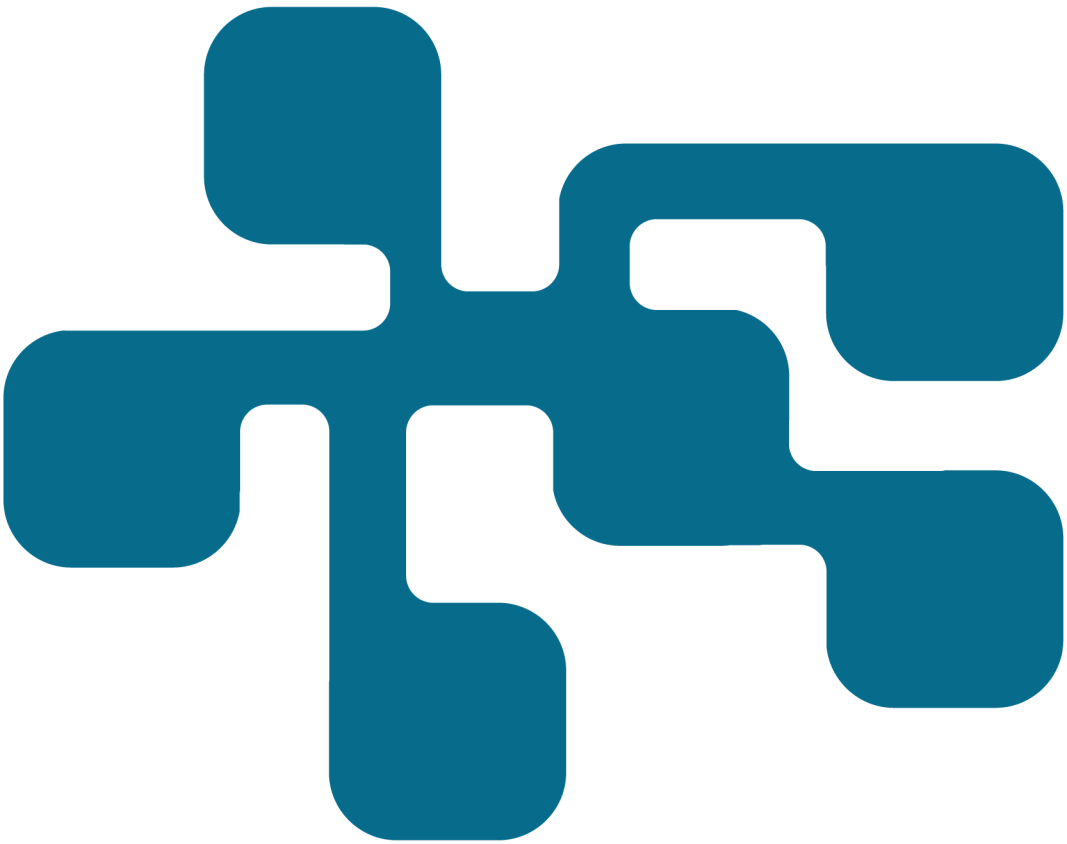
NCS3 - Elektromagnetiska hot mot trådlösa system

En studie av incidenter, möjliga hot och åtgärder

Anders Odell, Erik Zouave, Margarita Jaitner

FOI
MSB



FOI-R--4838--SE
MSB 2019-04982
ISSN 1650-1942

Maj 2020

Anders Odell, Erik Zouave, Margarita Jaitner

Elektromagnetiska hot mot trådlösa system

En studie av incidenter, möjliga hot och åtgärder

Titel	Elektromagnetiska hot mot trådlösa system – En studie av incidenter, möjliga hot och åtgärder
Title	Electromagnetic threats against wireless systems
Rapportnr/Report no	FOI-R--4838--SE
Månad/Month	Maj
Utgivningsår/Year	2020
Antal sidor/Pages	46
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	E13686
Godkänd av/Approved by	Malek Khan
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Denna studie har utförts av Totalförsvarets forskningsinstitut (FOI) på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), och utgör ett stöd i arbetet med att höja det nationella medvetandet om elektromagnetiska hot mot cyberfysiska system. Studien presenterar kortfattat hotbilden mot samhällsviktig verksamhet och ger exempel på både avsiktliga och oavsiktliga störningar i Sverige. Den redogör även för hypotetiska störningsscenarier och åtgärder mot elektromagnetiska hot, baserade på erfarenheter från berörda svenska myndigheter. Slutligen sammanfattar rapporten kort de bestämmelser som utvecklats för att främja elektromagnetisk säkerhet. Merparten av de åtgärder som studien identifierar är av förebyggande karaktär eller ingår som en del i ett strategiskt och mer övergripande arbete för att främja medvetenhet, samarbete och säkerhet. Utifrån de samlade resultaten föreslås ett antal områden för vidare studier.

Nyckelord: Elektromagnetiska hot, trådlösa system, cyberfysiska system.

Summary

This report presents a study carried out by the Swedish Defense Research Agency (FOI) on behalf of the Swedish Civil Contingencies Agency (MSB). The study aims to support the ongoing work to raise awareness about electromagnetic threats against wireless communication in cyber-physical systems. The report briefly summarizes the threat against critical infrastructure and systems in our society, and presents examples of intentional and non-intentional disruptions that has taken place in Sweden. Additionally, hypothetical scenarios of attacks and interruptions, as well as measures against electromagnetic threats, based on experiences among Swedish authorities, are presented. A short summary of existing regulations aimed to increase security against electromagnetic threats concludes the report. The majority of the measures identified in this study are either preventive in character, or are part of a strategic and comprehensive effort to raise awareness, increase spread of information, and enhance security. Based on the study´s collected result, a number of areas for further studies are proposed.

Keywords: Electromagnetic threats, wireless systems, cyber-physical systems.

Innehåll

1 Inledning

Denna rapport presenterar resultatet av en studie utförd av Totalförsvarets forskningsinstitut (FOI) på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB). Studien har utförts inom ramen för NCS3[1] som ett led i MSB:s arbete för att höja medvetenheten om riskerna med elektromagnetiska hot (EM-hot).

Målgrupp för rapporten är beslutsfattare, säkerhetsansvariga och tekniker med ansvar för styrsystem i samhällsviktig verksamhet.

1.1 Bakgrund

I takt med att allt mer elektronisk utrustning är uppkopplad blir det också vanligare med trådlösa förbindelser. Trenden med trådlös kommunikation framför trådbunden förekommer också inom sådana sektorer som traditionellt sett har lagt stor vikt vid robusthet i kommunikationssystemen. Idag återfinns trådlösa uppkopplingar i anslutning till den infrastruktur och utrustning som ligger till grund för många samhällsviktiga tjänster. Det kan medföra en sårbarhet för både avsiktliga och oavsiktliga incidenter som kan resultera i kommunikationsstörningar likväl som obrukbar utrustning. Ytterst kan det innebära att leveranser av samhällsviktiga tjänster blir påverkade. Ett första steg för att kunna hantera sådana risker är att höja medvetenheten om de potentiella sårbarheterna. Detta konstateras bland annat i rapporten *Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur*.[2]

Olika aktörers potentiella utsatthet för elektromagnetiska hot uppmärksammas även i den handlingsplan som myndigheterna i Samverkansgruppen för informationssäkerhet (SAMFI) har tagit fram som ett led i regeringens nationella strategi på området. I rapporten *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019 – 2022* åläggs MSB att ”tillhandahålla medvetandehöjande material om att minska störningskänsligheten vid användandet av trådlös kommunikation i industriella informations- och styrsystem som används i samhällsviktig verksamhet”.[3]

[1] NCS3 - Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet, https://www.foi.se/forskning/informationssakerhet/ncs3.html

[2] Hurtig, T. et al. 2018. Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur. FOI-S--5835--SE, MSB1180 - februari 2018

[3] MSB 2019. Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. MSB1351, 1 mars 2019

1.2 Syfte och mål

Denna rapport ska stödja MSB i arbetet med att höja medvetenheten om elektromagnetiska hot hos de aktörer som redan nu använder sig av trådlöst uppkopplade komponenter i anslutning till cyberfysiska system. Den ska också ge beslutsunderlag för de som i framtiden avser att använda sådana komponenter och system. Ett ytterligare syfte är att tillgängliggöra information och ge konkreta råd. Rapporten riktar sig främst till beslutsfattare och säkerhetsansvariga men också till teknisk personal som arbetar med utformning, anskaffning, drift och underhåll av system. Studien presenterar huvudsakligen åtgärder på ett övergripande plan, men ger även några konkreta åtgärdsförslag samt förslag på vidare studier inom området.

Följande frågor utgör studiens huvudfokus:

- Vilka typer av störningsincidenter kopplade till EM-hot och trådlösa system har förekommit i Sverige?
- Vilka typer av sådana störningar skulle kunna inträffa hos svenska aktörer?
- Vilka åtgärder har vidtagits, och kan fortsättningsvis vidtas, för att skydda verksamheten mot sådana typer av hot?

1.3 Metod och avgränsningar

Arbetet utgår ifrån den befintliga kunskap som har sammanställts i tidigare studier utförda av FOI och MSB inom ämnet elektromagnetiska hot. En inventering av öppet tillgängliga incidenter som har kopplats till elektromagnetisk påverkan har genomförts. Inventeringen inriktades huvudsakligen på sådana system som har trådlösa uppkopplingar och kan beskrivas som cyberfysiska system. Elektromagnetiska incidenter är svåra att identifiera som sådana, dels för att orsaken kan vara oklar på grund av låg medvetenhet om potentialen för den typen av störningar, dels för att en elektromagnetisk störning, i de fall den inte förstör utrustning, sällan efterlämnar några tydliga spår. En annan viktig aspekt, i synnerhet när det gäller system som är del av samhällsviktiga tjänster, är sekretess. En aktör som har drabbats av en elektromagnetisk incident kan vilja dölja detta, dels för att skydda information om hur systemen är uppbyggda, dels för att undvika nya incidenter via samma eller liknande attackvektorer.

Informationsinhämtning har genomförts genom litteraturstudier, intervjuer och en workshop. Vid workshopen deltog representanter från Försvarsmakten, Försvarets materielverk, Post- och Telestyrelsen, Fortifikationsverket, Luftfartsverket, Svenska Kraftnät och Teracom, med erfarenhet av att arbeta med att motverka elektromagnetiska hot.

Workshopen syftade till att samla in exempel på verkliga och hypotetiska incidenter samt åtgärdsförslag. Under workshopens första del ombads deltagarna att

fylla i en enkel incidentrapporteringsmall för att ”rapportera” händelser: sådana som har skett, och sådana som hypotetiskt skulle kunna ske i Sverige eller i Norden. Därefter sorterades idéerna med hjälp av post-it-lappar med syftet att skapa en kategorisering av verkliga och potentiella incidenter.

I workshopens andra del ombads deltagarna att utveckla åtgärdsförslag utifrån de incidentscenarion som de hade kunskap om. Åtgärdsförslagen kategoriserades efter en enkel uppdelning i förebyggande åtgärder, åtgärder som bör genomföras under en pågående incident, samt sådana som bör genomföras efter en konstaterad eller förmodad incident.

1.4 Definitioner

***Attackvektor*:** Ett tillvägagångsätt för angripare att störa eller skada ett mål. Exempelvis störsändare, mikrovågsvapen eller direktinjicering.

***Cyberfysiska system*:** System för fysisk styrning av maskiner och annan utrustning, alternativt system som använder sig av sensorer för datainhämtning från den fysiska omgivningen.[4]

***Elektromagnetiska hot, EM-hot*:** Avsiktlig eller oavsiktlig påverkan (inkluderat potential för genomförande) på system med elektromagnetisk strålning som resulterar i störning, förstörelse eller informationsläckage.

Elektromagnetisk kompatibilitet, (eng. ElectroMagnetic Compatibility) ***EMC*:** Egenskap hos elektronisk utrustning att fungera utan att störa annan utrustning, samtidigt som den tål den elektromagnetiska strålningen som finns i omgivningen.

Elektromagnetisk interferens, (eng. ElectroMagnetic Interference) ***EMI*:** När elektrisk eller elektronisk utrustning störs av fält eller strålning från ett utomstående objekt (annan utrustning eller naturliga källor).

Avsiktlig Elektromagnetisk interferens, (eng. Intentional ElectroMagnetic Interference) ***IEMI*:** När strålning eller elektromagnetiska fält avsiktligt genereras för att störa eller skada utrustning.[5]

Spoofing: Transmissionen av signaler med frekvenser som liknar legitima elektromagnetiska signaler, exempelvis inom GPS eller GNSS, i syfte att förfalska information eller lura en signalmottagare.[6]

---

[4] KTH 2017. Det här är cyberfysiska system. www.kth.se/blogs/reaktion/2017/08/det-har-ar-cyberfysiska-system/ (läst 2020-03-10)

[5] Giri, D.V. och Tesche, F.M. 2004. Classification of Intentional Electromagnetic Environments (IEME). IEEE Transactions on Electromagnetic Compatibility. vol. 46, no 3, pp. 322-328

[6] Huang, J. et al. 2016. GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky. ICT Express 2(1), 37-40 ; Chapman, A. 2017. GPS Spoofing. ECE Senior Capstone Project. 2017 Tech Notes

Mikrovågsvapen (eng. High Power Microwave) ***HPM-vapen***: Riktade mikrovågor med hög effekt i syfte att störa eller förstöra elektronisk utrustning.

1.5 Läsanvisning

I det första kapitlet presenteras bakgrunden till studien samt syfte, mål och metod. I kapitel 2 ges en kort bakgrund till elektromagnetiska hot samt hotbilden mot samhället. Kapitel 3 svarar på studiens två första huvudfrågor och redogör för de exempel på elektromagnetiska incidenter i Sverige, samt de hypotetiska incidentscenarier, som studien har identifierat. Därefter adresseras den tredje och sista huvudfrågan för studien. I kapitel 4 presenteras de åtgärdsförslag som identifierats, och i kapitel 5 sammanfattas kort de lagar och regleringar inom Sverige och EU som syftar till att minska risken för störningar från elektromagnetiska hot. Rapporten avslutas med en diskussion i kapitel 6 och sammanfattande rekommendationer i kapitel 7.

2 Hotbild

Här beskrivs kortfattat vad elektromagnetiska hot är, hur olika typer av elektromagnetiska incidenter kan kategoriseras, samt hur elektromagnetiska hot ingår i hotbilden mot Sverige.

2.1 Elektromagnetiska hot

Elektromagnetisk strålning utgörs av svängande kopplade elektriska och magnetiska fält, och uppstår då elektriska laddningar rör sig och ändrar hastighet. Frekvensen med vilka fälten svänger avgör vilken typ av strålning det rör sig om (t.ex. radiovågor, mikrovågor, synligt ljus eller gammastrålning).

Strålningen kan i sin tur accelerera elektroner i ledande eller halvledande material i objekt utanför strålningskällan så att elektriska strömmar uppstår i objektet, så kallade inducerade strömmar. Strömmarna kan ledas in i elektriska eller elektroniska komponenter via antenner, kablar eller höljen, eller induceras direkt i komponenterna. De kan där orsaka funktionsstörning eller, om strömmarna är tillräckligt starka, fysisk skada.

När elektromagnetisk strålning inducerar strömmar i komponenter genom antenner kallas det framvägskoppling. Det kan ske genom den frekvens utrustningen är konstruerad för att ta emot eller sända på och kallas då inombands framvägskoppling, eller genom andra frekvenser, vilket kallas utombands framvägskoppling. Om strålningen inducerar strömmar genom kablar, flänsar, höljen mm. som inte är antenner, kallas det bakvägskoppling. Kraftiga strömpulser kan också ledas in direkt på el- eller datakablar i en byggnad. Det kallas då direktinjicering.[7]

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.[8]

Effekttätheten hos den elektromagnetiska vågen avtar kvadratiskt med avståndet, d.v.s. en fördubbling av avståndet minskar effekttätheten med en faktor fyra. Att

[7] Wiklundh, K. et al. 2018. Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur. FOI-S--5840--SE, MSB1178 - februari 2018

[8] Hurtig, T. et al. 2018. Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur. FOI-S--5835--SE, MSB1180 - februari 2018

öka avståndet mellan verksamhetskritisk, känslig elektronisk utrustning och potentiella EM-hot är därför en effektiv åtgärd för att minska risken för negativ påverkan från elektromagnetisk strålning. Exempelvis bör det säkerställas att obehöriga inte kan komma i närheten av utrustningen.[9]

Ett elektromagnetiskt hot (EM-hot) utgörs av elektromagnetisk strålning eller av den utrustning som orsakar strålning, och som allvarligt kan skada utrustning och ge negativ påverkan på en verksamhet.

EM-hot kan klassificeras som naturliga, oavsiktliga och avsiktliga.[10] Naturliga hot är t.ex. blixtnedslag, solstormar och elektrostatiska urladdningar, Oavsiktliga hot är t.ex. när närliggande utrustning orsakar så kraftig elektromagnetisk interferens att en störning uppstår, eller när radiomottagare utsätts för radiofrekventa störningar. Avsiktliga hot innefattar alla fall då en antagonist avsiktligt genererar strålning i syfte att störa eller skada utrustning. Källorna för strålningen kan grovt delas in i störsändare och HPM-vapen.

Störsändare sänder en kontinuerlig eller intermittent signal, i ett eller flera frekvensband i syfte att störa en mottagare (eng. ”jammers”). Det finns tillfällen då aktörer kan använda störsändare legitimt, exempelvis kriminalvården för att förhindra att intagna kommunicerar med personer utanför anstalterna.

Mikrovågs- eller HPM-vapen sänder ut kortvariga men mycket kraftiga riktade pulser med radio- eller mikrovågsfrekvens som kan störa eller förstöra elektronisk utrustning eller komponenter.

Incidenter kan klassificeras på flera olika sätt. Antingen utifrån om de är naturliga, oavsiktliga eller avsiktliga, eller utifrån hur signalen tar sig in i utrustningen. De kan delas upp beroende på om störningen är temporär (den pågår endast så länge störsignalen är aktiv), eller bestående, antingen genom att störsignalen har orsakat fysisk skada som kräver reparation eller genom att utrustningen har försatts i ett icke fungerande tillstånd och kräver omstart. De kan också klassificeras utifrån vilken verksamhet som störs, vad syftet är, vilka konsekvenserna blir, vem som ligger bakom attacken, antagonistens förmåga (lekman, viss teknisk kompetens, expertkunskap) och vilken utrustning som används (kommersiell, ingenjörsmässig, militär).

[9] Hurtig, T. et al. 2018. Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur. FOI-S--5835--SE, MSB1180 - februari 2018

[10] Fortifikationsverket 2015. FortV Handbok 2015: Nyttosignaler och IEMI

Den här studien fokuserar på avsiktliga och/eller oavsiktliga incidenter. Den information eller data som krävs för att placera en misstänkt incident i de andra kategorierna kan vara svår att få tag på. Svårigheten att bedöma och analysera incidenter beror ofta på att det kan vara mycket svårt att i efterhand avgöra vad orsaken till en inträffad incident var, efter det att strålningen som orsakade störningen eller skadan upphört.[11] Detta medför att aktörer och verksamheter kan ha varit utsatta för elektromagnetiska hot utan att veta om det.

2.2 Hotbilden mot samhället

I Sveriges nationella säkerhetsstrategi[12] listas ett antal primära hot som på kort och lång sikt utmanar förmågan att skydda befolkningen och vårt land. Försvarsberedningen påtalar också i sina delrapport Motståndskraft att ett väpnat angrepp mot Sverige inte kan uteslutas, och belyser innebörden av begreppet gråzonsproblematik.[13] Flertalet av de hot och risker som säkerhetsstrategin och Försvarsberedningens rapport pekar ut skulle kunna utgöras av, realiseras genom eller påverkas av elektromagnetiska hot. Elektromagnetiska hot skulle dessutom antagligen kunna utgöra en del i gråzonsproblematik.

Särskilt kritiska för att skydda befolkningen och vårt land är samhällsviktiga verksamheter.[14] En stor del av de sektorer i samhället som MSB listar, där samhällsviktiga verksamheter återfinns, är genom digitaliseringen sårbara för elektromagnetiska hot. Antagonistiska aktörer som skulle kunna ligga bakom att realisera dessa hot utgörs i synnerhet av främmande militär makt, terroristorganisationer, våldsbejakande extremister och organiserad brottslighet.

Detta belyser vikten av att adressera elektromagnetiska hot och arbeta för att minimera sårbarheterna för dessa inom samtliga sektorer i samhället, och särskilt inom de som innefattar samhällsviktig verksamhet.

[11] Denna uppfattning uttrycktes vid workshopen.
[12] Regeringskansliet 2017. Nationell Säkerhetsstrategi. Statsrådsberedningen
[13] Försvarsberedningen 2017. Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025. Försvarsdepartementet, Ds 2017:66
[14] MSB. Samhällsviktig verksamhet. www.msb.se/samhallsviktigverksamhet (läst 2020-03-09)

3 Elektromagnetiska incidenter

Här presenteras ett antal exempel på incidenter identifierade genom litteratursökning, intervjuer och under workshopen.

3.1 Exempel på störningsincidenter hos svenska aktörer

Det finns ett antal incidenter i Sverige där den troliga orsaken var elektromagnetisk strålning. Dock är det svårt att avgöra i efterhand vad orsaken varit, vilket redan påpekats i kap. 1.1. Här redovisas ett antal exempel på incidenter i Sverige där orsaken med stor sannolikhet var, eller har bekräftats vara, EM-strålning. Incidenterna identifierades genom litteratursökning och intervjuer. Intervjuerna genomfördes över telefon.

3.1.1 Avsiktliga störningar

Ett anmärkningsvärt fall av kriminell användning av störsändare inträffade i samband med de så kallade Göteborgskravallerna under EU-toppmötet 2001. Demonstranter använde sig av störsändare för att störa polisiär radiokommunikation under kravallerna.[15] Polisradion var vid den tidpunkten inte krypterad, som Rakel nu är, vilket möjliggjorde detta tilltag.

Tjuvar har använt störsändare i samband med olika typer av stölder. I butiksmiljö skickar störsändarna ut radiovågor som gör butikernas larmbågar obrukbara. Tjuvarna kan promenera ut från butiken med stöldgods utan att larmet aktiveras. Att konstruera sådana sändare kräver visst tekniskt kunnande men är egentligen inte särskilt svårt. Sändarna är ungefär lika stora som ett cigarrettpaket.[16]

Användning av störsändare har också förekommit i samband med bilstölder. Störsändarna används då för att störa ut signaler från bilnycklar vid låsning av fordon. Bilarna står sedan olåsta och tillgängliga för tjuvarna.[17,18] I modernare bilar utan fysisk nyckel har tjuvar även börjat använda ”reläattacker” för att stjäla bilar. I

[15] Stenumgaard, P. 2011. Störningskänslighet hos civil trådlös konsumentteknik. FOI-R--3216--SE
[16] Göteborgsposten 2005. Störsändare mot larmbågar. www.gp.se/nyheter/göteborg/störsändare-mot-larmbågar-1.1166183 (läst 2020-01-15)
[17] Polisen 2019. polisen.se/utsatt-for-brott/skydda-dig-mot-brott/stold-och-inbrott/bilstold/ (läst 2020-03-20)
[18] Mitti.se 2016. Så lätt upptäcker han tjuvarnas störsändare. mitti.se/nyheter/upptacker-tjuvarnas-storsandare/?omrade=jarfalla. (läst 2020-01-15)

dessa attacker förstärker tjuven radiosignalen från en elektronisk nyckel (till exempel i hemmet) för att låsa upp och starta fordonet (exempelvis på parkeringen utanför).[19]

Polismyndigheten befarar att störsändare har blivit vanligare i bostadsinbrott för att störa ut larmtjänster. Trots att det endast i ett fåtal fall kunnat påvisas att störsändare använts misstänks att de använts i flera fall där bostadslarm inte fungerat eller gett sent utslag. Därför har vissa larmtjänster börjat rekommendera system med dubbla larmkanaler som säkerhetsåtgärd.[20]

3.1.2 Oavsiktliga störningar

Vattenproducent[21]

I samband med den amerikanska presidenten Barack Obamas besök i Stockholm 2013 upplevde en större vattenproducent störningar i radiokommunikationen till flera av sina anläggningar. Vattenreservoarer och pumpstationer i vattennätet övervakas från ett centralt kontrollrum genom radiolänkar. Kommunikationen är uppbyggd genom att signaler reläas från station till station. Därför kan kontrollrummet tappa kommunikationen med flera anläggningar även om det bara är en radiosändare/mottagare som störs ut. Radiostörningarna innebar dock inte några större driftsproblem eftersom anläggningarna är autonoma och aktören har god kunskap om vid vilka tidpunkter förbrukningen är stor och reservoarer behöver fyllas på. De har dessutom driftspersonal som kan åka ut och styra anläggningar på plats vid rapporterade fel. Störningen var inte heller kontinuerlig utan kontakten med anläggningarna ”kom och gick”.

Vattenproducenten lyckades inte lokalisera källan till störningen under tiden den pågick. Det är inte heller i efterhand klarlagt vad störningarna berodde på. Möjliga orsaker kan ha varit störsändare i anslutning till president Obamas bilkortege,[22] eller mobila radaranläggningar som det svenska försvaret placerade ut i Stockholm för att övervaka luftrummet.[23]

Vattenproducenten hade redan innan incidenten under president Obamas besök börjat ersätta radiolänkar med fiber. Huvudsyftet var då att bygga bort kritiska

[19] Motormagasinet 2018. Nyckellösa bilar stjäls genom relä-attacker. www.motormagasinet.se/article/view/622792/nyckellosa_bilar_stjals_genom_relaattacker (läst 2020-01-15)
[20] Sveriges radio 2017. Tjuvar slår ut villalarm med störsändare. sverigesradio.se/sida/artikel.aspx?programid=93&artikel=6659331 (läst 2020-01-20); SVT Nyheter 2015. Tjuvar använder störsändare – slår ut larmet. www.svt.se/nyheter/lokalt/smaland/fler-tjuvar-anvander-storsandare-slar-ut-larmet (läst 2020-01-15)
[21] Intervju med enhetschef vid vattenproducent, 2020-02-26.
[22] Aftonbladet 2013. Obamas bilar kan ha olaglig störutrustning. www.aftonbladet.se/nyheter/a/ng0yjo/obamas-bilar-kan-ha-olaglig-storutrustning (läst 2020-04-16)
[23] DN 2013. Försvaret hjälper till att skydda Obama. www.dn.se/nyheter/sverige/forsvaret-hjalper-till-att-skydda-obama/ (läst 2020-04-16)

sektioner i radionätet. Radiolänkarna är känsliga för t.ex. åska och kan alltså påverkas eller förstöras av naturliga händelser.

Efter incidenten intensifierades arbetet med att ersätta radiolänkarna och kommunikationen är idag mer robust. Dock kan beroendet av radiolänkarna inte byggas bort helt då vissa stationer ligger på platser som gör att det är svårt eller dyrt att dra fiber dit. Vid nybyggnation av anläggningar används fler alternativ för kommunikation.

Vattenproducenten har idag en större kunskap om risker med elektromagnetiska hot och är mer observant kring mönster och systematik vid störningar. De har också en aktiv omvärldsanalys för att förutse eller förstå liknande händelser.

Leverantören av radioutrustningen till vattenproducenten använder idag inte system med kända svagheter vid nyinstallation av radioutrustning. De bygger också bort dessa svagheter i befintliga radionät genom att installera annan radioutrustning.[24]

Bergbanan Skansen[25]

I samband med president Obamas besök upplevde även bergbanan på Skansen störningar. Bergbanan har ett trådlöst nödstopp som behöver ha kontinuerlig kontakt med en styrenhet för att inte stoppa tåget, en form av död-mans-grepp. Den trådlösa kontakten fungerade intermittent, vilket gjorde att bergbanan stannade hela tiden. Vid felsökning kunde leverantörens servicepersonal konstatera att den mottagande enheten registrerade en mycket hög brussignal, vilket störde ut den riktiga signalen. Bergbanan stoppades tills störningen försvann.

Hamn[26]

I en större hamn inträffade en incident där en entreprenör inom tungdykning upplevde att radiokommunicerande utrustning inte fungerade. Det omfattade störningar i kommunikationen med dykarna, radiostyrning av en höglyft, start av personbilar via key-less system och att låsa/öppna dörrar på personbilar (totalt 6 st. olika personbilar). Störningen pågick under en kortare period.

Entreprenören frågade hamnbolaget om de hade någon störsändare, vilket inte var fallet. Bolaget i sin tur frågade fartyg i hamnen om någon hade en störsändare, men inget fartyg uppgav att de hade någon sådan. Hamnbolaget gjorde en utredning av incidenten där det konstaterades att störningen hade kunnat orsakas av en typ av störsändare som visserligen inte är avancerad, men som inte är tillåten att använda i Sverige. Utredningen kunde inte fastlägga orsaken till störningen men antog att den orsakades av någon eller några personer som inte förstod vilken typ av utrustning de använde, alternativt inte förstod konsekvenserna av att

[24] Intervju med leverantör av radioutrustning, 2020-02-27.
[25] Intervju med konsult med ansvar för drift av bergbanan, 2020-02-27.
[26] Intervju med enhetschef vid hamnen, 2020-03-02

använda den. Ytterligare en hypotes var att störningen utfördes medvetet som ett test.

Hamnbolaget informerade Säpo, den lokala Polisen, Transportstyrelsen, MSB, Kustbevakningen och Försvarsmakten om incidenten. Bolaget kontaktade även andra hamnar i Sverige, men ingen annan hamn hade varit med om någon liknande incident. Bolaget har inte vidtagit några åtgärder efter incidenten då de upplever att de saknar kunskap om vad de skulle kunna göra för att skydda sig.

Elbolag[27]

Ett större elproduktions- och distributionsbolag i Sverige råkade ut för en incident där det centrala kontrollrummet tappade radiokontakten med ett antal anläggningar. Incidenten ledde inte till något avbrott i eldistributionen då anläggningarna fungerar autonomt. Däremot kunde bolaget inte genomföra planerad service vid de påverkade anläggningarna under tiden störningen pågick. Störningen pågick under några dygn och bolaget kunde inte vidta några direkta åtgärder. När störningen försvann återknöts radiokontakten med anläggningarna.

Orsaken till störningen var att bolaget använde radioutrustning som arbetade på en frekvens som Försvarsmakten nyttjade. Försvarsmakten hade meddelat detta tidigare men den informationen hade inte nått rätt instans inom elbolaget för att åtgärder skulle vidtas. Anledningen till det antas av respondenten vara att den person eller enhet inom bolaget som mottog informationen inte förstod vidden eller konsekvenserna av den. Respondenten förklarar vidare att det inom bolaget har funnits en övertro på anläggningarna och utrustningen, eftersom den har fungerat problemfritt under så många år. I elnätet finns det mycket gammal utrustning som inte byts ut så länge den fungerar.

Bolaget har efter incidenten vidtagit åtgärder. Radiolänkar har bytts ut på flera stationer till sådana som arbetar på andra frekvenser. Bolaget jobbar också på att höja kunskapen kring radiostörningar. Detta anges vara särskilt viktigt inom de centrala säkerhetsfunktionerna eftersom det är de som har kontakt med externa aktörer som MSB, Försvarsmakten och Fortifikationsverket.

Respondenten menar att lärdomen av denna och liknande incidenter är att radiobandet är enormt belastat och att det kräver minutiös kontroll för att undvika överbelastning. Dessutom använder många aktörer samma leverantörer vilket leder till att samma typ av utrustning finns på många platser. Detta ökar också riskerna för störningar.

[27] Intervju med ansvarig för informationssäkerhet, 2020-03-02.

Andra incidenter

Det finns uppgifter om att legitima störsändare kan störas ut av andra signaler. Exempelvis menar Kriminalvården vid Norrtäljeanstalten och Hall att deras störsändare som förebygger mobilkommunikation till och från intagna påverkats av placeringen av mobilmaster i kommunen. Mobilmasterna ska ha varit så nära anstalterna och signalerna så starka att störsändarna inte haft avsedd verkan.[28]

Vid en annan incident hade en trådlös streckkodsläsare installerats vid ett köpcentrum i Borås. Vid läsaren fanns en basstation som gav upphov till kontinuerlig strålning. Signalen var så stark att den blockerade alla andra mottagare i området. Källan till störningen hittades genom pejling. Det är dock inte säkert att den metoden fungerar i alla fall då störsändare misstänks. Störningar kan vara intermittenta vilket gör sändarna svåra att hitta.[29]

Piloterna kunde vid flera tillfällen inte använda flygradion vid start och landning vid Trollhättan-Vänersborgs flygplats.[30] Orsaken var att en stor elektronisk reklamskylt störde ut flygradion. Mekanismen bakom att reklamskyltar kan störa ut radiokommunikation är att lysdioderna i skyltar snabbt växlar mellan på och av, vilket i sin tur ger upphov till EM-strålning. Varje lysdiod har en mycket låg effekt men eftersom skylten är uppbyggd av många dioder kan den sammanlagda effekten bli hög. Även styrningen av skyltarna eller kraftförsörjningen kan ge störningar.

Stenumgaard har tidigare redogjort för ett antal oavsiktliga störningar:

- Störning av trådlös länk i processmaskin med produktionsstopp till följd.
- Störningar av fjärrstyrda billås för bevakningspersonal i vissa industriområden med blockerad upplåsning till följd.
- Störning av räddningstjänstens radiosystem orsakad av elektriska installationer.[31]

[28] ComputerSweden 2005. Fångvårdens störsändare slås ut av mobilmaster. computersweden.idg.se/2.2683/1.8642/fangvardens-storsandare-slas-ut-av-mobilmaster (läst 2020-01-16)
[29] Sveriges radio 2011. Radiostörning ligger bakom krånglande billås. sverigesradio.se/sida/artikel.aspx?programid=105&artikel=4753042 (läst 2019-11-04)
[30] Olsson, H. 2011. Radiostörningar från reklamskyltar i Vänersborg. Elsäkerhetsverket Dnr 11EV4910
[31] Stenumgaard, P. 2011. Störningskänslighet hos civil trådlös konsumentteknik. FOI-R--3216--SE

3.2 Exempel på incidentscenarier och möjlig effekt på samhället

Här presenteras fyra exempel på EM-incidenter baserade på resultaten från workshopen. Deltagarna fick arbeta i mindre grupper för att föreslå incidentscenarier med information om eventuella angreppsvektorer, utrustning, metoder och effekter. Dessa incidentscenarier utvecklades och sammanställdes sedan av rapportförfattarna.

3.2.1 Spoofing av globala satellitnavigationssystem

Globala satellitnavigationssystem GNSS (Global Navigation Satellite System) tillhandahåller korrekt position och tid. Användningen av GNSS är utbredd inom transportsektorn, vilket gör att många system och tjänster är beroende av GNSS för att fungera korrekt. Det gör att en störning i GNSS kan få allvarliga konsekvenser. GNSS-mottagare är mycket lätta att störa, exempelvis på grund av att den mottagna satellitsignalen är svag.

Spoofing mot GNSS innebär att en mottagare får signaler som anger exempelvis felaktig positioneringsdata. Ett sådant angrepp kan få mottagaren att uppfatta en falsk position (till och med fel världsdel).[32] Om tiden i GNSS spoofas kan det dröja innan det upptäcks (någon förklaring till detta gavs inte men en möjlig förklaring kan vara att digitala tidsangivare normalt anses trovärdiga, och att dessa därför sällan kontrolleras mot andra källor). Eftersom mänsklig styrning lättare uppfattar uppenbara fel torde effekterna av angrepp med förfalskad positioneringsdata förmodligen vara mer påtagliga i en framtid med hög grad av automatisering av olika typer av fordon och robotar.

Workshopdeltagarna bedömde att spoofing vid flygplatser är ett scenario med hög sannolikhet men att konsekvenserna inte behöver bli särskilt allvarliga. För att störa flygtrafiken behöver en hotaktör inte nödvändigtvis inrikta spoofingen mot flygbolag. Autonoma underhållsrobotar för plogning och gräsklippning skulle kunna störas så att de exempelvis kör ut på landningsbanor och skapar förseningar i flygtrafiken. Deltagarna ansåg också att konsekvenserna skulle kunna bli allvarligare vid angrepp mot bagagesystemen på flygplatser eftersom inga flygplan kan lyfta om de inte lastats med rätt bagage.

Deltagarna bedömde att konsekvenserna av spoofing mot förarlös kollektivtrafik skulle kunna bli omfattande. Om GNSS eller trafikstyrningssystem för förarlösa bussar slås ut skulle kollektivtrafiken förmodligen bli stående, vilket skulle få negativ inverkan och medföra ekonomiska förluster för kollektivtrafiken, individer och företag.

[32] GPS World 2019. How do we ensure GNSS security against spoofing? www.gpsworld.com/how-do-we-ensure-gnss-security-against-spoofing/ (läst 2020-01-16)

I ytterligare ett hypotetiskt exempel används spoofing för att styra om automatiserade vägtransporter för att stjäla lasten. Hotaktören påverkar då fordonets system med falsk positioneringsdata och får fordonet att transportera godset till en plats där det ostört kan lastas om. Störning av GNSS-signaler skulle även kunna göra att det inte går att spåra transporterna. Liknande angrepp skulle potentiellt kunna få större konsekvenser om syftet inte är att stjäla gods, utan att få fordon att agera unisont med svärmbeteende för att störa annan trafik eller sabotera mål.

3.2.2 Störning av automatiserade spärr- och gränskontroller

I detta scenario används störsändare, som i dagsläget blivit relativt vanliga redskap bland brottslingar (till exempel stöldligor), för att efterlikna eller störa ut de frekvenser som annan teknologi är beroende av.

I workshopdeltagarnas scenario används handhållna störsändare för att slå ut automatiserade passkontroller. Detta tvingar personalen vid flygplatser och andra gränskontroller att återgå till manuella kontroller. Konsekvenserna blir personalplaneringsproblem, köbildning och försvårad implementering av säkerheten vid gränskontrollerna. Sådana incidenter skulle kunna vara ett första steg i ett större angrepp som exempelvis en terrorattack, genom att angripa den folksamling som uppstår till följd av flaskhalsen.

3.2.3 Radar slår ut eller kopplar in på utrustning

Radarteknik (Radio Detecting and Ranging) förlitar sig på kortvågiga radiovågor för att identifiera och positionera objekt. Dessa radiovågor kan plockas upp av annan elektronisk utrustning. I situationer där radarn används i olika farkoster kan andra system påverkas allteftersom farkosten förflyttar sig på ett oförutsägbart sätt. Detta kan försvåra spårningen av störningarnas orsak.

I workshopdeltagarnas scenario plockar oskärmat kablage eller antenner i fordon upp signaler från radar. Ett modernt fordon kan ha ett stort antal antenner.[33] Detta kan hypotetiskt orsaka att fordonet stannar eller inte går att manövrera. I ett exempel med allvarliga konsekvenser påverkas en lastbil eller liknande tungt motorfordon vid eller på en bro av en fartygsradar. Fordonets styrning slås ut så att det kraschar in i ett brofundament, vilket gör att trafiken över bron stoppas till dess att skadan på bron kan bedömas och åtgärdas.

[33] Valassi, C. och Gustafsson, T. 2018. NCS3 - Kartläggning av elektroniska styrsystem i tunga fordon. FOI Memo 6358

3.2.4 Bredbandiga störningar orsakade av konsumentelektronik

Bredbandiga störningar i varierande frekvensband kan uppstå från billig konsumentelektronik som solceller och LED-lampor och andra vanliga installationer.[34, 35] En underliggande orsak kan vara otillräcklig EMC-testning eller standardisering för utrustningen. Mängden elektroniska apparater ökar i samhället och även sådana som är trådlöst uppkopplade. Strålningen påverkar möjligheten för radiokommunikation. Konsekvenserna av dessa vardagliga EM-störningar kan i vissa fall vara allvarliga. Exempelvis kan de störa ut AM-flygradio, vilket påverkar flygsäkerheten. Också annan radio kan störas och påverka kommunikationen vid krishantering och räddningstjänst, vilket påverkar aktörers operativa förmåga. I ett större samhällsperspektiv kan konsekvensen av ökad vardagsanvändning av utrustning som skapar bredbandiga störningar bli att radiokommunikation försvåras generellt.

[34] Elsäkerhetsverket 2019. www.elsakerhetsverket.se/om-oss/press/nyhetsbrev/2019/december/storande-solceller/ (läst 2020-03-20)

[35] Elsäkerhetsverket 2018. www.elsakerhetsverket.se/om-oss/press/nyhetsbrev/nyhetsbrev-elinstallatorer/2018/nummer-2/installera-belysning-ratt-och-undvik-emc-problem/ (läst 2020-03-20)

4 Åtgärder mot EM-relaterade störningsincidenter

Här presenteras exempel på åtgärder för att skydda trådlösa system och cyber-fysiska system mot EM-relaterade störningsincidenter. Åtgärderna har identifierats genom litteratursökning och vid workshopen, där myndighetsexperter på området deltog. Under workshopen sammanställdes deltagarnas åtgärdsförslag och kategoriserades efter en enkel uppdelning i förebyggande åtgärder, åtgärder som bör genomföras under en pågående incident samt sådana som bör genomföras efter en konstaterad (eller förmodad) incident. Utifrån dessa källor har författarna av denna rapport genomfört en förfining av kategoriseringen av åtgärderna. Åtgärdskategorierna illustreras i Figur 1.

Figur 1. Kategorier av olika åtgärder som framkom vid workshopen. Att höja medvetenheten bedöms av rapportförfattarna som grundläggande för de andra åtgärderna.

4.1 Höj medvetenheten

Workshopdeltagarna påpekade att medvetenheten och kunskapen om EM-hot generellt sett måste höjas. Att höja medvetenheten är en grundläggande åtgärd för samtliga påföljande åtgärder och incidenthanteringsförmågan på alla nivåer i samhället. På ledande nivåer innebär en låg medvetenhet om riskerna och låg kunskap inom området att frågorna inte prioriteras eller uppmärksammas tillräckligt inom organisationer.

Deltagarna föreslog ett par medvetandehöjande åtgärder. Först behöver myndighetssamverkan utökas för att möjliggöra fler erfarenhetsutbyten. Det kan möjliggöra att individer och organisationer kan lära av varandra vad det gäller sårbarheter, hot, åtgärder och metoder, samt ger möjlighet att identifiera och bevaka

sektoröverskridande beroenden. Det ger också möjlighet att dela lärdomar efter incidenter. Deltagarna efterfrågade även utbildning för exempelvis verksamhetsansvariga, upphandlare, och inköpare inom fler sektorer än de som primärt sysslar med trådlös kommunikation, exempelvis elproduktion.

Författarna av denna rapport tillägger till detta att kvaliteten på medvetandehöjande insatser förmodligen är avhängig myndigheters och andra organisationers förmåga att detektera och hantera misstänkta EM-incidenter. Medvetenhet byggs till del genom erfarenhet, bland annat genom att detektera och hantera incidenter, samt genom att utvärdera arbetet med incidenterna i efterhand.

4.2 Reglera

Deltagarna på workshopen ansåg att arbetet med att reglera och utöva tillsyn över användningen av trådlös datakommunikation behöver fortsätta.

Med ökad användning av elektronisk utrustning i allmänhet och trådlös kommunikation i synnerhet blir frekvensmiljön mer och mer fylld och förorenad. Samtidigt blir fler verksamheter mer beroende av radio- och trådlös datakommunikation och sårbarheterna ökar. Deltagarna efterfrågade lagkrav på säkerhet och redundans, speciellt för samhällsviktig verksamhet.

Utökad reglering skulle även innebära behov av effektiv tillsyn för att tillgodose att bestämmelserna efterlevs. Aktörer behöver i samband med detta också vägledning och stöd för att kunna uppfylla kraven. Exempelvis kan vägledning kring hur redundans ska säkerställas behövas.

Ytterligare ett exempel på reglering är avskilda frekvensband för vissa verksamheter där inga andra sändningar får förekomma. Detta kräver i så fall en rigorös tillsyn så att inga otillåtna sändningar på frekvensen förekommer, och så att utrustning som kan sända på aktuell frekvens inte säljs i landet.

Deltagarna lyfte också vikten av att specificera och följa EMC-standarder och certifieringar för utrustning. Att standarder efterlevs av aktörer måste följas upp, men även bättre marknadskontroll av produkter behövs. Här ansåg deltagarna att tillsynsansvariga myndigheter måste ha större befogenheter att utreda och ta bort osäkra produkter från marknaden och införa sanktioner mot undermåliga leverantörer eller försumliga användare. Som en åtgärd föreslogs skapandet av en expertgrupp med hög teknisk kännedom och auktoritet som skulle ansvara för kommunikation med den högsta ledningen inom organisationer inom respektive sektor.

Det påpekades även att tillsynsansvariga myndigheter och ansvariga för arbetet med reglering behöver återkoppling från aktörernas erfarenheter från arbetet med EM-hot. På detta sätt kan det skapas en överblick för att tillgodose att regleringen har de effekter som avsetts och att den kan uppdateras för att tillgodose gemensamma behov.

En övergripande frågeställning som workshopdeltagarna diskuterade var om det behövs en annan struktur för teknikregleringen. Medför komplexitet, resurskrav och höga kompetenskrav behov av centraliserad kontroll? Ett förslag var en myndighet med större möjlighet att exempelvis stoppa vissa produkter på marknaden. En sådan myndighet kan också utveckla eller rekommendera verifierings- och valideringsmetoder för att säkerställa att utrustning klarar elektromagnetiska störningar, enligt deltagarna.

4.3 Kravställ

Vid inköp av utrustning eller upphandling av system och tjänster måste en tydlig kravställning för utrustningen eller mot leverantören finnas. Kraven kan exempelvis handla om EMC, tålighet mot EM-hot, redundans med mera.

Vilka krav som bör ställas måste noggrant analyseras innan inköp eller upphandling. Generella krav och allmängiltiga säkerhetskrav utarbetas exempelvis lämpligen inom ramen för en säkerhetsskyddsanalys[36] och utifrån nätverks- och informationssäkerhet.[37] Deltagarna lyfte frågan om hur höga eller långtgående säkerhetskrav som kan ställas. Att exempelvis köpa in och underhålla redundanta system blir troligtvis dyrt.

Försvarsmakten kravställer exempelvis att tekniska system ska vara robusta, enligt representanten vid workshopen. Det innebär att utrustning och system ska kunna bibehålla en begränsad funktionalitet även när en stor del av den har förstörts eller inte längre fungerar. Funktionaliteten och prestandan avtar gradvis när fler och fler komponenter fallerar. Syftet är att undvika plötsligt totalt avbrott i funktionalitet eller verksamhet.[38]

4.4 Förebygg

Organisation och rutiner för kontinuerligt säkerhetsarbete och incidenthantering måste vara utformade redan innan incidenter inträffar. Vid en incident och bortfall av funktionalitet måste det finnas tydliga rutiner för personer på alla nivåer om hur de ska agera och med vilka de ska kommunicera. Detta kan handla om inarbetade kommunikationsvägar inom en verksamhet, eller mellan verksamheter och myndigheter. Särskilt viktigt är att beslutsfattande och ledande nivåer informeras tidigt. Rutiner för incidenthantering måste också övas på alla nivåer.

[36] Säkerhetspolisen 2019. Säkerhetspolisens föreskrifter om säkerhetsskydd. PMFS 2019:2
[37] MSBFS 2018:8. Föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. Myndigheten för samhällsskydd och beredskaps författningssamling
[38] SearchNetworking 2007. Graceful Degradation. searchnetworking.techtarget.com/definition/graceful-degradation (läst 2020-03-09)

Olika typer av analyser (exempelvis säkerhetsskyddsanalys) är grundläggande för att kunna förebygga att hot realiseras och incidenter blir kritiska. Analyserna bygger oftast på att metodiskt identifiera hot, sårbarheter och risker i den egna verksamheten och därefter utarbeta lämpliga åtgärder. Analytiska metoder som kan användas är:

- FMEA (Failure Modes and Effects Analysis), feleffektsanalys. Innebär att systematiskt förutsäga möjliga fel och konsekvenser, och att bedöma lämpliga åtgärder.
- FTA (Fault Tree Analysis), felträdsanalys. En deduktiv metod som klargör de logiska kopplingarna mellan orsaker, delhändelser och fel.

Försvarsmakten arbetar med metodutveckling inom området och kan tjäna som en förebild eller inspiration.

System bör prövas och analyseras innan de tas i drift eller köps in. Som ett exempel testas bilar för påverkan av störningar i fler frekvenser samtidigt. När ny utrustning ska inskaffas eller system upphandlas måste alltid frågan ställas om trådlös teknik alls ska användas. Vad är fördelarna med trådlöst och vad är riskerna? Dessa måste sedan vägas mot varandra.

Deltagarna ansåg att den första åtgärden för att minimera risken för EM-störningar bör vara inbyggt skydd i systemen och arkitekturen. Under workshopen diskuterades främst avskärmning, redundans och minimering av angreppsvektorer som konkreta åtgärder inom inbyggt skydd.

Avskärmning avser att bygga in fysiskt och tekniskt skydd i och omkring sin utrustning. Det kan exempelvis innebära att skärma av utrustningen för att skydda den mot strålning, (med en s.k. Faraday-bur[39]). För ledningsbundna signaler kan kontakter förses med filter som bara släpper igenom signaler med rätt frekvens eller signatur. 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[40] som hindrar alltför höga effekter att nå de känsliga komponenterna i mottagarenheten. Det hjälper dock inte mot störsändare.[41]

En annan aspekt av avskärmning är perimeterskydd. Det innebär fysiska barriärer som hindrar obehöriga från att komma i närheten av det som ska skyddas. Där ingår också patrullerande skyddsvakter med rätt utbildning, rutiner och utrustning.

[39] En Faraday-bur innebär att utrustningen är innesluten i ett metallskal eller metallnät som skyddar mot elektromagnetisk strålning av vissa frekvenser. Nätets finmaskighet avgör hur höga strålningsfrekvenser som nätet kan stoppa. För att skydda mot de högsta frekvenserna bör man använda ett solitt metallskal.

[40] Transientskydd utgörs av en anordning som kortsluter ledningsbunden elektromagnetisk energi om spänningen är över en viss nivå. I sin enklaste utformning kan det utgöras av ett gnistgap.

[41] Hurtig, T. et al. 2018. Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur. FOI-S--5835--SE, MSB1180 - februari 2018

De kan före eller under en incident upptäcka främmande apparater eller utrustning. En deltagare föreslog att skyddsvakter kan utrustas med HPM-källor som kan förstöra störande utrustning på avstånd. Ett utökat perimeterskydd, dvs. att öka avståndet mellan skyddsvärd utrustning och det område dit allmänheten har tillträde, är också en effektiv åtgärd, se kap. 2. Det bästa skyddet vad det gäller avskärmning, poängterade en deltagare, utgörs av bergrum. Den lösningen kan dock aldrig bli aktuell för alla aktörer som behöver skydda sina system, då antalet bergrum är starkt begränsat, och nya bergrum är kostsamma att anlägga. Ett alternativ för anläggningar som inte kan förläggas i bergrum är att placera viktig utrustning centralt i byggnaden, dvs. långt från ytterväggar. Det kan utgöra ett komplement eller alternativ till utökat perimeterskydd.

Redundans är ett annat sätt att tekniskt skydda system mot störningar. Detta är speciellt viktigt för systemkritisk funktionalitet och utrustning ansåg deltagarna. Redundans kan innebära separata system som inte kräver uppkoppling eller signalkommunikation om den primära är förstörd. Sådana system kan eventuellt till och med vara helt analoga.

Minimera angreppsvektorer är ytterligare en förberedande åtgärd som deltagarna diskuterade. Minimering av angreppsvektorer är både ett tekniskt och strukturellt problem. Inom vissa sektorer kan ett fåtal företag vara ansvariga för en stor del av verksamheten, och äger en stor del av infrastrukturen inom sektorn (man lägger många ägg i samma korg). Ett företag har ofta samma system i alla anläggningar vilket innebär att många anläggningar har samma sårbarheter och risker. Hittar en antagonist en angreppsvektor i ett system blir flera anläggningar sårbara. Å andra sidan kan det finnas fördelar med stora företag jämfört med många små. Stora företag kan ha större finansiella och resursmässiga möjligheter att bedriva ett systematiskt skyddsarbete. Små företag kanske inte alltid har förutsättningar för detta. Denna problematik kan eventuellt avhjälpas med bättre styrning och stöd från stat och myndigheter.

4.5 Detektera och hantera

En metod för att detektera störningar som föreslogs av deltagarna under workshopen är att ha en stor mängd detektorer eller störsensorer. Ett exempel är att skanna radiofrekvenser (RF-scanning[42]) för snabb detektion. Deltagarna ansåg att utrustning och system automatiskt bör kunna detektera avvikelser, störningar och fel i funktion, drift och verksamhet. Vid en anomali bör det finnas möjlighet att ”spela in” störningen eller signalerna i en ”svart låda”, oberoende av om systemet eller utrustning slås ut. Detta för att kunna analysera störningen i efterhand.

Deltagarna efterfrågade även automatiserade system som loggar signaler och data, rapporterar fel och larmar, samt vidtar enklare åtgärder som att stänga av vissa

[42] Radio Frequency – frekvenser inom radiobandet.

system eller nätverk, alternativt växlar över till en ostörd frekvens.[43] En fråga som lyftes var om det är möjligt att bygga in kontrollfunktioner som kan kontrollera och detektera störningar i funktionaliteten men som själva är okänsliga för EM-hot (och även andra typer av cyberhot). De lyfte också frågan om det är möjligt att ha funktioner för att få ut data från utrustning som slås ut eller förstörs.

Deltagarna vid workshopen poängterade att det är viktigt att logga den vanliga driften och den normala EM-miljön. Utifrån detta kan sedan en normalbild av tillståndet i systemen och i EM-miljön skapas. Det momentana tillståndet i systemen kan sedan jämföras mot detta normaltillstånd för att lättare upptäcka anomalier och incidenter. Detta möjliggör tidigare detektion av incidenter eller angrepp. Eventuellt ger det också en bättre förberedelse när en incident inträffar. Detta efterfrågades både lokalt för enskilda verksamheter, likväl som nationellt för hela landet.

Det poängterades att det är enklare att detektera störningar vid stationära system då man kontinuerligt kan scanna den omgivande miljön för avvikande signaler. Vidare kan påverkade organisationer, efter detektering, triangulera för att lokalisera störningskällor.

Har man förmågan att detektera störningar och incidenter måste även en beredskap finnas för att handskas med situationen. Om möjligt kan system stänga av komponenter som är påverkade, och eventuellt till och med koppla över till redundanta system. Avstängningar kan genomföras med manuella eller automatiserade åtgärder. Likaledes kan det vara möjligt att manuellt eller automatiskt växla över trådlös kommunikation till ostörda kanaler och frekvenser.[44]

4.6 Erfarenhetshantering

Efter en incident måste erfarenheterna tas till vara och användas i säkerhetsarbete, kravställning och reglering. Deltagarna föreslog att verksamheter bör upprätta en databas med incidenter, konsekvenser, agerande, lärdomar och vidtagna åtgärder. De måste ställa sig frågan vad som kan förändras för att incidenten inte ska kunna upprepas. Strategier och rutiner ska ändras efter lärdomar av incidenter.

Störningar och incidenter bör också kartläggas nationellt. Var och när sker de? För detta krävs en strukturerad incidentrapportering, och sannolikt fler mätstationer eller sensorer.

[43] Flera aktörer håller på att utveckla utrustning som kontinuerligt kan övervaka olika frekvensband, t.ex. RF-Oculus (Linder, S. et al. 2019. Telekonflikt - Sammanfattning 2018-2019. FOI-R--4832--SE).
[44] Jmfr. militär automatiskt frekvenshoppande utrustning.

5 Laglig förankring

Det finns i dagsläget ett antal bestämmelser som reglerar elektromagnetisk säkerhet. Utrustning som avger elektromagnetisk strålning[45] är reglerade i Sverige liksom användandet av radiofrekvenser. Detta innebär att det inte är tillåtet att använda utrustning med elektromagnetisk strålning för att störa annan teknisk utrustning. Flera lagar medför även krav på exempelvis tillverkare och distributörer att förebygga sådana störningar. Lagarna medför också påbud för vissa typer av verksamheter att skydda sina system mot elektromagnetiska störningar som en del i skyddet av nationell säkerhet, konsumenter och individers rättigheter. Sammantaget finns det alltså skyldigheter både att avstå från att störa verksamhet och teknik, samt att skydda verksamhet och teknik som riskerar att störas av elektromagnetiska emissioner.

Innan den svenska regleringen redovisas, finns det dock anledning att uppmärksamma regleringen av elektromagnetisk kompatibilitet på EU-nivå. Det finns även ett antal internationella EMC-standarder som kan vara relevanta.[46] Det finns dock inte utrymme för att redovisa dessa i den här studien.

5.1 Europeiska unionens EMC-direktiv

I takt med att samhället har blivit allt mer digitaliserat och beroende av elektronik och utrustning som avger elektromagnetisk strålning har det uppstått ett behov av reglering på området. Inom Europeiska unionen specificerar EMC-direktivet[47] hur elektromagnetisk kompatibilitet för elektroniskt styrda enheter ska utformas. Direktivet handlar inte om utrustningens säkerhet utan är begränsad till att reglera enbart aspekter av elektromagnetisk emission och kompatibilitet med fokus på produkternas användbarhet.[48]

Direktivet gäller, med få undantag, all utrustning inom unionens inre marknad, och inkluderar fasta anläggningar om de kan orsaka eller påverkas av elektromagnetiska störningar. Vissa specifika produkter som faller inom ramen för andra direktiv, exempelvis aeronautiska produkter,[49] är undantagna från EMC-direktivets bestämmelser.

Direktivet definierar ett antal grundläggande krav på utrustningen. Kraven fastställer vad utrustningen ska klara i tester men specificerar inte hur produkten ska

[45] ”Strålning” används här istället för ”emission” som används i lagrummen.
[46] Se exempelvis CISPR 16, IEC EN 61000-6-1 och IEC EN 61000-6-2, ISO 11452-serien, SAE J1113/21, EN 50 081 och Mil-STD-464.
[47] Europaparlamentets och rådets direktiv 2014/30/EU om harmonisering av medlemsstaternas lagstiftning om elektromagnetisk kompatibilitet (omarbetning).
[48] Guide for the EMCD (Europaparlamentets och rådets direktiv 2014/30/EU)
[49] Europaparlamentets och rådets förordning (EG) nr 216/2008

utformas. Utöver de generella kraven fastställer direktivet även ett antal specifika krav för fast installerad utrustning. Direktivet ställer också krav på produktens tekniska dokumentation som bland annat skall innehålla en riskanalys avseende produktens elektromagnetiska kompatibilitet.

När produkten har genomgått den nödvändiga prövningen och godkänts, kompletteras den med en EU-försäkran, Declaration of Conformity[50] och förses med en CE-märkning (Conformité Européenne). I grunden innebär CE-märkningen att produkten överensstämmer med ett lämpligt EU-direktiv, i det här fallet med EMC-direktivet.

5.2 Bestämmelser om elektromagnetisk kompatibilitet

Lag (1992:1512) om elektromagnetisk kompatibilitet är av intresse vid elektromagnetiska störningar då den (bland annat) reglerar skydd för liv, personlig säkerhet och hälsa samt elektromagnetisk kompatibilitet. Elektromagnetisk kompatibilitet omfattar egenskaper för utrustnings tillfredställande funktion i sin elektromagnetiska omgivning, inklusive skyldigheter vid inträffade elektromagnetiska störningar.[51] Förordning (2016:363) om elektromagnetisk kompatibilitet definierar begreppet elektromagnetisk störning som:

> ett elektromagnetiskt fenomen i form av ett brus, en oönskad signal, en förändring i själva överföringsmediet eller något annat som kan försämra funktionen hos en utrustning.[52]

Förordningen, med stöd av Elsäkerhetsverkets föreskrift om elektromagnetisk kompatibilitet,[53] tydliggör även skyddskrav för utrustning som kan alstra eller bidra till elektromagnetisk emission.[54] Skyddskravet är att utrustningen ska vara tillverkad, användas och ändras på ett sätt som inte stör annan utrustnings funktionalitet, och själv ha en förväntad tålighet mot störningar.[55] Elsäkerhetsverkets föreskrift behandlar (bland annat) att utrustningen överensstämmer med kraven, såsom efterlevnad med europeisk standardisering, intern tillverkningskontroll, typkontroll, EU-försäkran om överensstämmelse, CE-märkning med mera.[56]

[50] CEmarking.net. What is the EU declaration of conformity? cemarking.net/declaration-conformity/ (läst 2020-03-09)
[51] 2§ Lag (1992:1512) om elektromagnetisk kompatibilitet
[52] 4§ Förordning (2016:363) om elektromagnetisk kompatibilitet
[53] Elsäkerhetsverkets föreskrifter om elektromagnetisk kompatibilitet. ELSÄK-FS 2016:3
[54] 6§ Förordning (2016:363) om elektromagnetisk kompatibilitet; 1 kap. 1§ Elsäkerhetsverkets föreskrifter om elektromagnetisk kompatibilitet. ELSÄK-FS 2016:3
[55] 6, 8, 9§§ Förordning (2016:363) om elektromagnetisk kompatibilitet
[56] Elsäkerhetsverket (2016). Elsäkerhetsverkets föreskrifter om elektromagnetisk kompatibilitet. ELSÄK-FS 2016:3

5.3 Bestämmelser om elektronisk kommunikation

Lag (2003:389) om elektronisk kommunikation (även kallad LEK) och förordning (2003:396) om elektronisk kommunikation innehåller bestämmelser om (bland annat) säker elektronisk kommunikation. Dessa omfattar även rätten att använda radiofrekvenser, de tillstånd som behövs för användning av radiosändare och vissa frekvensutrymmen, vilka bevis och kompetenskrav användare av amatörradiosändare behöver med mera.[57] Lagen reglerar även skadliga elektromagnetiska störningar:

> skadlig störning: störning som äventyrar funktionen hos en radionavigationstjänst eller någon annan säkerhetstjänst, eller som på annat sätt allvarligt försämrar, hindrar eller upprepat avbryter en radiokommunikationstjänst som fungerar i enlighet med gällande bestämmelser, inbegripet störning av befintliga eller planerade tjänster på nationellt tilldelade frekvenser,[58]

Enligt dessa bestämmelser är en förutsättning för beviljande av tillstånd för radiosändare att användningen av radiofrekvenserna inte medför risk för otillåten skadlig störning.[59] De som har tillstånd för radiosändare är även skyldiga att säkerställa att otillåtna störningar upphör eller minimeras. Dessutom är det förbjudet att använda elektriska eller elektroniska anläggningar som alstrar radiofrekvent energi på ett sätt som inte följer regeringens föreskrifter.[60] Detta innebär att det är förbjudet att använda störsändare i Sverige (förutom för vissa undantagna aktörer som Försvarsmakten och Kriminalvården).[61]

LEK innehåller även skyldigheter att åtgärda störningar vid viss verksamhet. Tillhandahållare av allmänna kommunikationsnät och elektroniska kommunikationstjänster ska:

- säkerställa driftsäkerhet genom tekniska och organisatoriska åtgärder,
- anpassa åtgärderna till risken för störningar med hänsyn till tillgänglig teknik och kostnader,
- rapportera störningar av betydande omfattning till Post- och telestyrelsen,
- informera allmänheten om störningar då Post- och telestyrelsen begär detta.[62]

[57] 3 kap. Lag (2003:389) om elektronisk kommunikation
[58] 1 kap. 7§ Lag (2003:389) om elektronisk kommunikation
[59] 3 kap. 6§ Lag (2003:389) om elektronisk kommunikation
[60] 3 kap. 13-14§§ Lag (2003:389) om elektronisk kommunikation
[61] Post och telestyrelsen. Förbud mot störsändare. pts.se/sv/Privat/Radio/Utrustning/Forbud-mot-storsandare/ (läst 2020-01-22)
[62] 5 kap. 6b-6c§§ Lag (2003:389) om elektronisk kommunikation

5.4 Bestämmelser om elsäkerhet

Under 2016 trädde elsäkerhetslag (2016:732) i kraft. Året därpå meddelades även elsäkerhetsförordning (2017:218). Lagen antogs med syftet att stärka konsumenters elsäkerhet samt förtydliga ansvarsförhållanden och tillsyn för elsäkerhet, och på så sätt skapa en sammanhållen lag[63] på området.[64] Elsäkerhetslagen införde även aktsamhetskrav för elsäkerhet.[65] Aktsamhetskravet gäller för starkströmsanläggningar och elektrisk utrustning och medför ansvar för personskador, sakskador, förmögenhetsskador och störningar orsakade av el eller säkerhetsbrister.[66] Kraven innebär att det behövs fortlöpande kontroll av starkströmsanläggningar för att säkerställa att anläggningen inte orsakar personskador och sakskador. Åtgärder ska vidtas för anläggningar som riskerar att vålla skador och driftstörningar.[67] Redan vid tillverkning måste elektrisk utrustning uppfylla säkerhetskrav enligt god praxis inom Europeiska unionen. Utrustningens innehavande medför krav på underhåll av säkerheten och dess användning ska vara säker och inte riskera människors, husdjurs eller egendoms säkerhet.[68]

5.5 Andra relevanta it-rättsliga bestämmelser

Det finns även flertalet andra bestämmelser om säkerhet i tekniska system som potentiellt skulle kunna omfatta EM-incidenter. Bestämmelserna i förordning (EU) 2016/679 (allmänna dataskyddsförordningen - GDPR) avser skyddet av identifierade eller identifierbara individers uppgifter.[69] EM-incidenter kan omfattas av säkerhetsbestämmelserna i GDPR om de riskerar att medföra oavsiktlig, obehörig eller otillåten behandling av personuppgifter,[70] exempelvis genom obehörig dataändring, dataläckage, eller dataförlust.[71] Direktiv (EU) 2016/1148,[72] lag (2018:1174)[73,] och förordning (2018:1175)[74] syftar till att höja säkerheten i samhällsviktig verksamhet och i de nätverks- och informationssystem som används i verksamheten. EM-hot kan omfattas av dessa säkerhetsbestämmelser om de exempelvis skulle påverka säkerheten, integriteten eller riktigheten i systemen på ett sätt som kan medföra en betydande störning i leveransen av den

[63] Elsäkerhetslagen sammanförde bestämmelserna i ellagen (1997:857), starkströmsförordningen (2009:22) och förordningen om elektrisk materiel (1993:1068)
[64] SOU 2014:89. Elsäkerhet – en ledningsfråga. sid 11-12
[65] Ibid.
[66] 28-29, 31-32§§ Elsäkerhetslag (2016:732).
[67] 6, 7 och 1§§ Elsäkerhetslag (2016:732).
[68] 16-19§§ Elsäkerhetslag (2016:732); 13§ Elsäkerhetsförordning (2017:218)
[69] Europaparlamentets och rådets förordning (EU) 2016/679. Artikel 4
[70] Ibid. Artikel 4
[71] Ibid. Artiklarna 5 och 33
[72] Europaparlamentets och rådets direktiv (EU) 2016/1148
[73] Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.
[74] Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

samhällsviktiga tjänsten.[75] Dessutom kan EM-hot omfattas av bestämmelserna i säkerhetsskyddslagen, skulle de ingå i exempelvis spionerі, terrorverksamhet eller andra angrepp som hotar verksamhet av betydelse för Sveriges säkerhet eller uppgifter som relaterar till sådan verksamhet.[76]

[75] Europaparlamentets och rådets direktiv (EU) 2016/1148 Artiklarna 4-6.
[76] 1 kap. Säkerhetsskyddslag (2018:585),

6 Diskussion

Deltagarna vid workshopen uttryckte att den allmänna utvecklingen i samhället är att mer och mer elektronisk utrustning är uppkopplad, och att antalet trådlösa uppkopplingar ökar. Detta medför fler och större sårbarheter mot intrång och angrepp, eftersom trådlösa system alltid har en möjlig ingång. Dock kan inga system göras helt säkra eftersom alla system förr eller senare kräver indata, exempelvis vid uppdateringar.

Dessutom poängterades att även icke trådlösa system i slutändan ofta är kopplad till någon radiolänk. Att skydda system lokalt kanske inte hjälper mot hot när sårbarheter finns centralt eller i angränsande system.

Samtidigt innebär ett ökat antal trådlösa uppkopplingar att frekvensutrymmet blir mer och mer fullt. Att det blir fler signaler i EM-miljön och att frekvenserna fylls, medför enligt workshop-deltagarna större risker för störningar och funktionsavbrott i system som förlitar sig på trådlös kommunikation.

Vid workshopen poängterades det också att hela it-branschen förskjuts från att förebygga till att hantera störningar. Detta kan bero på att antalet attacker och aktörer inom cyberdomänen är stort, och att utvecklingen av verktyg för att utföra cyberattacker går snabbt. Innebörden av det kan vara att verksamheter och organisationer hyser uppfattningen att de omöjligen kan skydda sig mot alla attacker, och därför fokuserar sitt arbete mot att kunna hantera attacker utan att drabbas av för stor skada på sina system eller sin verksamhet. Huruvida detta synsätt kan appliceras på EM-hot är däremot inte lika självklart. Antalet inträffade EM-incidenter verkar än så länge vara relativt litet, baserat på det insamlade materialet i studien, åtminstone i jämförelse med antalet cyberangrepp.[77] Å andra sidan behövs det en inte alltför stor insats för att skaffa eller konstruera en störsändare. En antagonistisk nation som vill använda EM-hot vid ett angrepp eller under gråzonsaktiviteter[78] kan antagligen göra det. Om aktörer som nyttjar cyberfysiska system och/eller trådlös kommunikation bör inrikta sitt säkerhetsarbete på att göra systemen mindre sårbara för EM-hot, eller på att kunna hantera EM-angrepp utan att drabbas av för stor skada, kan behöva utredas vidare.

De flesta av de föreslagna åtgärderna identifierade i den här studien riktar sig mer mot processer och organisationer än mot teknik och utrustning, och handlar i huvudsak om förebyggande arbete. Det är sannolikt en effekt av vilka personer som deltagit i intervjuer och workshops. Dessa personer har antingen chefsroller, verksamhetsansvar, eller är tjänstemän. Teknisk personal och experter har inte ingått i detta underlag. Att inte fler tekniska åtgärder identifierats kan också bero på att möjligheten till sådana är relativt begränsad. De föreslagna tekniska

[77] FRA. Årsrapport 2016.
[78] Se fotnot 13.

åtgärderna består till stor del av avskärmning mot elektromagnetiska vågor och filtrering av inkommande signaler, samt loggning och analys av signaldata för att upptäcka incidenter. Sådana åtgärder kan förefalla självklara, men troligtvis krävs det en förståelse och kunskap för hoten och riskerna högre upp i organisationer för att åtgärderna ska vidtas. Därmed kan studiens resultat vara väl så relevanta i arbetet för att minimera riskerna med elektromagnetiska incidenter i samhällsviktiga verksamheter.

Workshop-deltagarna uttryckte också en önskan om lagkrav på säkerhet och redundans, speciellt för samhällsviktig verksamhet (kap. 4.2). Dock finns det redan nu skrivelser som hanterar detta. Exempelvis NIS-direktivet[79] innefattar explicita incitament för samhällsviktig verksamhet att tillgodose alternativa metoder för tjänsteleverans (annat än genom nätverks- och informationssystem) samt reglering om att skydda och återställa drift i tjänsteleveranser.

[79] MSB. NIS-direktivet. www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ (läst 2020-03-09)

7 Sammanfattning och vidare arbete

Här presenteras en sammanfattning av vilka åtgärder för att skydda verksamheter mot EM-hot som bör vidtas av olika aktörer, samt förslag på hur arbetet med dessa åtgärder kan fortsätta.

7.1 Åtgärder för olika aktörer

De föreslagna åtgärderna som presenteras i kap. 4 lämpar sig olika väl för olika typer av organisationer och aktörer. Även om studiens huvuduppgift är att stödja säkerhetsarbetet i samhällsviktiga verksamheter, kan en del av åtgärderna tillämpas av, eller för, också andra typer av aktörer. Dessa aktörer kan ha olika intressen av att skydda sin verksamhet. Deras verksamheter kan dock indirekt påverka samhällets funktion eller medborgares vardag och förtroende för samhället vid en kris.

Här presenteras en sammanfattning av vilka åtgärder som kan vara relevanta och viktiga för olika typer av aktörer. Åtgärderna baseras på det samlade resultatet i studien och anpassas för de olika typerna av aktörer.

Enskilda och små aktörer

Detta gäller privatpersoner och mindre företag som kanske inte har resurser för att arbeta strukturerat med säkerhetsskydd eller för att köpa in dyr utrustning.

Följa relevanta bestämmelser och regleringar – Handlar främst om bestämmelser kring elektromagnetisk kompatibilitet.

Beakta möjligheten att använda certifierade produkter och tjänster – För att försäkra sig om att utrustning och tjänster uppnår den nivå av säkerhet som är vedertagen standard. Att certifiering finns och är tillförlitlig kommer till stor del hjälpa slutanvändare som små aktörer att bedöma förmågan för och säkerheten i deras tekniska investeringar.

Tillgodogöra sig information och utbildning – För att informera sig och höja sin kunskapsnivå.

Större aktörer och organisationer

Detta gäller större företag och organisationer som använder trådlösa system och cyberfysiska system men som inte bedriver samhällsviktig verksamhet.

Följa relevanta bestämmelser och regleringar – Handlar främst om bestämmelser kring elektromagnetisk kompatibilitet.

Systematiskt och strukturerat säkerhetsarbete – Exempelvis följa de dokumentationsstandarder som är praxis i branschen.

Inventera tillgångar och utrustning – För att identifiera osäker utrustning och system och möjliga attackvektorer, identifiera vilka av dessa som är kritiska, samt prioritera tillgångar.

Tillgodogöra sig information och utbildning – För att informera sig och höja sin kunskapsnivå.

Erfarenhetshantering – För att bygga upp kunskap om hot, incidenter och åtgärder, samt för att kontinuerligt utveckla skyddet av sin utrustning och verksamhet.

Samhällsviktig verksamhet

Detta gäller större företag, organisationer och myndigheter som bedriver samhällsviktig verksamhet.

Följa relevanta bestämmelser och regleringar – Handlar exempelvis om bestämmelser kring elektromagnetisk kompatibilitet, säkerhetsskydd och NIS-fördraget.

Säkerhetsskyddsanalyser och RSA[80] – För att kontinuerligt inventera och identifiera sårbarheter och skyddsvärda verksamheter så att dessa kan åtgärdas och skyddas.

Inventera tillgångar och utrustning – För att identifiera osäker utrustning och system och möjliga attackvektorer, identifiera vilka av dessa som är kritiska, samt prioritera tillgångar.

Tillgodogöra sig information och utbildning – För att informera sig och höja sin kunskapsnivå.

Erfarenhetshantering – För att bygga upp kunskap om hot, incidenter och åtgärder, samt för att kontinuerligt utveckla skyddet av utrustning och verksamheter.

Delta i samverkansforum för informationsspridning och delade erfarenheter – För att sprida kunskap om hot, incidenter och åtgärder bland fler aktörer, samt för att kontinuerligt utveckla skyddet av utrustning och verksamheter brett i samhället.

Incidentrapportering – Incidenter måste rapporteras till ansvariga myndigheter för att de ska kunna få en bild av hot och sårbarheter, samt för att kunna utarbeta stöd och vägledningar för säkerhetsarbete.

[80] MSB. Risk- och sårbarhetsanalyser. www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/risk--och-sarbarhetsanalyser/ (läst 2020-04-20)

Nationell nivå (lagstiftande och reglerande)

Detta gäller lagstiftande nivå och myndigheter som har ansvar för att reglera användningen av trådlös utrustning och cyberfysiska system.

Nationell strategi – Så att alla aktörer arbetar utifrån samma utgångspunkter och mot samma mål vad det gäller att skydda samhällsviktig verksamhet.

Reglering av verksamhet med trådlös utrustning – För att undvika sårbarheter i kritiska verksamheter, och för att säkra funktionen för kritisk radiokommunikation.

Certifiering av utrustning – Så att aktörerna kan lita på att den utrustning de använder är säker. Att certifiering finns och är tillförlitlig kommer till stor del hjälpa slutanvändare att bedöma förmågan för och säkerheten i deras tekniska investeringar.

Vägledning – Så att alla aktörer kan arbeta för att lev upp till samma lägstanivå vad det gäller skydd.

Investeringsstöd för robusta anläggningar och säkra kommunikationsmedel – Så att aktörer kan säkra samhällsviktig verksamhet.

Lättillgänglig information och utbildningsmaterial för beslutsfattare, verksamhets- och tekniskt ansvariga – Så att aktörerna kan informera sig och höja sin kunskapsnivå både på beslutande, ledande och teknisk nivå.

Rekommendationer om rutiner, avväganden vid inköp av trådlös utrustning och lämpliga åtgärder och utrustning för att skydda sig – För att stödja aktörerna vid beslut om inköp och hur de bäst skyddar sig.

Utveckla samverkansforum för informationsspridning och delade erfarenheter – För att utveckla och sprida kunskap om hot, incidenter och åtgärder bland fler aktörer, samt för att kontinuerligt utveckla skyddet av utrustning och verksamheter brett i samhället.

Utveckla struktur för incidentrapportering – För att aktörer enkelt ska kunna rapportera incidenter till ansvariga myndigheter. Så att dessa ska kunna få en bild av hot och sårbarheter, samt för att kunna utarbeta stöd och vägledningar för säkerhetsarbete.

Underrättelseverksamhet mot terrorist- och extremistgrupper samt organiserad brottslighet – Så att ansvariga myndigheter och aktörer kan vara extra uppmärksamma när specifika hot föreligger eller när den allmänna hotbilden höjs.

Tillverkare

Certifiera produkter och tjänster – För att göra sina produkter och tjänster tillgängliga för samhällsviktig verksamhet.

7.2 Förslag på vidare arbete

Utifrån de samlade resultaten av studien ges här förslag på ett antal aktiviteter för att arbeta med de identifierade åtgärderna för att höja säkerheten mot elektromagnetiska hot och incidenter i samhället.

Höj medvetenheten om elektromagnetiska hot. Representanter från de svenska ansvariga myndigheterna har efterfrågat tillgång till fler utbildningar och mer erfarenhetsutbyte för personer som ansvarar för säkerheten mot elektromagnetiska hot. Rapportförfattarna tillägger att ett informellt samarbete för återkommande erfarenhetsutbyten skulle kunna hanteras genom MSB:s sammanslutningar för informationsdelning (så kallade FIDI-grupper). Exempelvis finns det forum för informationsdelning om informationssäkerhet kopplat till industriella styrsystem (FIDI-SCADA), telekom (FIDI-Telekom) och it-drift (FIDI-Drift) med mera. En liknande struktur skulle kunna appliceras på informationsdelning om EM-hot.

Stöd detekteringen och rapportering av elektromagnetiska hot mot samhällsviktig verksamhet. Under studiens genomförande har representanter från de svenska behöriga myndigheterna påtalat behovet av ett sensornätverk som kan skapa en normalbild över hur den elektromagnetiska signalbilden ser ut i Sverige i samband med samhällsviktig verksamhet, samt detektera avvikelser och incidenter. Det behövs insatser för att säkerställa att elektromagnetiska störningar mot samhällsviktig verksamhet upptäcks och rapporteras enligt de krav och rutiner som finns för verksamheten, samt att detekteringsarbetet bidrar till utvecklingen av en nationell lägesbild.

Utred åtgärder för att hantera elektromagnetiska hot. Denna studie har endast identifierat några exempel på möjliga åtgärder för att hantera EM-hot. Förslagsvis behövs det ytterligare insatser för att samla tekniska experter från berörda myndigheter samt experter från den tekniskt inriktade forskarkåren för att identifiera ett större urval av möjliga åtgärder. Tekniska åtgärder för att hantera EM-hot bör särskilt utredas vidare. I vilken mån kan kritiska system skyddas mot EM-hot? Går det att bygga redundanta system som är okänsliga för EM-hot? Hur ska detta göras så att det blir ekonomiskt hanterbart för olika aktörer. Detta bör förslagsvis även kopplas till en kartläggning av tillgängliga kommersialiserade motåtgärder.

Utred och validera tillämpningen av vedertagna säkerhetskrav och officiella rekommendationer. Under studien har ett antal aktörer uttryckt behov av ytterligare reglering och kravställning. Många av de bestämmelser som finns i dagsläget är nya, och ett brett spektrum av standarder finns som stöd för att säkra tekniska system. Samtidigt är flera av de rekommendationer som publicerats i Sverige uppbundna i ett relativt begränsat underlag av rapporter och vägledningar. Workshop-deltagarnas förslag om reglering och kravställning bör ses i denna kontext. Ytterligare kunskap behövs om hur kännedomen om existerande krav ser ut hos berörda aktörer, deras mognadsgrad i tillämpning (vad som tillämpas och

hur), samt om berörda aktörer ser att kraven får önskad effekt. Effekter och behov kopplat till kommunal och övrig RSA[81] om EM-hot bör även utvärderas. Har de tidigare publicerade handledningarna och vägledningarna kring EM-hot och RSA haft effekt? Kan, eller behöver de utvecklas? Även frågor kring hur aktörerna uppfattar skillnaden i NIS-direktivets[82] och MSB:s definition av samhällsviktig verksamhet kan behöva studeras.

Öva hantering av elektromagnetiska hot. Realistiska EM-hotsscenarier bör ingå i nationella krishanterings- och cybersäkerhetsövningar. För att kunskapen och medvetenheten om dessa hot ska stärkas måste de synliggöras. Övningar kan vara ett bra tillfälle för erfarenhetsutbyten eftersom de ofta samlar många aktörer från flera olika verksamheter. Sker det dessutom vid krishanterings- eller beredskaps-övningar förstärks bilden av att EM-hot innebär risker för säkerhet och beredskap. Övningar medför också möjligheten att lära sig vad som kan göras för att förebygga och hantera hot. Övningar kan även utformas för att validera och utvärdera implementering av säkerhetskrav från exempelvis lagar, standarder, vägledningar och internt uppsatta regler inom berörda verksamheter.

[81] MSB. Risk- och sårbarhetsanalyser. www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/risk--och-sarbarhetsanalyser/ (läst 2020-04-20)

[82] MSB. NIS-direktivet. www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ (läst 2020-03-09)

Referenser

Rapporter, utredningar, artiklar etc.

Chapman, A. 2017. GPS Spoofing. ECE Senior Capstone Project. 2017 Tech Notes

Fortifikationsverket 2015. FortV Handbok 2015: Nyttosignaler och IEMI

FRA. Årsrapport 2016.

Försvarsberedningen 2017. Motståndskraft. Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025. Försvarsdepartementet, Ds 2017:66

Giri, D.V. och Tesche, F.M. 2004. Classification of Intentional Electromagnetic Environments (IEME). IEEE Transactions on Electromagnetic Compatibility. vol. 46, no 3, pp. 322-328

Huang, J. *et al.* 2016. GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky. ICT Express 2(1), 37-40

Hurtig, T. *et al*. 2018. Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur. FOI-S--5835--SE, MSB1180 - februari 2018

Linder, S. *et al*. 2019. Telekonflikt - Sammanfattning 2018-2019. FOI-R--4832--SE

Olsson, H. 2011. Radiostörningar från reklamskyltar i Vänersborg. Elsäkerhetsverket Dnr 11EV4910

SOU 2014:89. Elsäkerhet – en ledningsfråga

Stenumgaard, P. 2011. Störningskänslighet hos civil trådlös konsumentteknik. FOI-R--3216--SE

Valassi, C. och Gustafsson, T. 2018. NCS3 - Kartläggning av elektroniska styrsystem i tunga fordon. FOI Memo 6358

Wiklundh, K. *et al.* 2018. Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur. FOI-S--5840--SE, MSB1178 - februari 2018.

Lagar, förordningar, regleringar etc.

Elsäkerhetsförordning (2017:218). Regeringskansliet

Elsäkerhetslag (2016:732). Regeringskansliet

Elsäkerhetsverket (2016). Elsäkerhetsverkets föreskrifter om elektromagnetisk kompatibilitet. ELSÄK-FS 2016:3

Europaparlamentets och rådets direktiv 2014/30/EU om harmonisering av medlemsstaternas lagstiftning om elektromagnetisk kompatibilitet (omarbetning).

Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Europaparlamentets och rådets förordning (EG) nr 216/2008 av den 20 februari 2008 om fastställande av gemensamma bestämmelser på det civila luftfartsområdet och inrättande av en europeisk byrå för luftfartssäkerhet, och om upphävande av rådets direktiv 91/670/EEG, förordning (EG) nr 1592/2002 och direktiv 2004/36/EG.

Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (Text av betydelse för EES), EUT L 119, 4.5.2016, s. 1–88, Artikel 4.

Europeiska kommissionen 2018. Guide for the EMCD (Europaparlamentets och rådets direktiv 2014/30/EU)

Förordning (2016:363) om elektromagnetisk kompatibilitet. Regeringskansliet

Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster. Regeringskansliet

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster. Regeringskansliet

Lag (1992:1512) om elektromagnetisk kompatibilitet. Regeringskansliet

Lag (2003:389) om elektronisk kommunikation. Regeringskansliet

MSBFS 2018:8. Föreskrifter om informationssäkerhet för leverantörer av samhällsviktiga tjänster. Myndigheten för samhällsskydd och beredskaps författningssamling

MSB 2019. Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. MSB1351, 1 mars 2019

Regeringskansliet 2017. Nationell Säkerhetsstrategi. Statsrådsberedningen

Säkerhetspolisen 2019. Säkerhetspolisens föreskrifter om säkerhetsskydd. PMFS 2019:2

Säkerhetsskyddslag (2018:585). Regeringskansliet

Webbsidor

Aftonbladet 2013. Obamas bilar kan ha olaglig störutrustning. www.aftonbladet.se/nyheter/a/ng0yjo/obamas-bilar-kan-ha-olaglig-storutrustning (läst 2020-04-16)

CEmarking.net. What is the EU declaration of conformity?. cemarking.net/declaration-conformity/ (läst 2020-03-09)

ComputerSweden 2005. Fångvårdens störsändare slås ut av mobilmaster. computersweden.idg.se/2.2683/1.8642/fangvardens-storsandare-slas-ut-av-mobilmaster (läst 2020-01-16)

DN 2013. Försvaret hjälper till att skydda Obama. www.dn.se/nyheter/sverige/forsvaret-hjalper-till-att-skydda-obama/ (läst 2020-04-16)

Elsäkerhetsverket 2018. www.elsakerhetsverket.se/om-oss/press/nyhetsbrev/nyhetsbrev-elinstallatorer/2018/nummer-2/installera-belysning-ratt-och-undvik-emc-problem/ (läst 2020-03-20)

Elsäkerhetsverket 2019. www.elsakerhetsverket.se/om-oss/press/nyhetsbrev/2019/december/storande-solceller/ (läst 2020-03-20)

FOI 2018. NCS3 - Nationellt centrum för säkerhet i styrsystem för samhällsviktig verksamhet. www.foi.se/forskning/informationssakerhet/ncs3.html (läst 2020-03-10)

GPS World 2019. How do we ensure GNSS security against spoofing? www.gpsworld.com/how-do-we-ensure-gnss-security-against-spoofing/ (läst 2020-01-16)

Göteborgsposten 2005. Störsändare mot larmbågar. www.gp.se/nyheter/göteborg/störsändare-mot-larmbågar-1.1166183 (läst 2020-01-15)

KTH 2017. Det här är cyberfysiska system. www.kth.se/blogs/reaktion/2017/08/det-har-ar-cyberfysiska-system/ (läst 2020-03-10)

Mitti.se 2016. Så lätt upptäcker han tjuvarnas störsändare. mitti.se/nyheter/upptacker-tjuvarnas-storsandare/?omrade=jarfalla. (läst 2020-01-15)

Motormagasinet 2018. Nyckellösa bilar stjäls genom relä-attacker. www.motormagasinet.se/article/view/622792/nyckellosa_bilar_stjals_genom_relaattacker (läst 2020-01-15)

MSB. NIS-direktivet. www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/ (läst 2020-03-09)

MSB. Risk- och sårbarhetsanalyser. www.msb.se/sv/amnesomraden/krisberedskap--civilt-forsvar/risk--och-sarbarhetsanalyser/ (läst 2020-04-20)

MSB. Samhällsviktig verksamhet. www.msb.se/samhallsviktigverksamhet (läst 2020-03-09)

Polisen 2019. polisen.se/utsatt-for-brott/skydda-dig-mot-brott/stold-och-inbrott/bilstold/ (läst 2020-03-20)

PTS. Förbud mot störsändare. pts.se/sv/Privat/Radio/Utrustning/Forbud-mot-storsandare/ (läst 2020-01-22)

SearchNetworking 2007. Graceful Degradation. searchnetworking.techtarget.com/definition/graceful-degradation (läst 2020-03-09)

Sveriges radio 2011. Radiostörning ligger bakom krånglande billås. sverigesradio.se/sida/artikel.aspx?programid=105&artikel=4753042 (läst 2019-11-04)

Sveriges radio 2017. Tjuvar slår ut villalarm med störsändare. sverigesradio.se/sida/artikel.aspx?programid=93&artikel=6659331 (läst 2020-01-20)

SVT Nyheter 2015. Tjuvar använder störsändare – slår ut larmet. www.svt.se/nyheter/lokalt/smaland/fler-tjuvar-anvander-storsandare-slar-ut-larmet (läst 2020-01-15).

Bilaga 1 – Intervjumall

Information om sekretess och personuppgiftsbehandling ges till respondenten.

Frågor om incidenter

Beskriv vad som hände.

Hur upptäcktes incidenten?

Aktiverades någon speciell krisplan eller organisation?

Vilken del av verksamheten drabbades? Vilken typ av utrustning? Trådlös?

Påverkade störningen någon kritisk del av verksamheten?

Hade ni vidtagit några åtgärder innan incidenten för att skydda er mot EM-hot?

Ser du nu i efterhand något som ni borde ha gjort annorlunda?

Hur följdes incidenten upp? Har ni vidtagit fler åtgärder nu?

Har incidenterna rapporterats till något forum/samarbetsgrupp/myndighet?

Hur bedömer du din/organisationens kunskap om elektromagnetiska hot?

Behöver kunskapen höjas?

Hur ser hotbilden ut mot er organisation?

Hur ser ni på användning av trådlösa system framöver?

Vill du tillägga någonting?

Frågor om respondenten

Hur skulle du beskriva din roll i organisationen?

Hur bedömer du din kunskap om elektromagnetiska hot? Hur har du fått kunskapen? Vilka praktiska erfarenheter har du?

Hur skulle du beskriva din organisation?

Hur utsatt är er verksamhet och mot vilka slags hot?

I vilket mån använder ni styrsystem, alternativt cyberfysiska system?

Använder din organisation trådlösa system i anslutningen till styrsystemen, alternativt cyberfysiska systemen?

Vilken typ av utrustning är trådlöst ansluten? Vilken typ av anslutning används?

Är de trådlöst anslutna systemen kritiska, och för på vilket sätt?

Kan de trådlösa systemen stängas ner vid behov? Finns det någon alternativ lösning? Vad skulle föranleda beslutet att stänga ner de trådlösa uppkopplingarna?

Hur fattades beslutet att ha dessa system trådlösa? På vilken nivå i organisationen fattades beslutet? Hade det varit möjligt att ansluta dessa system trådbundet? Vilken roll har säkerhetsaspekterna spelat i beslutet?

Vilka hot har tagits höjd för vid övervägningarna? Vad har ni utgått ifrån, t.ex. vägledningar och bäst praxis?

Har några särskilda säkerhetssystem, rutiner mm implementerats? Vilka alternativ fanns? Varför har just de som implementerats valts ut?

Har det skett någon intern utbildning gällande hot/elektromagnetiska hot för personalen som jobbar med systemet?

Finns det några scenarion där ni tror er vara skyddade mot?

Finns det scenarion som bedömdes som osannolika (och därför inte tagits höjd för)?

Hur övervakas systemets funktionalitet? Hur upptäcker ni störningar? Hur attribuerar ni dessa?

Har det förekommit (misstänkta) incidenter rörande de trådlösa systemen?

Kan du beskriva incidenterna?

Har någonting åtgärdats i efterhand? Varför?

Har incidenterna rapporterats till något forum/samarbetsgrupp/myndighet?

Får ni reda om förekomsten av incidenter hos andra aktörer? Hur?

Hur ser ni på användning av trådlösa system framöver?

Hur tror du att hoten utvecklas?

Vill du tillägga någonting?

Frågor om organisationen

Hur skulle du beskriva organisationens och din roll gentemot aktörer som opererar cyberfysiska system? Vilka är aktörerna? Finns det något formellt ansvar?

Hur bedömer du din kunskap om elektromagnetiska hot? Hur har du fått kunskapen? Vilka praktiska erfarenheter har du?

Tar ni emot rapportering om incidenter gällande trådlös utrustning och/eller elektromagnetiska företeelser?

Kunskap inom EM-hot (hur har du fått kunskapen, kunskapsnivå, praktisk erfarenhet)

Utbildar ni aktörer i EM-hot och säkerhet vid trådlös kommunikation? Har ni några standardråd/vägledningar mm?

Har ni blivit kontaktade med uppgifter om störningar i trådlösa kommunikationer, i synnerhet i anslutning till cyberfysiska system?

Har ni kunnat ge perspektiv på incidenten (hjälp med bedömning) och råd till aktörerna?

Kan ni berätta om sådana incidenter?

Vilka råd kunde ni ge?

Vilka säkerhetsåtgärder hade aktören implementerat själv vid tillfället? Vilka nya åtgärder implementerades?

Har ni någon form av omvärldsbevakning gällande elektromagnetiska hot eller hot mot trådlös utrustning?

Vad sker med de inrapporterade incidenterna, hur bearbetas och sprids kunskapen? När skulle en ingående undersökning ske? Samarbetar ni med andra myndigheter i saken?

Hur utsatta är aktörerna inom ert område för just EM-hot mot trådlös utrustning?

Hur ser ni på användning av trådlösa system framöver?

Hur tror du att hoten utvecklas?

Vill du tillägga någonting?

Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

www.msb.se