SÄRTRYCK UR *STRATEGISK UTBLICK 8*

Antagonistiska elektromagnetiska hot mot det civila försvaret

Sten E Nyholm, Tomas Hurtig, Kia Wiklundh och Sara Linder

Flera samhällsviktiga verksamheter förlitar sig idag på elektroniska styrsystem och trådlösa kommunikationssystem, som GPS, mobiltelefoni och WiFi. Många talar idag om cyberhot mot mjukvaran i datoriserade system, men man får inte glömma bort hårdvaran eftersom trådlösa kommunikationssystem och oskyddad elektronik även kan vara känsliga för elektromagnetiska (EM) hot, såsom störsändare och mikrovågsvapen. Avsiktliga EM-störningar utgör ett hot mot det civila försvarets förmåga att stödja det militära försvaret. Det är därför viktigt att EM-hot beaktas i de risk- och sårbarhetsanalyser som görs av bland annat myndigheter, kommuner och privata aktörer med uppgifter inom det civila försvaret, speciellt avseende operativ förmåga vid höjd beredskap.

Ett EM-hotscenario

Föreställ dig följande: De senaste månaderna har kännetecknats av en tilltagande internationell spänning och ett ökande antal konfrontationer mellan militära fartyg och flyg i Östersjöområdet. Många servrar vid myndigheter, nyhetsbyråer och företag utsätts för avancerade cyberattacker, och falsk information sprids dagligen i sociala medier. Regeringen överväger att mobilisera totalförsvaret för att hantera situationen.

I detta läge utsätts ett större antal viktiga apparater, som datorservrar och trådlös kommunikation, i olika samhällssystem för EM-störningar och några upphör helt att fungera. Blåljusmyndigheternas kommunikationscentraler tappar kontakten med enheter ute på fältet. Passage- och larmsystem vid flera kraftverk och myndighetsbyggnader fungerar inte. Störningar i eldistributionen gör att reservkraftanläggningar vid sjukhus och larmcentraler startar. Det blir trafikkaos i storstäderna när trafikljusen i flera korsningar slocknar. Tåg blir stående på linjerna när signalsystem eller elförsörjning faller bort. Fasta telefoner och mobiltelefoner fungerar bara sporadiskt. Vattenförsörjningen i storstäderna fallerar eftersom pumparna inte har elkraft. Invånarna kan inte handla mat eller tanka bilar eftersom elektroniska betaltjänster upphört att fungera. Allmänheten kan inte ta emot några radio- eller TV-sändningar för att få veta vad som hänt eller vad man ska göra. Transporter av sådant som livsmedel och bränsle med mera försvåras kraftigt vilket leder till att matbrist uppstår och fordon blir stående.

Vad har hänt? Det visar sig så småningom att det finns ett stort antal störsändare utplacerade i bland annat bilar, väskor och barnvagnar i närheten av kommunikationscentraler, myndighetsbyggnader och kopplingsstationer för el- och telenäten. Störsändare på obemannade flygande farkoster som cirkulerar över större städer och flygplatser slår ut all trådlös kommunikation. Dessutom har elektroniska komponenter inuti viktiga apparater bränts sönder i radio- och TV-sändare, i styrutrustningen till ställverk och i vissa myndighetsbyggnader.

Hur sker en elektromagnetisk attack?

En elektromagnetisk attack åstadkoms med utrustningar som sänder ut elektromagnetisk strålning på radiofrekvenser, vilka i sin enklaste form kan exempelvis vara en vanlig radiosändare eller en mobiltelefon. Attacken kan ske med smalbandig radiostrålning av endast en eller ett fåtal frekvenser, eller med bredbandig strålning som täcker alla frekvenser inom ett brett frekvensintervall.

FOI Memo 6748
Projekt Nr I181103
Godkänd av Mike Winnerstig

Augusti 2019

En enkel metod är att använda störsändare som sänder ut ohörbart EM-brus. Det gör att datakommunikation, så kallade nyttosignaler, drunknar i bruset och den trådlösa kommunikationen på en eller flera frekvenser slutar att fungera eller försämras. Den kraftfullare strålningen från mikrovågsvapen kan störa funktionen i enskilda elektroniska komponenter, som transistorer eller mikroprocessorer, antingen så att de temporärt förlorar sin funktion eller fungerar på fel sätt, eller så att komponenter bränns sönder av en inducerad strömrusning i kretsarna. En skillnad mellan dessa verkansformer är att störsändare främst påverkar trådlös kommunikation, medan mikrovågsvapen kan påverka all elektronik, även icke-kommunicerande sådan. Gemensamt för dem är att de verkar lokalt inom sin räckvidd, vilken kan variera från några få meter till flera kilometer.

EM-attacker slår direkt mot hårdvaran i elektroniska system, och skiljer sig därigenom från cyberhot, som slår mot mjukvara i kommunicerande digitala system. Vissa tekniska system kan vara beroende av ett system som slås ut av en EM-attack, vilket kan vara mycket allvarligt och leda till kaskadeffekter som sprider sig i samhället. Till exempel slås vattenförsörjning och trafiksignaler ut om elförsörjningen upphör. Därför bör man vara särskilt uppmärksam på eventuella beroenden mellan olika samhällsviktiga system.

Bland potentiella antagonister som kan tänkas använda EM-hot finns främmande makt, terrorister och kriminella. Vid en militär konflikt är ett civilsamhälle som för sina viktigaste funktioner enbart förlitar sig på trådlös kommunikation och satellitbaserade navigeringssystem, som exempelvis GPS och den europeiska motsvarigheten Galileo, mycket sårbart för moderna telekrigsattacker. Med införandet av *Internet of Things* (IoT), det vill säga att fler saker kopplas upp mot internet, kommer denna sårbarhet sannolikt att öka ytterligare.

Samhällets ökande beroende av elektronik och kommunikation

Scenariot ovan skulle kunna inträffa eftersom alla samhällssektorer de senaste decennierna har genomgått en snabb utbyggnad av elektronisk utrustning för styrning av olika funktioner, databearbetning och kommunikation. Parallellt med detta har det tagits fram avancerade, kommersiellt tillgängliga, störsändare med kapacitet att störa flera olika frekvensband samtidigt (även om dessa är olagliga att inneha). I flera länder utvecklas militära mikrovågsvapen som kan störa eller fysiskt förstöra elektronik. Under det kalla kriget var dessa hot mot det civila försvaret inte lika påtagliga som idag.

Militära system har oftast försetts med skydd mot dessa verkansformer, medan civil elektronik vanligen är oskyddad. Under 1900-talet växte området telekrig fram som ett medel att skaffa sig informationsöverläge under militära konflikter. Detta består av elektronisk spaning (att man avlyssnar motståndarens signaler, såväl kommunikation som oavsiktliga signaler från utrustning), elektronisk attack (att man genom att sända ut elektromagnetisk energi stör eller förvillar motståndarens elektroniska apparatur) samt elektroniskt skydd (att man vidtar åtgärder för att minska effekterna av motståndarens telekrigförings-operationer). Det militära försvaret har sedan decennier utvecklat metoder och teknik för att hantera telekrig, inte minst för att skydda egna viktiga elektroniska system och stödfunktioner.

> “I flera länder utvecklas militära mikrovågsvapen som kan störa eller fysiskt förstöra elektronik. Under det kalla kriget var dessa hot mot det civila försvaret inte lika påtagliga som idag.”

Den snabba elektronikutvecklingen de senaste decennierna, med en enorm ökning av datorstyrning och trådlös kommunikation såväl mellan människor som mellan maskiner, har inneburit att många samhällsfunktioner kommit att basera sin funktion på denna teknologi. Exempel är styrning av industriella processer eller samhällsinfrastruktur via trådlösa nätverk, kontroll av behörighet vid inpassering till viktiga anläggningar, utfärdande

av varningar via radio och sms, betalsystem, med mera. Digitaliseringen av samhället fortgår inom alla sektorer, även samhällsviktiga tjänster. Det innebär att samhället blir allt mer beroende av att elektroniken fungerar samtidigt som man hittills inte har haft några incitament att införa skydd mot antagonistiska EM-störningar. Kanske saknas medvetenhet om sådana hot mot de egna systemen, eller så har man inte bedömt dem som särskilt allvarliga eller sannolika, och därför valt de kortsiktigt mest ekonomiska lösningarna vid anskaffning och installation. All kommersiell elektronik ska uppfylla svenska och internationella standarder vad gäller tålighet mot oavsiktliga störningar, som kan vara naturliga eller orsakade av andra apparater i närheten. Men dessa störnivåer ligger långt under vad som är möjligt att åstadkomma med avsiktliga EM-hot. För militära system ställs hårdare krav på tålighet mot störningar vilket ger ett betydligt bättre skydd men till en ökad kostnad.

Det händer ibland att elektronisk utrustning störs ut av naturliga fenomen, som åska och solstormar, eller oavsiktligt av andra elektroniska apparater i närheten. Men även kunniga privatpersoner kan störa samhällsfunktioner; exempelvis utsattes polisens radiokommunikation för störningar och falska meddelanden vid Göteborgskravallerna 2001. Sådana störformer är blygsamma jämfört med militär telekrigförmåga i en konfliktsituation. Det har även förekommit uppgifter om att mobiltelefoni och GPS har störts som en del av den ryska informationskrigföringen vid konflikterna i Ukraina och Syrien.

Totalförsvarstanken är idag central för att förbereda det svenska samhället inför många olika typer av hot. Ett sammanhållet totalförsvar innebär att civila aktörer måste överväga samma skyddsnivåer som Försvarsmakten. Idag finns begränsad medvetenhet och sparsamt med EM-skydd inom den civila sektorn medan Försvarsmakten sedan länge har tagit höjd för detta. Det är angeläget att inom civila samhällssektorer öka medvetenheten om bland annat antagonistiska EM-hot, så att man kan skydda de samhällsviktiga system som kommer att behövas vid höjd beredskap.

Hur kan man reducera sårbarheter för elektromagnetiska hot?

Uppbyggnaden av det nya totalförsvaret innebär att många myndigheter kan mötas skärpta krav på robusthet mot fler typer av avsiktliga och oavsiktliga störningar, däribland antagonistiska EM-hot. Samtidigt skapar den pågående digitaliseringen av samhället nya risker för olika typer av elektromagnetisk påverkan. Om totalförsvaret inte har detta i åtanke finns risken att man inte upptäcker eller åtgärdar sårbarheter. Vid eventuell nyanskaffning av utrustning är det ofta enklare och billigare att vidta skyddsåtgärder vid installationen i stället för att göra detta i efterhand.

Ansvariga för samhällsviktiga civila verksamheter har vanligen inte samma kännedom om EM-hot och skyddsåtgärder som finns inom den militära sektorn. Medvetenheten om de EM-hot som finns idag behöver öka för att kunna ta itu med dessa i risk- och sårbarhetsanalyser och för att kunna åtgärda identifierade kritiska svagheter.

Trådlös kommunikation är mycket svårare att skydda än ledningsbunden, som går i metalledningar eller optiska fibrer. Därför bör trådlösa kommunikationslösningar för samhällsviktiga funktioner göras tåliga mot störningar eller ha redundans. Detta kan realiseras på olika sätt. Exempelvis kan det ske med kommunikationssystem som byter frekvens antingen regelbundet eller vid störning. Tåligheten ökar med flera antenner placerade på olika platser, flera kommunikationssystem som använder olika frekvensområden eller genom att trådlösa kommunikationssystem kompletteras med fiberlösningar där så är möjligt.

Det är inte en trivial uppgift att utforma ett fullgott skydd mot oönskad elektromagnetisk strålning. Det finns ett flertal strategier för att skydda elektronisk utrustning mot EM-hot. Beroende på hur kritisk utrustningen är och vilken skyddsnivå man väljer kan skyddet konstrueras på olika sätt. När det gäller antagonistiska EM-hot mot verksamhetskritiska system finns dock några generella råd som kan ges:

- Sprid inte information i onödan om kritiska system och hur de fungerar, var utrustning finns och vilka frekvenser som används. Fienden kan utnyttja det vid ett angrepp

- Använd helst inte trådlös kommunikation mellan kritiska system utan hellre ledningsbunden kommunikation som är avsevärt mindre störningskänslig. Alternativt bör man använda utrustning med skydd mot telekrig eller ha redundanta system.
- Se till att det inte går att komma nära inpå kritiska system eftersom effekten avtar med avståndet mellan strålkälla och mål. Det lönar sig att flytta ut avspärrningar för att förhindra obehöriga med störutrustning att komma nära en kritisk anläggning.

Att säkra tillgången på reservdelar och se till att man har tillgång till snabb service eller reparation om systemet har blivit utsatt för en EM-attack är också en god strategi för att minimera störningar i elektroniska samhällsfunktioner. Man kan även behöva bygga in verksamhetskritisk utrustning i skyddande skal och montera skyddskomponenter eller olika typer av filter på ledningar.

Det är dock viktigt att inse att det inte går att skydda all kommunikation och elektronisk utrustning mot EM-hot. Man bör prioritera de system som har en kritisk funktion, det vill säga vilkas bortfall skulle leda till stora störningar i viktiga funktioner. För att åstadkomma detta bör man regelbundet genomföra risk- och sårbarhetsanalyser där man inkluderar de risker som EM-hot kan medföra för verksamheten. Det är alltid en avvägningsfråga vilka sårbarheter som ska åtgärdas och vilken skyddsnivå som krävs för att erhålla den robusthet som behövs för att en verksamhet ska kunna fungera om den utsätts för EM-angrepp i en allvarlig krissituation.

Ett första steg när det gäller att skydda kommunikationslösningar och elektronisk utrustning är att skaffa sig kunskap om vilka EM-hot som finns och hur man tar med dessa i en risk- och sårbarhetsanalys bland alla andra typer av hot som man har identifierat. Nästa steg är att bestämma om man har tillräcklig kunskap inom verksamheten för att genomföra en risk- och sårbarhetsanalys och åtgärda identifierade brister eller om man behöver anlita extern expertis. Slutligen gäller det att genomföra analysen, vidta lämpliga skyddsåtgärder, verifiera att dessa har gett önskad effekt, och därefter regelbundet tillse att skyddet bibehålls. Glöm inte bort hårdvaran!

För vidare läsning

Tomas Hurtig, Sara Linder, Kia Wiklundh, Karina Fors och Sten E. Nyholm, Introduktion till avsiktliga elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur, FOI-S--5835--SE, MSB1180 - februari 2018.

Kia Wiklundh, Sara Linder, Karina Fors, Tomas Hurtig, och Sten E. Nyholm, Vägledning för risk- och sårbarhetsanalys avseende antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur, FOI-S--5840--SE, MSB1178 - februari 2018.

Sten E. Nyholm, Tomas Hurtig, Sara Linder, Kia Wiklundh och Karina Fors, Genomförande av huvudstudie rörande antagonistiska elektromagnetiska hot mot samhällsviktig verksamhet och kritisk infrastruktur, FOI-S--5842--SE, MSB1179 – februari 2018.

FOI
Totalförsvarets forskningsinstitut
SE-164 90 Stockholm

Telefon: +46 8 5550 3000
www.foi.se