Radiostörningar – ett växande hot

PETER STENUMGAARD

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R—3494--SE
ISSN 1650-1942

Oktober 2012

Peter Stenumgaard

Radiostörningar – ett växande hot

Titel	Radiostörningar – ett växande hot
Title	Radio interference – an increasing threat
Rapportnr/Report no	FOI-R—3494--SE
Månad/Month	Oktober
Utgivningsår/Year	2012
Antal sidor/Pages	30 p
ISSN	1650-1942
Kund/Customer	FMV
FoT område	Ledning och MSI
Projektnr/Project no	E323293
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och Aerosystem

Sammanfattning

Denna rapport presenterar delresultat i den omvärldsbevakning som FOI utför på uppdrag av Försvarets Materielverk inom området telekonflikter och radiostörningar.

För somliga aktiviteter är trådlös teknik en nödvändighet. I militära operationer är fungerande trådlös teknik en grundförutsättning för att kunna genomföra insatser. I civila sammanhang är fungerande trådlös teknik ofta en avgörande nyckelfaktor exempelvis vid insatser där räddningspersonal och polis är inblandade. Bristande kommunikationsteknik i sådana fall kan få mycket allvarliga konsekvenser. Ett färskt exempel på detta är händelserna vid norska Utöya 2011 där radiokommunikationsproblem bland annat bidrog till att polisinsatsen fördröjdes. Orsaken var att anländande enheter använde det nya nationella radiosystemet som dock inte hade tillräcklig täckning vid Utöya

Den lavinartat ökande användningen av störningskänslig trådlös teknik i samhället innebär ökade risker för radiostörningar. Radiostörningar genereras dels naturligt av all elektronisk utrustning men även via avsiktliga störningssändare som säljs öppet, t ex via Internet. Situationen har öppnat för angripare som använder störsändning för att slå ut vitala kommunikations-, positionerings- och larmsystem i samband med kriminella aktiviteter och andra aktioner. Förmågan att effektivt utnyttja denna sårbarhet har tidigare enbart funnits hos militära aktörer men håller nu på att sprida sig även bland civila aktörer. Dessutom ökar antalet störningskänsliga trådlösa system som används i allt fler kritiska tillämpningar. Redan mängden oavsiktliga störningssignaler har lett till en rad incidenter på kritiska system som använder trådlös teknik. Dessa oavsiktliga störningar underlättar därmed för avsiktliga störningssändare att uppnå sitt syfte. Konsekvensen av denna utveckling är att vitala sambands-, positionerings- och larmsystem för olika samhällsfunktioner och även privat användning effektivt kan slås ut av en angripare i framtiden. Medvetenheten om störningskänsligheten hos trådlös teknik är idag relativt låg vilket i somliga fall

leder till ökad sårbarhet på grund av aningslös användning av störningskänslig teknik i kritiska tillämpningar. Denna medvetenhet behöver ökas exempelvis hos myndigheter och slutanvändare så att dessa aspekter beaktas i större utsträckning vid upphandling av nya system för kritiska tillämpningar.

Nyckelord:radiostörning, telekonflikt, störsändning, trådlösa system

Summary

This report presents interim results of the survey that FOI perform on behalf of the Swedish Defence Materiel Administration in the field of intersystem interference and radio interference.

For some activities, wireless technology is a necessity. Military operations are severely dependent on wireless technology for missions.In the civil context, functioning wireless technology is often a crucial key factor for instance in operations where rescue personnel and police are involved. Lack of communication in such cases may have very serious consequences. A recent example of this is the events at the Norwegian Utøya 2011 where radio communications problems was one contributing factor to delay in the police operation. The reason was that arriving units used the new national radio system that does not have adequate coverage at Utøya

The exponentially increasing use of interference-sensitive wireless technology in society means increased risk of radio interference. Radio interference is generated naturally in all electronic equipment. Also deliberate jamming increases due to that jamming equipment are sold openly, for example via the Internet. The situation has opened for attackers who use jamming to knock out vital communication, positioning and alarm systems associated with criminal activities and other actions. The ability to efficiently exploit this vulnerability has previously only been with military actors, but is now spreading even among civilian actors. Moreover, the number of disturbance-sensitive wireless systems used in more critical applications is constantly increasing. Even the amount of unintentional interference signals have led to a series of incidents on critical systems using wireless technology. This unintended interference facilitates the intentional jamming device to achieve its purpose more easily. The consequence of this development is vital systems such as communications, positioning and alarm systems for various social functions and even private use can be effectively

eliminated by an attacker in the future. Awareness of the interference susceptibility of wireless technology is now relatively low, which in some cases leads to increased vulnerability caused by clueless use of disturbing interference-sensitive technologies in critical applications. This awareness needs to be increased, for example at the authorities and end users so that these aspects are given greater consideration in the procurement of new systems for critical applications.

Keywords: Radio interference, jamming, wireless

Innehåll

VITAL TRÅDLÖS TEKNIK 9

1.1 BAKGRUND 9
1.2 STÖRNINGSHOT MOT TRÅDLÖSA SYSTEM 10

2 STÖRNINGSKÄNSLIGHET HOS TRÅDLÖS TEKNIK 13

2.1 STÖRNINGSKÄNSLIG TRÅDLÖS TEKNIK 13
2.2 HUR PÅVERKAS ETT RADIOSYSTEM AV STÖRNING? 13

3 OAVSIKTLIGA RADIOSTÖRNINGAR 17

1 Vital trådlös teknik

1.1 Bakgrund

För somliga aktiviteter är trådlös teknik en nödvändighet. I militära operationer är fungerande trådlös teknik en grundförutsättning för att kunna genomföra insatser. I civila sammanhang är fungerande trådlös teknik ofta en avgörande nyckelfaktor exempelvis vid insatser där räddningspersonal och polis är inblandade. Inom industrin används trådlös teknik i allt större utsträckning för övervakning och realtidsstyrning av processer och maskiner. Trådlös teknik är även vanlig inom olika typer av larmsystem som exempelvis villalarm, butikslarm och larmsystem för värdetransporter. Inom luftfart används trådlös teknik för exempelvis talkommunikation, identifiering, navigering och luftövervakning. Till sjöss används trådlös teknik för exempelvis talkommunikation, identifiering och övervakning av fartygsrutter.

Problem med radiostörningar orsakade av oavsiktliga störningssignaler från elektroniska system har varit kända sedan radions barndom och hamnade i fokus när rundradiosändningar startade för nästan 100 år sedan. Då uppmärksammades att elektriska system i hemmen kunde störa den mottagna radiosignalen vilket föranledde att standardiserade gränsvärden för maximal utsänd radiostörning utarbetades för elektrisk utrustning. Detta blev starten på det teknikområde som brukar förkortas EMC (eng. Electromagnetic Compatibility) och som idag är ett stort område med många delområden.

Det finns idag gott om exempel som visar på mycket allvarliga konsekvenser om trådlösa system blir störda i kritiska tillämpningar som exempelvis polis- och räddningsinsatser. Rökdykning är ett exempel på då trådlös kommunikation är helt avgörande för möjligheten att genomföra en insats. I ett exempel från 2010 i Cincinnati, USA, omkom två brandmän i en våldsam brand och efterföljande utredning visade att brandmännen vid upprepade tillfällen sänt ett ”Mayday”-meddelande från sina radioterminaler. Inget av dessa meddelanden hade nått räddningsledaren [16]. Flera liknande incidenter har lett till att The International Association of Fire Chiefs har publicerat en särskild rapport som rör sårbarheten hos radioteknik i samband med räddningsinsatser [2]. I samband med händelserna vid norska Utöya 2011 bidrog bland annat radiokommunikationsproblem till att polisinsatsen fördröjdes. Orsaken var att anländande enheter använde det nya nationella radiosystemet som dock inte hade tillräcklig täckning vid Utöya [21][3]. Detta ledde till att anländande enheter inte omedelbart kunde kommunicera med den personal som redan fanns på plats varför insatsen fördröjdes ytterligare. I samband med Göteborgskravallerna år 2001 lyckades demonstranterna störa polisens radiosystem vilket bidrog till den kaosartade situation som uppkom och med rättsliga efterspel som följd.

Ett annat viktigt exempel på vital trådlös teknik är GPS som både används för positionering av personal och enheter men även som noggrann tidssignal till bland annat data- och telekommunikationsnät. GPS-mottagare används redan i en rad system för civil kritisk infrastruktur. Exempel är:

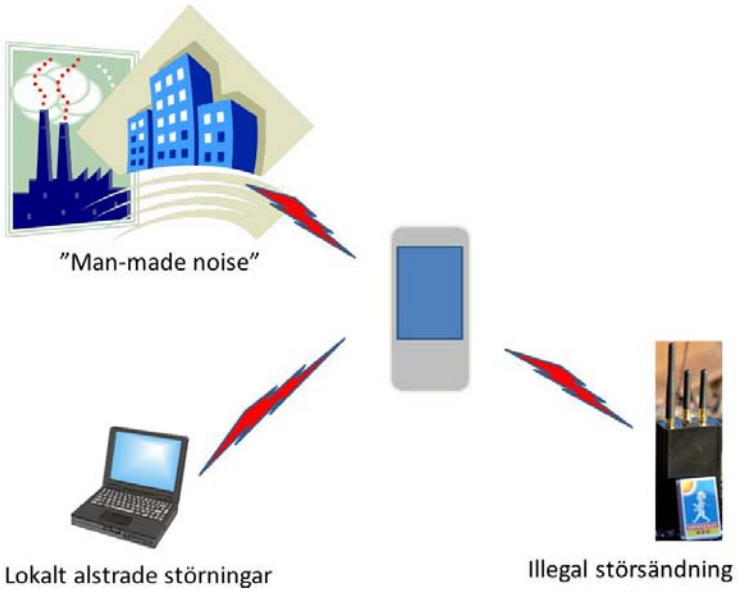
- Telekommunikationssystem
- Datornät
- Energidistribution
- Bank- och finanssystem

GPS-mottagare är mycket lätta att störa på grund av att den mottagna satellitsignalen är mycket svag. Detta i kombination med det snabbt ökande GPS-beroendet i kritiska tillämpningar öppnar för hög sårbarhet mot både oavsiktlig och avsiktlig störningssändning. Royal Academy of Engineering i Storbritannien gav 2010 ut en särskild rapport där denna ökade sårbarhet uppmärksammas [4]. Sammantaget sker således en snabbt ökande användning av trådlös teknik i kritiska tillämpningar där kommunikationsavbrott kan få mycket allvarliga konsekvenser.

Förutom att störa ut förbindelser så kan så kallad *spoofing* användas. Spoofing kan innebära att man tar kontroll över ett system i syfte att manipulera det utan att användaren märker något. Spoofing för att manipulera tidgivning till system har börjat uppmärksammas då det exempelvis finns pengar att tjäna om man lyckas manipulera tidgivningen till system för finansiella transaktioner. Tid från GPS-satelliter används idag för att ge samtidig tid till börsinstitutioner som ligger i olika delar av världen. Noggrannheten på denna tid är mycket hög för att förhindra att någon skaffar sig fördelar i så kallad högfrekvenshandel där datorer sköter serier av mycket snabba transaktioner

1.2 Störningshot mot trådlösa system

Som visats i föregående avsnitt så kan radiostörningar ha olika ursprung, se figur 1. Begreppet ”man–made noise” brukar användas för den allmänna störningsmiljö som alstras i tätorter, nära industrier mm. Gemensamt är att störningarna alstras av olika verksamheter och processer som involverar elektronisk utrustning. Den internationella teleunionen (ITU) tillhandahåller tumregler [23] över vilka nivåer dessa störningssignaler typiskt kan ha i olika miljöer. Lokalt alstrade störningssignaler kommer från olika elektroniska system som samlokaliseras vid en specifik radiomottagare.



Figur 1: Exempel på störningshot mot trådlösa system.

Typiska källor kan vara persondatorer, fordonsladdare, mikrovågsugnar, lågenergilampor etc. Den tredje gruppen av störningssignaler i figur 1 kommer från illegal störsändning där någon avsiktligt sänder störande radiosignal i syfte att försvåra eller helt blockera trådlös kommunikation. Som framgår av figur 1 så bidrar samtliga störnings-källor till den sammanlagda belastningen på det eventuella störskydd som finns hos radiosystemet. Om man exempelvis har installerat ett radiosystem i ett fordon som dessutom har elektroniska system såsom persondatorer med sig så bidrar fordonets egna system till att belasta eventuellt störskydd hos radiosystemet. Om nivån av ”man-made noise” och/eller lokalt alstrade störningssignaler är hög så kan en illegal störsändare åstadkomma skada på betydligt större avstånd än om radiosystemet finns i en miljö med låga omgivande störningssignaler [24].

2 Störningskänslighet hos trådlös teknik

2.1 Störningskänslig trådlös teknik

Vardagskonsumenter slutar inte använda mobiltelefoner även om samtalet ibland bryts när man exempelvis åker tåg. Inte heller slutar man använda trådlöst Internet även om man ibland inte får kontakt eller upplever att förbindelsen tidvis går långsamt. Denna acceptans mot störningar beaktas vid prioriteringar av tekniska egenskaper hos trådlös teknik för vardagskonsumenter. Hög störtålighet mot störningar kostar nämligen alltid kapacitet hos systemet [1]. Med kapacitet menar vi exempelvis datatakt (antal bitar per sekund) eller antal samtidiga användare i ett visst system. I civila trådlösa system prioriteras således kapacitet före störtålighet av rent kommersiella skäl. I militära trådlösa kommunikationssystem, såväl som i rymdtillämpningar, brukar man istället prioritera störtålighet då det är viktigt att man alltid har kontakt. Detta har man lärt sig av erfarenhet då störningsproblem kan orsaka både materiel- och personförluster.

I kritiska industritillämpningar finns oftast krav på avbrottsfrihet och maximal tidsfördröjning för data som skickas i trådlösa system. Dessutom kännetecknas ofta industrimiljöer av höga nivåer på elektromagnetiska störningssignaler vilket innebär en mycket krävande miljö för att åstadkomma tillförlitlig trådlös kommunikation. Ett annat civilt område med liknande krav är trådlös kommunikation för olika typer av säkerhetstillämpningar såsom larmsystem, personsäkerhet samt räddnings- och polisinsatser. Tidgivning via GPS-signalen är ytterligare exempel på tillämpning där man ofta har mycket höga krav på noggrannheten i signalen. Det finns således idag civila tillämpningar med krav som liknar de krav man normalt enbart brukar ställa på trådlösa system för militära applikationer. I många civila applikationer används dock trådlös teknik som är mycket störningskänslig beroende på orsaker som kostnadsskäl eller aningslöshet om hur sårbarheten skiljer sig åt mellan olika trådlösa tekniker.

2.2 Hur påverkas ett radiosystem av störning?

Digitala radiosystem kan reagera på olika sätt vid störning. Exempel på reaktioner är:

- Avbrott i förbindelsen
- Tidsfördröjning av data

- Fel i applikationen som använder radiosystemet
- Reducerat antal användare i systemet
- Minskad räckvidd för enskilda enheter

Avbrott i förbindelsen

Det typiska exemplet är när mobilsamtalet bryts när man åker tåg. Ena stunden fungerar förbindelsen men kan sedan mycket snabbt avbrytas. Digitala kodade radiosystem har egenskapen att övergången mellan funktion och avbrott går mycket snabbt utan att användaren hinner få någon förvarning. I digitala system såsom GSM, 3G och TETRA (TErrestrial TRunked RAdio) [20] får användaren således ingen tydlig förvarning om annalkande kommunikationsproblem, till exempel då signalstyrkan (radiokanalen) försämras på grund av radioskugga eller andra problem. I tidigare analoga system fanns inte detta problem på samma sätt eftersom en försämring av signalstyrkan kunde noteras direkt i form av hörbart brus. Digitala kodade system, å andra sidan, ger en konstant och god talkvalitet så länge signalstyrkan överstiger ett visst kritiskt tröskelvärde. Så snart signalstyrkan understiger denna tröskel så upphör kommunikationslänken emellertid att fungera på ett mycket abrupt sätt.

Tidsfördröjning av datatrafik

Ett typexempel på tidsfördröjning av datatrafik är när det börjar gå långsamt när man surfar trådlöst på Internet. Lokala nätverk som t ex W-LAN reagerar med ökande tidsfördröjningar när radiostörningar finns i luften. Samma sak inträffar om många W-LAN-system är igång samtidigt på en lokal plats. Detta kan märkas om man använder W-LAN på tågresan och det är många i samma tåg som använder det för internettrafik.

Fel i applikationen som använder radiosystemet

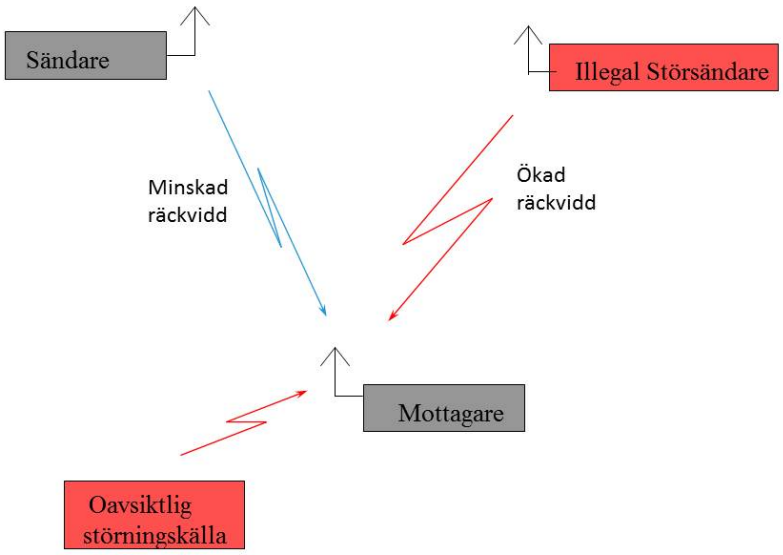
Ett exempel är de GPS-mottagare som fortsätter fungera vid radiostörning men börjar leverera felaktiga positionsdata till användaren.

Reducerat antal användare i systemet

Mobilsystem som exempelvis 3G kontrollerar alltid hur störningsmiljön ser ut innan en ny mobil släpps in i nätet. Om radiostörningarna ökar så kommer systemet därför att minska antalet användare.

Minskad räckvidd för enskilda enheter

Ett radiosystem som utsätts för radiostörning får alltid minskad räckvidd till andra system som det kommunicerar med. Detta beror på att en ökad störningsnivå i en mottagare leder till att insignalen från dem man kommunicerar med måste ökas i motsvarande grad för att upprätthålla samma kvalitet på förbindelsen. Detta kan göras på två sätt; antingen genom att omgivande enheter ökar sin utsända effekt eller att de flyttas närmare den störda enheten. Om omgivande enheter redan använder maximal uteffekt så återstår endast alternativet att flytta sig närmare vilket innebär reducerad räckvidd för förbindelsen, se figur 2. Praktiska erfarenheter visar att räckvidden för enskilda radiosystem kan bli så låg som 25% gentemot räckvidden då inga radiostörningar förekommer i närheten av systemet.



Figur 2: Oavsiktliga störningar minskar räckvidden för eget system och ökar räckvidden för en illegal störsändare.

3 Oavsiktliga radiostörningar

3.1 Allmänt

Störningsincidenter orsakade av oavsiktliga störningssignaler är idag vanligt förekommande och kan utgöra hot mot kritiska trådlösa system [1]. Det är dock inte alltid säkert att en användare kopplar samman kommunikationsproblem med störningsproblem då det inte alltid är uppenbart vad orsaken kan vara till kommunikationsproblemen. Störningssignaler som alstras naturligt av alla elektroniska system har idag ökat i en sådan omfattning att en rad allvarliga incidenter rapporterats.

3.2 Militära incidenter

Nedan ges några exempel på störningsincidenter orsakade av oavsiktliga störningskällor.

Falklandskriget 1982

Den 4 maj 1982 lyfte två Super-Etendardplan kl 10.00 på förmiddagen från det argentinska fastlandet. Under högervingen på varje plan hängde en franskbyggd sjömålsrobot av typen Exocet. Roboten är utrustad med 160 kg sprängmedel och har egen radarmålsökare. Målet för operationen var att slå mot de Engelska hangarfartygen *Hermes*' och *Invincibles* fjärrskydd bestående av de tre robotjagarna *Coventry*, *Sheffield* och *Glasgow*. Robotjagarna var utrustade med såväl egen spaningsradar som signalspaningsutrustning (SIS) som kunde registrera Super-Etendardplanens eldledningsradar. Detta visste de argentinska piloterna väl och flög därför under radarhorisonten under hela anflygningen. Sedan skulle de behöva göra en snabb upptagning (stiga från 20 till ca 60 meter), göra en kort radarobservation, och sedan dyka ned under Britternas radarlober igen. Vad de däremot inte visste var att de brittiska robotjagarna var behäftade med allvarliga störningsproblem [5] (så kallade telekonflikter) ombord. Om robotjagarna sände med sin spaningsradar störde de ut sin egen satellitkommunikation. Om de använde satellitkommunikationen störde de ut den signalspaningsutrustning som skulle registrera Super-Etendard-planens eldlednings-radar. Alltså: om man sände med satellit störde man ut sitt signalspaningssystem och var dessutom tvingad att ha egen spaningsradar avslagen. Denna ödesdigra kombination var aktiv på *HMS Sheffield* när Super-Etendardplanen gjorde sin upptagning varför man inte registrerade den anflygande fienden. Den första kontakten med missilen var optisk varför man aldrig hann aktivera motmedel i form av metallremsor som skulle lura missilens radarmålsökare. Missilen träffade kl 10.04 med 20 dödade och 24 skadade

besättningsmän som följd. *Sheffield* sjönk efter ett dygns häftig brand. Detta var första gången sedan andra världskriget ett brittiskt flottfartyg träffades av fientlig eld. Utredningen som följde pekade på att telekonflikten sannolikt var huvudorsaken till att missilen kunde avfyras och träffa *Sheffield* [5].

Incidenter med Black Hawk
Inför operation *Uphold Democracy* på Haiti 1994 användes helikopter UH-60 *Black Hawk*, på hangarfartyget *USS Eisenhower*. Den vapenlast som användes inom armén var inte testad för hangarfartygets störningsmiljö varför fartygets radar inte kunde användas. Detta för att inte risken att fartygets radar skulle vådautlösa vapenlasten på *Black Hawk*. Detta innebar operativa begränsningar [6] då *USS Eisenhower* inte kunde ha sin spaningsradar påslagen med *Black Hawk* ombord. *Black Hawk* har dessutom råkat ut för ett antal haverier (ett 20-tal omkomna totalt) där man misstänker att elektromagnetiska störningar varit orsaken.

Balkan
I samband med internationella insatser i forna Jugoslavien har man haft telekonflikter mellan flygburna störningssändare och artilleriradar [6].

Global Hawk
Vid testflygning i sydvästra USA med den obemannade *Global Hawk* fick man en telekonflikt med en markstation på samma frekvens som signalerna för fjärrmanövreringen. Detta resulterade i att självförstörelsemekanismen utlöstes på farkosten som alltså sprängdes [6].

3.3 Civila incidenter

Nedan ges några exempel på störningsincidenter orsakade av oavsiktliga störningskällor.

Elektronisk reklamskylt stör flygradio (Sverige)
På Trollhättan/Vänersborgs flygplats anmäldes radiostörningar på flygplan vid start och landning. En utredning genomförd av Elsäkerhetsverket visade att radiostörningarna orsakades av elektroniska reklamskyltar i närheten av flygplatsen[7].

Störning av telemetri för hjärtövervakning
I Dallas togs en tidigare ledig digital TV-kanal i bruk vilket ledde till att dess sändningar kom att blockera telemetrisignaler från hjärtövervakningen av 60 personer på stadens sjukhus [8].

Radiostyrd kran tappade sin last
I Storbritannien tappade en radiostyrd kran sin last på grund av radiostörningar från en förbipasserande truck. Lasten träffade en människa som avled [9].

Elektriska installationer stör räddningstjänstens radiosystem (Sverige)
Personal i räddningstjänsten har berättat för FOI att deras radiosystem slås ut i närheten av vissa automatstationer med säkringar för elektriska installationer.

Fjärrstyrda billås slås ut för bevakningspersonal (Sverige)
Bevakningspersonal har berättat för FOI att de råkat ut för att det inte går att använda bilens fjärrstyrda lås i vissa industriområden. Om de använder låset så leder störningssignaler i området till att bilen inte går att öppna när de återvänder till bilen.

Reglersystem för processtyrning störs ut (Sverige)
I ett forskningsprojekt som FOI deltog i fokuserades på trådlös kommunikation i tunga industrimiljöer. Ett reglersystem som styr en avancerad processmaskin innehåller en kort trådlös länk med W-LAN. Plötsligt började processen att få avbrott av och till med dyra produktionsstopp och förstörd materiel som resultat. Analysen visade att en felaktig kraftkomponent genererat radiostörningar som orsakat fördröjningar i W-LAN-länken. När kraftkomponenten åtgärdats fungerade systemet igen.

Utslagning av GPS-mottagare på fritidsbåtar (USA)
Amerikanska kustbevakningen samt *Department of Homeland Security* har vid ett flertal tillfällen varnat [10] båtägare för att använda vissa typer av antennförstärkare för TV-mottagare ombord. Antennförstärkare har orsakat ett flertal incidenter där GPS-mottagaren slagits ut eller visat felaktig position. Störningar har rapporterats på avstånd upp till ca 700 meter från vissa typer av antennförstärkare.

Kabel-TV stör radiokommunikation för banpersonal (Sverige)
I ett forskningsprojekt som FOI deltog i fokuserades på trådlös kommunikation i tunga industrimiljöer inklusive tågbangårdar. För kommunikation mellan banpersonal och lokförare på bangårdar används radio i vissa tillämpningar. Ett av systemen arbetar på frekvensen 423 MHz. Detta radiosystem störtes ut helt vid flera tillfällen. En utredning konstaterade att störningarna kom från ett lokalt kabel-TV-nät vid sändning av Canal Digital på kanal S36 (423.25 MHz). Kanalen byttes till S37 varefter störningarna upphörde.

4 Avsiktlig störning av trådlös teknik

4.1 Välkänd militär förmåga

I militära operationer har det alltid varit ett välkänt faktum att fungerande trådlös kommunikation är en förutsättning för att kunna leda insatser. Av det skälet är störning av radiokommunikation en sedan gammalt välkänd metod för att effektivt nedsätta en motståndares förmåga att leda sina förband. Det finns gott om öppna referenser [17] till händelser där radiostörning använts effektivt vid militära operationer.

4.2 Störsändning civilt

4.2.1 Exempel på störsändning

Störsändning mot radiosystem har historiskt varit en rent militär förmåga. Idag har den förmågan börjat sprida sig även i det civila samhället vilket innebär ett snabbt växande hot mot kritisk trådlös kommunikation för exempelvis polis, räddningstjänst, trådlösa larm- och övervakningssystem etc. Förmågan sprider sig i takt med att störutrustning idag säljs fritt via Internet, se figur 3.

Att innehav och användning av störsändare är förbjudet har inte hindrat marknaden för dessa att växa snabbt de senaste åren. En aktör som vill använda störningssändning kan redan idag för ett par tusenlappar köpa störningssändare anpassade mot samtliga existerande civila trådlösa system. Idag begränsas förmågan att använda dessa störsändare till enstaka händelser. Mycket tyder dock på att förmågan utvecklas i riktning mot ökad taktisk förståelse för hur denna teknik skall användas som del i en koordinerad insats för att effektivt slå ut vitala system för tal, larm och övervakning.

Rapporter om störningssändning mot polisens radiosystem började förekomma i början av 2000-talet i samband med demonstrationer och upplopp. Exempel på sådana tillfällen är

- Världsbanksmötet i Prag 2000

- EU-toppmötet 2001 (Göteborgskravallerna) [11]

- Upploppen i Sydney (Cronulla and Brighton le Sands) 2005

Vid dessa händelser förekom både ren störningssändning och sändning av falska anrop för att åstadkomma förvirring i polisinsatsen.

Figur 3: GPS-störsändare som säljs via Internet. Fotot taget av Mikael Alexandersson, FOI.

Störning av GPS-mottagare i fordon har ökat som ett resultat av att GPS-mottagare installeras i vissa fordon för att kunna övervaka hur fordonet används. Denna typ av mottagare installeras typiskt i vissa lastbilar och andra fordon för yrkestrafik. Som en motreaktion på detta så säljs GPS-störsändare som kan monteras i fordon av dem som inte vill att ens rörelsemönster skall loggas. Det finns flera dokumenterade fall då denna typ av störsändare stört ut andra GPS-mottagare i bilens närområde. Flera incidenter med utstörda GPS-mottagare på flygplatser [14] har rapporterats när fordon med störsändare passerat förbi.

Några exempel på störsändning som används vid olika typer av brottslig verksamhet ges i tabell 1.

Tabell 1: Exempel på störsändning i samband med brott.

Verksamhet	**Teknik**
Bilinbrott	Blockering av billås; störsändare placeras på parkeringsplatser till större köpcentra vilket hindrar bilens ägare från att låsa bilen med den trådlösa nyckeln.[12]
Stöld av butiksvaror	Störning av larmbågar i butiker [15] Bärbara störsändare som ryms i fickan används för att slå ut larmbågarnas funktion..
Villainbrott	Störning genom blockering av larmsystemets centralenhet och/eller länken från larmsystemet till mobilnätet [22].
Värdetransportrån	Störning av länken från larmsystemet till mobilnätet [13].
Butiksinbrott	Störning av länken från larmsystemet till mobilnätet [13](t ex juvelerarbutiker, bensinstationer)
Slå ut GPS-baserad loggning av fordons färdrutt.	Störning av GPS-mottagare i fordonet. Har bland annat lett till att GPS-mottagare samtidigt blivit störda på flygplats [14].
Undkomma GPS-baserade vägtullar.	Störning av fordonets GPS-mottagare [13][14].
Dölja stöldgods	Störning av GPS-mottagare som placerats på varor för att kunna följa dem [14][18].
Störning av flygplans GPS-mottagare.	Störning av flygburna GPS-mottagare vid Nordkoreas gräns [19]

4.2.2 Konsekvenser i ett EU-perspektiv

Inom Europa sker en snabb utveckling av teknikorienterade system för skydd mot terrorangrepp och organiserad brottslighet. I dessa systemlösningar sätts ofta stor tilltro till trådlös teknik för att sammanbinda olika sensor-, positionerings- och övervakningssystem. I takt med att fler länder ökar sin användning av trådlös teknik i säkerhetskritiska tillämpningar så bygger man samtidigt in en allvarlig sårbarhet mot avsiktlig störningssändning. Vi har redan Europeiska exempel där demonstranter stört ut polisradiosystem och där kriminella använt störningssändning i samband med brottslig verksamhet. Inom EU använder de flesta länder idag TETRA-standarden [20] för blåljuskommunikation. TETRA-baserade system är byggda för att vara säkra mot avlyssning men har i princip inte bättre tålighet mot radiostörningar som det äldre radiosystem som användes vid Göteborgskravallerna 2001. Denna sårbarhet blir extra problematisk i takt med att förmågan till störningssändning ökar även bland icke-militära aktörer. Enbart den växande förekomsten av störningssändare ökar i sig risken för rena olyckstillbud ifall störningssändare av misstag slår ut vitala system för exempelvis säkerhet, sjukvård och räddningstjänst.

Det finns som vi sett ovan flera exempel på när bortfall av radiokommunikation i samband med räddningsinsatser lett till dödsfall och fördröjningar. En aktör som väljer att effektivt använda störningssändning i samband med exempelvis en terrorattack kan således åstadkomma mycket stor skada både inför, under och efter en attack. Det ökande behovet av GPS för samhällssäkerhetskritiska system samt militära vapensystem utgör en global sårbarhet som kan orsaka mycket allvarliga problem om en angripare väljer att kombinera sina aktioner med störningssändning. Kombinationen av tilltron till trådlös i säkerhetstillämpningar tillsammans med att förmågan att taktiskt använda störningssändning långsamt sprider sig även bland icke-militära aktörer kommer sannolikt att öka sårbarheten för terrorangrepp ytterligare de närmaste åren.

4.2.3 Konsekvenser ur svenskt perspektiv

Sverige tillhör de länder i världen som varit tidig med att införa trådlös teknik i många tillämpningar som rör samhällssäkerhet och krisberedskap. Detta är naturligt då vi i Sverige länge haft en ledande roll inom telekommunikationsområdet och varit tidiga med att använda trådlös teknik både i vardagslivet och i andra tillämpningar. Baksidan med detta är att den sårbarhet som trådlös teknik utgör sprider sig snabbare i Sverige än i de länder där användningen av trådlös teknik ännu inte fått samma breda genomslag. Som en följd av detta finns det idag gott om svenska exempel då kriminella använder störningssändare mot larmsystem, billås och butikers stöldskyddssystem. Att icke-militära aktörer börjat skaffa sig förmåga att använda störningssändning innebär även ett växande hot mot förmågan att upprätthålla kritisk kommunikation vid insatser av olika slag. Göteborgskravallerna visade tydligt att

störning mot polisens radiokommunikation snabbt kan leda till att en situation blir kaosartad och svår att kontrollera. GPS används i mycket stor utsträckning i Sverige, och då både för positionering och för tidgivning åt radionät. En fortsatt ökad användning av störningskänslig trådlös teknik i kritiska samhällsfunktioner ökar dramatiskt sårbarheten mot avsiktlig störning. I takt med att förmågan att använda störsändning ökar bland civila aktörer är detta mycket viktigt att beakta de närmaste åren i alla situationer då trådlös teknik övervägs för kritiska samhällsfunktioner.

5 Slutsatser

Radiostörningsproblem orsakade av oavsiktliga störningskällor har varit kända sedan radions barndom och litteraturen är riklig när det gäller rapportering av olika störningsincidenter som inträffat genom åren. Idag har den trådlösa utvecklingen kommit mycket långt och trådlös teknik används idag i flera kritiska civila och militära tillämpningar. I takt med att mängden trådlös teknik ökar i olika tillämpningar så ökar samtidigt sårbarheten med oavsiktliga och avsiktliga störningssignaler.

Mängden elektroniska system i närheten av trådlös teknik ökar ständigt samtidigt som illegala störsändare sälj öppet på Internet. Användning av illegala störsändare har ökat i takt med tillgängligheten och det finns idag rapporter om störsändning mot en stor rad kritiska trådlösa system för kommunikation, larm och övervakning. I takt med att system för illegal störsändning används så kommer förmågan att använda dessa effektivt att öka på sikt. Detta i kombination med att trådlös teknik för civila tillämpningar i regel inte är störningstålig innebär en allvarlig sårbarhet om inte lämpliga motåtgärder vidtas. Medvetenheten om störningskänsligheten hos trådlös teknik är idag relativt låg vilket i somliga fall leder till ökad sårbarhet på grund av aningslös användning av störningskänslig teknik i kritiska tillämpningar. Denna medvetenhet behöver ökas exempelvis hos myndigheter och slutanvändare så att dessa aspekter beaktas i större utsträckning vid upphandling av nya system.

6 Referenser

[1] Peter Stenumgaard ” Störningskänslighet hos civil trådlös konsumentteknik”, Rapport nr FOI-R—3216-SE, Totalförsvarets forskningsinstitut (FOI), 2011.

[2] International Association of Fire Chiefs [2008]. Interim Report and Recommendations: Fireground Noise and Digital Radio Transmissions, http://www.iafc.org/associations/4685/files/digProj_DPWGinterimReport.pdf, Accessed June 3, 2009.

[3] *Police operation to rescue Norway terror attack victims hampered by communications blunder* . Ryan Parry, Daily Mirror 2/08/2011

[4] *Global Navigation Space Systems: reliance and vulnerabilities*, Report issued by the Royal Academy of Engineering, March 2011.

[5] Sandy Woodward, *100 dagar – striden om Falklandsöarna*, Marinlitteraturföreningen 1994.

[6] Mario Lucchese, C. Leslie Golliday jr, Anil N. Joglekar, ”Operational Evaluation of Electromagnetic Environmental Effects (E3), Institute for Defense Analyses, PM: May – June 2000.

[7] Henrik Olsson, ”Radiostörningar från reklamskyltar i Vänersborg”, 2011-12-16, Elsäkerhetsverket Dnr 11EV4910

[8] Cherry Clough Consultants *Banana Skins Compendium*, 7th October 2005. Also available [Online]: http://www.complianceclub.com/ archive/bananaskins/126-150.asp

[9] Cherry Clough Consultants *Banana Skins Compendium*, 7th October 2005. Also available [Online]: http://www.complianceclub.com/ archive/bananaskins/226-250.asp

[10] U.S. Department of Homeland Security & United States Coast Guard, LOCAL NOTICE TO MARINERS, January 11, 2006

[11] Polismyndigheten i Västra Götaland, EU-kommenderingen 2001, Utvärdering.

[12] Bilar plundras med hjälp av sändare, Svenska Dagbladet, 22 juni 2008.

[13] *Gangs using jammers to deactivate alarms*, John Mooney, Sunday Times April 25, 2010.

[14] GPS jamming - *No jam tomorrow*, The Economist March 10th, 2011.

[15] *Störsändare tystar butikslarm*, Trelleborgs Allehanda, 29 november 2007.

[16] *Radio woes: Digital radio problems surface in last week's mayday in Cincinnati. Newspaper looks at the issue*. Sharon Coolidge at statter911.com, January 16, 2010.

[17] *Military Communications: From Ancient Times to the 21st Century*, Christopher H. Sterling, ABC CLIO, Inc, Santa Barbara California 2008.

[18] *Störningssändare skulle skydda stöldgods*, Halmstadsposten 4 januari 2012

[19] *GPS utslaget hos sydkoreanska flyg*, Svenska Dagbladet 3 maj 2012

[20] ETSI EN 300 392-2 v3.2.1, 2007.

[21] NOU 2012: 14 Rapport fra 22. juli-kommisjonen. Oppnevnt ved kongelig resolusjon 12. august 2011 for å gjennomgå og trekke lærdom fra angrepene på regjeringskvartalet og Utøya 22. juli 2011.

[22] *Tjuvarnas nya metod gör dyra larm värdelösa*, Dagens Nyheter 22 augusti 2012

[23] Radio noise. ITU-R Recommendation P.372, International Telecommunication Union, Geneva, 2001.

[24] Sara Linder, Marcus rundgren, "Tatiska konsekvenser av telekonflikter", FOA-R-00-01704-504- - SE, december 2000, Försvarets forskningaanstalt (FOA).