Försvarsutskottets offentliga utfrågning om cybersäkerhet

ISSN 1653-0942
ISBN 978-91-88607-53-9
Riksdagstryckeriet, Stockholm, 2018

Förord

Den digitala tekniken har effektiviserat hela det svenska samhället samtidigt som flera händelser under de senaste åren påmint om att den nya tekniken också innebär en ökad sårbarhet. Hoten är många och kan se olika ut och det är en utmaning att i en alltmer transparent miljö skydda samhällsviktig, känslig och hemlig information från intrång, sabotage och läckor.

Riksdagens försvarsutskott anordnade den 17 april 2018 en offentlig utfrågning på temat cybersäkerhet. Utfrågningen genomfördes inom ramen för utskottets beredningsansvar för frågor som rör samhällets informations- och cybersäkerhet. Syftet med utfrågningen var att bidra till en fördjupad diskussion i ämnet med företrädare för myndigheter med ansvar för dessa frågor.

De inbjudna talarna var justitie- och inrikesminister Morgan Johansson, chefen för säkerhetspolisen, Klas Friberg, generaldirektören för Försvarsmakten, Peter Sandwall, generaldirektören för Myndigheten för samhällsskydd och beredskap, Dan Eliasson, samt överdirektören för Försvarets radioanstalt, Charlotta Gustafsson.

Efter presentationerna följde en diskussion mellan utskottets ledamöter och talarna.

I denna rapport publiceras en utskrift av utfrågningen.

Stockholm i juni 2018

Allan Widman (L)	Åsa Lindestam (S)
Ordförande	Vice ordförande

Lars Franzén
Kanslichef

Innehållsförteckning

Program för utfrågningen

Datum: tisdagen den 17 april 2018

Tid: kl. 10.00–12.15

Plats: Förstakammarsalen, Riksdagshuset

Program

10.00-10.05	Inledning, försvarsutskottets ordförande Allan Widman (L)
10.05-10.15	Justitie- och inrikesminister Morgan Johansson (S)
10.15-10.25	Säkerhetspolischef Klas Friberg, Säkerhetspolisen (Säpo)
10.25-10.35	Generaldirektör Peter Sandwall, Försvarsmakten
10.35-10.45	Generaldirektör Dan Eliasson, Myndigheten för samhällsskydd och beredskap (MSB)
10.45-10.55	Överdirektör Charlotta Gustafsson, Försvarets radioanstalt (FRA)
10.55-11.15	Paus
11.15-12.10	Försvarsutskottets utfrågning av inbjudna talare och gäster
12.10-12.15	Avslutning, försvarsutskottets vice ordförande Åsa Lindestam (S)

Stenografisk utskrift från utfrågningen

Ordföranden: God morgon och varmt välkomna hit till Förstakammarsalen i Sveriges riksdag! Mitt namn är Allan Widman, och jag är ordförande i försvarsutskottet. På min ena sida sitter utskottets vice ordförande, Åsa Lindestam, och på den andra sidan kanslichefen för försvarsutskottet, Lars Franzén.

Avsikten är att försvarsutskottet i dag ska hålla en öppen utfrågning om cybersäkerhet. Alla som sitter här är ju väl medvetna om att den digitala tekniken har effektiviserat hela vårt samhälle. Men de senaste åren har vi också påmints om den ökade sårbarhet som tekniken innebär. Främmande makt och enskilda aktörer försöker nu komma över hemlig information hos myndigheter och företag och inom politiken.

I höstas hade försvarsutskottet en motsvarande tillställning som denna, fast sluten, med flera av de myndigheter som är representerade här i dag. Men för utskottet är det viktigt att vi följer upp denna med en öppen, offentlig utfrågning.

Vår beredskap när det gäller cybersäkerhet är beroende av hur väl vi lyckas sprida både kunskaper och medvetenhet hos myndigheter, företag och även bland allmänheten.

Det är ett nöje för mig att välkomna hit justitie- och inrikesminister Morgan Johansson, chefen för Säkerhetspolisen, Klas Friberg, generaldirektören för Försvarsmakten, Peter Sandwall, generaldirektören för Myndigheten för samhällsskydd och beredskap, Dan Eliasson, samt överdirektören för Försvarets radioanstalt, Charlotta Gustafsson.

Morgan Johansson, justitie- och inrikesminister: Herr ordförande! Tack för möjligheten att vara här på denna verkligt vältajmade utfrågning kring cybersäkerhet. Det går knappt en dag utan att vi nås av nyheter eller ny information om frågeställningar som på ett eller annat sätt har koppling till det som vi ska tala om under denna förmiddag.

Precis som ordföranden sa befinner vi oss sedan länge i en situation där den moderna tekniken griper in i och påverkar oss praktiskt taget alltid, åtminstone under vår vakna tid. Man kan gå tillbaka till hur man levde för några decennier sedan jämfört med hur man lever nu. Så fort man vaknar sätter man på sin telefon och ser vad som har hänt under natten och vad det är för frågeställningar som rör sig. Vi är aktiva i sociala medier och hämtar en stor del av nyhetsrapporteringen från internet. Praktiskt taget all information har på något sätt koppling till den moderna teknik som vi får till oss på individnivå.

Också på samhällsnivå har enormt mycket hänt de senaste 15 20 åren. Alla våra bärande system är på ett eller annat sätt beroende av modern informationsteknik. Det gäller sjukvården, elförsörjningen, livsmedelsförsörjningen, vattenförsörjningen och försvaret. Alla våra samhällsbärande system bärs upp av den moderna informationstekniken i dessa dagar.

På många sätt har denna utveckling haft enormt positiva effekter, inte minst socialt genom de kontakter vi numera kan hålla, och ekonomiskt. Effektiviteten i hur vi producerar och använder våra resurser har ökat enormt till följd av den moderna tekniken – minskad resursanvändning. Människor kommunicerar över hela jordklotet, och marknaderna fungerar med ökad konkurrens på ett helt annat sätt än tidigare till följd av att man får mycket mer information om utbud på marknaden, priser och så vidare. Det har lett till enormt positiva ekonomiska och sociala effekter, också enormt positiva politiska och kulturella effekter – bara detta att vi numera alla kan delta i ett globalt politiskt samtal på ett sätt som vi aldrig kunde tidigare. Vi kan nå ut till fler människor än vad vi någonsin tidigare har kunnat göra. Det handlar om åsikter men också om kulturaktiviteter som vi kan ge uttryck för på olika sätt. Det är naturligtvis en enorm breddning av vår möjlighet att nå ut i världen.

En annan positiv aspekt att tänka på när det gäller den nya tekniken är att hela samhället tenderar att bli alltmer transparent, vilket är både positivt och negativt. Det är positivt därför att det innebär att granskningen av makthavare – politiska, ekonomiska eller i näringslivet – har förbättrats för exempelvis medierna. Det är en dramatiskt ökad transparens, något som på det hela taget är positivt. Men – och det är det som vi ska tala om nu under förmiddagen – det ökade beroendet av den moderna tekniken, som griper in överallt i alla våra samhällssektorer, medför också betydande risker för oss. Det gör oss, som ordföranden sa, mer sårbara än vad vi har varit tidigare.

Vad det handlar om är att även i det moderna samhället måste vi se till att vissa saker förblir hemliga. Det är det som är den stora utmaningen. Vad är det då för saker som ska vara hemliga? Det kan till exempel röra sig om känsliga personuppgifter som den offentliga sektorn kan ha, till exempel patientjournaler, uppgifter från brottsundersökningar och förundersökningar som polisen gör och mycket annat, men det kan också vara känsliga personuppgifter som den privata sektorn sitter på. Vi har precis kunnat följa den stora diskussionen om Facebook, där det verkar ha läckt uppgifter som inte var tänkta att läckas men som kom företaget Cambridge Analytica till del och sedan kunde användas på olika sätt, till exempel för att påverka opinionsbildning och samtalsklimat i olika länder och för att manipulera oss på olika sätt.

Känsliga personuppgifter som måste vara hemliga ska också vara hemliga. De ska inte säljas, de ska inte komma ut och hamna i vidare kretsar än vad som var tänkt.

Affärshemligheter måste också förbli hemliga, för om de kommer ut riskerar det att skada näringslivet väldigt allvarligt och därmed företagens konkurrenskraft. Också alla system som styr och bär upp sjukvård, el, livsmedel och andra viktiga samhällsfunktioner måste vara hemliga i den meningen att man inte ska kunna nästla sig in i dem för att kunna slå ut dem.

Slutligen och inte minst måste också försvarshemligheterna vara hemliga.

Vår utmaning är denna: Vi ska skydda samhällsviktig, känslig och hemlig information från intrång, sabotage och läckor, och vi ska göra det i en miljö som är mer transparent än någonsin. Det är detta som är den stora utmaning

som vi har framför oss, och den blir svårare eftersom vi dessutom vet att det finns de som på olika sätt faktiskt vill skada oss och våra system. De ägnar sig inte åt mediers legitima granskningsuppdrag, som ju är *en* sak, utan de vill på olika sätt destabilisera, förstöra och skaffa sig en förmåga att slå ut viktiga samhällsfunktioner. Hoten kan se olika ut. Vi kan ha att göra med enskilda hackare, som i många fall kanske bara vill testa om det går att ta sig in i systemen, kanske för att bli hjältar i den egna subkulturen. Dessa individer finns, vilket är illa nog, och det ska vi förstås se allvarligt på.

Det blir dock ännu värre när man har ett ont uppsåt för att ta sig in i de här systemen. Här kan det röra sig om olika aktörer, till exempel terroristgrupper som ju kan inrikta sig på att slå ut viktiga samhällsfunktioner för att på det sättet sätta skräck i befolkningen och driva fram en egen politisk agenda. Det är för övrigt bakgrunden till att också dataintrång nu tas in på listan över brott som kan utgöra terrorbrott. Detta är en del i det nya EU-direktivet som definierar terrorbrott. Från och med att det implementeras blir också dataintrång klassat som ett möjligt terroristbrott.

Vi kan ha att göra med hot som terroristgrupper. Sedan kan naturligtvis också främmande makt utgöra ett hot. Syftet kan vara att försöka komma åt våra hemligheter i fredstid för att kunna använda dem i krigstid eller i tider av höjd beredskap. De kan kanske till och med använda sig av uppgifterna som ett första angrepp mot ett land, först cyberangrepp för att därefter gå vidare till militära angrepp. Det kan mycket väl vara en strategi som främmande makt kan ägna sig åt.

Det finns alltså ett stort behov för oss av att höja säkerheten och vår beredskap generellt sett i det här avseendet, och det vet jag att det råder mycket stor enighet om. Det kom till uttryck i Försvarsberedningens senaste rapport. Det har också kommit till uttryck i de blocköverskridande försvarspolitiska uppgörelser som har träffats under denna mandatperiod. Den senaste uppgörelsen innebar en höjning av ambitionsnivån när det gäller det civila försvaret på ett sätt som vi inte har sett de senaste 15 20 åren.

Nu går vi in med mer pengar, sammanlagt 1,3 miljarder, över 400 miljoner kronor per år 2018, 2019 och 2020, för att höja den civila beredskapen generellt sett. Det handlar om en lång rad åtgärder, också på cybersäkerhetsområdet. Vi talar till exempel om ökade anslag för MSB, Säkerhetspolisen och FRA för att stärka vår motståndskraft mot it-angrepp. Vi talar om särskilt riktade pengar mot kommuner och landsting, 130 miljoner kronor bara till den sektorn, för att de bland annat ska kunna höja sin beredskap och stärka informationssäkerheten.

I vårändringsbudgeten, som vi presenterade i går, finns ytterligare drygt 100 miljoner kronor avsatta till Försvarsmakten för att höja sin cyberförsvarsförmåga. I vårändringsbudgeten finns också ytterligare pengar, 34 miljoner till MSB och de myndigheter som ska bli tillsynsmyndigheter, när vi implementerar NIS-direktivet.

Jag ska säga några ord om NIS-direktivet. Det är en ny lag om informationssäkerhet för samhällsviktiga och digitala tjänster. Det medför krav på leverantörer av samhällsviktiga tjänster inom energi-, bank- och transportsektorerna, finansmarknaderna, hälso- och sjukvården, dricksvattenområdet och den digitala infrastrukturen att höja beredskapen och säkerheten. De nya kraven omfattar också, till skillnad från tidigare, en stor mängd privata aktörer. Propositionen om implementeringen av NIS-direktivet har lämnats från regeringen till riksdagen för behandling.

Detta är bara en del av de åtgärder som vi har genomfört. Det allra första vi gjorde den här mandatperioden var att införa en obligatorisk it-incidentrapportering. Man funderar över varför det aldrig har gjorts tidigare. Nu har vi för första gången ett system där det är obligatoriskt för de statliga myndigheterna att anmäla till Försvarsmakten och MSB om man utsatts för olika former av it-incidenter av mindre eller större karaktär. Nu får vi för första gången i alla fall ett grepp om vad det är vi ställs inför och vad det är för typ av hot det handlar om. Nu är detta på plats, och vi har därmed en mycket bättre utgångspunkt.

År 2017 tog vi fram Sveriges första strategi just för informations- och cybersäkerheten. Allt det som vi gör nu utgår från denna. Vi moderniserar säkerhetsskyddslagen. Det är också en produkt som ligger på riksdagens bord. Nuvarande säkerhetsskyddslag är från 1996, så då förstår man att det finns ett stort reformbehov. Den nya säkerhetsskyddslagen stramar upp och skärper kraven och kommer också att kompletteras med sanktioner. Om man bryter mot säkerhetsskyddslagen måste det finnas sanktioner. En särskild utredare, Stefan Strömberg, tittar på frågan.

Den 1 april trädde den nya förordningen om samrådsplikt och vetorätt vid utkontrakteringar i kraft. Det innebär att statliga myndigheter måste samråda med antingen Säkerhetspolisen eller Försvarsmakten när man ska göra utkontrakteringar när det gäller säkerhetskänsliga uppgifter. Om Säpo eller Försvarsmakten säger att man inte ska gå vidare med en upphandling eller privatisering, då är det ett nej som gäller. De får helt enkelt vetorätt mot att fortsätta med den typen av processer. Säpo och Försvarsmakten får alltså sista ordet.

Vi är just nu i färd med att genomföra de mest omfattande satsningarna och lagskärpningarna på mycket länge på området cybersäkerhet. Men vi är naturligtvis fortfarande bara i början, för vi måste under ett antal år fortsätta att successivt höja säkerhetsnivån.

Avslutningsvis ska jag nämna ytterligare några initiativ som ligger framför oss.

Det första är en utredning som ser över gränserna för utkontraktering. Det är för övrigt Stefan Strömberg som är utredare också i den delen. Vår utgångspunkt har varit att vissa saker som samhället inte måste ha i egen regi kan läggas ut på entreprenad och utkontrakteras, naturligtvis om det finns ett bra säkerhetsskyddsavtal att utgå från. Men sedan finns det vissa saker vilka inte ska utkontrakteras och som måste hanteras oerhört hemligt och säkert i bergrum, avlyssningsskyddade lokaler och ingenting annat. Då måste man veta vad

det är för typ av information. Därför måste vi höja myndigheternas kunskaper om vad det är för typ av uppgifter som de hanterar och sitter på. Gränserna för detta har hittills varit oklara.

Det andra jag vill nämna är att vi följer upp Försvarsberedningens förslag om en särskild myndighet för det psykologiska försvaret. Det är nu direktiv på gång till en sådan utredning.

Det tredje jag vill nämna är att vi i år krigsplacerar personal på alla de bevakningsansvariga myndigheterna, vilket ställer höga krav på att se till att också dessa uppgifter är hemliga. I krig måste vi naturligtvis hålla den typen av uppgifter för oss själva.

Slutligen har vi gett MSB två nya uppdrag, dels att stärka allmänhetens och företagens motståndskraft mot it-incidenter, dels att tillsammans med länsstyrelserna förbättra kommunernas informationssäkerhet. MSB kommer under de kommande åren att arbeta med detta.

Vi är alltså mitt inne i en sådan process och ett sådant arbete. Jag har bara väldigt översiktligt berört några av de frågor som vi jobbar med. Jag lämnar över detaljerna till de kommande föredragningarna från Säkerhetspolisen, Försvarsmakten, MSB och FRA. Jag tror att detta blir en väldigt nyttig och lärorik förmiddag.

Klas Friberg, Säkerhetspolisen: Herr ordförande och ledamöter! Tack för inbjudan!

Det kan inte nog betonas hur värdefullt och viktigt det är att den fråga som vi talar om i dag adresseras både brett och djupt.

Allmänt kan man säga i dag att det säkerhetspolitiska läget i Europa har förändrats. De senaste årens händelseutveckling i Östersjöregionen och Sverige har gjort att Sverige har fått en ökad militärstrategisk betydelse.

Säkerhetspolisen, liksom andra av våra samarbetsmyndigheter, kan konstatera att det finns ökade militära förmågor i vårt närområde och att Sverige utsätts för it-angrepp. Detta visar att det finns både reella och allvarliga hot mot Sveriges säkerhet. Den förändrade hotbilden mot Sverige har, som bekant, också inneburit att totalförsvarsplaneringen har återupptagits.

Säkerhetspolisen är en av de myndigheter som har en viktig roll i det här arbetet. Vi har ett uppdrag inom säkerhetsskyddsområdet, där vi framför allt bidrar med rådgivning och tillsynsarbete. Jag vill gärna framhålla att vi i detta och mycket annat arbete har ett mycket gott samarbete med FRA, Must och MSB. Det ger både bredd och djup i Sveriges förmåga att arbeta inom säkerhetsskyddsområdet.

Det mest skyddsvärda i samhället är det som regleras i säkerhetsskyddslagstiftningen och omfattar i dag mer än 600 verksamheter i Sverige. Det är verksamheter som är av vital betydelse för samhällets funktionalitet, vårt demokratiska system och politiska beslutsfattande. Det är verksamheter där konsekvenserna av en informationsförlust kan bli kritiska eller oacceptabla för Sverige som stat.

Vi jobbar med att stärka skyddet hos de objekt och mål som är skyddsvärda utifrån Sveriges säkerhet. Sårbarheter i it-system, bristande skydd av byggnader och illojal personal är exempel på sådant som aktörer kan utnyttja för att komma åt eller förstöra hemlig information hos myndigheter och institutioner.

När Säkerhetspolisen för en tid sedan gjorde en inventering på ett antal myndigheter kunde vi konstatera att det finns mycket som fungerar men också det motsatta. Det är framför allt tre saker som behöver uppmärksammas och åtgärdas: bristande säkerhetskultur, otillräckliga säkerhetsanalyser och utkontrakteringar som har gjorts eller görs.

Det här är en enkel bild som visar vad vi kallar skyddsvärde, sårbarhet och hot. Den är tänkt som en förklaring till hur vi jobbar men framför allt hur vi vill att andra som jobbar med säkerhetsskyddsfrågor ska jobba. Några av de absolut viktigaste iakttagelser vi har gjort är att de myndigheter som är aktuella har bristande säkerhetsanalyser. De är inte på det klara med vilket skyddsvärde de sitter med och jobbar med. Då är det också svårt att göra en analys av vilket hot som finns mot dessa.

Att skydda känslig information handlar i dag lika mycket om att undvika följdeffekter, till exempel av att information som blockeras eller saboteras i ett centralt it-system får återverkningar i andra it-system som står i beroendeförhållande. I många fall ser vi att flera känsliga system hamnar i samma korg, på samma plats och i samma system. Det inträffar bland annat när verksamheter väljer att utkontraktera till exempel driften av it-system.

Man ska komma ihåg att målet för angriparna inte alltid är att genomföra ett angrepp för att tillskansa sig information. Det kan även handla om att till exempel skapa förutsättningar att i ett senare skede påverka systemet. Man skapar möjligheten att påverka en vital sektor. Då kanske inte själva intrånget visar sig förrän långt senare, till exempel i samband med en krissituation. För att använda ett bildspråk som både försvaret och vi inom polisen ofta använder arbetar angriparna med att ta fram insatsplaner. De är inne i systemen och skaffar sig en bild av hur de ska kunna agera när de vill skada oss.

Cyberhotet mot företag och myndigheter i Sverige är omfattande och ofta målinriktat. Angriparna som ligger bakom cyberhoten kan vara statliga aktörer eller, som justitieministern nämnde, enskilda aktörer.

Målet för de statliga aktörerna är ofta det som är mest skyddsvärt och också det som säkerhetspolisen skyddar, nämligen Sveriges demokrati. Informationen som angriparna vill komma över är vitala delar för demokratins funktion. Ett exempel är försvarsstrukturer och försvarsindustrin, då dessa verksamheter ytterst garanterar Sveriges frihet och suveränitet. Andra exempel är finansiella system eller finansiella data.

Det svenska samhällets kritiska infrastruktur är i hög grad integrerad med internet. Ett cyberangrepp kan få allvarliga konsekvenser för Sveriges säkerhet och nationella intressen.

Brister som säkerhetspolisen återkommande upptäcker är exempelvis bristande säkerhetsinfrastruktur, såsom brandväggar, skydd mot skadlig kod och loggning av säkerhetsincidenter men också brister i det mest grundläggande skyddet, såsom lösenordshantering och internetåtkomst till nät för dem som inte bör ha det.

I takt med digitaliseringen och ett ökat beroende av informationstekniska system har sårbarheterna i samhället blivit allt fler. Den högre graden av digitalisering leder till större sårbarhet samtidigt som hotet ökar. Gapet mellan hot och skydd växer, vilket vi bedömer som mycket oroande.

De elektroniska angreppen mot svenska myndigheter ökar, och cyberangreppen blir mer avancerade. Säkerhetspolisen är medveten om underrättelsehot från andra länder, vilka sker bland annat genom påverkansoperationer och underrättelseverksamhet. Sannolikt kommer utvecklingen mot en alltmer lättillgänglig angreppsteknik att fortsätta, och fler länder kommer att bygga upp förmågan att utföra cyberangrepp.

Det finns inte några avgörande skillnader i de verktyg som används av statsaktörer och olika kriminella grupperingar. Dock skiljer sig målvalen. En statsunderstödd aktör har förutsättningar att under lång tid och med uthållighet genomföra cyberangrepp jämfört med kriminella aktörer som har kortare uthållighet.

Omfattande elektroniska angrepp är en stor utmaning. För att lyckas behöver vi titta på olika delar av hotet och sårbarheterna.

Vi behöver också ha rätt kompetenser, framför allt inom it-säkerhetsområdet.

Vi ser framför oss ett utökat samarbete mellan myndigheter och med den akademiska världen. Bland förändringarna i vår omvärld märker vi ett påtagligt underrättelsehot från främmande makt. Vi ser ett bredare hot, vilket har blivit alltmer påtagligt i och med att påverkansoperationer och underrättelseverksamheten har fått mer uppmärksamhet i medierna.

Sammantaget visar detta på vikten av att arbeta för att minska sårbarheten och öka skyddet för skyddsvärda verksamheter. Ett bra skydd handlar om fysiska skydd, som lås eller larm. Det handlar om ett fungerande skydd för informationssäkerheten – hur vi förvarar och skyddar hemligheter. Det kan vidare handla om personalsäkerhet och om säkerhetsprövning av personer som anställs. Det kan även handla om att göra säkerhetsskyddade upphandlingar. Utan detta finns risken att Sverige inte kan skydda sig mot angrepp mot vår verksamhet.

Herr ordförande! Jag vill säga några framåtblickande ord. Trots att gapet mellan hot och skydd och växer ser vi flera viktiga förändringar i arbetet med säkerhetsskyddsfrågorna. Den ökade mediala uppmärksamheten vad gäller säkerhetsfrågor och säkerhetsskyddsfrågor är positiv därför att allt fler aktörer påminns om vikten av ett proaktivt säkerhetsskyddsarbete.

Som justitieministern nämnde har vi från den 1 april 2018 en ny lagstiftning som gör att statliga myndigheter före utkontraktering av den egna verksam-

heten som innebär krav på säkerhetsskyddsavtal ska samråda med Säkerhetspolisen eller i vissa fall med Försvarsmakten. Det är bra. En del av satsningen inom säkerhetsskydd handlar om att proaktivt möta cyberangrepp, vilket Säkerhetspolisen gör tillsammans med andra myndigheter.

Vi är även positiva till att regeringen har tillsatt en utredning om att ge Säkerhetspolisen och Polismyndigheten tillgång till FRA:s signalspaning parallellt med pågående förundersökningar. Detta skulle ge oss bättre möjligheter att utreda aktören bakom ett pågående cyberangrepp.

Jag anser att vi framför allt behöver fortsätta att arbeta för att utveckla vår nationella förmåga att skydda samhällets mest skyddsvärda verksamheter mot allvarliga cyberangrepp. Vi behöver ständigt förbättra vår förmåga att upptäcka och respondera mot pågående cyberangrepp. Vi behöver vidareutveckla ett nära samarbete mellan myndigheter och andra samhällsaktörer för att bygga upp kompetens. Alla som bedriver säkerhetskänslig verksamhet har en nationell skyldighet att prioritera säkerhetsfrågor högt.

Jag är personligen övertygad om att medvetenheten och kunskapen om säkerhetsfrågorna hos de berörda verksamheternas chefer och ledningar har ökat det senaste året, av väl kända skäl. Däremot är jag mer tveksam till om allvaret har nått chefer längre ned i organisationerna och myndigheterna och medarbetarna längre ned i organisationerna och myndigheterna i deras vardagliga arbete, där de har att prioritera effektivitet, budget och andra frågor. För att detta ska fungera krävs ett långsiktigt och uthålligt arbete med att öka förståelsen för säkerhetsskydd. Eventuellt kan ett sådant arbete adresseras under paraplyet totalförsvarsplanering.

Arbetet med att skydda oss är ett ansvar för hela samhället. Säkerhetspolisen och försvarsunderrättelsemyndigheterna gör en viktig del av detta arbete, men vi behöver stöd av fler aktörer för att lyckas med vårt mål: ett säkert Sverige.

Peter Sandwall, Försvarsmakten: Herr ordförande och ärade ledamöter! Tack för inbjudan!

Statsrådet tog upp möjligheten när det gäller hot från främmande makt. Med det som utgångspunkt tänkte jag knyta an till regeringens informations- och cybersäkerhetsstrategi, där det anges att det ska finnas ett utvecklat cyberförsvar för att säkerställa den funktionalitet som behövs för att skydda samhällsviktiga funktioner och det som är mest skyddsvärt mot kvalificerade antagonistiska angrepp.

Samma strategi anger också att Försvarsmakten ska stärka den förmåga som vi har att försvara oss mot den typen av angrepp. Det är precis det vi gör – det är detta vi jobbar med dagligdags. Vi gör det genom det cyberförsvarskoncept som vi har för Försvarsmakten. Detta är ett koncept som handlar om Försvarsmaktens förmåga att genomföra defensiva operationer, det vill säga

att förvägra en motståndare möjligheten att påverka Försvarsmaktens olika system. Det handlar också om förmågan till ett offensivt agerande, som ytterst syftar till att avbryta ett pågående angrepp, till exempel vid höjd beredskap.

Denna förmåga och detta koncept bygger på ett antal olika faktorer på ett antal olika områden. Det handlar om att skapa säkra system och säkra processer genom kvalificerad drift och förvaltning, genom att vi ställer säkerhetsskyddskrav och åstadkommer såväl fysiskt som logiskt skydd för våra system och verksamheter samt genom att vi anpassar regelverk av olika slag – det kan gälla administrativa regelverk och för den delen också juridiska regelverk när så behövs.

Det handlar om att vi kan bedriva en konstant utvecklingsverksamhet med forskning och innovation vad gäller såväl materiel som processer. Det handlar inte minst om kompetensförsörjning, vilket jag tror att vi kommer att komma in på vid flera tillfällen under denna förmiddag. Det gäller både rekrytering och hur vi utvecklar kompetensen hos de arbetare vi har i våra respektive organisationer. Det handlar även om bred samverkan, såväl mellan myndigheter som ut mot resten av samhället.

Alla dessa olika områden och faktorer är grundpelarna i det koncept som vi jobbar med.

Vad gör vi då? Jag tänkte berätta lite mer i detalj vad vi arbetar med inom dessa olika områden i dagsläget. Allmänt kan man säga att vi arbetar aktivt med de olika frågorna. Vi tar fram ett ganska stort antal åtgärdsförslag. Vissa rör sådant som vi genomför i Försvarsmakten nu, medan andra rör sådant som vi räknar med att kunna genomföra, bland annat utifrån de ekonomiska tillskott som statsrådet nämnde annonseras i vårändringsbudgeten och utifrån andra åtgärder som vi har kommunicerat till regeringen som önskvärda i vårt senaste budgetunderlag.

Generellt när det gäller åtgärder för informations- och cybersäkerhet handlar det om att separera system inom Försvarsmakten. Vi arbetar med att separera system som hanterar öppen information och system som hanterar sekretessklassad information. Syftet med detta är att skapa ett ändamålsenligt skydd för det som är riktigt skyddsvärd information samtidigt som vi vill förbättra tillgängligheten till, och metoderna att arbeta med, det som är öppen information för att få en bättre fungerande vardag i verksamheten. Detta gäller både tekniska och administrativa åtgärder.

Vi arbetar med att modernisera den tekniska infrastrukturen, till exempel transmissionsnät och datanät. Vi ersätter successivt äldre system med mer moderna system som är lättare att både försvara och hantera. Vi har till exempel ett nytt telefonsystem under utveckling. Detta är ett sätt att modernisera de system som vi har.

Vi vet att det är viktigt att vara snabba i uppdateringen av såväl hårdvara som mjukvara. Erfarenhetsmässigt vet vi att snabbheten i uppdateringar är avgörande för en god säkerhet. Dessa åtgärder gagnar inte bara säkerheten i Försvarsmakten och i det som vi gör utan får också positiva effekter ut mot resten av totalförsvaret.

Vi förstärker också ledningen och samordningen vad gäller incidentrapportering och incidenthantering – två viktiga områden – samt den interna ledningen och samordningen i Försvarsmakten genom organisatoriska åtgärder.

Jag ska nämna något mer specifikt om vad vi gör för att hantera de mest kvalificerade hoten. Vi utvecklar vår förmåga att successivt utarbeta lägesbilder. Dessa lägesbilder behandlar både statusen i Försvarsmaktens system och hoten mot dem. Vi jobbar med åtgärder för att tidigt upptäcka intrång eller försök till intrång och genomför också en förstärkt incidenthantering, vad gäller både snabbhet och adekvata åtgärder, när vi väl konstaterar försök till intrång. Sammantaget handlar det om stärkt förmåga vad gäller både den defensiva och den mer aktiva komponenten i cybermiljön.

Utökad samverkan med andra parter är ett viktigt område. Jag ansluter mig gärna till det som chefen för Säkerhetspolisen sa om att vi har en god samverkan med de myndigheter som vi jobbar närmast, till exempel FRA, Säpo och MSB. Vi har också en utökad samverkan och ett utökat samarbete med den privata sektorn angående hotanalys och ny teknologi.

Metoder för uttagning och rekrytering av personal samt för kompetensförsörjning är andra viktiga åtgärder. Här arbetar vi i Försvarsmakten på metoder för att genomföra rekrytering av it-soldater, för att sedan kunna krigsplacera personer som har adekvat kompetens i organisationen. Vi vill också genomföra utveckling av former för gemensam kompetensutveckling mellan myndigheterna. Jag tror att det är viktigt att hitta flöden där våra medarbetare över tid kan utveckla sin kompetens genom att jobba i olika samhällssektorer och på så sätt öka både den personliga kompetensen och den samlade kompetensen för organisationerna.

Sist men inte minst behöver vi också stärkta möjligheter att träna och öva vår cyberförsvarsförmåga.

Detta var en tämligen översiktlig genomgång av det vi arbetar med just nu. Vi vidtar ett ganska stort antal åtgärder. Vi har alla typer av förmågor på plats, men vi arbetar med att successivt utveckla dessa förmågor på bred front. Vi vet att det är en utveckling där vi aldrig kommer att bli färdiga, givet den utveckling som sker såväl i samhället som internationellt.

Dan Eliasson, Myndigheten för samhällsskydd och beredskap: God förmiddag, herr ordförande, herr minister, utskottsledamöter och kollegor! Jag vill börja med att ge eko till tidigare talares uppskattande ord om att denna utfrågning om cybersäkerhet nu ordnas. Det är väldigt viktigt och ligger väldigt bra i tiden.

Detta är en av de mest prioriterade frågorna för MSB, och jag tror att vi alla är överens om att den inte kommer att minska i betydelse. Detta är en fråga som följer med oss såväl i vardagen som i krisen och vid höjd beredskap, om något sådant skulle ske i framtiden, vilket vi inte hoppas. Vi arbetar före, under och efter händelser i hela hotskalan.

Herr ordförande! Jag ska försöka att förmedla några budskap i dag. Det första budskapet är att vår sårbarhet ökar. Den minskar inte, trots alla åtgärder, och detta är viktigt att konstatera. Jag återkommer till det.

Försvarsmakten och Säpo talade – apropå min andra punkt – en hel del om det som är mest skyddsvärt. Jag vill understryka att vi inte bör glömma bort att hela samhället behöver höja lägstanivån.

Den tredje punkten gäller att man bör vara försiktig och inte ha en övertro på att man kan organisera fram cybersäkerhet.

Den sista punkten är inte särskilt gloriös utan rör det faktum att det i grund och botten är ett ganska vardagligt och tröstlöst gnetande som måste till för att skapa ett systematiskt informations- och cybersäkerhetsarbete. Detta ska jag försöka att tala mer om.

Den första frågan gäller den bild som jag nu visar. Den är viktig. Vi gör, som de flesta andra, bedömningen att det finns stora brister när det gäller informations- och cybersäkerheten i samhället. Mängder av åtgärder vidtas på politisk nivå, och resurser skjuts till. Detta är bra, men mer måste göras. I regeringens strategi på området, i Försvarsberedningens rapport och i Riksrevisionens granskningar ser vi att det finns stora brister. Detta kompletteras av det arbete och de granskningar som vi själva gör i olika verksamheter.

I det incidentrapporteringssystem som nu har inrättats får vi också uppgifter som inte är särskilt glädjande. Det finns brister. Även i den privata samverkan bekräftas bilden av att gapet ökar snarare än minskar, trots alla våra goda föresatser och insatser. Detta länder till eftertanke.

Vad är viktigt i samhället? Det är att slå in öppna dörrar när vi talar om att cyberattacker utgör ett allvarligt hot mot befolkningens liv och hälsa, mot samhällets funktionalitet och mot vår förmåga att upprätthålla våra grundläggande värden. Vi vet alla – som justitie- och inrikesministern underströk i sin inledning och som även ni, herr ordförande, talade om – att samhället i dag är sammankopplat för att kunna producera och distribuera de nyttigheter som vi tar för givna. Alla viktiga funktioner i samhället i dag är beroende av modern teknik för att på ett effektivt sätt bedriva sin verksamhet. Det flöde av pengar, varor och information som krävs för att upprätthålla vår livskvalitet och konkurrenskraft är i dag internationellt, och det är – som Säpochefen sa – inte ovanligt att samhällsviktig verksamhet i dag ägs eller drivs av någon som hör hemma utanför Sveriges gränser. Det är också värt att tänka på.

Den bild som jag nu visar tycker jag är spännande. Den visar att digitaliseringsgapet ökar. På nästa bild, som jag nu visar, ser ni ett antal saker, varav vissa är väldigt skyddsvärda medan andra är vardagliga, till exempel dagstidningar, vattenverk, teleoperatörer och kollektivtrafik. Det är detta som det handlar om: hela samhället. Det finns mängder av verksamheter som vi måste värna för att upprätthålla våra grundläggande värden.

Sjukvård, dricksvatten, transporter, elektroniska kommunikationer och medier är några viktiga verksamheter i samhället. Det handlar om vår offentliga förvaltning och om centrala delar av näringslivet. För att skapa motståndskraft räcker det inte med att bara fokusera på de mest skyddsvärda verksamheterna

i samhället. Jag menar därför att det ”civila cyberförsvaret” inte går att bygga bara utifrån det som är det mest skyddsvärda, utan det måste vara ett försvar av hela samhällets vitala funktioner och informationstillgångar. Detta är viktigt för mig att förmedla.

Herr ordförande! Det går att peka på flera utmaningar i samhället, men jag vill lyfta fram kompetensförsörjning – som Försvarsmakten var inne på – och resurser hos alla de aktörer som ska vidta praktiska åtgärder för att öka säkerheten. Debatten om cybersäkerhet handlar ofta om hur vi ska styra och organisera på en central nivå, och dessa frågor är självklart viktiga. Men det som oroar mig och oss på MSB mest är hur vi som samhälle ska kunna skapa ett ökat arbete och ett ökat engagemang ute i verksamheterna runt om i hela Sverige.

Det kompetenstillskott och de resurser som krävs är omfattande, herr ordförande. I Ekonomistyrningsverkets uppföljning av digitaliseringen av det offentliga Sverige anges till exempel att endast 15 procent av kommunerna har implementerat en modell för att arbeta systematiskt med informationssäkerhet. Vi vet alla hur stor och viktig verksamheten i de kommunala sektorerna är i förhållande till bland annat statlig verksamhet. Våra egna siffror om kommunernas arbete 2015 ger inte heller anledning till några glädjeskutt, kan jag säga.

För att organisationer ska kunna öka sin säkerhet krävs kunskap. Det kostar också pengar att öka säkerheten. Som ni vet kom jag ganska nyligen från polisen. Vi pekade på den tiden ganska kraftfullt på behovet av resursförstärkningar för att kunna möta samhällets utmaningar. Jag kommer nu in i en ny sektor, som innefattar cybersäkerhet, och jag konstaterar att samtalen påminner om varandra. Det saknas poliser – då gör vi någonting åt det. Vi höjer antagningen på Polishögskolan, ökar anslagen och anställer fler. Vi konstaterar nu att det finns brist på kompetens även på detta område. Då måste vi vidta åtgärder även här – det är centralt för tryggheten i framtiden.

Jag vill säga några ord om vad vi behöver göra och om vad som görs. Det är fortfarande så att vi kan komma långt med det som är grundläggande. Angriparnas förmåga har ökat, men fortfarande skulle många angrepp kunna förhindras om organisationerna bara uppgraderade sina system och utbildade sina användare i grundläggande cyberhygien. Jag tror att det var Säpochefen som talade om att man inte ska klicka på konstiga länkar och att man ska använda starka lösenord. Det här är ganska enkla grejer som skulle göra en stor skillnad.

Ett systematiskt och riskbaserat arbete med informationssäkerhet lägger grunden för en cyberhygien och för att skydda organisationens information. I detta arbete kan MSB bidra på flera sätt och gör också det, bland annat genom det metodstöd för systematiskt och riskbaserat informationssäkerhetsarbete som finns på webbsidan informationssakerhet.se. Vi har även en datorstödd informationssäkerhetsutbildning för användare som vi kallar Disa.

För oss är det viktigt att öka säkerheten i de industriella styrsystemen, som ibland kallas Scadasystemen. Dessa är system som till exempel styr och övervakar vår vattenförsörjning och vår elförsörjning. Här kan cyberangrepp inte

bara leda till informationsförluster utan också till fysiska konsekvenser och i värsta fall förlust av människoliv. Man kan angripa oss bakvägen, helt enkelt.

När det gäller förmågor på samhällsnivå är det mycket svårt för en enskild organisation att ha all den kompetens som krävs för att klara av att bedriva ett kvalificerat arbete. Det kan handla om kravställning, metodstöd eller risk- och hotbedömningar. I dag finns många viktiga förmågor utspridda i samhället. För att arbetet ska bedrivas resurseffektivt krävs att statliga myndigheter samordnar sitt stöd samt att vi skapar samlade förmågor i samhället.

Det första som jag skulle vilja trycka på är behovet av ett samordnat informationsutbyte och samverkan mellan privata och offentliga aktörer. Det är avgörande att de privata aktörerna integreras mer i det nationella arbetet med informations- och cybersäkerhet. Vi på MSB har arbetat aktivt med denna fråga sedan starten 2009 och driver i dag ett antal forum där vi utbyter information om risker, sårbarheter och lösningar. Detta samarbete är otroligt viktigt också när det händer någonting. Då kan vi snabbt komplettera den offentliga kunskapen med kunskap från den privata marknaden för att få en så bra lägesbild som möjligt och för att kunna ge en adekvat respons. Detta är ett arbete som naturligtvis måste fortsätta att utvecklas.

Nästa punkt handlar om en samordnad kravställning och tillsyn. Snart kommer NIS-direktivet. Här ingår en mer samordnad kravställning, tillsyn och incidentrapportering. Det kommer att ställas krav på leverantörer av samhällsviktiga tjänster i flera sektorer, exempelvis energisektorn och transportsektorn. I detta ingår även tillsyn. Vi kan nu hamna i ett läge där privata företag utövar tillsyn utifrån föreskrifter som liknar dem som statliga myndigheter ska följa när det gäller informationssäkerhet. Detta är bra. Jag konstaterar dock att till exempel vi själva inte har något mandat eller någon tillsyn från de statliga myndigheterna. Man kan alltså säga att kontrollen av de privata aktörerna kan bli tuffare än kontrollen av de statliga. Det kanske ska vara så – jag vet inte – men det länder i alla fall till eftertanke.

Så till den tredje punkten. För att öka cybersäkerheten behöver vi bygga en ännu mer samlad nationell förmåga att upptäcka och hantera cyberangrepp och cyberkriser. Vi på MSB ansvarar för funktionen Cert.se, som förebygger och hanterar it-incidenter på nationell nivå och som även är en del i det internationella samarbetet med så kallade CERT-funktioner. CERT står för computer emergency response team.

Detta är ett sätt att bygga en samlad nationell och, faktiskt, internationell förmåga att detektera vad som händer och ge adekvat respons. I mitten av februari övade 200 personer i cybersäkerhetsövningen Nisö 2018. 25 organisationer från områden som energi, transporter, elektroniska kommunikationer och sjukvård var med. 50 procent av deltagarna kom från den privata sidan, vilket är otroligt viktigt. Detta var den tredje nationella övningen, och vi ser framför oss att göra det igen snart.

Den sista punkten som jag vill nämna är en samordnad kunskapsutveckling och kompetensförsörjning. Detta är helt avgörande för att vi ska kunna öka informations- och cybersäkerheten i samhället. Jag var inne på parallellerna

till polisen – här behöver vi göra mycket mer. Jag tyckte att det som Försvarsmakten nämnde om kompetensutvecklingsinsatser var spännande. Vi funderar mycket på hur vi ska kunna vara relevanta och rekrytera rätt personal inom MSB. Vi behöver jobba tillsammans och inte konkurrera om kompetensen.

Jag tycker att det initiativ som Stiftelsen för strategisk forskning tog för några månader sedan var spännande. Man delade ut 300 miljoner kronor till tio projekt om cyber- och informationssäkerhet. Detta kommer att bygga både förmåga och kompetens. Denna typ av insatser kommer att behövas, herr ordförande.

Slutligen har jag en sammanfattning. Vi har ökat tempot i arbetet med cybersäkerhet, men gapet sluts inte – det ökar. Vi på MSB har en roll när det gäller informations- och cybersäkerhet. Vi tar den rollen – vi kommer att stiga fram tydligare – men vi behöver också regeringens och riksdagens hjälp att ställa högre krav på det offentliga. Ett systematiskt och riskbaserat arbete med informations- och cybersäkerhet är en grundförutsättning; alla organisationer måste få detta på plats.

För att skapa motståndskraft och ett civilt cyberförsvar i samhället räcker det inte med att fokusera på de mest skyddsvärda verksamheterna, utan vi måste höja nivån i hela samhället. Glöm inte bort detta område när ni talar om resurser – detta är en investering för framtiden!

Charlotta Gustafsson, Försvarets radioanstalt: Jag vill börja med att tacka för möjligheten att få beskriva vad FRA gör på detta område. Under mina tio minuter har jag tänkt att beskriva FRA:s roll inom cybersäkerhetsområdet, och sedan kommer jag att berätta om vår verksamhet inom detta område.

Redan inledningsvis skulle jag vilja ringa in vilket område vi arbetar inom: fientliga aktiviteter som kommer från utländska statliga aktörer eller statsunderstödda aktörer. Det är framför allt detta som utgör hotet mot Sverige och mot våra viktigaste samhällsfunktioner. FRA bidrar till att skydda de viktigaste funktionerna i vårt samhälle. Vi hanterar bara de hot som kommer från statsaktörer, men ändå har vi tillräckligt mycket att göra. Vi ser ett mycket stort antal angrepp från utländska statsaktörer. De visar en utomordentlig målmedvetenhet när det gäller att systematiskt hacka sig in i våra viktigaste system. Ändå ser vi på FRA inte allt.

Vilka syften ligger då bakom detta? Syftena varierar, men de domineras av en vilja att komma åt information. Man kan ha rent kommersiella syften. Man vill ha information om kvalificerad teknik och om sådant utvecklingsarbete som har kostat mycket tid och pengar.

Men vissa utländska statsaktörer är också intresserade av vapensystem och vill genom kunskap om svensk försvarsförmåga utveckla sitt eget militära uppträdande. Det handlar om klassiskt spionage som genom internet har blivit väsentligt mycket enklare, billigare och riskfriare än med tidigare metoder. En annan fullt tänkbar strävan är att genom skadlig kod sabotera vårt samhälle så

att vi inför en militärt skärpt situation ska mista de funktioner som vi behöver för att kommunicera, handla mat eller värma upp våra bostäder.

Vi har redan hört beskrivas vikten av ett gott och systematiskt informationssäkerhetsarbete. Man ska ha genomtänkta system där skyddet dimensioneras efter de risker man ser. Att förbättra informationssäkerheten är såklart väldigt viktigt, men för de utländska statsaktörer som jag har beskrivit finns det inga inbrottssäkra miljöer. Enheter som är uppkopplade mot internet går att hacka sig in i; det är bara en fråga om tid, kompetens och resurser. Utländska statsaktörer har alla tre sakerna: De har tid, kompetens och resurser.

Bara genom att själv ha samma typ av kompetens och resurser kan man bygga upp ett skydd som kan upptäcka de mest kvalificerade angreppen. Detta har vi byggt upp på FRA under lång tid. Vår förmåga inom cybersäkerhet är i dag väl utvecklad, och den utvecklas också löpande.

En fördel vi har på FRA är vår traditionella verksamhet, signalunderrättelsetjänsten. En stor del av den verksamheten sker numera på det globala nätet. Vi har stor kunskap om en del statsaktörers sätt att agera – vi vet hur skadlig kod används, och vi ser hur den används i praktiken. Det är kunskap vi får genom signalunderrättelsetjänsten.

I dag är arbetet med signalspaning mot omvärlden och med att skydda Sverige mot angrepp verksamheter som är ömsesidigt beroende av varandra. Signalspaningsförmågan ger nämligen en unik bild av utländska angripare och deras angreppsmetoder. Förmågan gör att vi har kvalificerad kunskap som också kan användas i arbetet med att stärka Sveriges informationssäkerhet. Signalunderrättelseverksamheten och arbetet mot statsunderstödda it-angrepp vinner båda mycket på att finnas i samma organisation.

Cybersäkerheten ger inte full effekt om den bara utförs *åt* andra. Vårt enskilda arbete på FRA är självklart viktigt, men det får bäst utväxling om det sker tillsammans *med* andra. Genom de fyra myndigheter som finns representerade här i dag ser vi hur staten har fördelat sina kompetenser och uppgifter. Vi gör det inte som isolerade öar utan genom ett gott samarbete, såväl systematiserat som mer informellt. Tillsammans bygger vi Sveriges cyberförsvar.

Vad gör vi då konkret på FRA för att hantera den cybermiljö vi har beskrivit? Från FRA:s sida bistår vi myndigheter och statliga bolag i deras informationssäkerhetsarbete. En rad myndigheter har fått sin it-säkerhet analyserad av oss. I det uppdrag vi får från myndigheterna ingår ofta att testa och försöka skaffa oss kontroll över deras it-system. När vi har avslutat granskningen brukar vi ha en diskussion tillsammans om hur deras it-säkerhet bäst ska utvecklas.

Utländska statsaktörer har också resurser att utveckla skräddarsydda program för att tränga sig in i utvalda it-system. Då finns det i förväg ingen kunskap eller kännedom om vilka program som används – inga antivirusprogram kommer att varna, hur uppdaterade de än är. Därför har FRA utvecklat ett tekniskt detekterings- och varningssystem som larmar när det känner av vad som kan vara ny eller tidigare okänd kod. Information om angreppet skickas tillbaka till FRA för analys. Vi kallar det TDV, och det är i drift hos ett antal

myndigheter. Detta ersätter inte befintliga skydd, men det är ett viktigt komplement.

FRA lämnar stöd till samhällsviktiga funktioner när det gäller att använda säkra kommunikationer. Försvarsmakten har ansvaret för att krypton utvecklas och håller nödvändig kvalitet. FRA har kontakterna med de civila myndigheter som använder krypton. Vi utbildar personalen och uppdaterar system.

Ingen i det här rummet har missat debatten om outsourcing av it-tjänster och hur detta ska kunna göras mer eller mindre smart. Från FRA:s sida har vi publicerat en öppen rekommendationsskrift till dem som överväger att låta underleverantörer hantera it-driften. Om man följer våra rekommendationer kommer man att göra viktiga överväganden som avgör om outsourcing är en bra idé eller om det bara är att bjuda in till intrång från obehöriga.

Regeringen gav FRA och Säkerhetspolisen ett uppdrag som motiverades av it-angrepp som till exempel Cloud Hopper. Vi skulle inleda ett fördjupat samarbete kring de mest skyddsvärda verksamheterna i vårt samhälle och hur de bör skyddas mot de allvarligaste hoten. Vi tycker att det är bra att ytterligare fördjupa samarbetet mellan oss på FRA, som ju har signalspaning och cybersäkerhet som uppdrag, och Säkerhetspolisen, som är Sveriges säkerhetstjänst. Nyligen har regeringen också sett till att Försvarsmakten är med i detta arbete.

Till slut: Regeringen har gett Försvarsmakten uppdraget att utveckla och förstärka cyberförsvaret, och det ska enligt direktivet göras i nära samverkan med FRA. En väsentlig del i detta arbete är frågan om svensk kapacitet i aktiva förmågor i cybermiljön. En sådan kapacitet vore väldigt viktig och en mycket naturlig del av ett framtida svenskt cyberförsvar.

Som ni hör genomförs det mesta av FRA:s verksamhet inom cybersäkerhet i nära samverkan med andra. Vi vet att cybersäkerhetsarbetet ger full effekt och får bäst utväxling om det utförs tillsammans med andra. Det är grunden för att åstadkomma ett bättre skydd, tror vi. Vad vi också behöver göra för att stärka cybersäkerheten i Sverige är att utveckla våra resurser på FRA så att vi kan hålla samma takt som de utländska statsaktörerna gör när de utvecklar sina förmågor.

Därmed vill jag tacka. Jag har gått igenom de viktigaste delarna av FRA:s verksamhet och ser fram emot att svara på era frågor. Stort tack!

Ordföranden: Tack för detta anförande! Nu är det dags för paus. Det finns kaffe i korridoren utanför. Vi återsamlas här inne kl. 11.25, och då vidtar en frågestund med dem som har hållit anföranden.

Ordföranden: Vi har nu kommit till frågestunden. Det är ledamöterna i försvarsutskottet som kommer att ställa frågor. Det skulle uppskattas om man kunde rikta frågan till den det berör, det vill säga den aktuella myndighetsrepresentanten eller för den delen ministern.

Peter Jeppsson (S): Herr ordförande! Jag vill tacka alla som har talat och tagit upp detta viktiga ämne. Jag kommer att ställa mina frågor till både FRA och MSB, och sedan får vi se hur mycket det går att svara på mina frågor och filosofiska tankar.

Jag har till att börja med en direkt fråga, och det är: Kan vi se ökade aktiviteter och attacker mot Sverige nu när vi börjar närma oss valet? Har vi sett någon tydlig del där detta har ökat och vad det skulle kunna innebära?

När det gäller sårbarheten har jag en tanke. I den militära delen är man ju van att hantera information om system och har huvud- och reservalternativ. Men i det civila är allting kanske på ett annat sätt. Lager rullar – jag läste någonstans att en vara byter ägare kanske hundra gånger innan den kommer till sin slutdestination, med allt vad det innebär av säkerhet kring detta. Kan man se hur mycket som behöver göras egentligen? Vi är ju väldigt digitaliserade men också internationaliserade. Frågan är alltså: Kommer vi att ta ett helhetsgrepp, och kommer våra internationella delar av det här att kunna finnas med i det arbete vi kan göra, både inom Sverige och inom EU?

Dan Eliasson, Myndigheten för samhällsskydd och beredskap: Tack för frågan, Peter Jeppsson! Om vi börjar med det här med ökade attacker inför valet handlar det i grund och botten om påverkansprocesser. Detta ligger kanske lite utanför ämnesområdet men ändå i anslutning till det.

Vi har fortfarande inte, från våra utgångspunkter, sett några tydliga tecken på att främmande makt försöker påverka valet. Det är vårt ställningstagande just nu. Vi följer dock detta löpande, hela tiden, för att se om det finns någon asymmetri i flödet av information som kommer till Sverige utifrån.

När det gäller sårbarheter tror jag att den frågan är väldigt viktig. Någonting som riksdagen behöver fundera på – och regeringen med, för den delen – är hur man ska ta sig an frågeställningen om cybersäkerhet och informationssäkerhet när så många aktörer är inblandade. Jag försökte i mitt inledningstal understryka vikten av att inte tro att man kan organisera fram cybersäkerhet. Cybersäkerhet måste för mitt vidkommande finnas i *alla* aktörers tänkande.

Jag tror att det var John F Kennedy som sa ungefär: The incoming tide lifts all boats. Systemet måste alltså höjas sammantaget, och det är det förhållningssättet som är viktigt. Där FRA, Must och Säpo har spetskompetenser kring det allra mest skyddsvärda är MSB mer inne på bogen på det övriga samhället och ger stöd och support för att de aktörerna ska kunna bli duktigare på det systematiska och riskbaserade informations- och cybersäkerhetsarbetet.

Charlotta Gustafsson, Försvarets radioanstalt: Jag kan bara understryka det Dan Eliasson har sagt. Vi ser också ökade attacker, men vi kan inte härleda dem till just valet.

Vad gäller den andra frågan är den samverkan vi har mellan alla de myndigheter som jobbar med cybersäkerhet viktig. Det är också viktigt att titta på

vilka processer vi har för att hantera cybersäkerhetsfrågorna och ensa dem och våra åtgärder i hela samhället.

Hans Wallmark (M): Mycket intressant har sagts inledningsvis. Jag delar ministerns synpunkt att hemliga uppgifter ska hållas just hemliga. Det är nog en slutsats vi kan dra efter säkerhetshaveriet i Transportstyrelsen förra året. Nog om det.

Myndigheterna är inne på att vi måste förbereda bättre och höja vår beredskap. Generaldirektör Dan Eliasson säger att det också handlar om resursförstärkningar. Jag tror att det i MSB:s budgetunderlag för 2019 finns ett äskande om 189 miljoner kronor mer.

Jag vänder mig nu till Försvarsmakten. Försvarsmaktens budgetunderlag för de tre kommande åren är allt som allt ungefär 18 miljarder. Om man inte skulle komma upp i dessa nivåer för 2019–2021, vilka blir då konsekvenserna för just cybersäkerheten? En del av de saker som görs och är planerade att göras i Försvarsmakten handlar om den aktiva cyberförmågan, om övningar och om investeringar i infrastruktur som ledning och samband.

Alltså: Vad blir konsekvenserna för cybersäkerheten om man skulle ligga väsentligen under det äskande Försvarsmakten har i sitt budgetunderlag för åren 2019–2021?

Peter Sandwall, Försvarsmakten: Frågan handlar om Försvarsmaktens budgetunderlag och den hemställan om ökad ekonomi vi har där och om konsekvenserna om denna hemställan inte materialiseras.

Så som vi har lagt upp vårt underlag har vi redovisat för regeringen i en särskild bilaga just behoven inom cyberförsvarsdelarna. Det är en del av det senaste budgetunderlaget. Om det blir väsentligt lägre ekonomiska nivåer än de vi hemställer om kommer det att ge en fortsatt ökad förmåga i cyberförsvarsoperationer men i en lägre takt. Hur mycket lägre takten i så fall blir är givetvis en fråga om hur de ekonomiska resurserna fördelas och prioriteringar inom myndighetens verksamhet. Men att det blir en lägre tillväxt i den förmågeutveckling som vi bedömer är viktig är givet.

Kalle Olsson (S): Herr ordförande! Jag tackar talarna. Flera av er har varit inne på vikten av att i vardagen jobba systematiskt med dessa frågor. Ni har också pekat på vikten av att höja lägstanivån och att jobba med kulturfrågorna i myndigheterna. Detta är påpekanden som ligger väl i linje med de rekommendationer som Riksrevisionen har i sina återkommande granskningsrapporter.

Med risk för en ledande fråga: Utifrån den obligatoriska it-incidentrapporteringen, hur många av dessa intrång och attacker hade kunnat undvikas med relativt enkla medel, alltså att vi tar frågor om lösenord på allvar och inte slarvar med usb-stickor och så vidare?

Dan Eliasson, Myndigheten för samhällsskydd och beredskap: Herr ordförande! Frågan handlar om vad det går att föregripa med hyfsat enkla medel.

Låt mig börja med att reflektera något över hur vi på MSB har utformat rapporteringsskyldigheten. Vi har fått ge närmare förskrifter, och vi har sorterat på att det är allvarligare incidenter som ska rapporteras. När vi ser hur rapporteringen ser ut finns det anledning att fundera på om vi behöver justera och nyansera detta något för att få ett bättre underlag, för det är inte tillräckligt många som rapporterar i dag. Vi måste utöka rapporteringsgraden från myndigheter och berörda aktörer och få alla att inse att man är en del av ett gemensamt system. Det låter kanske lite schablonaktigt, men det är tillsammans som vi blir starka.

Jag kommer inte ihåg alla detaljer, men när vi ser vad som rapporteras in är det dels angrepp, dels brister i hård- och mjukvara och dels trojaner och sådant som skickas in mot oss. Jag talade med chefen för avdelningen för cybersäkerhet hos oss, och mycket handlar om att cyberhygien skulle förbättra läget.

Som Säpochefen sa har de högsta cheferna i organisationerna nog lärt sig den hårda vägen de senaste åren att detta är allvarlig materia och frågor som kanske underskattades tidigare. De har fått detta skarpt inpräntat i sig, inte bara genom mediernas hantering utan också via sina uppdragsgivare, omgivning, verksamhetens logik med mera. Det är dock inte säkert att hela organisationerna inser allvaret på samma sätt, och därför behöver vi jobba systematiskt och riskbaserat i dessa frågor för att komma framåt.

Beatrice Ask (M): Tack för spännande dragningar! Jag har en fråga till justitie- och inrikesministern.

Det är bra att regeringen har satt igång direktivarbetet vad gäller ett nytt psykologiskt försvar. Det är också en fråga som har lyfts upp i Försvarsberedningen. Det är dessutom en gammal moderat käpphäst, så det är positivt. Försvarsberedningen har tittat ganska ingående på dessa frågor, och en slutsats som vi drog gemensamt är att vi tycker att regeringen ska se över hur tillsyn och övervakning ska samordnas. Det är ganska många myndigheter inblandade, och fler blir det med NIS-direktivet.

Min fråga till statsrådet är: När tar regeringen ett initiativ vad gäller att samordna tillsynen? När många kockar har samma uppdrag är risken stor att saker hamnar mellan stolarna.

J*ustitie- och inrikesminister Morgan Johansson*: Vi jobbar givetvis på det. Vi jobbar med direktiven för Utredningen om psykologiskt försvar, och vi kommer att kunna presentera direktiven under våren. Därefter ska vi utse en utredare och få igång själva processen. Uppdraget pågår till 2021 då den nya myndigheten ska vara på plats. Jag tror att vi behöver göra två saker: först se över upplägget av en ny myndighet och sedan ha ett särskilt uppdrag för att sjösätta denna myndighet. Det blir alltså två steg i denna uppbyggnad.

Vad gäller tillsyns- och övervakningsfrågorna är det givetvis också ett arbete som vi kommer att inleda. Det finns flera olika spår. Vi har samordningen av det civila försvaret. Här jobbar vi med direktiven till denna utredning, som också kommer från Försvarsberedningen. Vi har också den övergripande tillsynsfrågan. Vi återkommer givetvis i den delen när vi är färdiga med det arbetet.

Roger Richtoff (SD): Till Försvarsmakten: Jag ser cybersäkerhet som ett vapensystem som ingår i en vapenarsenal. Det kan användas på många olika sätt. Hur ser ni själva på att betrakta detta som ett vapensystem?

Jag undrar också om det behövs ytterligare forskningsresurser för denna verksamhet eller om det räcker som det är.

Till FRA och Säpo: Kan man peka ut vilka länder som sysslar med denna typ av främmande påverkan? Har ni ett underlag som gör att ni med säkerhet kan säga vilka länder som sysslar med detta?

Till MSB: I texterna står det mycket om samordning, vilket är glädjande. Det krävs samordning om det ska få någon riktig verkan. Jag vill gärna ha en kommentar från MSB om länsstyrelserna och kommunerna. En del kommuner har inga handlingsplaner för att kunna fortsätta sin verksamhet i händelse av en beredskapshöjning, medan andra har det. Har MSB ansvar för att följa upp hur det ser ut?

Peter Sandwall, Försvarsmakten: Hur ska man se på cyberförsvar? Generellt sett arbetar Försvarsmakten alltid med att kunna anpassa de förmågor vi har till en hotmiljö, framför allt en hotmiljö i höga konfliktnivåer.

Man kan dra en parallell till telekrigsförmåga. Det är en känd förmåga som Försvarsmakten har sedan ett stort antal år tillbaka. Det handlar om att upptäcka vad motståndaren gör på telekrigsarenan och att själv ha förmåga att kunna verka på telekrigsarenan. Man kan dra paralleller till cyberoperationer utifrån samma tänkande, så i någon mån kvitterar jag att det är ett system som går att likställa med andra system som Försvarsmakten har när det gäller hantering på höga konfliktnivåer.

När det gäller behovet av forskning tror jag att vi alla svarade på det under förmiddagens sejour, och svaret på frågan är: Ja, vi behöver forska och hitta nya innovativa metoder för hårdvara, processer och mjukvara.

Klas Friberg, Säkerhetspolisen: Jag tar mig friheten att också kommentera den första frågan om vapen. Jag är väl medveten om att vi talar om cybersäkerhet, men några av oss har också nämnt påverkan och påverkansoperationer. Det är bra att hålla i minnet att det är ett brett spektrum av åtgärder som kan vidtas, allt från inlägg på Facebook till avancerade, kraftiga cyberangrepp. Allt detta finns inom spannet, och det är viktigt att ha i minnet.

Vilka länder handlar det om? Det finns ett antal länder, men det land som har såväl avsikt som förmåga och uthållighet är Ryssland. Man jobbar systematiskt inom hela det spann av påverkansoperationer som jag nämnde inledningsvis.

Charlotta Gustafsson, Försvarets radioanstalt: Av säkerhetsskäl berättar vi inte vem som ligger bakom angreppen, men vi vet ju.

Dan Eliasson, Myndigheten för samhällsskydd och beredskap: Herr ordförande! Som vi vet är det ansvarsprincipen som är den bärande i den svenska samhällsstrukturen, vilket innebär att var och en har ansvar för sin egen information och för att skydda det som ska skyddas. Det gäller också kommunerna.

MSB:s allmänna uppdrag är att stötta och samordna offentliga aktörer och organisationer som har informationssäkerhetsansvar, inte att ansvara för informationssäkerheten. Det hindrar dock inte att vi bör ta ytterligare ett steg framåt, inte minst enligt regeringen, som har skjutit till mer pengar till informationssäkerhetsarbetet både till oss och till andra aktörer och gett oss ett uppdrag att jobba mer med kommunerna.

För oss är det en spännande utmaning, för vi har ganska stora problem att jobba direkt med alla kommuner. De är många, så vi måste hitta plattformar för att jobba med kommunerna. Då är länsstyrelserna viktiga för oss, men vi har också andra plattformar för att ge stöd och inriktning till kommuner. Ungefär så ser situationen ut.

Lotta Johnsson Fornarve (V): Händelserna i samband med Transportstyrelsen visar på risken med utkontraktering av viktig och känslig it-verksamhet. Det är uppenbart att det är ett stort riskmoment att lägga ut säkerhetskänslig information. Min uppfattning är att utkontraktering av it-verksamhet inom den offentliga förvaltningen ska undvikas så långt det är möjligt.

Mot bakgrund av det vi har hört i dag från justitieministern och chefen för Säkerhetspolisen är min fråga till främst ministern: Är de åtgärder som hittills vidtagits tillräckliga, eller behöver vi utveckla ännu tydligare riktlinjer för utkontraktering av it-verksamhet i den offentliga verksamheten?

Justitie- och inrikesminister Morgan Johansson: Det korta svaret är: Nej, de är inte tillräckliga. Det var därför jag nämnde den särskilda utredning som jag har bett Stefan Strömberg att göra för att se över just gränsdragningarna. Vad kan man egentligen utkontraktera med ett säkerhetsskyddsavtal? Vad är det man inte ska utkontraktera, och vad måste vi se till att hantera under ännu säkrare former? Det finns ju ärenden vi bara hanterar i avlyssningssäkra rum där mobilerna får stanna utanför.

Det handlar om hur gränsdragningarna ska göras och hur myndigheternas kompetens ser ut för bedömningen av de olika uppgifter som de sitter på. Jag tror nämligen att en del av de problem vi har stött på har att göra med att myndigheterna inte alltid förstår vilken känslig information de sitter på. Säpochefen var också inne på att det finns en stor brist här vad gäller beredskap och kompetens, och det måste vi jobba med. Men det behövs även ett utökat regelverk, och därför har vi gett detta uppdrag.

Det har nog varit en kultur ibland av att lägga ut saker på entreprenad för att det ska vara så. Men den principen är nu bruten, och det är säkerheten först som gäller.

Anders Schröder (MP): Min fråga går i första hand till statsrådet.

Vi har diskuterat det nationella samarbetet mycket och hur vi ser till att cybersäkerheten funkar mellan myndigheter och så. Men frågan är också, åtminstone delvis, internationell till sin karaktär vad gäller desinformationsproblemet, som är något som många europeiska länder känner igen sig i, och intrång och olika sårbarheter, som kan finnas i många olika länder.

Kan statsrådet utveckla hur de internationella samarbetena ser ut inom EU och inom andra forum för att motverka detta?

Justitie- och inrikesminister Morgan Johansson: Herr ordförande! NIS-direktivet, som nu ligger på riksdagens bord, är ett exempel på nödvändigheten av att lyfta upp säkerhetstänkandet i hela EU-sfären så att det blir en generell uppstramning på EU-nivå. Det är ganska ingripande, för det gäller inte bara offentliga aktörer. I och med implementeringen kommer vi att ställa mycket högre krav även på privata aktörer och leverantörer av olika tjänster.

I RIF-rådet för vi inrikesministrar givetvis en diskussion om de påverkansoperationer som kan pågå mot oss. På EU-nivå finns en hög medvetenhet om detta, och det vidtas åtgärder i hela organisationen för att säkra upp den.

Klas Friberg, Säkerhetspolisen: Låt mig bara kort kommentera den tidigare frågan om lagstiftningen är tillräcklig när det gäller utkontraktering. Inom Säkerhetspolisen använder vi oss av ett sätt att försöka förklara detta: En del av det är säkert lagligt, men de som vill göra det borde fundera på lämpligheten. Som ministern var inne på tidigare och som jag försökte förklara är det viktigt att man dels gör ordentliga riskanalyser av vilket skyddsvärde man sitter på, dels tänker i två eller tre led på om den information man vill utkontraktera medför risker för den egna verksamheten eller för andras. Alltså: laglighet, ja, men också lämplighet. Jag anser att aktörerna själva måste ta ansvar för detta.

Trots min korta tid på denna position upplever jag att det finns ett mycket bra samarbete i dessa frågor med säkerhetstjänsterna i såväl Norden som övriga Europa. Det är högst aktuella frågor för oss där vi hela tiden diskuterar

och tittar på modus och på vilka skyddsåtgärder och sårbarhetsreducerande åtgärder vi kan vidta.

Alexandra Völker (S): Min fråga går främst till Säkerhetspolisen och MSB och utgår från det som Säpochefen sa om sårbarheten på grund av otillräckliga säkerhetsanalyser och okunskap om vad som behöver skyddas.

Jag undrar hur det ser ut i kommuner och landsting i denna del och vad som kommer att krävas för att öka medvetenheten och kunskapen i dessa frågor i just kommuner och landsting.

Dan Eliasson, Myndigheten för samhällsskydd och beredskap: Herr ordförande! Jag tror att jag nämnde i min inledning, måhända alltför snabbt uppläst för att uppfattas i alla delar, att det enligt Ekonomistyrningsverket är endast 15 procent av kommunerna som genomför regelrätta, systematiska och riskbaserade informationssäkerhetsanalyser. Denna siffra måste upp betydligt, och det är ett av skälen till att regeringen har agerat, skjutit till pengar och gett oss i uppdrag att stötta ytterligare.

Det är som jag sa i min inledning om det fjärde budskapet: Det är vardagsarbete. Den nya dimensionen av offentlig förvaltning är att ha en god cyberhygien och att kunna identifiera vilken skyddsvärd information man har. Vad är det allra mest skyddsvärda, och vad måste man till varje pris ha bra system för? Vilka system har man, och hur är de sammanbundna med varandra? Många gånger har vi kanske bra säkerhet i vissa system, men de är sammanbundna med andra som inte har så bra system. Jag minns att inom polisen fanns det väldigt många system, och alla hade inte samma säkerhetsnivå.

Det är ett gediget hantverksarbete som ska till på detta område, och vi har en modell som vi erbjuder som stöd för detta. Givet det uppdrag vi har fått får vi se hur vi kan flytta fram positionerna ytterligare.

Så till landstingen. Vi har ett särskilt uppdrag sedan början av året att titta på hälso- och sjukvårdens förmåga. Vi är inte färdiga med det arbetet, men jag blir förvånad om vi hittar system som är helt säkra och trygga, med tanke på att det inte finns i resten av samhället. Jag misstänker att vi kommer att hitta brister, som vi ska påtala och arbeta med tillsammans.

Markus Ekbäck, Sveriges Kommuner och Landsting: Frågan om plattformar för att nå ned till kommunerna var uppe förut. I det nya regeringsuppdraget till MSB står det om samverkan med SKL och samarbete med länsstyrelserna.

Sedan rapporten 2015 har mycket skett. I dag bedriver kommunerna ett högkvalificerat arbete, och SKL tillhandahåller ett nationellt metodstöd som går hand i hand med MSB:s metodstöd. De aktuella siffrorna visar att vi har 245 organisationer som arbetar med detta i över 200 kommuner och, till dags

dato, 2 700 handlingsplaner. Man går alltså från klassning ned till upphandlingskrav och ISO-säkerhetsskydd. Det är ganska unikt. Jag vill lyfta fram att detta är en viktig del i samverkan att nå ned.

Mikael Oscarsson (KD): Tack för intressant information! Cyberattacker ökar hela tiden, och flera av er har varit inne på att detta ökar hoten. I dag står det i tidningarna om den varning som gick ut från USA och Storbritannien i går om en pågående global cyberattack riktad mot myndigheter och företag. Man påstår att det är Ryssland som har tagit kontroll över miljontals routrar och kan läsa all information.

Det var Morgan Johanssons kollega i USA som hade kommenterat detta. Har ministern eller någon annan här någon information om detta? Man påstår att man har varnat för att Sverige också kan drabbas.

Min andra frågar riktar jag till Säpochefen. Hur skyddas valsystemet konkret? Det sägs på SVT i dag att man har problem att ta bort gamla konton på kontoret. Hur är det egentligen, kan vi i dag försäkra dem som är oroliga att ni har kontroll över it-riskerna kopplade till valet i höst?

Klas Friberg, Säkerhetspolisen: När det gäller den första frågan har vi känt till denna varning och detta modus ganska länge. Vi vet att det finns och att det har använts tidigare. Jag har ingen kunskap om att vi just i går fick en underrättelse genom våra kanaler, men vi är inte överraskade av detta.

Den specifika frågan om kontona kan jag inte svara på, för det har jag ingen kunskap om.

När det gäller valet och Valmyndighetens ansvar och uppdrag, där vi har varit med under ganska lång tid och gjort analyser och stöttat med rådgivning, är vår bild att vi har ett robust valsystem i Sverige, bland annat för att vi inte är helt beroende av cyber, internet eller data eftersom det till stora delar är manuellt. Även om Sverige skulle utsättas för påverkansoperationer i detta avseende känner vi oss trygga med att det kan genomföras ett val som blir rätt och riktigt. Men någon försäkran vill jag inte ge.

Justitie- och inrikesminister Morgan Johansson: När det gäller valsystemet vill jag påminna om att vi för några år sedan hade en rätt stor diskussion om att gå över till digitala val också i Sverige. Det fanns konkreta förslag på detta. Vi valde att säga nej till det av just det skäl som togs upp, nämligen en väsentligt ökad sårbarhet. Att ha valsedlar i papper som vi låser in, räknar och sedan kan kontrollräkna om det behövs ger ett mycket säkrare system. För bara några år sedan var vi alltså på väg in i ett digitalt system, men på bland andra vårt initiativ avstod vi från det. Det system vi har i dag känns både säkert och stabilt. Det kan förstås utsättas för olika risker, men riskerna hade ökat betydligt om vi hade gått över till ett digitalt system.

Dan Eliasson, Myndigheten för samhällsskydd och beredskap: Herr ordförande! Vi har ett särskilt uppdrag att titta på påverkansoperationer i cybermiljö inför valet och följer naturligtvis detta nogsamt. Min uppfattning och den kunskap vi har är att den företeelse som Mikael Oscarsson nämnde och som nämns i medierna i dag har funnits under en längre tid.

Vi har fått kunskap och information om detta via den funktion som vi har. Detta har diskuterats. För någon dag sedan kom mer formell information om analys, konsekvenser och respons, och vi håller på att titta på den för att se om det finns någon anledning att göra någon typ av reflektion från vår sida.

Detta har en längre historia, och det är internationellt snarare än kopplat till det svenska valet. Det är vår uppfattning.

Lotta Olsson (M): Jag har en fråga till justitieministern om it-kompetensen hos politiker i våra politiska beslut.

Vi ser att vi måste ta hänsyn till ekonomi, tänka på frågor jämställdhetsmässigt och ha många olika perspektiv, men it-säkerheten har aldrig varit på agendan på det sättet när vi fattar beslut. Utifrån sommarens händelser kan vi se att det var lägre kompetens inom politiken som gjorde att det blev problem.

Har justitieministern några planer för hur vi som politiker ska bli bättre på dessa frågor?

Justitie- och inrikesminister Morgan Johansson (S): Just den frågan är föremål för granskning av KU, så vi ska inte springa före där när det gäller att fördela skuld och vem som egentligen bär ansvaret för den delen.

Allmänt kan jag dock säga att jag tror att vi alla måste ha it-säkerhetsaspekterna i åtanke när vi fattar nya beslut. Det som jag precis nämnde om vårt valsystem var precis en sådan situation. När jag gick ut och sa att vi inte ska gå över till ett digitalt röstningssystem reagerade oppositionen i KU – era kollegor. De sa: Vad är nu detta? Tänker regeringen lägga om politiken? Det är klart att vi ska ha ett digitalt valsystem.

Vi hade ett samtal på Justitiedepartementet med oppositionspartierna i KU om detta, och vi kom gemensamt fram till att det nog inte var någon bra idé och att vi skulle ha kvar det röstningssystem som vi har. Det är ett exempel på där man ser vilka risker man löper och därmed lägger om politiken.

Jag tror att vi på alla kanter behöver bli lite bättre på att ta in dessa aspekter när vi fattar beslut.

Mikael Jansson (-): Jag har tre frågor. När det gäller personalförsörjning var det tidigare självklart inom totalförsvaret att personer på nyckelbefattningar skulle ha svenskt medborgarskap.

Vi har nu sett hur känsliga myndighetsnätverk har outsourcats till företag i andra länder, där man inte har svenskt medborgarskap. Outsourcing ses nu över, och det är jättebra. Men vore det inte bra att sätta en klar gräns och ha en

fast styrning där – att man ska ha svenskt medborgarskap om man ska handha känsliga myndighetsnätverk?

Sedan har jag en fråga om system och integration. Vi har massor med känsliga myndighetsnätverk på många olika myndigheter. Ofta har man olika hårdvarulösningar, mjukvarulösningar och konsulter. Skulle det inte vara bra om staten, genom det civila försvar som byggs eller genom MSB, tillhandahåller standardplattformar som man kan styra in mot ökad säkerhet? Detta innebär inte att man ställer dataföretagen utanför, för det är de som tillverkar de egentliga varorna.

Jag har också en fråga om det aktiva it-försvaret. Det är en ny verksamhet. Kommer reglerna för det aktiva it-försvaret att vara offentliga, eller kommer de att vara säkerhetsklassade i sig?

Ordföranden: Jag uppfattade det så att de första två frågorna var riktade till justitieministern och den sista till Försvarsmakten.

Justitie- och inrikesminister Morgan Johansson: När det gäller medborgarskap finns det regler i dag om vilka tjänster man får lov att ha om man är svensk medborgare och vilka man inte får lov att ha om man inte är det.

Vi prövar dessa frågor ofta, för det finns också särskilda regler om undantag för en del fall. Då prövar vi dem från fall till fall, och det systemet fungerar bra. Vi har generellt sett en god kontroll över vem som hanterar känsliga uppgifter, och det finns ett regelverk för det.

När det gäller konsultfrågan och standardplattformar vill jag be myndigheterna att utveckla det, för det är på en tekniknivå som Regeringskansliet kanske inte riktigt når upp till. Jag vill gärna höra hur de ser på den frågan.

Peter Sandwall, Försvarsmakten: När det gäller insatsregler för aktiva cyberförsvarsoperationer använder vi allmänt sett – detta är viktigt att understryka – samma regelverk och samma författningar vad gäller Försvarsmaktens agerande som för all annan verksamhet och alla andra operationer. Dessa författningar är i allra högsta grad offentliga.

När det gäller själva metoderna – hur vi skulle planera och lägga upp en operation – är dessa av samma självklara skäl sekretessbelagda. Men själva det regelverk som vi opererar inom skiljer sig inte från andra insatsregler.

Jan R Andersson (M): Rapporteringsskyldigheten för it-incidenter infördes för två år sedan. Sverige var ganska sent ute – många andra europeiska länder hade haft den ordningen under lång tid.

MSB konstaterar i sin årsrapport att det exempelvis finns en underrapportering. Huvuddelen av de svenska myndigheterna rapporterar ingenting alls, och det kanske är anmärkningsvärt i någon mening.

Generaldirektören beskrev att MSB:s roll är att ha en samlad förmåga och att upptäcka, varna, stödja och samordna hantering vid eventuella incidenter. Min fråga är: Påverkar underrapporteringen er förmåga att bygga upp kunskap som sedan kan vara behjälplig i olika situationer?

En annan fråga som dyker upp i samma sammanhang är om det faktum att man inte rapporterar möjligtvis kan bero på att man saknar en medvetenhet. På en tidigare fråga svarade generaldirektören att det skulle ses över hur rapporteringsformerna ser ut, men om det är medvetenheten som saknas spelar ju inte formerna någon roll. Man måste jobba på flera plan här.

Min fråga, utöver om er förmåga påverkas, är: Har ni några åtgärder planerade utöver det du tidigare beskrev?

Dan Eliasson, Myndigheten för samhällsskydd och beredskap: Herr ordförande! Det är riktigt som Jan R Andersson sa att min och MSB:s bedömning är att det är en underrapportering i dag. Det är fortfarande ett ganska nytt system.

Jag tror att det finns två skäl, precis som Jan R Andersson sa. Det ena är de kriterier som vi har satt upp för rapportering av allvarligare incidenter, där saker som vi borde ha med kanske sållas bort. Det andra är medvetenheten om detta.

Jag är inte redo att i dag tala om hur vi tänker adressera dessa två frågeställningar. Vi har just lämnat in rapporten till regeringen, men dessa två bogar måste vi jobba med på ett eller annat sätt för att få till en bättre och mer fyllig kunskapsmassa som berikar oss i vår förmåga. Vi behöver mer information – så enkelt är det.

Åsa Lindestam (S): Som ni hör vill vi i försvarsutskottet ha en offentlig och öppen debatt. Intresset är stort för dessa frågor hos oss. Det hör ni på de frågor som ni föreläsare har fått svara på.

Det som vår justitieminister inledde med var en bra start. Internet är en positiv företeelse. Den är också mycket effektiv när man vill känna till information. När jag hade börjat på min första chefstjänst och hade fyra telefonsamtal på förmiddagen upptog det hela mitt arbete den förmiddagen, men i dag klarar jag av fyra samtal på ett par tre minuter, genom internet. Det finns alltså mycket som är positivt.

I den här församlingen behöver vi diskutera hur vi ska hålla det hemliga hemligt. Det är väldigt svårt. Den obligatoriska incidentberedskapen är viktig. Vi ser fram emot att ta del av den i försvarsutskottet, och jag hoppas att vi får det. Vi har pratat en hel del om detta.

Vi har lärt oss i dag att den information som vi har och som man vill komma åt är både omfattande och målinriktad. Detta gör att vi måste bli ännu vassare i dessa frågor.

Vi måste också på något sätt få till forskningen så att vi vet vad den innehåller, kanske inte bara för denna församling utan också för gemene man, som måste förstå hur detta ska hanteras.

Kompetensförsörjningen är svår. Många försöker dra till sig just den kompetens som vissa har, men ibland står man där utan. Det är en av de utmaningar vi står inför. Men rekryteringen är tvungen att fortgå, för det är ett behov vi har.

Vi kan inte organisera fram säkerhet, sa Dan Eliasson. Det håller jag verkligen med om. Det är ett tröstlöst letande, men vi får inte ge upp för den sakens skull. Vi måste fortsätta att ta kliv på denna väg, för detta är allvarligt.

Det som Charlotta Gustafsson sa om att statsaktörerna har såväl tid som kompetens och resurser gör att detta har en betydande inverkan på vårt samhälle. Det måste vi anamma och ta till oss.

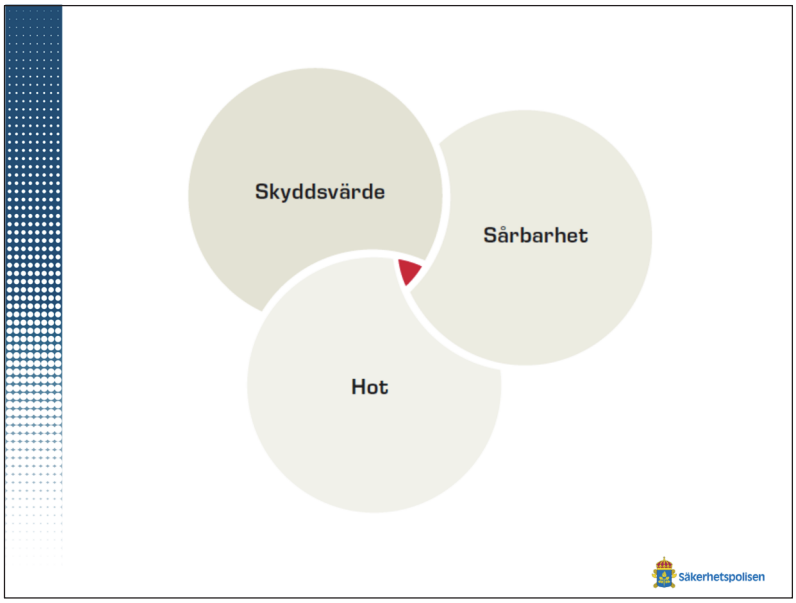
Jag skulle vilja säga tre ord som jag tycker har kommit fram från många av er som har talat på denna konferens, och det är samverkan, cyberhygien och systematik. Jag vill med dessa ord säga tack så mycket till er som har kommit till oss och berättat om hur det ser ut på era myndigheter men också till försvarsutskottet och ordföranden för att vi har fått möjlighet att ha denna stund.

Jag tror att detta kommer att återupprepas framöver, för det här är viktiga frågor. Tack så hemskt mycket för i dag!

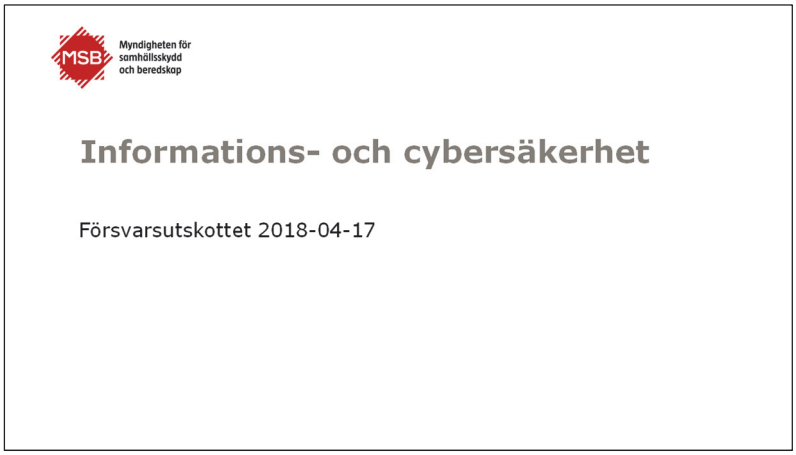
BILAGA 1

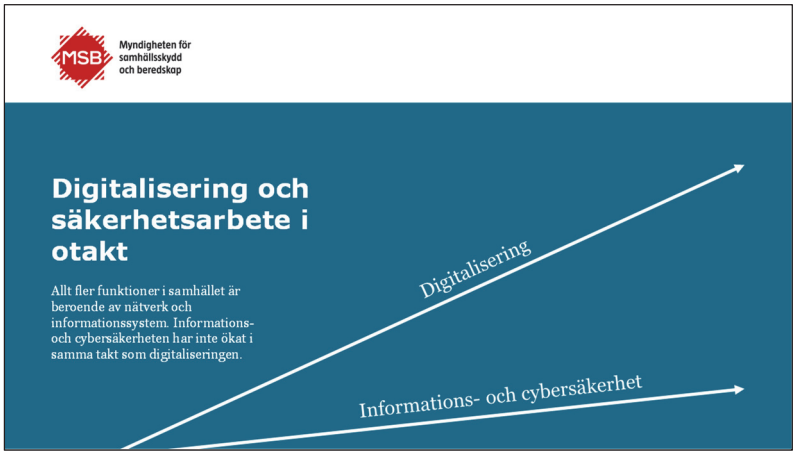
Bildpresentationer från utfrågningen

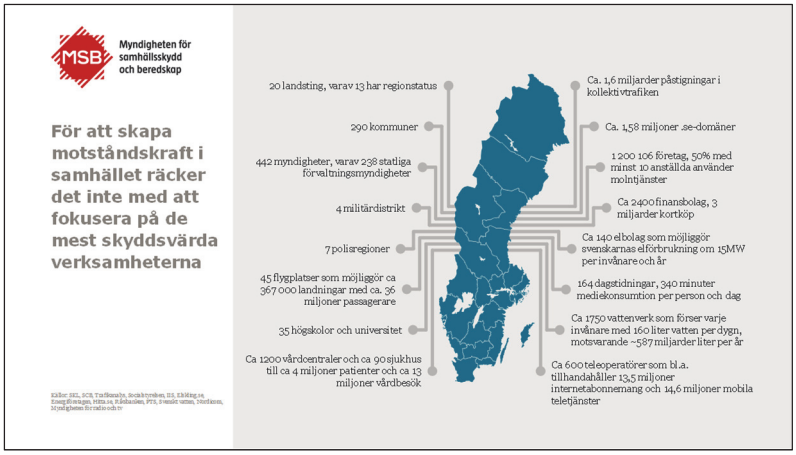
Bilder som Klas Friberg från Säpo visade under sin presentation



Bilder som Dan Eliasson från MSB visade under sin presentation







Myndigheten för samhällsskydd och beredskap

Att utveckla på organisationsnivå

- **Systematiskt och riskbaserat informationssäkerhetsarbete**

Att utveckla på samhällsnivå

- Samordnat informationsutbyte och samverkan mellan privata och offentliga aktörer
- Samordnad kravställning och tillsyn
- Samordnat arbete med att säkerställa tillgång till säkra och robusta nätverk, it-produkter och it-system
- Samlad förmåga att upptäcka, varna, stödja och samordna hantering vid it-relaterade incidenter och kriser
- Samordnad kunskapsutveckling och kompetensförsörjning

Metodstöd för systematiskt informationssäkerhetsarbete

Säkerhet i cyber-fysiska system

Utbildning
http://disa.msb.se

Myndigheten för samhällsskydd och beredskap

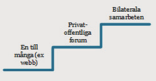
Att utveckla på organisationsnivå

- Systematiskt och riskbaserat informationssäkerhetsarbete

Att utveckla på samhällsnivå

- **Samordnat informationsutbyte och samverkan mellan privata och offentliga aktörer**
- Samordnad kravställning och tillsyn
- Samordnat arbete med att säkerställa tillgång till säkra och robusta nätverk, it-produkter och it-system
- Samlad förmåga att upptäcka, varna, stödja och samordna hantering vid it-relaterade incidenter och kriser
- Samordnad kunskapsutveckling och kompetensförsörjning

Privat-offentliga samverkansforum



MSB:s koncept för samverkan

Myndigheten för samhällsskydd och beredskap

Att utveckla på organisationsnivå

- Systematiskt och riskbaserat informationssäkerhetsarbete

Att utveckla på samhällsnivå

- Samordnat informationsutbyte och samverkan mellan privata och offentliga aktörer
- **Samordnad kravställning och tillsyn**
- Samordnat arbete med att säkerställa tillgång till säkra och robusta nätverk, it-produkter och it-system
- Samlad förmåga att upptäcka, varna, stödja och samordna hantering vid it-relaterade incidenter och kriser
- Samordnad kunskapsutveckling och kompetensförsörjning

NIS-direktivet
Ställer nya krav inom EU på säkerhet i nätverk och informationssystem. De nya reglerna omfattar leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster.

Myndigheten för samhällsskydd och beredskap

Att utveckla på organisationsnivå

- Systematiskt och riskbaserat informationssäkerhetsarbete

Att utveckla på samhällsnivå

- Samordnat informationsutbyte och samverkan mellan privata och offentliga aktörer
- Samordnad kravställning och tillsyn
- **Samordnat arbete med att säkerställa tillgång till säkra och robusta nätverk, it-produkter och it-system**
- Samlad förmåga att upptäcka, varna, stödja och samordna hantering vid it-relaterade incidenter och kriser
- Samordnad kunskapsutveckling och kompetens-försörjning

RAKEL – trygg kommunikation

Signalskydd och andra kryptolösningar

Myndigheten för samhällsskydd och beredskap

Att utveckla på organisationsnivå

- Systematiskt och riskbaserat informationssäkerhetsarbete

Att utveckla på samhällsnivå

- Samordnat informationsutbyte och samverkan mellan privata och offentliga aktörer
- Samordnad kravställning och tillsyn
- Samordnat arbete med att säkerställa tillgång till säkra och robusta nätverk, it-produkter och it-system
- **Samlad förmåga att upptäcka, varna, stödja och samordna hantering vid it-relaterade incidenter och kriser**
- Samordnad kunskapsutveckling och kompetens-försörjning

CERT-SE

Obligatorisk it-incidentrapportering

Övningar

Myndigheten för samhällsskydd och beredskap

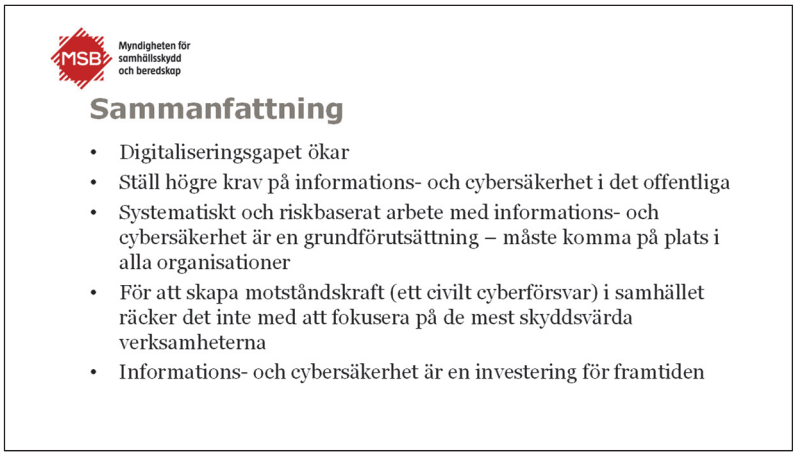
Att utveckla på organisationsnivå

- Systematiskt och riskbaserat informationssäkerhetsarbete

Att utveckla på samhällsnivå

- Samordnat informationsutbyte och samverkan mellan privata och offentliga aktörer
- Samordnad kravställning och tillsyn
- Samordnat arbete med att säkerställa tillgång till säkra och robusta nätverk, it-produkter och it-system
- Samlad förmåga att upptäcka, varna, stödja och samordna hantering vid it-relaterade incidenter och kriser
- **Samordnad kunskapsutveckling och kompetensförsörjning**

4th Annual Cyber 9/12 Student Challenge, Geneva


MSB
Myndigheten för samhällsskydd och beredskap
Sammanfattning
• Digitaliseringsgapet ökar
• Ställ högre krav på informations- och cybersäkerhet i det offentliga
• Systematiskt och riskbaserat arbete med informations- och cybersäkerhet är en grundförutsättning – måste komma på plats i alla organisationer
• För att skapa motståndskraft (ett civilt cyberförsvar) i samhället räcker det inte med att fokusera på de mest skyddsvärda verksamheterna
• Informations- och cybersäkerhet är en investering för framtiden

BILAGA 2

Deltagare

Interna deltagare

Försvarsutskottets ledamöter och suppleanter

Allan Widman (L), ordförande
Åsa Lindestam (S), vice ordförande
Hans Wallmark (M)
Peter Jeppsson (S)
Beatrice Ask (M)
Alexandra Völker (S)
Mikael Jansson (-)
Jan R Andersson (M)
Anders Schröder (MP)
Lotta Olsson (M)
Roger Richtoff (SD)
Lotta Johnsson Fornarve (V)
Mikael Oscarsson (KD)
Mattias Ottosson (S)
Kalle Olsson (S)
Lars Püss (M)
Kerstin Lundgren (C)
Pål Jonson (M)
Björn Söder (SD)

Externa deltagare

Regeringskansliet

Försvarsdepartementet
Martina Bozzo, rättssakkunnig
Maria Fahlén, kansliråd
Fredrik Norberg, kansliråd
Christina Wilén, kansliråd

Justitiedepartementet

Karin Erlingsson, departementsråd, enhetschef

Morgan Johansson (S), justitie- och inrikesminister

Emelie Juter, departementssekreterare

Annette Norman, ämnesråd

Emelie Smiding, rättssakkunnig

Sara Yazdanfar, politiskt sakkunnig

Centrala myndigheter

E-hälsomyndigheten

Stephen Dorch, säkerhetsskyddschef

Charlotta Sandström, t.f. enhetschef Juridik

Finansinspektionen

Liselotte Bohman, senior it-riskexpert

Fortifikationsverket

Kristina Malmström, säkerhetsskyddschef

Försvarets radioanstalt (FRA)

John Ahlmark, kommunikatör

Charlotta Gustafsson, överdirektör

Fredrik Wallin, kommunikatör

Försvarsmakten

Patrik Ahlgren, överste

Jan Kinnander, kommendör, stf chef för Säkerhetskontoret, Must

Peter Sandwall, generaldirektör

Livsmedelsverket

Mats Hellman, informationssäkerhetschef/signalskyddschef

Myndigheten för samhällsskydd och beredskap (MSB)

Dan Eliasson, generaldirektör

Åke Holmgren, t.f. avdelningschef, avdelningen för cybersäkerhet och skydd av samhällsviktig verksamhet

Nils Svartz, överdirektör

Polismyndigheten

Johanna Mannung, it-säkerhetsenheten/it-avdelningen

Jim Keyzer, utredare, Nationellt it-brottscentrum/Noa

Post- och telestyrelsen (PTS)

Annica Bergman, avdelningschef, nätsäkerhetsavdelningen

Kim Hakkarainen, informationssäkerhetsspecialist, nätsäkerhetsavdelningen

Riksrevisionen

Helena Lindberg, riksrevisor

Jörgen Lindström, enhetschef

Skatteverket

Lars-Erik Bergwall, chef sektion 1 säkerhetsenheten

Socialstyrelsen

Pontus Rotter, utredare, generaldirektörens stab, krisberedskap

Sveriges riksbank

Anders Knutsson, säkerhetsrådgivare

Säkerhetspolisen (Säpo)

Klas Friberg, säkerhetspolischef

Karl Melin, presschef

Annica Viksten, strategisk rådgivare

Totalförsvarets forskningsinstitut (FOI)

Anders Norén, enhetschef, Försvarsanalys

Teodor Sommestad, förste forskare avdelningen för ledningssystem

Trafikverket

Mathias Persson, it-direktör

Erica Willborg, enhetschef, it-infrastruktur

Tullverket

Daniel Reinholdsson, informationssäkerhetsstrateg

Regional och kommunal nivå

Länsstyrelsen i Uppsala län

Peter Huotila, nationell programledare kontinuitet och resiliens

Sveriges Kommuner och Landsting (SKL)

Markus Ekbäck, informationssäkerhetsspecialist

Organisationer

Folk och Försvar (FoF)

Maud Holma von Heijne, generalsekreterare

Matilda Karlsson, projektledare, försvarspolitik

Sveriges Civilförsvarsförbund

Gunilla Nordgren, förbundsordförande

Säkerhets- och försvarsföretagen (SOFF)

Andreas Lundgren, marknads- och kommunikationschef, IBM Svenska AB

Richard Oehme, direktör, PwC

2015/16:RFR16	UTBILDNINGSUTSKOTTET Utbildningsutskottets offentliga utfrågning inför proposition om forskning och innovation
2015/16RFR17	KULTURUTSKOTTET Offentlig utfrågning om förutsättningar för svensk film
2015/16RFR18	UTBILDNINGSUTSKOTTET Digitaliseringen i skolan – dess påverkan på kvalitet, likvärdighet och resultat i utbildningen
2015/16RFR19	UTBILDNINGSUTSKOTTET Autonomi och kvalitet – ett uppföljningsprojekt om implementering och effekter av två högskolereformer i Sverige
2015/16RFR20	FINANSUTSKOTTET Offentlig utfrågning om utvärderingen av penningpolitiken 2010-2015 12 maj 2015
2015/16RFR21	FINANSUTSKOTTET Öppen utfrågning om Finanspolitiska rådets rapport 2016
2015/16RFR22	UTBILDNINGSUTSKOTTET Utbildningsutskottets öppna utfrågning om lärarbrist
2015/16RFR23	SOCIALUTSKOTTET Socialutskottets seminarium om cancervården – utmaningar och möjligheter
2015/16RFR24	UTBILDNINGSUTSKOTTET Utbildningsutskottets öppna utfrågning om brist på utbildade inom naturvetenskap och teknik
2015/16RFR25	NÄRINGSUTSKOTTET Näringsutskottets offentliga utfrågning om piratkopiering och andra rättighetsintrång på den digitala marknaden
2015/16RFR26	TRAFIKUTSKOTTET Offentlig utfrågning om finansieringsmodeller för transportinfrastruktur
2015/16RFR27	CIVILUTSKOTTET Civilutskottets offentliga utfrågning om familjerätten är i takt med tiden

2017/18:RFR1	KONSTITUTIONSUTSKOTTET Öppen utfrågning om Riksrevisionen - en del av riksdagens kontrollmakt
2017/18:RFR2	ARBETSMARKNADSUTSKOTTET Vägen till arbete för unga med funktionsnedsättning – en uppföljning och utvärdering
2017/18:RFR3	FINANSUTSKOTTET Offentlig utfrågning om den aktuella penningpolitiken 28 september 2017
2017/18:RFR4	CIVILUTSKOTTET Civilutskottets offentliga utfrågning om barns skuldsättning
2017/18:RFR5	SOCIALUTSKOTTET Samordnad individuell plan (SIP) – en utvärdering
2017/18:RFR6	NÄRINGSUTSKOTTET Näringsutskottets offentliga utfrågning om internationell handel
2017/18:RFR7	KULTURUTSKOTTET Offentlig utfrågning om framtidens spelpolitik
2017/18:RFR8	FINANSUTSKOTTET Offentlig utfrågning om finansiell stabilitet och makrotillsyn den 23 januari 2018
2017/18:RFR9	ARBETSMARKNADSUTSKOTTET Offentlig utfrågning om vägen till arbete för unga med funktionsnedsättning – en uppföljning och utvärdering
2017/18:RFR10	SOCIALUTSKOTTET Personlig assistans – effekter av rättsutvecklingen
2017/18:RFR11	KONSTITUTIONSUTSKOTTET Forskarhearing om nya svenskar och demokratin
2017/18:RFR12	FINANSUTSKOTTET Offentlig utfrågning om den aktuella penningpolitiken den 6 mars 2018
2017/18:RFR13	TRAFIKUTSKOTTET Fossilfria drivmedel för att minska transportsektorns klimatpåverkan – flytande, gasformiga och elektriska drivmedel inom vägtrafik, sjöfart, luftfart och spårbunden trafik
2017/18:RFR14	TRAFIKUTSKOTTET Offentlig utfrågning om konkurrens på lika villkor inom luftfarts- och åkerinäringarna
2017/18:RFR15	UTBILDNINGSUTSKOTTET Offentlig utfrågning om trygghet och studiero i skolan
2017/18:RFR16	TRAFIKUTSKOTTET Järnvägstunnlar och skogsbilvägar – en uppföljning av klimatanpassningsåtgärder för infrastruktur
2017/18:RFR17	FINANSUTSKOTTET Öppen utfrågning om Riksbankens rapport Redogörelse för penningpolitiken 2017