SVERIGES RIKSDAG

Motion till riksdagen 2023/24:422

av Tobias Andersson m.fl. (SD)

En framtidsinriktad it-politik

Förslag till riksdagsbeslut

1. Riksdagen ställer sig bakom det som anförs i motionen om att skapa företagsklimat och arenor som främjar testning, utveckling och anpassning av tjänster och idéer och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att styra utbildningssystemet mot att stärka humankapitalet till techsektorn och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att utvärdera och eventuellt stärka arbetet genom Nationellt cybersäkerhetscenter och andra myndigheter för att förebygga, upptäcka och hantera cyberangrepp och it-incidenter och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att bedriva ett effektivt informationsarbete för att höja medvetenheten om hot, sårbarheter och risker och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om att nätinfrastrukturens resiliens ska stärkas genom samarbete i kris mellan olika företag och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om att utveckla former för samverkan och informationsdelning mellan myndigheter och privata företag och organisationer för att öka säkerheten och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om att öka antalet personer med informationssäkerhetskompetens för att stödja företag, den offentliga sektorn och andra organisationer och tillkännager detta för regeringen.
8. Riksdagen ställer sig bakom det som anförs i motionen om att skapa ändamålsenlig lagstiftning som kan hantera den snabba teknik- och brottsutvecklingen och tillkännager detta för regeringen.
9. Riksdagen ställer sig bakom det som anförs i motionen om att utveckla polisens, åklagarnas och domstolars kompetens och resurser för att bekämpa nätbrottslighet och cyberhot och tillkännager detta för regeringen.

Främja Sverige som it-nation

Sverige behöver en bra utvecklingsmiljö för att stödja entreprenörer och startupföretag och detta gäller inte minst inom många framtidsbranscher inom tech och it. Det måste vara gynnsamt att prova nya idéer och koncept och vi behöver en företagsvänlig atmosfär och platser där företag får experimentera och utveckla sina tjänster och idéer. Arenor där olika aktörer kan mötas kan samfinansieras för att accelerera utveckling och användning, skapa större samverkan mellan stora och små bolag samt få ett mer diversifierat och innovativt utbud av tjänster och produkter.

Sveriges utbildningssystem har under decennier fallit jämfört med omvärlden, vilket gör att högteknologiska företag har allt svårare att rekrytera på den svenska arbetsmarknaden, detta parallellt med en stor arbetslöshet. Att svenska företag och universitet tar in spetskompetens från utlandet innebär också en förhöjd risk för spioneri. Studenter kan rekryteras av främmande underrättelsetjänster för att samla in information eller bedriva spionage. Det kan inkludera försök att få tillgång till forskningsresultat, teknisk information eller andra känsliga uppgifter. Det är viktigt att skapa en balans mellan att upprätthålla säkerheten och skydda landets intressen samtidigt som man främjar en öppen och inkluderande akademisk miljö. Det handlar om att vara medveten om riskerna och vidta åtgärder för att minimera dem utan att diskriminera utländska studenter.

Just nu tas viktiga steg i politiken för att vända på utvecklingen och det är viktigt att säkerställa att Sverige satsar på tekniska och naturvetenskapliga ämnen och att väcka barn och ungdomars teknikintresse tidigt. Ett mål bör vara att kraftigt öka antalet examinerade elever från naturvetenskaplig eller på motsvarande nivå teknisk utbildning. På högskole- och universitetsnivå behövs framåtriktade strategier för att öka antalet utbildade ingenjörer inom olika grenar inom it, så som dataingenjörsvetenskap, systemutveckling, artificiell intelligens och cybersäkerhet.

Cybersäkerhet

Cyberhot och cyberbrottslighet är växande problem och kommer i olika former. Företag utsätts t.ex. för brott i form av ransomware med efterföljande utpressning, medborgare utsätts för bedrägerier, staten och myndigheter utsätts för diverse angrepp från främmande makt och allt detta kan förväntas öka såväl i intensitet som sofistikeringsgrad i och med introduktionen av nya verktyg av artificiell intelligens.

Nationellt cybersäkerhetscenter, som är ett samarbete mellan Försvarsmakten, FRA, MSB och Säkerhetspolisen, har i uppdrag att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot. Det är rimligt att dessa myndigheter såväl som centret har förmåga och vilja att ta sig an nya än mer sofistikerade hot som följer av utvecklingen inom AI. Utifrån den premissen bör man utvärdera och eventuellt stärka arbetet genom Nationellt cybersäkerhetscenter och andra myndigheter för att förebygga, upptäcka och hantera cyberangrepp och it-incidenter.

Regeringen och dess myndigheter bör också tydligt verka för att höja medvetenheten om hot, sårbarheter och risker vad gäller cyberhot, inte minst vad gäller företag. Här bör staten vara på tårna och verka uppsökande.

I en värld som alltmer blir beroende av en sömlös digital kommunikation och anslutning är det av yttersta vikt att säkerställa nätinfrastrukturens robusthet och förmåga att hantera kriser och angrepp. Detta kräver en ny grad av samarbete mellan olika företag,

inte minst vad gäller nätinfrastrukturens resiliens. Genom att bilda en krisgemenskap kan vi dra nytta av varandras resurser för att effektivt hantera eventuella hot mot våra digitala nätverk. Detta skulle t.ex. kunna handla om att i händelse av att en av landets mobiloperatörer slås ut så ska dess kunder direkt och automatiserat kopplas upp mot en av konkurrenterna. En pålitlig och stabil kommunikationsinfrastruktur för våra medborgare blir en allt mer viktig samhällsfunktion i och med digitaliseringen. Utifrån det ovan angivna bör regeringen utreda frågan om krisgemenskap för nätinfrastrukturens resiliens.

Det behövs utveckling av samarbetsformer och informationsdelning mellan det offentliga och näringslivet. Idag kräver myndigheterna information och ställer krav på säkerhet från företag men ger inte tillbaka information eller resultat av sitt arbete inom informations- och cybersäkerhet. Genom att skapa trygga former för att dela relevant information kan säkerheten för fler aktörer förbättras. Det är viktigt att stärka samarbetet och möjliggöra dubbelriktad information för att stödja företag och organisationer i deras arbete med informations- och cybersäkerhet.

För att minska sårbarheten gentemot cyberangrepp behövs kompetensförstärkning på alla nivåer. Efterfrågan på kunskap om informations- och cybersäkerhet måste få större genomslag i utbildningssystemet. Försvarsmakten och andra myndigheter som jobbar med cybersäkerhet måste kunna hitta rätt kompetens för att försvara svenska intressen.

Förutom att förebygga och försvara oss mot cyberattacker och bedrägerier behöver vi skapa ändamålsenlig lagstiftning som kan hantera den snabba teknik- och brottsutvecklingen. Kriminella element måste effektivt kunna lagföras i de fall de ertappas och i sammanhanget gäller därför också att polisens, åklagarnas och domstolars kompetens och resurser för att bekämpa nätbrottslighet och cyberhot förstärks. Här krävs också fördjupat internationellt samarbete.

Artificiell intelligens

Artificiell intelligens står nu inför sitt stora genombrott och kommer att totalt revolutionera vårt samhälle. Det vore djupt olyckligt om vi om några år ser tillbaka på en tid med passivitet inför dessa tekniksprång och medföljande samhällsförändringar där vi inte gjorde vad vi kunde för att såväl ta vara på möjligheterna som hantera riskerna. Vi har i en separat riksdagsmotion utvecklat vår syn på AI.

Tobias Andersson (SD)

Josef Fransson (SD)

Eric Palmqvist (SD)

Jessica Stegrud (SD)

Johnny Svedin (SD)

Mattias Bäckström Johansson (SD)