Kommittémotion

Motion till riksdagen 2017/18:341

av Hans Wallmark m.fl. (M)

med anledning av skr. 2016/17:213 Nationell strategi för samhällets informations- och cybersäkerhet

Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om att samla och tydliggöra ansvaret för it-säkerheten och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att se över möjligheten att använda lagen om upphandling på försvars- och säkerhetsområdet i större utsträckning och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om vikten av att införa ett sanktionssystem för överträdelser mot säkerhetsskyddslagen och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att utreda behovet av ett svenskt myndighetsmoln och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om aktiv cyberförmåga och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om behovet av en ökad samverkan med näringslivet för att åstadkomma en bättre cybersäkerhet och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om behovet av en tydlig svensk linje i det internationella arbetet med it-säkerhet och tillkännager detta för regeringen.

Inledning

En väl fungerande informations- och cybersäkerhet är helt grundläggande för att samhället ska kunna fungera såväl i fred som i kris och krig. Under de senaste åren har flera granskningar pekat på allvarliga brister i säkerhetsskyddsarbetet hos både offentliga och privata aktörer. De brister som identifierats i årsrapporterna från Säkerhetspolisen (Säpo), Militära underrättelse- och säkerhetstjänsten (Must) och

Försvarets radioanstalt (FRA) pekar på svagheter i säkerhetskulturen, bristande säkerhetsanalyser och brister i de fysiska infrastrukturerna på it-säkerhetsområdet bland svenska myndigheter. Vidare innehöll Riksrevisionens granskning av it-säkerheten på nio svenska myndigheter bitvis svidande kritik mot flera av dessa myndigheter.

De stora brister som finns beträffande säkerhetskulturen på svenska myndigheter har med all tydlighet även framgått genom det haveri som uppdagats på Transportstyrelsen under det senaste året samt regeringens hanterande av denna fråga. Det understryker även att Regeringskansliet så som det är organiserat för närvarande inte klarar av att hantera säkerhetsskyddsfrågor som berör rikets säkerhet på ett adekvat sätt.

Under det senaste året har även bristerna i säkerhetsskyddet åskådliggjorts genom ett antal omfattande cyberangrepp. I april framkom det att Sverige var ett av de länder som under en längre tid drabbats av cyberangreppet Cloud Hopper. Detta angrepp var framför allt inriktat på drifts- och tjänsteleverantörer och syftade till att få tag på känslig information. I maj genomfördes ett stort ransomware-angrepp på global nivå som enligt uppgifter i medier även drabbade Timrå kommun. Ransomware-angreppen är ett sätt att kunna begära lösensummor av de som drabbas.

Hot, risker och sårbarheter

Det finns en rad hot, risker och sårbarheter i cybermiljön som behöver hanteras. Regeringens it- och cybersäkerhetsstrategi berör ett antal av dessa, men analysen försämras av att det saknas ett tydligt aktörsperspektiv i regeringens skrivelse. Aktörsperspektivet påverkar vilket lagrum som ska användas i syfte att förhindra eller hantera ett cyberangrepp. I grunden bör en väsentligt tydligare avgränsning göras för vad som är statssanktionerade cyberangrepp mot samhällsviktig verksamhet samt vad som kan beskrivas som it-relaterad brottslighet.

Olika former av cyberangrepp från statssanktionerade aktörer har ökat högst avsevärt under de senaste åren enligt svensk säkerhets- och underrättelsetjänst. Enligt FRA utsätts svenska myndigheter för ca 10 000 it-angrepp i månanden från främmande makt. Statssanktionerade angrepp kan innefatta t.ex. cyberspionage, påverkansoperationer i cybermiljön samt cyberoperationer i form av angrepp mot samhällsviktig verksamhet.

It-relaterad brottslighet utförs i allmänhet av individer, grupperingar eller nätverk. Det kan innefatta cyberaktivism och cybervandalism men även cyberkriminalitet driven av ekonomiska incitament. Den it-relaterade brottsligheten har ökat med närmare 900 procent under det senaste årtiondet och då framför allt kopplat till olika former av bedrägeribrott på nätet. Svenska rättsvårdande myndigheters förmåga att utreda och lagföra denna form av brottslighet är mycket begränsad enligt Brottsförebyggande rådet.

Regeringens nationella strategi

Regeringens nationella strategi för samhällets informations- och cybersäkerhet utgår från målen för Sveriges säkerhet så som de är beskrivna i den nationella säkerhetsstrategin samt målsättningen att Sverige ska bli bäst i världen på att utnyttja digitaliseringens möjligheter. För att uppnå detta har regeringen identifierat sex generella målsättningar relaterat till it- och cybersäkerhet. En strategi bör normalt sett innefatta tre M: Mål, Medel och Metod. Regeringens skrivelse kan dock mer liknas vid

en vision än en strategi. Bredd sker på bekostnad av djup i analysen, och skrivelsen saknar besked om *hur* målsättningarna i strategin ska uppnås. Vidare belyser inte skrivelsen heller vilka medel som ska tillföras för att stärka Sveriges informations- och cybersäkerhet.

Slutligen är det viktigt att påpeka att regeringens strategi inte heller för en diskussion om hur förtroendet för samhället och vårt demokratiska system riskerar att påverkas om det skulle förekomma påverkanskampanjer och it-angrepp i syfte att störa de svenska valen under 2018. De internationella erfarenheterna från ett flertal länder där främmande makt har försökt påverka debatten och valutgången visar vilken sprängkraft som ligger i detta hot. Sverige måste vara rustat för eventuella försök att påverka den demokratiska processen.

Moderata förslag

I flera av de moderata kommittémotionerna i år läggs ett antal förslag fram i syfte att förbättra den svenska it-säkerheten, såväl den militära som den civila. Vi föreslår t.ex. etablerandet av ett cybercentrum inom Försvarsmakten som ska ha särskilda it-förband underställda, satsning på att rekrytera civil it-kompetens till försvaret, ökade krav på civila leverantörer av tjänster och produkter inom it-området samt satsningar på att höja kunskapen om it-säkerhet hos medborgarna.

I denna följdmotion lägger Moderaterna fram ytterligare förslag för att stärka arbetet med den svenska it- och informationssäkerheten.

Samlat ansvar för it-säkerheten

Ansvaret för it-säkerheten ligger i dag på ett flertal ställen, och Myndigheten för samhällsskydd och beredskap (MSB) har ansvaret för att koordinera detta arbete samtidigt som såväl Säpo och Must har tillsynsansvar. Denna styrningsmodell, med ett till stora delar delegerat ansvar, är i linje med den svenska förvaltningsmodellen. I praktiken har detta betytt att varje offentlig aktör har fått ansvar för att skapa sin egen lösning för it-driften. Vi ser också i dag en bred palett med olika lösningar för hur arbetet med it-drift och it-säkerhet bedrivs.

Detta kan vara en styrka då varje aktör kan skräddarsy sin lösning efter sina behov. Men det kan också vara en källa till problem då upphandling av komplexa it-system är något som kräver en mycket hög upphandlingskompetens och ett kontinuerligt arbete med it-frågorna som är förankrat i respektive organisations ledningsgrupp. De granskningar som gjorts av bl.a. Riksrevisionen pekar på att säkerhetskulturen uppvisar stora brister på många håll och att det i princip är omöjligt att få en helhetsbild av it-säkerhetsarbetet hos svenska myndigheter och statliga bolag.

Ett konkret exempel där det i dag behövs en ökad styrning är hur olika offentliga aktörer behandlar säkerhetsklassad information och använder krypton. Skyddsvärd information behandlas i dag på olika sätt hos olika myndigheter, när olika aktörer ska dela information. Här finns behov av tydligare regelverk och möjligheter att följa upp att regelverket åtföljs.

Moderaterna vill därför se en tydligare styrning och stöd för arbetet med it-säkerhet hos svenska offentliga aktörer. Den samlade utmaningen från hybridhoten, däribland cyberhot, kräver också ett samlat ansvar. Erfarenheterna från bl.a. Transportstyrelsen

visar även på att koordineringen inom Regeringskansliet på cybersäkerhetsområdet försämras av att ansvaret delvis är delat mellan fyra ministrar och sex myndigheter.

Alliansregeringen inrättade ett kriskansli på Statsrådsberedningen som den nuvarande regeringen flyttade till Justitiedepartementet. Moderaterna anser att detta var ett misstag. För att stärka kompetensen i krishanteringsarbetet kring statsministern bör kansliet flyttas tillbaka till Statsrådsberedningen, och man skulle även kunna överväga att utöka kansliets mandat för att stärka den nationella krisledningen, och särskilt när det gäller it-säkerheten. En nationell koordinator för it-säkerhet på kriskansliet skulle bidra till ökad tydlighet.

Det finns många aktörer som skulle kunna bidra till att utveckla en tydligare styrningsmodell för krisledning på nationell nivå. Till exempel hos Försvarshögskolan (FHS) finns en stor sakkunskap i frågor som rör krishantering och krisledning.

Moderaterna vill även stärka och fördjupa myndighetssamverkan inom informationssäkerhetsområdet. Detta skulle kunna göras genom att inrätta ett myndighetsråd, som i så fall skulle ersätta det myndighetssamarbete som i dag sker inom ramen för Samverkansgruppen för informationssäkerhet (Samfi). Samfi består i dag av Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt, Post- och telestyrelsen, Polismyndigheten, Säkerhetspolisen och Myndigheten för samhällsskydd och beredskap.

Genom att formalisera gruppen i ett myndighetsråd skulle den kunna hantera regeringsuppdrag och arbeta mer metodiskt med frågor som bl.a. upphandling och certifiering. Bland annat Riksrevisionen har pekat på att det finns brister när det gäller hur olika myndigheter tillämpar MSB:s föreskrifter och arbetar generellt med informationssäkerhet.

Myndighetsrådet skulle ha som uppgift att förebygga, följa och åtgärda brister i statens informationssäkerhet. MSB bör med tanke på myndighetens särskilda ansvar för informationssäkerhetsfrågorna leda myndighetsrådet och sköta administrationen. Förslaget om inrättandet av ett myndighetsråd återfinns i Utredningen om informations- och cybersäkerhet i Sverige, SOU 2015:23 (kapitel 9.2.2).

Förändrade upphandlingsrutiner

Utredningen om informations- och cybersäkerhet i Sverige (SOU 2015:23) pekar även på att lagen om offentlig upphandling (LOU) kan vara ett problem vid offentliga aktörers upphandling av it-drift då frågor om it- och informationssäkerhet kan prioriteras ned på bekostnad av ett lägre pris.

Vi vill därför att regeringen ser över hur offentliga aktörer ska kunna använda sig av lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFS) i större utsträckning. LUFS innehåller till skillnad från LOU bestämmelser om bl.a. informationssäkerhet och stärker därmed möjligheterna för bl.a. myndigheter att kravställa utifrån nödvändiga säkerhetshänsyn.

Sanktionssystem kopplat till säkerhetsskyddslagen

Säkerhetsskyddslagen syftar till att säkerställa skydd för det allra mest skyddsvärda i samhället. I lagen finns bestämmelser om åtgärder som ska vidtas för att skydda

säkerhetskänslig verksamhet, tillträdesbegränsning till känsliga byggnader och områden, säkerhetsprövning av personal och informationssäkerhet.

I dag saknas sanktionsmöjligheter mot den aktör som har brutit mot säkerhetsskyddslagens bestämmelser. Detta är en brist som måste åtgärdas. Det räcker inte med att det finns relevanta bestämmelser om säkerhetskänslig verksamhet. För att skapa en större tyngd i lagstiftningen måste den även innehålla möjligheten att vidta sanktioner mot dem som bryter mot bestämmelserna.

För närvarande pågår utredredningsarbete (kommittédir. 2017:32) när det gäller möjligheten att införa ett sanktionssystem kopplat till säkerhetsskyddslagen. Utredningen ska presentera sina förslag senast den 1 maj 2018.

Moderaterna vill peka på vikten av att det snarast kopplas sanktionsmöjligheter för att ingripa mot de som inte följer säkerhetsskyddslagens bestämmelser.

Utredning om ett svenskt myndighetsmoln

Frågan om en gemensam statlig molntjänst för myndigheternas it-drift har lyfts av flera aktörer. Tidigare under året redovisade Statens servicecenter ett förslag om att en statlig molntjänst bör införas där merparten av de statliga myndigheternas it-drift bör samordnas. Enligt utredningen skulle en statlig montjänst hantera många av de utmaningar som finns när det gäller myndigheternas it-drift.

Det skulle innebära samordningsvinster och i förlängningen besparingar för myndigheterna, en förenkling för myndigheterna och viktigast av allt – att it-säkerheten och driftssäkerheten skulle förstärkas kraftigt.

Även FRA har förordat en molntjänst för Sveriges myndigheter och de statliga bolagen. FRA pekar på att många av de avtal som statliga aktörer har slutit med andra aktörer om it-drift har varit mycket undermåliga ur it- och informationssäkerhetssynpunkt. Anledningen till detta är ofta att det brister i upphandlingskompetens.

Därför landar FRA i slutsatsen att ett statligt myndighetsmoln med en egen driftcentral skulle kunna vara en bra lösning. Myndigheter och statliga bolag skulle då ha tillgång till en enkel lösning som skulle kunna skräddarsys efter de it-säkerhetsbehov som finns hos statliga aktörer. Dock betonar FRA att outsourcing av it-drift inte per definition är dåligt så länge avtalen är tillräckligt bra, och så länge ingen känslig information läggs ut i molnet.

Även andra som Säkerhets- och försvarsföretagen (Soff) och IIS-stiftelsen har pekat på att de vill se ett statligt myndighetsmoln. Detta utifrån de anledningar som anges ovan. Man lyfter även fram möjligheten att en statlig molntjänst skulle minska den Stockholmskoncentration som i dag finns inom myndigheternas it-drift och därmed skapa kvalificerade arbetstillfällen på andra platser i Sverige och dessutom minska sårbarheten vid t.ex. ett större strömavbrott i Stockholmsområdet.

Med anledning av att det finns ett stort behov av att stärka statliga aktörers it-säkerhet och då flera viktiga aktörer inom it-säkerhetsområdet vill se att det etableras ett myndighetsmoln anser Moderaterna att denna möjlighet bör utredas.

Bättre samarbete med näringslivet

It-säkerhetsfrågor skär över såväl gränser som sektorer, och därför är det viktigt med ett helhetstänkande när strategier för it-säkerhet tas fram. Samhällets funktionalitet är i dag starkt beroende av näringslivet för att betalningsströmmar, elförsörjning och informationsflöden ska fungera, bara för att ta några exempel.

I princip all produktutveckling inom it-säkerhetsområdet sker inom det privata näringslivet, och den teknikkompetens som finns bland dessa företag är ofta väsentligt högre än den som finns på statliga myndigheter. Men för att uppnå en fungerande marknad som kan leverera de lösningar och produkter som statliga myndigheter behöver i framtiden krävs det en långsiktig strategisk dialog mellan myndigheter och företag om teknikutvecklingstrender samt hot, risker och sårbarheter i cybermiljön.

Genom en sådan dialog kan svensk underrättelse- och säkerhetstjänst få en bättre överblick över hur tekniktrender på cybersäkerhetsområdet kommer att påverka behovet av säkerhetsskydd. Formerna för en sådan dialog bör avgöras efter behov och är avhängiga att den personal som medverkar från företagen är säkerhetsklassad.

Regeringens nationella strategi för samhällets informations- och cybersäkerhet innehåller dock inga konkreta förslag på hur samverkan med näringslivet kan förbättras och hur samhällets it-säkerhet som helhet kan dra nytta av den teknikkompetens som finns på området i Sverige. Till exempel skulle en utökad användning av Näringslivets säkerhetsdelegation i cybersäkerhetsfrågor kunna främja en effektivare samverkan med näringslivet.

Det finns en stor vilja hos flera aktörer inom näringslivet att i ökad utsträckning ta samhällsansvar genom att bidra till arbetet med att stärka totalförsvaret, detta inte minst inom it-säkerhetsområdet. Vi måste ta vara på det samhällsengagemanget genom att skapa bättre samverkan mellan näringsliv, stat och samhälle i syfte att öka skyddet mot olika former av cyberhot.

I Moderaternas försvars- och krisberedskapsmotioner läggs ett antal förslag fram för att stärka it-säkerheten i Sverige. Bland annat vill vi se att det etableras ett frivilligt nätverk där it-kompetens från såväl offentlig som privat sektor samverkar för att stärka it-säkerheten.

På EU-nivå slöt kommissionen 2016 avtal med näringslivet om it-säkerhet för att möta de ökade hoten. Detta avtal är ett offentlig-privat partnerskap som syftar till att främja samarbete och skapa it-säkerhetslösningar för olika sektorer, t.ex. energi, hälsa, transport och finans. Samarbetet finansieras av EU tillsammans med marknadsaktörer.

Moderaterna vill att det görs en särskild översyn av hur samverkan med näringslivet kan förbättras och bli mer effektiv inom it-säkerhetsområdet. Den bör se på hur relevanta konkreta samverkansformer kan etableras och på vilka områden som bör omfattas. Relevanta internationella exempel bör beaktas.

Aktiv cyberförmåga

I regeringens inriktningsproposition för försvaret beskrivs den svenska cyberförmågan. Inriktningspropositionen bygger på den försvarsuppgörelse som träffades i april 2015 mellan Moderaterna, Centerpartiet och Kristdemokraterna samt Socialdemokraterna och Miljöpartiet.

I propositionen står det:

”I det nya osäkrare säkerhetspolitiska läget är försvarsunderrättelse- och cyberförsvarsförmåga centralt. Grunden för denna förmåga är att kunna skydda vitala system från angrepp. För det krävs att även kunna genomföra aktiva operationer i cybermiljön.”

Den svenska försvarsmaktens militärstrategiska doktrin från 2016 beskriver också vikten av en god cyberförmåga. ”Cyberrymden innebär strategiskt ett globalt gränslöst utrymme för att på distans genomföra attacker, underrättelsetjänst, påverkan, opinionsbildning och propaganda. Försvarsmaktens resurser ska stödja defensiva och offensiva operationer i syfte att stärka skyddet av Sverige i cyberrymden.”

Sverige ska med andra ord ha en aktiv (offensiv) förmåga att genomföra cyberattacker mot andra aktörer. Försvarsminister Peter Hultqvist lyfte också frågan i media i samband med att inriktningspropositionen presenterades, och pekade ut Danmarks arbete med att skapa en aktiv cyberförmåga som en förebild.

Konceptet med en aktiv cyberförmåga är dock inte oproblematiskt och kräver att centrala frågor om hur, när och var förmågan ska kunna användas besvaras. Rättsläget när det gäller huruvida krigets lagar och internationell rätt är tillämpbara på cyberkrigföring är oklart även om dessa lagar rent generellt ska tillämpas teknikneutralt baserat bl.a. på principerna om proportionalitet om urskiljning. Aktiv cyberförmåga är dessutom ett instrument som kan ha långtgående konsekvenser på samhällets funktionalitet hos det land som utsätts för det. Vissa menar därmed att det är att jämställa med massförstörelsevapen.

Ytterst handlar den aktiva cyberförmågan om att avhålla andra aktörer från att genomföra cyberangrepp mot samhällsviktig verksamhet eftersom Sverige då har en förmåga till vedergällning. Men för att denna förmåga ska vara effektiv och inte behöva användas krävs det att den kommuniceras på ett tydligt och vederhäftigt sätt. Regeringen bör därför återkomma med en inriktning eller doktrin för när, var och hur den aktiva cyberförmågan eventuellt ska användas. Alternativt bör detta bli föremål för ett kompletterande uppdrag för Försvarsberedningen i syfte att uppnå en bred politisk samsyn i frågan.

Med anledning av ovanstående bör regeringen klargöra den svenska positionen när det gäller användandet av en aktiv cyberförmåga. Regeringen bör dessutom verka för att driva frågan om hur cyberkrigföringen förhåller sig till krigets lagar i internationella forum som FN:s säkerhetsråd.

Internationell samverkan

It-frågor är per definition internationella och gränsöverskridande. Våra it-system i Sverige är sammankopplade med system i andra länder i ett globalt nätverk. Detta skapar stora möjligheter att ha kontakt och handla med hela världen, men det exponerar oss även för hot från andra delar av världen. Det kan röra sig om en lång rad aktörer som av olika orsaker vill skada Sverige och svenska intressen.

På grund av den gränsöverskridande dimensionen i it-frågorna är det internationella samarbetet för att stärka it-säkerheten centralt. För svenskt vidkommande måste vi ha en tydlig position kring hur vi ser på frågorna och hur vi vill agera i internationella forum. Det kräver att Sverige kan definiera vad vi anser vara mest skyddsvärt, var de främsta samarbetsvinsterna finns och med vilka aktörer Sverige vill samverka.

Det internationella samarbetet kring cybersäkerhet bedrivs framför allt inom EU och Nato. Sverige deltar t.ex. vid Nato Cooperative Cyber Defence Centre of Excellence i

Tallinn samt återkommande inom ramen för EU:s samarbete med arbetet att ta fram en ny cybersäkerhetsstrategi för unionen.

Regeringen säger sig vilja verka för ett starkare internationellt samarbete på detta område men klargör inte hur den avser att driva dessa frågor inom dessa organisationer eller vad den vill åstadkomma. Regeringen bör därför återkomma med en redovisning av hur den vill utveckla det internationella samarbetet på detta område.

Hans Wallmark (M)

Lena Asplund (M)

Jan R Andersson (M)

Lotta Olsson (M)

Dag Klackenberg (M)