SVERIGES RIKSDAG

Motion till riksdagen 2020/21:3444

av Pål Jonson m.fl. (M)

Cybersäkerhet och cyberförsvar

Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om en bred utredning om cybersäkerhet som underlag för en svensk cybersäkerhetsstrategi och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om cybersäkerhetscentrumet och om strukturer för ledning och ansvar på cybersäkerhetsområdet och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om en förstärkt samverkan mellan staten och näringslivet på cybersäkerhetsområdet och tillkännager detta för regeringen.
4. 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.
5. Riksdagen ställer sig bakom det som anförs i motionen om ett sanktionssystem knutet till säkerhetsskyddslagen och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om en svensk cyberförsvarsdoktrin och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om Sveriges roll i det internationella arbetet för att skapa nya lagar och regler som reglerar användandet av nya teknologier i modern krigföring och tillkännager detta för regeringen.
8. Riksdagen ställer sig bakom det som anförs i motionen om utvecklingen av det svenska cyberförsvaret och tillkännager detta för regeringen.

Motivering

Cyber- och informationssäkerhet blir en allt viktigare del av såväl den allmänna samhällssäkerheten som av Sveriges totalförsvar. Den snabba utvecklingen inom AI-sektorn kommer att förstärka den utvecklingen ytterligare. 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.

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.

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 kan utgöra grundplåten för 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 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.

När utredningen är klar bör den stöpas om till 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 egen budget samt cyberkoordinator

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).

Cybersäkerhetscentrumet 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 egen budget och ett starkt mandat att samverka med näringslivet, samt att det kan utgöra knutpunkten i det nationella och internationella cybersäkerhetsarbetet.

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.

En 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.

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.

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.

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 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 bland annat myndigheter att ställa krav 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 åtgärder mot dem som bryter mot bestämmelserna.

I den utredning om kompletteringar till den nya säkerhetsskyddslagen (SOU 2018:82) vilken presenterades i november 2018 föreslog utredningen att tillsynsmyndigheten bör få besluta om sanktionsavgifter för överträdelser av bestämmelserna i säkerhetsskyddslagen. Moderaterna anser att regeringen snarast bör återkomma när det gäller möjligheten att sanktionsavgifter.

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).

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. Moderaterna vill därför att Sverige ska ha en tydlig cyberdoktrin som stipulerar hur vi ser på principerna för användandet av den aktiva cyberförmågan.

Sveriges 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.

Pål Jonson (M)

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

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