Kommittémotion M

SVERIGES RIKSDAG

Motion till riksdagen 2021/22:3639

av Pål Jonson m.fl. (M)

Cybersäkerhet och cyberförsvar

Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om en översyn av cybersäkerhetsområdet med tydliga delredovisningar och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige ska få en ny cyberstrategi och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att ge det nya cybercentrumet ett tydligt mandat och en ändamålsenlig budget och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att införa en cyberkoordinator på Regeringskansliet och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om risk- och sårbarhetsanalyser och en enhetlig kravställning och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om att inrätta haverikommissioner vid större cyberangrepp mot samhällsviktig verksamhet och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om vikten av ett starkare samarbete mellan staten och näringslivet inom cyberområdet och tillkännager detta för regeringen.

8. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige bör främja ett djupare samarbete inom Norden och EU samt med Nato på cybersäkerhetsområdet och tillkännager detta för regeringen.
9. Riksdagen ställer sig bakom det som anförs i motionen om att använda lagen om upphandling på försvars- och säkerhetsområdet (LUFS) i större utsträckning och tillkännager detta för regeringen.
10. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige bör upprätta en cyberdoktrin för den defensiva och offensiva cyberförmågan och tillkännager detta för regeringen.
11. Riksdagen ställer sig bakom det som anförs i motionen om att använda tidvis tjänstgörande personal och hemvärnet för att utveckla cyberförsvaret och tillkännager detta för regeringen.
12. Riksdagen ställer sig bakom det som anförs i motionen om att ge FRA ett utökat uppdrag att skydda samhällsviktiga företag och tillkännager detta för regeringen.
13. Riksdagen ställer sig bakom det som anförs i motionen om att ge Försvarsmakten och KTH ett uppdrag att föreslå en process och struktur för att ta fram nya tekniska lösningar inom cyberförsvaret och tillkännager detta för regeringen.

Motivering

Inledning – åtgärder för stärkt cybersäkerhet och cyberförsvar

Sverige är ett av världens mest digitaliserade länder, men när det gäller cybersäkerhet ligger vi betydligt sämre till enligt internationella jämförelser.

På ett antal områden finns det en stor förbättringspotential. Det gäller allt från kompetensförsörjning och teknikutveckling till samarbete med näringslivet samt att det finns relevanta lagar, riktlinjer och myndighetsstrukturer.

Dessa svagheter har visats flera gånger de senaste åren vid till exempel olika cyberangrepp mot svenska myndigheter och företag, men även då svenska myndigheter som Transportstyrelsen har misskött sin cyber- och informationssäkerhet. I somras kunde vi till exempel se hur dagligvarukedjan Coop lamslogs när den drabbades av ett så kallat ransomware-angrepp vilket lamslog verksamheten under flera dagar.

Moderaterna lägger i denna motion ett antal förslag som syftar till att stärka såväl den svenska cyber- och informationssäkerheten brett, men även det svenska cyberförsvaret.

Det finns ett antal områden som behöver stärkas i Sverige när det kommer till cybersäkerhet. Det handlar bland annat om kompetensförsörjning, större och effektivare satsningar på forskning inom akademin samt bättre samarbetsstrukturer med näringslivet och ett bättre och mer sammanhållet författningsstöd. Det finns också ett stort behov av att investera i kommunikationer med ett högre säkerhetsskydd då återuppbyggnaden av det civila försvarsvaret kräver en bättre ledning och samverkan. Vidare bör kompetensen kring cybersäkerhetsfrågor på regeringskansliet stärkas högst avsevärt.

Det är nödvändigt att Sverige även utvecklat en offensiv cyberförmåga. Men frågan är inte helt okomplicerad ur ett legalt perspektiv. Det har också varit en debatt om de etablerade lagar kring krigföring vi har i dag är tillämpbara när nya teknologier och förmågor som cyber, artificiell intelligens och autonoma system skapar en helt ny spelplan och blir en allt mer integrerad del av försvaret. Sverige bör som en ledande tekniknation aktivt forma den internationella policydebatten kring dessa frågor. Vidare bör en doktrin utvecklas som ger vägledning för tillämpningen av defensiva och offensiva cyberoperationer.

De nordiska länderna bör samordna och öva sina Computer Emergency Response Team (CERT) gemensamt och intensifiera samarbete kring utbyggnaden 5G inklusive de säkerhetsaspekter som är kopplade till detta arbete. Sverige bör också bejaka möjligheterna som finns att använda EU:s verktygslåda för cyberdiplomati om vi drabbas av omfattande cyberangrepp.

Etablerandet av det nya cybersäkerhetscentrat är en viktig byggsten i detta arbete. Det behöver skyndsamt bli operativt och utveckla ett nära samarbete med näringslivet. Vidare bör centret även ha en nära samverkan med den nya myndigheten för psykologiskt försvar bland annat eftersom båda aktörerna ska arbeta med att identifiera, hantera och bemöta angrepp och påverkansoperationer i digitala miljöer.

Det behövs också initieras en större utredning som ska stödja och utveckla en ny svensk cybersäkerhetsstrategi.

Den cybersäkerhetskoordinator som Moderaterna föreslår ska införas på säkerhetsrådet kommer att ha huvudansvar för att utveckla strategin framgent. Cybersäkerhetskoordinatorn kommer även att få en central roll i att hålla ihop hela cybersäkerhetsarbetet på regeringskansliet.

Utredning om cybersäkerhet och en svensk cybersäkerhetsstrategi

Det behövs ett samlat grepp kring hur Sverige kan stärka och kontinuerligt arbeta med cybersäkerhet. Etablerandet av det nya cybersäkerhetscentrat är en viktig byggsten i detta arbete. Det behövs dock ett större samlat grepp för att identifiera risker och möjligheter när det gäller svensk cybersäkerhet. Moderaterna vill därför initiera en större utredning som ska stödja och utveckla en svensk cybersäkerhetsstrategi.

Utredningen bör ha en bred ansats och utgå ifrån hotbilden, hur den förväntas utvecklas och vilka krav den ställer på svensk cybersäkerhet framgent. Faktorer som kompetensförsörjning, forskning och teknikutveckling samt framtagning av certifierade produkter bör vara en central del i utredningen. Andra relevanta saker som bör genomlysas är samarbetet mellan det offentliga och näringslivet samt lärdomar från andra relevanta länder. För att minska ledtiden till dess att utredningen är klar bör det göras ett antal delredovisningar på specifika prioriterade områden före slutredovisningen.

Utredningen ska kontinuerligt stärka en skarp svensk cybersäkerhetsstrategi som utgör en del av den svenska nationella säkerhetsstrategin. Det innebär att den cybersäkerhetskoordinator som Moderaterna föreslår ska införas på regeringskansliet kommer att ha huvudansvar för att utveckla strategin framgent. Detta tillsammans med det nyligen etablerade cybersäkerhetscentrumet.

Den nationella strategi för samhällets informations- och cybersäkerhet som regeringen presenterade 2018 i en skrivelse påminner mer om en vision än en konkret strategi. En strategi bör normalt sett innefatta tre M: Mål, Medel och Metod. 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.

Ett cybersäkerhetscentrum med en ändamålsenlig budget samt en cyberkoordinator på Regeringskansliet

Ett viktigt steg för att stärka den svenska cybersäkerheten är inrättandet av det nya svenska cybersäkerhetscentrumet. Det är ett samarbete mellan de fyra myndigheterna Försvarets radioanstalt (FRA), Försvarsmakten, Säkerhetspolisen (Säpo) och Myndigheten för samhällsskydd och beredskap (MSB).

Cybersäkerhetscentrat ska arbeta brett med både offentliga och privata aktörer för att stärka svensk cybersäkerhet. Moderaterna har varit pådrivande för att få centrumet på plats och vi har särskilt tryckt på behovet att det bidrar till att stärka cybersäkerheten

hos privata aktörer så att Sverige betraktas som en säker marknadsplats där både svenska och utländska företag kan verka.

Huvudmannaskapet för centrat bör läggas hos FRA som besitter en stor kompetens när det gäller cybersäkerhet. Innan dess att Moderaternas och försvarsberedningens förslag om ett totalförsvarsdepartement med ansvar för både militärt och civilt försvar har genomförts bör Justitiedepartementet ges mandat för inriktning av FRA:s verksamhet på cybersäkerhetsområdet med ett särskilt regleringsbrev vid sidan av det generella som Försvarsdepartementet har.

Cybersäkerhetscentrumet bör ges en ändamålsenlig budget där det finns en balans mellan mål och medel och ett starkt mandat att samverka med näringslivet, samt att det kan utgöra knutpunkten i det nationella och internationella cybersäkerhetsarbetet. Det är oroväckande att regeringen inte har utpekat en tydlig huvudman eller tillfört medel som möjliggör för centrat att kunna utföra sitt uppdrag fullt ut.

Slutligen så bör det återinföras en cyberkoordinator på Regeringskansliet för att kunna samla ansvaret i en fråga som idag är uppdelad på fyra departement och åtta myndigheter. Koordinatorn ska ha ett tydligt mandat, ett eget kansli, utgöra kontaktyta mellan Regeringskansliet och det nya cybersäkerhetscentrat samt ingå i det nationella säkerhetsrådet. Koordinatorn med tillhörande kansli bör kunna utgöra en egen underavdelning på det nationella säkerhetsrådet.

Risk- och sårbarhetsanalyser för en enhetlig kravställning

Utredningen Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63) konstaterar att det finns allvarliga brister när det gäller såväl statliga myndigheter som regioner och kommuner men även organisationer och näringslivet. Bristerna gäller både vad avser det systematiska informationssäkerhetsarbetet och vad avser säkerhet i olika nätverks- och informationssystem.

Utredningen föreslår därför att regeringen ger Försvarets materielverk (FMV) i uppdrag att, i samråd och samverkan med främst de myndigheter som ingår i det nationella cybersäkerhetscentret, utveckla formerna för hur gemensamt framtagna hot-, sårbarhets- och riskbedömningar samt skyddsprofiler kan tas fram till stöd för kravställning på IKT-produkter, -tjänster och -processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet.

Utifrån de allvarliga brister som har konstaterats anser Moderaterna att det är prioriterat att gå vidare med utredningens förslag rörande hot-, sårbarhets- och riskbedömningar vilka kan fungera som stöd för kravställning.

Haverikommission vid större IT-störningar i samhällsviktig verksamhet

IT-störningar i samhällsviktig verksamhet, såväl offentlig som privat, kan få mycket långtgående konsekvenser för samhällets funktionalitet. Exempel på detta kunde vi se när Coops betalningssystem gick ner efter att det utsatts för en ransomware-attack. Detta ledde till att dagligvarukedjan tvingades stänga merparten av sina butiker i flera dagar. I vissa glesbygdskommuner med bara en matbutik blev konsekvenserna särskilt svåra.

Motsvarande cyberattacker på till exempel större banker, sjukhus eller anläggningar för vatten- eller elförsörjning skulle innebära mycket stora problem. Antalet attacker ökar också exponentiellt utifrån att de är relativt enkla att genomföra och ger möjligheten för angriparen att kunna pressa måltavlan för angreppet på stora summor.

IT-systemen är dessutom ofta komplexa system av system där tjänster och produkter köps in från olika underleverantörer. Detta gör att det kan vara svårt att identifiera och åtgärda alla svagheter i helheten. I fallet med Coop så var det just en underleverantör som angreps.

Sverige behöver bli bättre på att kunna identifiera, analysera och möta angrepp på samhällsviktig verksamhet. Moderaterna vill därför att det upprättas en haverikommission när större cyberangrepp har drabbat samhällsviktig verksamhet. På så sätt kan sårbarheter identifieras och analyseras och lärdomar dras för framtiden.

Samverkan mellan stat och näringsliv för en starkare cybersäkerhet

En bra samverkan mellan stat och näringsliv är centralt om samhällets samlade resurser ska kunna användas effektivt för att stärka såväl krisberedskap som totalförsvar. Stora delar av de samhällsviktiga resurserna och tillhörande kompetens ligger idag hos det privata näringslivet. Detta gäller inte minst på cyberområdet.

Moderaterna ser det därför som centralt att länken offentligt-privat fördjupas på cyberområdet för att stärka svensk säkerhet brett. Därför anser vi, vilket anförs ovan, att en förbättrad samverkan med näringslivet bör vara en viktig punkt i den utredning om cybersäkerhet som Moderaterna föreslår.

I princip all produktutveckling inom cybersäkerhetsområdet 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. En viktig del i detta är dock att beredskapssektorn elektronisk kommunikation och post kommer på plats så snart som möjligt för att kunna bli ett viktigt forum för framtidsfrågor i skärningspunkten mellan offentligt och privat som till exempel den framtida kommunikationsstrukturen.

Regeringens nationella strategi för samhällets informations- och cybersäkerhet innehåller dock inga konkreta förslag på hur samverkan med näringslivet kan förbättras och hur samhällets cybersäkerhet 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 och/eller näringslivet totalförsvarsråd, som försvarsberedningen föreslår, 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 cybersäkerhetsområdet. 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.

Ett sätt att ytterligare stärka samverkan mellan stat och näringsliv är att använda tidvis anställda och reservofficerare inom försvaret som kan kombinera en anställning inom IT-industrin med tjänstgöring inom försvaret med liknande uppgifter.

På EU-nivå slöt kommissionen 2016 avtal med näringslivet om cybersäkerhet för att möta de ökade hoten. Detta avtal är ett offentlig-privat partnerskap som syftar till att främja samarbete och skapa cybersäkerhetslösningar för olika sektorer, till exempel energi, hälsa, transport och finans. Samarbetet finansieras av EU tillsammans med marknadsaktörer. Sverige bör inta en aktiv roll i det EU-samarbetet kring cybersäkerhet och särskilt driva frågan om att inkludera näringslivet i detta.

Internationell samverkan

De nordiska länderna bör samordna och öva sina Computer Emergency Response Team (CERT) gemensamt och intensifiera samarbete kring utbyggnaden 5G inklusive de säkerhetsaspekter som är kopplade till detta arbete. Förstärkt nordiskt samarbete på cybersäkerhetsområdet ingår också som ett förslag i Björn Bjarnasons rapport om hur de nordiska länderna kan stärka sitt samarbete när det gäller utrikes- och säkerhetspolitik.

EU lanserade 2020 en ny cybersäkerhetsstrategi som när den implementeras fullt ut kommer att bli ett viktigt verktyg för både unionen och medlemsländerna. Strategin innehåller såväl operativa förslag som att skapa gemensam cyberenhet för att intensifiera insatserna vid storskaliga säkerhetsincidenter som att arbeta med partners internationellt för att skapa och upprätthålla normer och standarder i cyberdomänen. EU har avsatt särskilda medel i långtidsbudgeten för ökad cybersäkerhet. Projekt för att stärka cyberförsvaret bedrivs också inom ramen för den europeiska försvarsfonden. Sverige bör bedriva ett aktivt arbete för att kunna få del av de medlen. Sverige bör vidare bejaka möjligheterna som finns att använda EU:s verktygslåda för cyberdiplomati om vi drabbas av omfattande cyberangrepp. En annan del i EU-samarbetet kring cybersäkerhet är det nätverk av nationella samordningscentrum som nu är under uppbyggnad. MSB har fått i uppdrag att vidta förberedelser för att bli nationellt samordningscenter kopplat till det europeiska kompetenscentret för cybersäkerhet. Dessa kompetenscentrum bör bejaka möjligheten att arbeta parallellt med cybersäkerhet och cyberförsvar. Civil och militära lösningar när det gäller såväl cybersäkerhet och cyberförsvar som teknologi i stort blir allt mer integrerade och detta bör även avspeglas i arbetet hos EU:s kompetenscentrum för största möjliga synergieffekter.

Cyberförsvar kommer även att bli en allt viktigare del av Natos kollektiva försvar. Vid Natotoppmötet i Bryssel 2021 lyftes behovet av ett ökat fokus på cybersäkerhet och cyberförsvar fram och i ljuset av den exponentiella ökningen av cyberattacker. Sverige bör samarbeta med Nato i största möjliga utsträckning även när det gäller cyberförsvar. Vi har redan nu representation på Nato kompetenscentrum i Tallinn och Sverige har deltagit i komplexa Nato-ledda övningar som Locked Shields där det svenska bidraget rönte stor framgång.

Förändrade upphandlingsrutiner

Utredningen om informations- och cybersäkerhet i Sverige (SOU 2015:23) pekar på att lagen om offentlig upphandling (LOU) kan vara ett problem vid offentliga aktörers

upphandling av IT-drift då frågor om cyber- och informationssäkerhetkan prioriteras nedpå 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 bland annat informationssäkerhet och stärker därmed möjligheterna för myndigheter att ställa krav utifrån nödvändiga säkerhetshänsyn. LOU ska fortsatt användas där det går. Det förutsätter dock att upphandlingskompetensen när det gäller cybersäkerhet stärks.

Det svenska cyberförsvaret

Cyberförsvar är numera en central del i det samlade totalförsvaret. I vissa länder, som till exempel USA, Tyskland och Norge har cyberförsvaret kommit att bli en egen försvarsgren. I Sverige har viktiga steg i att stärka det svenska cyberförsvaret tagits i och med införandet av ett nytt centrum för cyberförsvar och informationssäkerhet, att Försvarsmakten har infört en spetsutbildning för cybersoldater samt att Försvarsmakten byggt en fullskalig övningsanläggning för att kunna öva cyberkrigföring. Cybercentrat är ett samarbete mellan Försvarsmakten och Kungliga Tekniska Högskolan (KTH). Ett annat viktigt steg är att Försvarsmakten nu även kommer att införa en särskild utbildning för specialistofficerare med inriktning mot cyber.

En svensk cyberförsvarsdoktrin

Ett trovärdigt cyberförsvar handlar om förmågan att kunna skydda de egna IT-systemet från angrepp, men även om att cyberförsvaret ska ha förmågan att kunna slå tillbaka mot en potentiell angripare – en så kallad aktiv cyberförmåga. Det finns en bred politisk enighet kring att Sverige ska ha en offensiv förmåga på cyberområdet, men denna förmåga ställer också svåra frågor. Den aktiva cyberförmågan kräver att det tas fram ett förhållningssätt för hur, var och när den i så fall ska användas. Detta som en del i det svenska försvarets samlade avskräckningsförmåga. Det behövs en motsvarighet till den IKFN-förordning som Försvarsmakten använder. Där finns handlingsregler för olika fall av kränkningar som är utformade så att de följer folkrättsliga regler. Moderaterna vill därför att Sverige ska ha en tydlig cyberdoktrin som stipulerar hur vi ser på principerna för användandet av den aktiva cyberförmågan.

Sveriges bör även spela en större roll i att skapa ett relevant internationellt regelverk för nya teknologier. Frågan om att använda aktiv cyber och tillexempel ta sig in i andra länders IT-system är inte helt okomplicerad ur ett legalt perspektiv. Det har också varit

en debatt om de etablerade lagar kring krigföring vi har idag är tillämpbara när nya teknologier och förmågor som cyber, artificiell intelligens och autonoma system skapar en helt ny spelplan och blir en allt mer integrerad del av försvaret.

Det finns uppenbart svåra frågor som till exempel vem som bär ansvaret för de skador som uppkommer utan att ett mänskligt beslut ligger till grund för det autonoma systemets agerande i fält.

Sverige bör, som en framstående tekniknation, ta en ledande roll i arbetet för att skapa nya relevanta internationella lagar och regler som är applicerbara på nya teknologier i en krigföringskontext. Detta skulle vara en betydligt bättre användning av svenska diplomatiska resurser än att som regeringen gjort driva frågan om en kärnvapenkonvention som skulle motverka svenska säkerhetsintressen och bara gynna auktoritära kärnvapenstater.

Utveckling av cyberförsvaret

Behovet av att resurssätta och kompetensförsörja det svenska cyberförsvaret kommer att bli en viktig framtidsfråga. Försvaret kommer fullt ut inte att kunna konkurrera med det privata näringslivet när det gäller lön. Därför måste Försvarsmakten dels fortsatt vidareutveckla möjligheten att själv utbilda cybersoldater och dels upprätta fler samarbeten med företag i det svenska näringslivet som besitter stor kompetens på IT-området. Viktiga forum för denna samverkan bör vara såväl näringslivets totalförsvarsråd som försvarsberedningen föreslagit som det försvarsindustriråd som Moderaterna föreslagit.

Det finns en stor potential att utnyttja de som i dag är tidvis tjänstgörande soldater när det gäller cybersäkerhet. Detta sker redan i viss utsträckning genom samarbeten mellan större it-företag och försvaret där de anställda delar sin tid mellan de två arbetsgivarna.

Möjligheten att knyta upp civil IT-kompetens genom motsvarande hemvärnsavtal och via frivilliga försvarsorganisationer bör också undersökas. I förlängningen skulle detta kunna leda till etablerandet av digitala hemvärnsförband och en frivillig försvarsorganisation med koppling till cyberförmågan.

FRA utför idag ett viktigt arbete när det gäller att stödja statliga myndigheter och statligt ägda bolag med att identifiera och möta hot mot cyber- och informationssäkerheten. Ett viktigt verktyg som FRA använder är Tekniskt detekterings- och varningssystem (TDV). Det är ett varningssystem som kan upptäcka avancerade IT-angrepp som normalt inte upptäcks av kommersiella antivirusskydd.

Uppdraget som det är formulerat idag begränsar FRA:s arbete till statliga myndigheter och bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende. Utifrån den breddade hotbild vi ser idag där även samhällsviktiga företag är primära mål för cyberattacker från statsstödda aktörer anser Moderaterna att §4 i Förordning (2007:937) med instruktion för Försvarets radioanstalt bör utökas till att även gälla samhällsviktiga företag.

Ett effektivt cyberförsvar är beroende av att det finns relevant teknik i framkant att tillgå. Ofta handlar det om skräddarsydda tekniska lösningar som inte finns på marknaden. Ett sådant exempel är just TDV som används av FRA.

Försvarsmakten bör ges ökade möjligheter att genom innovationsupphandling kunna ta fram nya tekniska lösningar för att stärka cyberförsvaret. Här bör Försvarsmaktens och KTH:s centrum för cyberförsvar och informationssäkerhet kunna spela en viktig roll som nod mellan försvarsmyndigheter, näringsliv och akademi.

Moderaterna vill därför att Försvarsmakten och KTH ges ett särskilt uppdrag att ta fram förslag på hur en process och struktur för att ta fram nya tekniska lösningar inom cyberförsvaret skulle kunna se ut.

Pål Jonson (M)

Jan R Andersson (M) *Jörgen Berglund (M)*

Alexandra Anstrell (M) *Jessika Roswall (M)*