FOI MEMO

Projekt/Project

Analys av informations- och cybersäkerhet i NRFB

Projektnummer/Project no
E13421

Kund/Customer
MSB

FoT-område

Handläggare/Our reference
Ester Veibäck, Fredrik Malmberg Andersson, Erik Carlsson

Datum/Date
2014-11-06

Memo nummer/number
FOI Memo 5100

Informations- och cybersäkerhet i nationell risk- och förmågebedömning – diskussion och presentation av en tankemodell

Sändlista/Distribution:
Kerstin Borg, MSB
Magnus Winehav, MSB
Christina Goede, MSB
Maria Bergstrand, FOI
Per Sundström, MSB
Lars Westerdahl, FOI
Ulrik Franke, FOI
Tommy Gustafsson, FOI

Innehållsförteckning

1 Introduktion

1.1 Syfte

Syftet med nationell risk-och förmågebedömning (NRFB) är att utveckla samhällets förmåga att förebygga och hantera kriser. Allvarliga risker i Sverige identifieras och analyseras för att utreda vilka konsekvenser de kan ge upphov till samt vilken förmåga som krävs för att förebygga och hantera dem. Analysen görs normalt genom scenarioanalys där ett stort antal aktörer är delaktiga i att diskutera händelsens konsekvenser samt hanteringen. Arbetsprocessen bidrar också till att skapa en gemensam förståelse för de analyserade riskerna.

Detta memo utgör en avrapportering avseende arbetet som gjorts för att analysera cyber- och informationssäkerhet. Syftet var från början att analysera cyber- och informationssäkerhetsaspekten genom ett antal exempelscenarier och koppla detta arbete till MSB:s förmågedimensioner. På grund av förändringar under arbetets gång har dock förmågedelen varit tvungen att strykas.

Syftet med arbetet blev därmed ändrat till att ge en grund för att i framtiden på ett tydligare sätt integrera cyber- och informationssäkerhet i NRFB. Detta görs genom att se på området informations- och cybersäkerhet med hjälp av en tankemodell som anpassats efter MSB:s terminologi, och ge ett urval exempel på händelser som skulle kunna uppstå.

Projektet har genomförts av Totalförsvarets forskningsinstitut (FOI) på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB).

1.2 Slutsatser av tidigare utfört arbete

I memo 4936, *Ett första steg mot informations- och cyberrelaterade analyser i NRFB*, presenterades en kartläggning av vad som karakteriserar området informations- och cybersäkerhet, olika typer av hot, ett utvecklat antagonistiskt scenario som slår ut vattenförsörjningen i en kommun, samt ett påbörjat scenario som leder till problem inom en viss typ av läkemedelsdosering.

Slutsatserna av det arbetet landade i att cyberområdet är så integrerat med samhället och dess funktioner att det inte går att se som en isolerad företeelse. Vidare är det en stor utmaning att beskriva ett scenario, som är begränsat till en sektor, tillräckligt representativt och intressant för en övergripande analys. Kartläggningen av informations- och cyberområdets karakteristik visade på bredden i utmaningar som representativa scenarier bör kunna beskriva, vilket också tydliggjorde att alla dessa inte ryms inom ett, eller två, scenarier.

Liksom MSB konstaterar i en tidigare rapport[1] sluter vi oss till synsättet att informations- och cybersäkerhet angår alla och är en övergripande utmaning för samhället. Detta gör det svårt att analysera konsekvenser genom enstaka enskilda scenarier. Alternativa strategier skulle kunna vara att analysera olika beroenden i ett bredare perspektiv, till exempel olika verksamheters beroende av elektroniska kommunikationer eller informationshantering. En beroendeanalys ger dock inte heller en fullständig bild av vad som kan inräknas som en informations- och cybersäkerhetshändelse, och vilka typer av förmågor en sådan händelse skulle ställa krav på.

En idé som kläcktes var att istället göra en överskådlig tankemodell ur vilken olika typer av scenarier skulle kunna tas fram, samt ge en flora av enklare scenarier som återspeglar olika aspekter av området. Detta ledde till att det vidare arbetet koncentrerades till tankemodellen och att beskriva ett antal exempelscenarier sprungna ur den. Den huvudsakliga analysen av cyber- och informationssäkerhet bör sedermera genomföras integrerat i samband med övriga scenarioanalyser, då de flesta händelser kan innebära aspekter som har bäring på detta.

[1] MSB 2013 *Övergripande utmaningar för samhällsskydd och beredskap - Analys av fem scenarier om samhället år 2031* Publikation MSB 563

2 Metod

Arbetet är en direkt fortsättning på ett tidigare projekt med målet att skapa scenarier inom cyber- och informationssäkerhetsområdet.

Inledningsvis skapades en tankemodell för hur händelser inom området skulle kunna beskrivas. Genom ett arbetsmöte med Lars Westerdahl, Tommy Gustafsson och Ulrik Franke, experter inom informationsteknik vid FOI, testade vi dessa tankar samt skapade en koppling till arbetet med att identifiera och beskriva trender[2] inom cyber- och informationssäkerhetsområdet. Med stöd av modellen tog projektgruppen fram förslag till exempelscenarier, vilka också utgör exempel på några av de trender som beskrivs.

Exempelscenarierna var tänkta att ligga till grund för en diskussion om olika typer av särskilda förmågor som krävs för att förebygga och hantera cyber- och informationssäkerhetshändelser. Det arbetsmöte som genomfördes med syfte att kartlägga detta, med representanter från MSB:s UL-ANA och ICS, gav inte de önskade resultaten, varefter målet att beskriva förmågor ströks. Vi har istället gjort en genomgång av tidigare genomförda scenarioanalyser för att peka på vilka informationssäkerhetsaspekter som de aktualiserar.

[2] Ett arbete som leds av MSB, se den tidigare rapporten: MSB (2012) *Trendrapport – samhällets informationssäkerhet 2012*

3 En tankemodell för informations- och cybersäkerhetshändelser

Arbetet har som nämndes inledningsvis inriktats på att ta fram ett antal enkla exempelscenarier i syfte att belysa en större bredd av händelser. För att strukturera detta arbete utvecklade projektet en tankemodell. Modellens syfte är att utgöra ett redskap för att fundera och diskutera kring möjliga händelser inom informations- och cybersäkerhetsområdet. Modellen bör kunna beskriva redan inträffade händelser, men också tillåta spekulation om möjliga händelser, och på detta vis stödja arbetet med att ta fram exempelscenarier.

Om alla upptänkliga händelser skall kunna beskrivas i modellen krävs att den tar hänsyn till en stor mängd olika aspekter på en stor mängd olika nivåer, men komplexiteten i modellen blir snabbt för stor för att den ska vara praktisk för detta arbete. Detta, kompletterat med tidigare nämnda resonemang, bidrog till beslutet att hålla modellen enkel, och i stället separat redovisa en lista med aspekter som också kan vara till nytta i arbetet.

3.1 Aspekter på cybersäkerhet

Under arbetet med att ta fram modellen diskuterades många olika aspekter[3] av informations- och cybersäkerhetshändelser, exempelvis:

Skillnaden mellan orsak och verkan i tid och rum – olika händelser kan ha väldigt skilda händelseförlopp. I vissa fall finns det en tydlig orsak/verkan-koppling, i andra är det mycket mer diffusa samband, eller kaskader av effekter. En avgrävd fiberkabel får omedelbara och tydliga konsekvenser, medan konsekvenserna av en säkerhetslucka i ett kommunikationsprotokoll kan vara svårare att fånga.

Avgränsningar mellan cyberproblematik, informationssäkerhet och it-säkerhet – vad avgör om en händelse är av ”cyber”-karaktär till skillnad från informationssäkerhet och it-säkerhet? I de förda diskussionerna framträdde gradvis en konsensus kring tanken att en cyber-händelse innefattar både informationslagret och den verkliga världen. Ett tydligt exempel är skadlig kod vars syfte är att förstöra en industrianläggning – här är orsaken ett medvetet angrepp genom informationslagret med konsekvenser i den fysiska världen. Men i andra fall är det tänkbart att orsakskedjan startar i den fysiska tillvaron och får konsekvenser i informationslagret, som i sin tur ger konsekvenser åter i den fysiska tillvaron. Resultatet av dessa diskussioner blev att modellen inte skall begränsas till en onödigt snäv definition av cyberproblematik, utan i stället kunna beskriva även intilliggande fenomen.

Stort beroende av informationsteknologi i samhället – i dagens samhälle är informations- och kommunikationsteknologi så starkt integrerat i alla samhällsfunktioner att det blir meningslöst att försöka separera ut detta som en egen domän. I stället bör man se it som en del av infrastrukturen, precis som el och vatten.

Snabb spridning – Eftersom informationslagret endast har en väldigt svag rumslig koppling till den fysiska tillvaron, kan effekter av en informations- eller cybersäkerhetshändelse sprida sig från lokal till global nivå oerhört snabbt. Andra sidan av jordklotet är på sätt och vis lika nära som grannkommunen. Då krishanteringsorganisationen i Sverige är organiserad utifrån en geografisk indelning (kommuner, länsstyrelser, regioner) kan just spridningen vara svår att hantera.

Snabb teknikutveckling inom området – informationsteknologi, och de sätten som it används på, utvecklas i en hela tiden ökande takt. Detta innebär – tillsammans med samhällets allt större beroende av it – att nya och större risker hela tiden skapas, och att kunskap om området allt snabbare blir inaktuell.

[3] Delvis beskrivna i kartläggningen i FOI-memo 4936. *Ett första steg mot informations- och cybersäkerhetsrelaterade analyser i nationell risk- och förmågebedömning*

Antagonistiska och icke-antagonistiska hot – inom informationssäkerhet är ofta ett antagonistiskt hot implicerat, medan det inom it-säkerhet även diskuteras icke-antagonistiska hot, såsom felaktigt handhavande eller miljörisker. I modellen bör således både antagonistiska och icke-antagonistiska hot kunna beskrivas. En potentiell angripares förmåga ökar i takt med teknikutvecklingen – det skapas hela tiden allt kraftfullare verktyg – och samhällets sårbarhet för attacker ökar med det allt större beroendet av it.

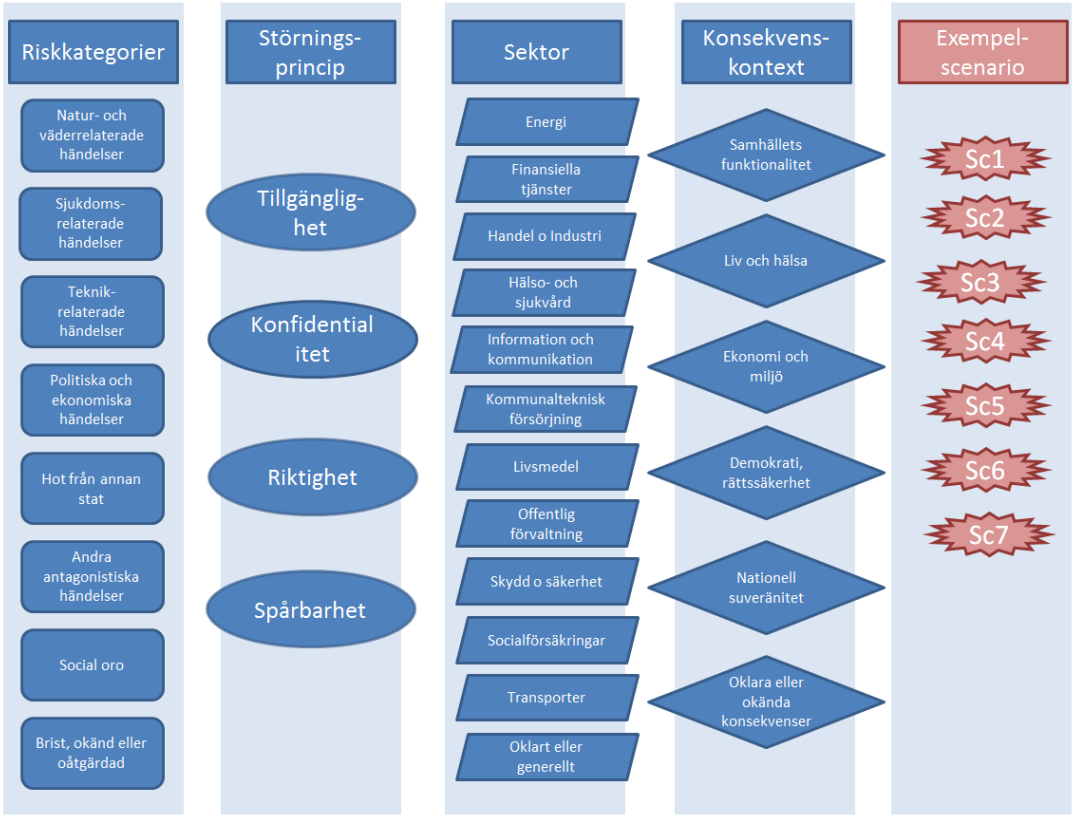
Heterogen gentemot homogen informations- och kommunikationsmiljö – i arbetet diskuterades också på vilka sätt homogenitet eller heterogenitet i olika verksamheters it kunde påverka deras sårbarhet. Användningen av breda lösningar som finns på marknaden, eller specialdesignade lösningar för särskilda ändamål. Ett totalt beroende av enskilda leverantörer eller diversifiering, osv.

Flera av de aspekter som diskuterades är relevanta och viktiga, men då vi försökte passa in dessa i en gemensam modell hamnade den på en för djup detaljeringsnivå.

3.2 Tankemodellen

I Figur 1 nedan visas den resulterande tankemodellen. I dialog med MSB valdes att använda begrepp som redan existerade inom NRFB-arbetet.

Riskkategorierna är hämtade från arbetsmaterial inom NRFB (augusti 2014). Kategorierna överensstämmer med dessa, dock är ”Antagonistiska händelser och social oro” här uppdelat i tre kategorier: ”Hot från annan stat”, ”Andra antagonistiska händelser” och ”Social oro”. En anledning till detta är bland annat att händelser inom informations- och cyberområdet sällan håller sig inom nationella gränser då internet är ett globalt fenomen.



Figur 1: Tankemodell för informations- och cybersäkerhetshändelser

Störningsprinciper utgörs av begreppen *tillgänglighet, konfidentialitet, riktighet* och *spårbarhet*, vanliga begrepp i diskussioner kring informationshantering.

Sektorerna kommer från MSB:s arbete med samhällsviktig verksamhet. Syftet med dessa är att fundera på vilket beroende som finns i den aktuella sektorn av informationshantering, och på vilket sätt den påverkas av störningen. Detta är också ett stöd för att fundera på var i samhället som konsekvenser uppstår, eller som inspiration när man designar scenarier och vill pröva slå mot olika kombinationer av sektorer. Vi har lagt till en kategori ”Oklart eller generellt” eftersom (beroende på vilket håll man går i modellen) det finns händelser som sker sektorsövergripande, där det är oklart var problem har uppstått eller att till exempel främst privatpersoner drabbas.

Konsekvenserna kan sedan relateras till de fem skyddsvärdena, samhällets funktionalitet, människors liv och hälsa, ekonomi och miljö, demokrati, rättssäkerhet och mänskliga fri- och rättigheter, samt nationell suveränitet. Här har vi lagt till ”Oklara eller ännu okända konsekvenser” för den typ av händelse där konsekvenserna uppdagas först långt senare, eller då det råder osäkerhet kring om en sårbarhet i system har utnyttjats eller inte (exempelvis Heartbleed-buggen).

Genom att kombinera olika ingående tillstånd från kategorierna kan olika typer av händelser beskrivas, eller exempelscenarier genereras, vilket beskrivs i nästa avsnitt. Nedan följer en implementation av modellen i verktyget Casper. Verktyget underlättar den praktiska hanteringen av modellen via olika interaktiva funktioner.

Med tankemodellen som utgångspunkt konstruerades en morfologisk modell i verktyget Casper[4], som möjliggör interaktion med modellen. Det går att lägga in nya exempel – verkliga eller påhittade – och kategorisera dessa genom att ange vilka händelsekategorier de tillhör, vilken påverkan de har, vilka samhällssektorer som drabbas och vilka skyddsvärden som riskeras.

Exempel	Händelse- kategorier	Påverkan	Sektor	Konsekvens-kontext
Osäkerhet juridik upphandling moln,	Natur- och väderrelaterade händelser	Tillgänglighet	Energi	Liv och hälsa
Tillgänglighet - Leverantör av drift/tjänst får problem	Sjukdomsrelaterade händelser	Konfidentialitet/ sekretess	Finansiella tjänster	Samhällets funktionalitet
Designade bakdörrar i hårdvara eller mjukvara	Teknikrelaterade händelser, olyckor.	Riktighet	Handel o Industri	Demokrati och rättssäkerhet, mänskliga
Bred säkerhetslucka i logiska lagret för internet	Politiska och ekonomiska händelser	Spårbarhet	Hälso- och sjukvård	Ekonomi och miljö
Information läcker ut att Sverige stöttat NSA genom	Hot från annan stat	N/A	Information och kommunikation	Nationell suveränitet
Framtidstrend: Användarinsamlad	Andra antagonistiska händelser		Kommunalteknisk försörjning	Oklara, eller ännu okända konsekvenser
Utpressning mot Sverige genom hot om attack av	Social oro		Livsmedel	
Pro-kurdiska aktivister i Sverige genomför	Brist, okänd eller oåtgärdad		Offentlig förvaltning	
Insiderproblematik?	N/A		Skydd och säkerhet	
Allvarlig solstorm påverkar GNSS och radioburen			Socialförsäkringar	
Kesslereffekten (rymdskrot)			Transporter	
Tillgänglighetsproblem pga klimatförändring -			Oklart eller generellt	
Kriminella som stjäl uppgifter för kommersiella				
En (eller flera) nyckelpersoner i företag X				
Händelse på sociala medier som leder till social oro				
Uppploppsscenario				

Figur 2: Tankemodellen som en morfologisk modell i verktyget Casper. Exempelscenariot ”Tillgänglighetsproblem pga klimatförändring” är markerat, och dess kategorisering i de övriga dimensionerna är markerade.

För att tillse att modellen var tillräckligt generell för att fånga bredden av möjliga händelser gjordes ett test att med modellen beskriva tidigare händelser såsom Heartbleed-buggen, Tieto-haveriet och Instagram-

[4]Stenström, M; *Morphological Analysis in Groups: A Personal Guide* (FOI 2013)

uppploppet i Göteborg. Vi beskrev också de trender som MSB identifierat inom informations- och cybersäkerhetsområdet (Trendrapport 2012 och samtal med Ulrik Franke avseende trender 2014).

3.3 Hur kan tankemodellen användas?

En fördel med att använda modellen är att kunna föreslå ett antal exempelscenarier som skiljer sig från varandra och tillsammans berör så stor del av olika aspekter av cyber- och informationssäkerhetsområdet som möjligt. Beroende på vad man vill utforska kan man välja att ”gå in i” modellen från olika håll. I Figur 3 nedan visas vilka exempel som har konsekvenser för *demokrati och rättssäkerhet samt mänskliga rättigheter.*

Exempel	Händelse- kategorier	Påverkan	Sektor	Konsekvens-kontext
Osäkerhet juridik upphandling moln,	Natur- och väderrelaterade händelser	Tillgänglighet	Energi	Liv och hälsa
Tillgänglighet - Leverantör av drift/tjänst får problem	Sjukdomsrelaterade händelser	Konfidentialitet/ sekretess	Finansiella tjänster	Samhällets funktionalitet
Designade bakdörrar i hårdvara eller mjukvara	Teknikrelaterade händelser, olyckor.	Riktighet	Handel o Industri	Demokrati och rättssäkerhet, mänskliga
Bred säkerhetslucka i logiska lagret för internet	Politiska och ekonomiska händelser	Spårbarhet	Hälso- och sjukvård	Ekonomi och miljö
Information läcker ut att Sverige stöttat NSA genom	Hot från annan stat	N/A	Information och kommunikation	Nationell suveränitet
Framtidstrend: Användarinsamlad	Andra antagonistiska händelser		Kommunalteknisk försörjning	Oklara, eller ännu okända konsekvenser
Utpressning mot Sverige genom hot om attack av	Social oro		Livsmedel	
Pro-kurdiska aktivister i Sverige genomför	Brist, okänd eller oåtgärdad		Offentlig förvaltning	
Insiderproblematik?	N/A		Skydd och säkerhet	
Allvarlig solstorm påverkar GNSS och radioburen			Socialförsäkringar	
Kesslereffekten (rymdskrot)			Transporter	
Tillgänglighetsproblem pga klimatförändring -			Oklart eller generellt	
Kriminella som stjäl uppgifter för kommersiella				
En (eller flera) nyckelpersoner i företag X				
Händelse på sociala medier som leder till social oro				
Uppploppsscenario				

Figur 3: Vilka exempel (kolumnen längst till vänster) har konsekvenser för skyddsvärdet *Demokrati och rättssäkerhet samt mänskliga rättigheter?*

I Figur 4 har vi snävat in urvalet genom att begränsa dimensionen påverkan till *spårbarhet*. På detta sätt kan man – givet ett tillräckligt stort antal existerande exempel – ta fram de mest relevanta exemplen för den problematik man vill belysa.

Exempel	Händelse- kategorier	Påverkan	Sektor	Konsekvens-kontext
Osäkerhet juridik upphandling moln,	Natur- och väderrelaterade händelser	Tillgänglighet	Energi	Liv och hälsa
Tillgänglighet - Leverantör av drift/tjänst får problem	Sjukdomsrelaterade händelser	Konfidentialitet/ sekretess	Finansiella tjänster	Samhällets funktionalitet
Designade bakdörrar i hårdvara eller mjukvara	Teknikrelaterade händelser, olyckor.	Riktighet	Handel o Industri	Demokrati och rättssäkerhet, mänskliga
Bred säkerhetslucka i logiska lagret för internet	Politiska och ekonomiska händelser	Spårbarhet	Hälso- och sjukvård	Ekonomi och miljö
Information läcker ut att Sverige stöttat NSA genom	Hot från annan stat	N/A	Information och kommunikation	Nationell suveränitet
Framtidstrend: Användarinsamlad	Andra antagonistiska händelser		Kommunalteknisk försörjning	Oklara, eller ännu okända konsekvenser
Utpressning mot Sverige genom hot om attack av	Social oro		Livsmedel	
Pro-kurdiska aktivister i Sverige genomför	Brist, okänd eller oåtgärdad		Offentlig förvaltning	
Insiderproblematik?	N/A		Skydd och säkerhet	
Allvarlig solstorm påverkar GNSS och radioburen			Socialförsäkringar	
Kesslereffekten (rymdskrot)			Transporter	
Tillgänglighetsproblem pga klimatförändring -			Oklart eller generellt	
Kriminella som stjäl uppgifter för kommersiella				
En (eller flera) nyckelpersoner i företag X				
Händelse på sociala medier som leder till social oro				
Uppoppsscenario				

Figur 4: Vilka exempel handlar om påverkan genom spårbarhet och har konsekvenser för skyddsvärdet demokrati och rättsäkerhet samt mänskliga rättigheter?

Ett annat sätt att använda modellen på är att till exempel börja med en störningsprincip och ställa frågor som: vilken typ av konsekvenser ger en störning i *tillgängligheten* för verksamheter i de olika sektorerna? I de fall en händelse ger upphov till en kaskad av effekter, kan man använda modellen för att identifiera den primära påverkan, och därefter analysera vilka sekundär- och tertiär-effekter som kan uppstå.

I nästa kapitel presenteras i korthet några av de exempelscenarier som utvecklades.

4 Exempelscenarier

Scenarierna i detta kapitel är framtagna utifrån den tankemodell som presenterades i föregående kapitel. Alla exempel inleds med en kort beskrivning av vad som sker och sedan en kommentar till detta. I samband med det första exemplet presenteras också ett förslag till hur förmåga utifrån exempelscenariet skulle kunna diskuteras övergripande och kartläggas.

4.1 Osäkerhet i upphandling av it-tjänster

Vad händer?

Bristande juridikkunskaper samt frånvaron av en genomgående säkerhetskultur har i detta scenario lett till att information rörande vårdtagare läckt ut på internet.

En kommun har använt sig av en molntjänst för drift av kritisk it-verksamhet samt för lagring av information av olika känslighetsgrad. Känslig information om vårdtagare har på något sätt läckt ur molnet och hamnat på publika delar av internet. En utredning initieras som visar att leverantören har levererat enligt avtal, och att datahanteringen har brustit i delar som inte täcks av avtalet. Därmed står man utan möjlighet att utkräva ansvar. Detta kommer till allmän kännedom genom reportage lokala massmedier.

Bakgrunden till scenariot kan man tänka sig är att en kommun utkontrakterat it-drift, men att de på grund av resursbrist bara fått med de grundläggande kraven vad gäller kontinuitet och styrning/ledning gentemot leverantören. De har kanske bara haft möjlighet att sikta in sig på de grundläggande frågorna kring konfidentialitet, integritet, tillgänglighet spårbarhet, och missat att ställa krav och reglera motpartens interna säkerhetsstruktur och processer. Osäkerhet i juridiken kring upphandling av molntjänster i kombination med fallerande it- och verksamhetssystem har möjliggjort att problemet uppstått. Drabbade är främst de individer vars uppgifter läckt ut på nätet. Efter att information om detta blivit allmänt känt kommer förtroendet för ansvariga parter att rubbas.

Kommentarer

Här finns möjlighet att belysa både bristande rutiner/processer och bristande teknisk säkerhet hos tredje part. Om en aktör missat att säkerställa ett antal viktiga krav vad gäller informationssäkerhet (kombinerat med att juridiken inom detta område har svårt att hänga med den snabba teknikutvecklingen) kan svårtydda situationer uppstå. Detta scenario lägger fokus både på den förebyggande och på den hanterande aspekten. Särskilt fokus läggs också på juridik i förhållande till it. Påverkan i ett scenario som detta kan spänna över tillgänglighet, konfidentialitet eller integritet utefter vad man vill fokusera på. Den sektor som drabbas primärt är i exemplet offentlig förvaltning då kommunen inte kan utföra sin normala it-beroende verksamhet. Slutligen blir den primära konsekvenskontexten samhällets funktionalitet.

Koppling till förmågor

För att föra en diskussion kring vilka typer av förmågor som aktualiseras av de olika scenarierna skulle MSB:s förmågedimensioner kunna användas, dvs. ”Förebyggande” och ”Hanterande” på ena axeln samt ”Ledarskap”, ”Ledning”, Samverkan”, ”Kommunikation”, ”Kompetens”, ”Resurser” på andra axeln.

I tabell 1 nedan ges ett exempel på hur det skulle kunna se ut, exemplifierat med exempelscenariot ovan. När ett scenario väl är utvecklat och förmågor kartlagt på detta sätt kan man lättare gå vidare till nästa steg som skulle vara att belysa och hjälpa aktörer att i slutändan hantera sin förmåga. Vid genomgång av denna övning framkommer snart att vissa händelser fokuserar mer på exempelvis förebyggande insatser medan vissa fokuserar mer på den hanterande fasen. Vissa är mer av ledningskaraktär medan vissa handlar mer om resursfrågor osv. Detta skulle sedan kunna tas vidare i det större nationella arbetet för ett mer förberett samhälle.

Tabell 1: Ansats till kartläggning av förmågor att förebygga och hantera en viss händelse.

Osäkerhet i upphandling…	Förebyggande	Hanterande (inklusive återställande)
Ledarskap		
Ledning	Viktigt säkerställa beställarkompetens…	
Samverkan	Erfarenhetsutbyte, tex i SAMFI, avseende juridik…	
Kommunikation		Kommunicera till berörda parter…
Kompetens	Viktigt med tillräcklig juridisk kompetens (och upphandlingskompetens)…	
Resurser	Personal med tillräcklig tid …	

4.2 Bred säkerhetslucka i logiska lagret för internet upptäcks

Vad händer?

Cyberincident uppdagas i ett sent skede, drabbar ”alla”, och har redan hunnit ge de största effekterna vad gäller informationssäkerhet.

En tidigare okänd svaghet i en utbredd tjänst (till exempel ett protokoll, Open SSL) upptäcks. Dock är det oklart om, när och i vilken utsträckning som denna lucka har exploaterats (jämför till exempel med Heartbleed-buggen som uppmärksammades i april 2014). Det står klart att i princip alla användare av digital kommunikation vid något tillfälle använt tjänsten. Luckan har möjliggjort massiv integritets- och dataförlust. (Mer konkret exempel: VPN-tunnling utifrån in i Svenska myndigheter påverkas genom att det inte går att avgöra huruvida den dator som ansluter faktiskt är den som den uppger sig vara.) Kanske har opportunister utnyttjat detta för att få tag på känslig information, kanske inte.

Faktorer som verkar för att detta scenario alls kan realiseras är flera. Ur ett rent tekniskt perspektiv är det dels oerhört svårt att konstruera dessa komplexa system med dess stora mängder interaktionspunkter utan att göra minsta fel, dels omöjligt för gemene man att kontrollera att all hård- och mjukvara är säker, och dels det faktum att det finns aktörer som har intresse i att hemlighålla luckor. En av poängerna med ett scenario av denna karaktär är att man inte vet vem som drabbats. Det kan vara allt från privatpersoner som förlorar information eller datakapacitet (botnets), till organisationer och stater som förlorar viktig information. Upptäckten tydliggör att ”alla” potentiellt är drabbade.

Kommentarer

Detta ställer främst krav i den hanterande fasen. Aktörer behöver ha kompetens och resurser att ordentligt kunna rensa, återställa/uppdatera och få igång it-strukturer på bred front inom rimlig tid. Detta kan visa sig vara mer utmanande än man tror i och med ett ökat beroende mellan olika aktörer och deras system. Man kan behöva säkerställa strukturer och förmåga att komma ut med information till de drabbade snabbt. Detta är ett scenario med tydligt teknikfokus. Informationsbärare drabbas av bristande konfidentialitet, riktighet och spårbarhet, eller rättare sagt; detta är de potentiella brister som utnyttjats. Sektorsspridningen är total, alla som använder tekniken är potentiellt drabbade. Vad gäller konsekvenskontexten kan spridningen även här vara total, beroende på vilken data som fallit i ”fel” händer.

4.3 Leverantör av drifttjänster får problem

Vad händer?

Outsourcing av it-drift, tillsammans med fallerande it-system får samhällseffekter. (exempel Tietohändelsen)

En leverantör av driftstjänster får problem, vilket innebär att ett stort antal kunder inte har tillgång till sina system, med de effekter detta medför för samhället.

It-driftsleverantören DriftIT råkar ut för brand under natten mot lördag. Olyckligtvis hinner branden ta sig fort och ger stora skador innan brandkår är på plats. Dagen efter kontaktas kunderna som får en beskrivning av läget. Kunderna meddelas att man naturligtvis kommer gå över till de backups som gjorts, men att det kan ta någon dag innan allt är igång igen. DrifIT:s personal gör under söndagen och måndagen den högst oroväckande upptäckten att backupsystemen är belamrade med en bug som ser ut att innebära att de back-ups som gjorts de senaste fyra månaderna är som bortblåsta.

Oavsett vem som gjort fel och hur så innebär scenariot att ett stort antal kunder står utan tillgång till ID-drift och utan tillgång till de senaste fyra månadernas loggar. Vilka kunder som drabbas är till synes god-tyckligt. Under Tieto drabbades bland andra Apoteket, flera kommuner, Bilprovningen och ett stort transportföretag. Beroende på it-leverantörens storlek kan fler eller färre kunder drabbas. De verksamheter som är vana vid it-avbrott, eller av annan anledning har tradition av att arbeta ”manuellt”, drabbas mindre. Dock tappas den manuella kunskapen mer och mer i och med den kontinuerligt sakta ökande digitalise-ringen.

Kommentarer

I detta scenario belyses både den förebyggande och den hanterande aspekten. Detta scenario behöver inte fokusera på leverantören, det kan lika gärna vara uppbyggt så som norska DSB:s scenario där samhället i princip får totalstopp i sin it under ett antal dagar (hur drabbas samhällsfunktioner, hur påverkar de varan-dra, hur påverkas samhället/medborgarna?).

Detta belyser behov av fungerande manuella rutiner samt fungerande rutiner för att övergå till manuella rutiner. Även förebyggande aspekter så som att säkerställa redundans belyses. Scenariot kan ha flera orsaker (beroende på om det exempelvis är en olycka eller en medveten handling som ligger bakom.) I scenariots utformning så som det står skrivet ovan ligger fokus, vad gäller påverkan, på tillgänglighet. Vilka sektorer som blir påverkade beror helt på vilka kunder som anlitar företaget. Konsekvenskontexten blir likeledes beroende på vilka kunder som anlitar företaget, och vad dessa kunder bedriver för verksam-het. Vad gäller utvecklingen ligger scenariot helt i linje med en ökad koncentrering och centralisering av it-drift.

4.4 Information sprids att Sverige stöttat NSA genom bevakning av egen befolkning

Vad händer?

Staten agerar tvärtemot folkets vilja. Resultatet blir stort socialt missnöje.

Information läcker ut att Sverige otillbörligt stöttat utländsk makt genom bevakning av egen befolkning. Politikerna som går att nås för kommentarer hävdar antingen okunskap eller förnekar sanningshalten i påståendena. Dokument och loggar av olika slag kommer fram och pekar på att anklagelserna ser ut att stämma.

Oavsett sanningshalten i detta orsakar det stort socialt missnöje och oro (demokratifråga). Detta är droppen som får bägaren att rinna över för många, och protesterna blir de mest högljudda hittills. På alla fronter uppstår massiv kritik, med protesttåg, sammandrabbningar, anmälningar och krav på avgångar.

Att det överhuvudtaget har kunnat hända, d.v.s. att man har hamnat i ett läge då man avlyssnar medborgarna utan deras principmedgivande, beror på flera olika faktorer, otillräcklig legal kompetens bland beslutsfattare, otydlig bild över vems säkerhet som är det primära vad gäller staten kontra medborgarna, teknikens utveckling och de möjligheter som detta erbjuder. De som drabbas blir främst privatpersoner och deras känsla av trygghet och integritet.

Kommentarer

Om påståendet i scenariot bevisligen är sant kan scenariot belysa både hanterande och förebyggande aspekter. Detta scenario rör sig på en ”hög” nivå, där frågor som transparens i besluts- och regeringsprocesser kan belysas (förebyggande) och frågor om juridik och cyber. Även hanterande aspekter så som hantering av social oro och ”mediastorm” på nätet. Problemställningarna som aktualiseras i och med ett scenario som detta kan variera oerhört, både i bredd och omfattning. Orsaker och konsekvenser kan ses på/från teknisk nivå upp till frågor kring samhällsstyrning. I den andan kan man kategorisera händelsen som teknikrelaterad likväl som ”social oro” eller ”politiska och ekonomiska händelser”. Den påverkan som ledde till att händelsen i detta fall uppdagades var bristande konfidentialitet. Det är svårt att tala om någon egentligt drabbad sektor. (Troligtvis drabbas några sektorer indirekt så som skett i tidigare fall tå till exempel kreditkortsföretag attackerats av missnöjda aktivister.) Konsekvenskontexten hamnar tydligt i sfären demokrati och rättssäkerhet. Om incidenten skapar tillräckligt missnöje kan man även inkludera ett fokus på social oro. En trend som ligger i linje med scenariot ligger inom ramen för ”Säkerhets och politiska aspekter”, i och med trenden med en ökande övervakning på internet.

4.5 Aktivister i Sverige genomför it-attack mot IS

Vad händer?

En grupp aktivister använder it- och cyberarenan för att, från Sverige och andra länder, attackera ISIS och dess bundsförvanter i hela världen[5]. ISIS anser att Sverige står bakom dessa aktivister (åtminstone de som befinner sig i landet) och därmed skall stå till svars för deras handlingar. ISIS svarar upp mot aktionen genom att genomföra it-attacker mot några Svenska myndigheter och företag. Samtidigt genomför ISIS en underrättelseoperation på nätet för att identifiera de som deltagit i aktionen i Sverige för att därefter söka upp aktivisterna i sina hem för att ta livet av dem eller deras familjer.

Kommentar

Ett scenario som detta har många nivåer och aspekter att analysera. Hur skall staten förhålla sig till aktivister som agerar självständigt och därmed sätter samhället i risk? Hur skulle ett dylikt scenario påverka invandrings- och integrationspolitik? Hur kan myndigheter agera för att få tillräckligt med information om de olika aktörernas agerande för att kunna förhindra dödligt våld? Hur mycket internationellt samarbete krävs för att ha ett tillräckligt bra informationsläge?

4.6 Utpressning via SCADA-attack

Vad händer?

En utpressare tar hjälp av en hackergrupp för att angripa och ta över styrningen av ett vattenreningsverk. Bedriften följs upp med hot om vidare attacker mot SCADA-system.

Detta scenario är en kortare version av det scenario som projektet utarbetade under våren 2014.

X är en kriminell organisation vilken är under hård press från samhället. Under det senaste året har polisen genomfört en riktad aktion mot X i syfte att förstöra organisationen. Efter ett antal större tillslag har flera av

[5] Det var först under skrivandet av detta memo som vi upptäckte att Anonymous faktiskt genomför en operation ”NO2ISIS” i detta syfte. (http://anonhq.com/anonymous-hacker-group-goes-isis/)

X:s ledare gripits och inväntar nu rättegång. De kvarvarande inom X beslutar sig för att hämnas mot samhället som helhet, vilka de anser vara skyldiga till polisens agerande.

X utarbetar, tillsammans med en hackergrupp, en plan där stadens vattenverk skall angripas med målsättningen att skapa kaos genom allmän spridning av magsjuka, för att sedan med en kampanj på nätsidor utöva påtryckning mot samhället.

Hackergruppen kommer över en opublicerad sårbarhet vilken kan möjliggöra kontroll över enskilda vattenpumpar av den sort som används inom vattenverket. Dessutom lyckas man få ett antal anställda att svara på designade mejl med länkar till websidor förberedda för att överföra skadlig kod till besökaren.

Själva vattenverket är i stort automatiserat vilket gör att det endast är bemannat under vissa tider och då främst normal arbetstid under veckodagarna. Angreppet inleds med att hackergruppen slår ut de pumpar som trycksätter det utgående vattenledningssystemet. Detta leder i förlängningen till att vattnet i ledningarna riskerar förorenas. Efter detta raderar gruppen styrprogrammen på hårdvaran i vattenverket för att försvåra återställande till normal verksamhet.

I övervakningscentralen för reningsverket läser operatörerna av rapporterna från reningsverket. Under själva angreppet märker de inte av något i och med att rapporteringen inte skiljer sig från vad de väntar sig. Efter hand, timmar senare, kommer dock signaler från andra delar av distributionsnätet för rent vatten. Varningssignaler för sänkt tryck i nätet inkommer från flera håll.

Samtidig skickar den jourhavande driftsingenjören ut ett meddelande till lokalradion om ett önskemål att alla i staden är sparsamma med sin vattenkonsumtion för att trycket inte skall sjunka för mycket innan en motåtgärd kan sättas in.

Strax efter att lokalradion har gått ut med vattenverkets begäran om återhållsam vattenkonsumtion börjar organisation X proklamera över egna webbsidor, Twitter och nyheternas kommentatorfält att de har stängt av reningsverket och att detta är en inledande hämndaktion mot samhället. Om inte X:s medlämmar friges kommer fler liknande angrepp mot samhället att ske, inte bara inom en stad utan i flera där X har förgreningar.

Trycket i vattenledningen har nu sjunkit så lågt att kvalitéen på vattnet inte längre kan garanteras. Den tidigare uppmaningen via lokalradion fick tillsammans med X:s informationskampanj motsatt effekt då en stor del av befolkningen genast började lagra vatten i de kärl som de hade tillgängliga. Detta har medfört att trycket sjunkit betydligt mer och snabbare än initialt beräknat. Jourhavande driftsingenjör vänder sig åter till lokalradion för att meddela invånarna att de numera bör koka sitt vatten för att vara säkra på att det är tjänligt.

Kommentar

Scenariot sätter fingret på ett antal olika aspekter. Dels de rent it-tekniska och konsekvenserna av automatiserade uppkopplade system, och dels de samhällsorienterade aspekterna så som reaktioner och beteenden hos allmänhet. I detta scenario drabbas primärt alla som är kopplade till det aktuella vattenverket, dels i form av vattenbrist och möjliga sjukdomar, och dels av förtroendebrist i en grundläggande samhällsfunktion (tillgång till rent vatten). I detta scenario är orsakenen blandning av antagonist och teknik. I termer av påverkan kan man peka på bristande skydd av tillgänglighet och förmåga att upprätthålla riktighet. Sektorn är i scenariot bestämt i och med att ett vattenreningsverk angrips, men det skulle kunna röra sig om någon annan sektor. Konsekvenskontexten fokuserar på liv och hälsa, samhällets funktionalitet och ekonomi och miljö. Alla dessa kan i varierande grad påverkas i scenariot, beroende på vad som händer i detalj. Scenariot ligger helt i linje med den ökande aktivitet som sker inom området industriella styrsystem.

4.7 Skyfall

Vad händer?

Skyfall och blixtnedslag orsakar lokala störningar i data- och teletrafik.

Ett omfattande oväder med skyfall och blixtnedslag sveper in över ett område i Sverige. Översvämningar och utslagna el- och kommunikationsstationer orsakar stora störningar i den digitala trafiken under ett antal dagar. Detta scenario analyserades inom ramen för myndigheters risk- och förmågebedömning 2014. Exempel på effekter är att verksamhet som har fokus på tjänster och information får svår att bedriva verksamhet överhuvudtaget. Utslagen kommunikation leder inte bara till stopp i mailsystemen, utan kan påverka saker som passersystem och TiB-funktioner. Oförmåga att ta in information bidrar till isolering och störd verksamhet för de organisationer som drabbas. Om detta scenario förläggs till en ort där någon it-leverantör befinner sig kan sekundäreffekterna bli ännu större vad gäller cyberkomponenter.

Kommentar

Scenariot, så som det är beskrivet ovan är en kortfattad sammanfattning av det scenario som myndigheter analyserade under 2014. Detta är ett bra exempel på ett scenario som i grunden inte är ett cyberfokuserat scenario, men som ändå får konsekvenser inom cyberdomänen. Många ”vanliga” scenarier är av samma karaktär. Det blir där tydligt att cyberdomänen lämpar sig bäst att belysas som en del i alla sammanhang. (Istället för som en isolerad ”cyberhändelse”.)

5 Informations- och cybersäkerhet i tidigare scenarier

Vi har gått igenom tidigare analyserade scenarier i NRFB och funderat på vilket sätt cyber- och informationssäkerhet är relevant i dem. I något fall kan problemen i informationshanteringen utgöra en trigger, något som utlöser andra händelser, i andra fall är det en påverkande (försvårande eller underlättande) faktor.

I de flesta fallen är inte de tidigare scenarierna utvecklade i syfte att utreda informations- och cybersäkerhetsaspekten, varför det kan saknas uppgifter och detaljer i beskrivningarna som är viktiga för att kunna utvärdera vad som händer i informations- och cybersfären. Detta avsnitt syftar till att kommentera vad som kan påverkas och peka ut några intressanta aspekter.

Våldsamma upplopp

Scenariot går i korthet ut på att det uppstår upplopp och kravaller i flera städer parallellt, och detta pågår i drygt en veckas tid med olika intensitet. Den utlösande faktorn till uppploppen är en försenad ambulansinsats då också upprörda filmer sprids i sociala medier, samt ett polisingripande i startskedet som anses vara hårdhänt av flera inblandade. En starkt bidragande faktor till spridning av händelsen till flera städer är hur information och bilder delas via sociala medier. De bakomliggande orsakerna till den sociala oron redogörs det emellertid inte för.

Enligt analysen visar scenariot på att det finns två arenor för händelseutvecklingen, dels den som fysiskt äger rum i de berörda städerna och stadsdelarna, dels den som sker på internet i olika sociala medier och i de traditionella nyhetsmedierna. Myndigheterna måste förhålla sitt agerande till dessa båda arenor, och till samspelet dem emellan.

Cyber är i detta scenario ett verktyg, eller en del av själva scenariot. Händelseutvecklingen accelererar genom informationsspridningen. Informationshantering spelar därmed en stor roll för scenariot, som annars inte skulle uppnått den snabba informationsspridningen och uppploppen kanske inte skulle spridas mellan olika städer. Detta är därmed ett exempel på en händelse som både rör informationshantering och verkliga händelser.

Influensapandemi

I scenariot muterar en influensabakterie och blir smittsam mellan människor vilket den tidigare inte har varit. Under flera månader härjar pandemin som når stora delar av världen. I Sverige skördar influensan många liv och omkring 30 procent av befolkningen har vid något tillfälle under förloppet varit sjuka.

Vid en genomgång av pandemianalysen konstateras att informations- och cybersäkerhetshantering inte är den centrala aspekten. Dock kommer informationsspridning att vara av största vikt för hanteringen av händelsen och en aspekt som kan underlätta scenariot. Som under många typer av kriser kommer kommunikation vara av avgörande betydelse för hur människor hanterar och påverkas av händelsen. Det kan leda till ryktesspridning. Särskild med tanke på massvaccineringen blir informationskanalerna viktiga.

En ökad personalbrist på grund av sjukfrånvaro och VAB kan drabba de verksamheter som ansvarar för itdrift i olika organisationer. Det kan göra att samtidiga händelser blir svårare att hantera och kan leda till större konsekvenser än det normal skulle ha gjort. Samtidigt kommer i stort sett hela samhället att gå lite långsammare under perioden.

Det finns ingen tydlig informationssäkerhetsaspekt i scenariot. Via cyber kan händelseförloppet snarare underlättas. Det blir en mildrande komponent i scenariot.

Terrorattentat

Flera bomber briserar i centrala Stockholm (på Sergels torg och i tunnelbanan) vilket ger ett masskadeutfall som är svårt att hantera eftersom det är nere i tunnelbanan.

Informationssäkerhetsaspekten av detta är inte närmare kartlagd i scenarioanalysen, men det är mycket tänkbart att samhället drabbas på flera sätt. Dels kan infrastruktur och kablage påverkas av bomberna och branden i tunnelbanan så att avbrott sker. Tillgängligheten till data och system påverkas. Med tanke på de verksamheter som finns geografiskt i centrala Stockholm, såsom regeringskansliet och flera banker kan påverkan på ekonomin bli omfattande.

I analysen lyfter man frågetecken kring hur det ska gå att upprätthålla samband mellan ett så stort antal enheter som kommer att krävas för hanteringen av händelsen, på en så pass liten yta med höga byggnader som kan ge radioskugga. Detta är ett potentiellt problem som kan påverka händelseutvecklingen.

Även denna kris kommer också att bli en omfattande informationshändelse med allt som det innebär i form av ryktesspridning och spekulationer i sociala medier. Informationsspridningen kan också underlätta för hanteringen i vissa fall.

Detta är ett exempel på ett scenario där cyber kan sägas vara en komponent i scenariot.

Värmebölja

Värmeböljan i sig uppstår helt oberoende av informationssäkerhetsaspekter. Informationsspridning blir som vanligt viktigt för hanteringen, då information om tips för hur man kan hantera värmen bör spridas till allmänheten. Värmen kan leda till viss ansträngning av kablage, och skogsbränder som uppstår av värmen kan också påverka tillgängligheten till information.

Värmeböljescenariot är därmed ett scenario som kan få konsekvenser inom cybersfären, men som huvudsakligen har effekter i den fysiska tillvaron.

Dammbrott

En stor och viktig kraftverksdamm går i brott, vilket leder till en flodvåg som drar med sig infrastruktur och byggnader i sin väg. Bland annat kapas flera av de viktigaste broarna över älven. Detta kommer att påverka både elförsörjning och kommunikation eftersom kablar är dragna under broar och i banvallar.

Detta scenario är, samtidigt som det påverkar stora delar av samhället, en omfattande cyber- och informationssäkerhetshändelse. Att all kommunikation norrut bryts kan ge konsekvenser som närmast är oöverblickbara. I analysen omnämns exempelvis att kontakt med 112 i området blir lidande, alla myndigheter och företag med kundtjänster och datacentraler vid eller norr om älven kan få problem med förbindelser till dessa eftersom kablar slits av. De nordliga länsstyrelserna kommer att få interna kommunikationsproblem på grund av störningar på LSTNET. Även landstingen i Jämtlands och Gävleborgs län kommer att få stora svårigheter på grund av fallerande elektroniska förbindelser.

I detta scenario kommer påverkan på tillgänglighet till information och kommunikation i de sektorer som drabbas vara stor. Analysen skulle stärkas av att göra en genomgång av vad den påverkade informationsinfrastrukturen ger för konsekvenser. Detta skulle kunna göras sektorsvis och är en omfattande analys.

Scenariot är ett exempel på scenario som mycket tydligt får en konsekvens i cybersfären och därefter i flera steg, trots att det inte startat som en ”cyberhändelse”.

GNSS

Scenariot Avbrott i GNSS kan innebära att elektroniska kommunikationer påverkas och slås ut. Här skulle det vara intressant att bryta ut informationsdelen och först göra en egen (omfattande) analys på den. Scenariot är ett tydligt ”cyber-scenario” i och med att tidssynkroniseringen påverkas, vilket leder till konsekvenser inom andra områden och sektorer. Detta kan påverka både tillgänglighet, riktighet och spårbarhet.

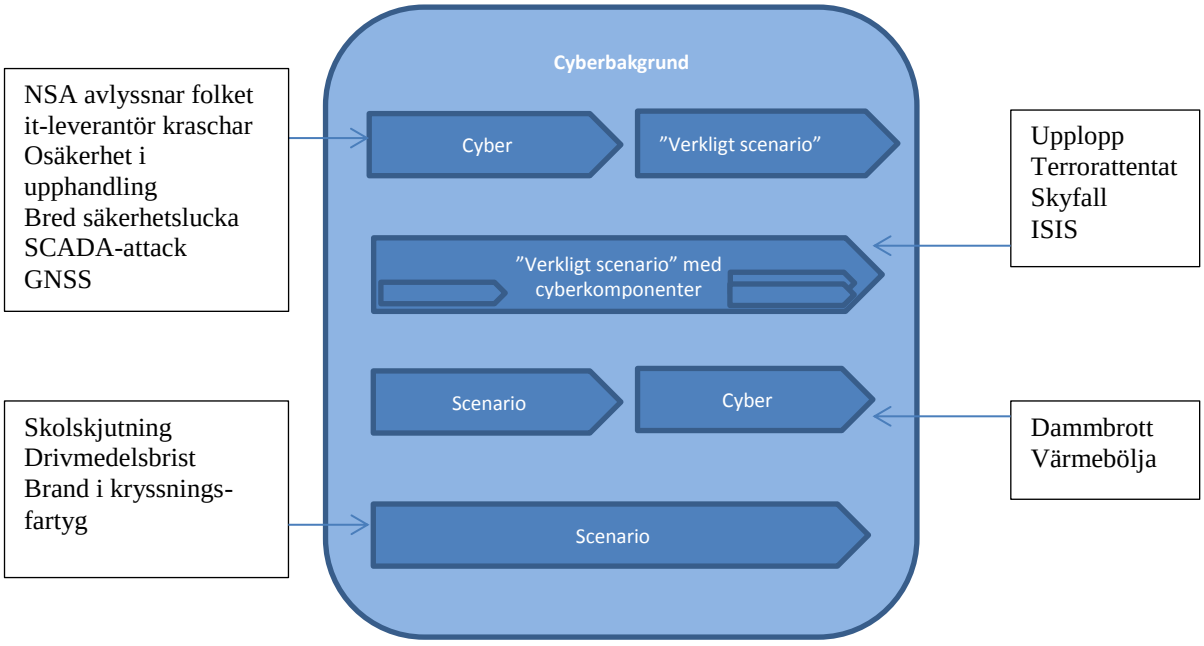
För Skolskjutning, Brand i kryssningsfartyg och Drivmedelsbrist ser vi inte att informations- och cybersäkerheten har en central betydelse för utvecklingen av scenariot. Det kommer att ske en omfattande informationsspridning och möjligen också ryktesspridning, men den påverkan informationshanteringen har i detta är inte mer omfattande än i ”normalfallet”.

6 Diskussion och slutsats

Arbetet med att dels försöka skapa ”cyberscenarier” för NRFB, dels att övergripande försöka analysera cyberområdet utan detaljerade scenarier har gett vissa erfarenheter. Den främsta (vilket också var en utgångspunkt i detta arbete) är att cyber är en integrerad del av vårt samhälle och att det därmed är svårt att analysera det som en egen riskkategori. Slutsatsen blir att ”cyber” inte ska ses som ett eget riskområde utan att informationssäkerhetsaspekter ska analyseras i samband med ordinarie scenarioanalyser i NRFB.

Genom de exempel som ges i detta memo och den genomgång av tidigare analyserade scenarier som presenterats visar vi på att ”cyber” kan ingå i scenarierna på olika sätt och i olika stor grad. Det går naturligvis att forma scenarier där huvuddelen av händelseutvecklingen sker i ”informationslagret”, men att det sedan får konsekvenser i världen utanför. Exempel på dessa är den breda säkerhetsluckan i internet, problem hos en leverantör av drifttjänster, scada-attacken på ett vattenverk. För att det ska bli intressant att analysera i NRFB ska händelsen uppnå vissa dimensioner och också ge konsekvenser i den ”verkliga” världen, alltså att människor skadas eller omkommer, samhällets funktionalitet försämras, egendom går förlorad, miljön blir kraftigt påverkad, värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter hotas eller hot mot den nationella suveräniteten.

Scenarier som är kopplade till cybersfären kan alltså kategoriseras utifrån karaktären på kopplingen till cyberdomänen. En del scenarier har som fokus fallerande it-system, medan andra scenarier orsakar cyberrelaterade händelser i ett senare skede. I figur 5 nedan visas några alternativ.



Figur 5: Skiss över olika scenariers koppling till cybersfären.

Vissa scenarier har it/cyber som grund för ett skeende. Man kan tänka sig att scenarier som t.ex. ”NSA avlyssnar folket”, eller ”it-leverantör kraschar”, eller ”SCADA-attack” som typiskt cyberfokuserade, och som i sin tur kan leda till andra större händelseutvecklingar så som dåligt dricksvatten eller icke-fungerande samhällstjänster.

Den andra kategorin scenarier är sådana som inte primärt orsakas av, eller handlar om, cyberhändelser men som ändå tydligt innehåller vissa cyberaspekter. Exempel på sådana är upplopp (påverkas av exempelvis sociala medier), och ”ISIS-scenariot”.

En tredje kategori scenarier är t.ex. värmebölja och dammbrott som inte primärt är cyberrelaterade men som ändå ger stora konsekvenser i cyberdomänen, till exempel genom att ge begränsningar i kommunikationsmöjligheterna. Den fjärde kategorin är scenarier som vi inte ser har den tydliga kopplingen till cyber. Givet att *allt* sker mot en cyberbakgrund i dag kan de flesta scenarier mer eller mindre långsökt kopplas till något cyberrelaterat.

En av slutsatserna av det genomförda arbetet är att det är möjligt att studera cyberaspekten i efterhand på analyserade scenarier, men att det bästa är att fundera på att öppna upp för en sådan analys redan i början av arbetet. Det krävs i de flesta fall mer detaljer och information för att kunna göra denna analys med större djup. Ytterligare en slutsats är att det är möjligt att, via enklare övergripande modeller, stödja scenarioutveckling inom området cyber. En ökad detaljeringsgrad i modellen öppnar upp för tyngre analys av enskilt scenario men blir snabbt mer svårhanterlig när blicken lyfts mot den bredare samhällsnivån och det breda täcke som it och cyber utgör.

7 Referenser

MSB (2013) *Övergripande utmaningar för samhällsskydd och beredskap - Analys av fem scenarier om samhället år 2031* Publikation MSB 563

MSB (2012) *Trendrapport – samhällets informationssäkerhet 2012* MSB505

Stenström, M (2013) *Morphological Analysis in Groups: A Personal Guide* FOI R-3678

Veibäck, E., Malmberg Andersson, F., Westerdahl, L. (2014) *Ett första steg mot informations- och cybersäkerhetsrelaterade analyser i nationell risk- och förmågebedömning* FOI-memo 4936

http://anonhq.com/anonymous-hacker-group-goes-isis/