SVERIGES RIKSDAG

Försvarsutskottets betänkande 2021/22:FöU10

Cybersäkerhetsfrågor

Sammanfattning

Utskottet föreslår att riksdagen avslår alla motionsyrkanden om cybersäkerhet, främst med hänvisning till regeringens och det nyligen tillskapade nationella cybersäkerhetscentrets pågående arbete samt beredningsläget i fråga om olika utredningar med bäring på området.

I betänkandet finns 24 reservationer (M, SD, C, KD, L).

Behandlade förslag

Cirka 50 yrkanden i motioner från allmänna motionstiden 2021/22.

Innehållsförteckning

Utskottets förslag till riksdagsbeslut

Systemfrågor

1. En översyn av cybersäkerhetsområdet

Riksdagen avslår motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del,
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 24,
2021/22:3368 av Viktor Wärnick m.fl. (M) yrkande 20 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 1 och 2.

Reservation 1 (M, KD)
Reservation 2 (SD)
Reservation 3 (C)

2. Inrättandet av en it-haverikommission

Riksdagen avslår motionerna
2021/22:3227 av Niels Paarup-Petersen m.fl. (C) yrkande 22,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 20 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 6.

Reservation 4 (M, C)

3. Risker och sårbarheter

Riksdagen avslår motionerna
2021/22:624 av Markus Wiechel och Björn Söder (båda SD),
2021/22:2934 av Jimmy Ståhl m.fl. (SD) yrkande 6,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 26 och 29 samt
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 5.

Reservation 5 (M)
Reservation 6 (SD)
Reservation 7 (C)

Cyberförsvar

4. Försvarsmaktens förmåga

Riksdagen avslår motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del,
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 2, 12, 13 och 15,
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 10 och
2021/22:3998 av Joar Forssell m.fl. (L) yrkande 10.

Reservation 8 (M, KD)
Reservation 9 (SD)
Reservation 10 (C)
Reservation 11 (L)

5. Kompetensförsörjning

Riksdagen avslår motionerna
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 10 och 11 samt
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 11 och 13.

Reservation 12 (M, KD)
Reservation 13 (C)

6. Förfogandelagstiftning

Riksdagen avslår motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 14.

Reservation 14 (C)

Övriga frågor

7. Samhällets förmågeutveckling

Riksdagen avslår motionerna
2021/22:1078 av Edward Riedl (M),
2021/22:1394 av Larry Söder (KD),
2021/22:3227 av Niels Paarup-Petersen m.fl. (C) yrkande 25,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 28, 31, 34, 36, 38 och 39,
2021/22:3753 av Maria Stockhaus m.fl. (M) yrkandena 12 och 14 samt
2021/22:4197 av Elisabeth Falkhaven m.fl. (MP) yrkande 3.

Reservation 15 (M)
Reservation 16 (C)

8. Samverkan med näringslivet

Riksdagen avslår motionerna
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 7 och 12 samt
2021/22:3640 av Pål Jonson m.fl. (M) yrkandena 16 och 17.

Reservation 17 (M)

9. Cybersäkerhet på universitet och högskolor

Riksdagen avslår motionerna
2021/22:3640 av Pål Jonson m.fl. (M) yrkande 18 och
2021/22:4161 av Pia Steensland m.fl. (KD) yrkande 32.

Reservation 18 (M, KD)

10. It-upphandlingar ur ett cybersäkerhetsperspektiv

Riksdagen avslår motionerna

2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 22, 23 och 27 samt
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 9.

Reservation 19 (M)
Reservation 20 (C)

11. Internationella överenskommelser

Riksdagen avslår motionerna
2021/22:2279 av Maria Nilsson (L),
2021/22:2351 av Robert Hannah (L),
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 6 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 8.

Reservation 21 (M)
Reservation 22 (C)

12. Arbetet inom EU

Riksdagen avslår motionerna
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 7, 8 och 25 samt
2021/22:3775 av Jessika Roswall m.fl. (M) yrkande 26.

Reservation 23 (M)
Reservation 24 (C)

Stockholm den 3 februari 2022

På försvarsutskottets vägnar

Niklas Karlsson

Följande ledamöter har deltagit i beslutet: Niklas Karlsson (S), Pål Jonson (M), Jan R Andersson (M), Roger Richthoff (SD), Mattias Ottosson (S), Daniel Bäckström (C), Hanna Gunnarsson (V), Jörgen Berglund (M), Caroline Nordengrip (SD), Kalle Olsson (S), Mikael Oscarsson (KD), Allan Widman (L), Per Söderlund (SD), Elisabeth Falkhaven (MP), Alexandra Anstrell (M), ClasGöran Carlsson (S) och Heléne Björklund (S).

Redogörelse för ärendet

Ärendet och dess beredning

I betänkandet behandlar utskottet ett femtiotal yrkanden om cybersäkerhet från allmänna motionstiden 2021/22.

Utskottet har löpande inhämtat information på området. Den 10 februari 2021 informerade t.ex. inrikesminister Mikael Damberg om Europeiska unionens strategi för cybersäkerhet för ett digitalt decennium. Utskottet överlade vid samma tillfälle med inrikesministern om kommissionens förslag till direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen. Utskottet besökte Försvarets radioanstalt (FRA) den 12 oktober 2021. Den 9 november 2021 informerade bl.a. chefen för Nationellt cybersäkerhetscenter Therese Naess, generaldirektör Björn Lyrvall från FRA, säkerhetspolischef Charlotte von Essen, avdelningschef Åke Holmgren från Myndigheten för samhällsskydd och beredskap (MSB) och generaldirektör Mikael Granholm från Försvarsmakten om cybersäkerhetsarbetet i Sverige.

Utskottets överväganden

Systemfrågor

Utskottets förslag i korthet

Riksdagen avslår motionsyrkanden om systemfrågor kopplade till cybersäkerhet.

Jämför reservation 1 (M, KD), 2 (SD), 3 (C), 4 (M, C), 5 (M), 6 (SD) och 7 (C).

Motionerna

En översyn av cybersäkerhetsområdet

Pål Jonson m.fl. (M) föreslår i kommittémotion 2021/22:3639 yrkande 1 en översyn av cybersäkerhetsområdet med tydliga delredovisningar.

I samma motion yrkande 2 föreslår motionärerna en utredning som ska stödja och utveckla en svensk cybersäkerhetsstrategi. Faktorer som kompetensförsörjning, forskning och teknikutveckling samt framtagande av certifierade produkter bör enligt motionärerna vara en central del i utredningen.

Viktor Wärnick m.fl. (M) understryker i kommittémotion 2021/22:3368 yrkande 20 vikten av ett starkt försvar mot yttre påverkan och att det brådskar med att den nya myndigheten för psykologiskt försvar och det nya cybersäkerhetscentret kommer till stånd och blir fullt verksamma.

I kommittémotion 2021/22:2531 yrkande 42 i denna del föreslår Roger Richthoff m.fl. (SD) att en samordnande myndighet ska ansvara för att den offentliga sektorn skyddas mot cyberangrepp. Björn Söder m.fl. (SD) föreslår samma sak i kommittémotion 2021/22:2579 yrkande 17 i denna del.

Niels Paarup-Petersen m.fl. (C) anför i kommittémotion 2021/22:3245 yrkande 24 att civilsamhället bör inkluderas i utvecklingen av policyer som påverkar medborgarnas digitala rättigheter.

Inrättandet av en it-haverikommission

Pål Jonson m.fl. (M) föreslår i kommittémotion 2021/22:3639 yrkande 6 att det ska inrättas haverikommissioner vid större cyberangrepp mot samhällsviktig verksamhet.

I kommittémotion 2021/22:3227 yrkande 22 föreslår Niels Paarup-Petersen m.fl. (C) att det inom den verksamhet som grundlagts genom bl.a. genomförandet av EU:s direktiv om nätverks och informationssystem (NIS), den nya säkerhetsskyddslagen och EU:s dataskyddsförordning (GDPR) skapas en it-haverikommission. Detta görs förslagsvis som en vidareutveckling av CERT-SE, dvs. Sveriges nationella it-incidentcentrum (Computer Security Incident

Response Team, CSIRT), i samband med utvecklingen av det nationella cybersäkerhetscentret.

Niels Paarup-Petersen m.fl. (C) föreslår i kommittémotion 2021/22:3245 yrkande 20 att uppdrag ska ges till relevanta myndigheter, t.ex. Statens haverikommission och den svenska myndighet som samlar in och sprider information om aktuella hot mot it-säkerhet (CERT-SE) att utreda stora it-relaterade incidenter.

Risker och sårbarheter

Pål Jonson m.fl. (M) föreslår i kommittémotion 2021/22:3639 yrkande 5 att regeringen ska ge Försvarets materielverk (FMV) i uppdrag att, i samråd och samverkan med framför allt de myndigheter som ingår i det nationella cybersäkerhetscentret, arbeta vidare med de förslag som utredningen Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63) tagit fram rörande hot-, sårbarhets- och riskbedömningar, vilka kan fungera som stöd för kravställning.

I kommittémotion 2021/22:2934 yrkande 6 av Jimmy Ståhl m.fl. (SD) anger motionärerna att viss infrastruktur är särskilt sårbar för dataintrång eftersom känslig information om medborgare, militär, politisk ledning m.fl. kan hamna i orätta händer. Motionärerna yrkar därför på att säkerhetsrutinerna för viss känslig it-infrastruktur ses över.

Niels Paarup-Petersen m.fl. (C) föreslår i kommittémotion 2021/22:3245 yrkande 26 att Post- och telestyrelsen (PTS) ska få i uppdrag att genomföra en utredning om sårbarheterna i fibernät och noder för att få en nationell lägesbild och kunna förebygga cyberattacker.

I samma motion yrkande 29 föreslår motionärerna att den kritiska infrastrukturen i Sverige ska sårbarhetstestas löpande. Motionärerna menar att vattenrening, elförsörjning och andra grundläggande delar av samhällets infrastruktur i dag är digitaliserade och därmed sårbara för cyberattacker.

Markus Wiechel och Björn Söder (båda SD) yrkar i motion 2021/22:624 på att det ska genomföras en bredare granskning av svenskarnas användning av teknik från länder som kan anses utgöra ett säkerhetshot.

Bakgrund

Tidigare behandling

När det gäller organiseringen av cybersäkerheten uttryckte utskottet i betänkande 2020/21:FöU4 att den delade regeringens och Försvarsberedningens bedömning att det behövs en högre grad av samordning på cybersäkerhetsområdet. I totalförsvarspropositionen beskrev regeringen att ett nationellt center för cybersäkerhet skulle inrättas under 2020 med syftet att stärka Sveriges förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska sårbarheter. Regeringen gav sålunda FRA, Försvarsmakten, MSB

och Säkerhetspolisen i uppdrag att förbereda centrets inrättande, vilket utskottet gav stöd åt. Vikten av detta underströks också i betänkande 2020/21:FöU6.

I betänkande 2021/22:FöU1 uttryckte utskottet att det bedömde att cyberhoten mot Sverige och svenska intressen var omfattande och ansåg att det var angeläget att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot, och att det nationella cybersäkerhetscentret där hade en viktig roll att fylla.

I fråga om att se över säkerhetsrutinerna för viss, känslig it-infrastruktur uttryckte utskottet i betänkande 2020/21:FöU6 att det är mycket angeläget att skydda säkerheten i nätverk, produkter och system. Det arbete som görs för att skapa en säker it-infrastruktur i landet ansågs därför välkommet. Inrättandet av det nya nationella cybercentret uttrycktes som en viktig del i denna utveckling och i arbetet med att skydda samhällsviktig infrastruktur.

Med anledning av ett yrkande om tillskapandet av en it-haverikommission uttryckte utskottet i betänkande 2020/21:FöU6 att de olika initiativ som regeringen tagit de senaste åren markerat en tydlig förändring av inriktningen på politiken för den digitala förvaltningen. Det nya cybersäkerhetscentrets uppgift att koordinera arbetet med att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter, förmedla råd och stöd i fråga om hot, sårbarheter och risker samt tillhandahålla lägesbilder och analyser i fråga om hot, sårbarheter och risker svarade enligt utskottet mot de krav som framställdes i den aktuella motionen. Utskottet såg därför inte skäl att vidta några åtgärder. Motionsyrkandet avstyrktes.

Pågående arbete

I budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 6) uttrycker regeringen att flera åtgärder har vidtagits för att öka informations- och cybersäkerheten i det svenska samhället. I juni 2017 fattade exempelvis regeringen beslut om en nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213) och i samband med denna fick ett antal berörda myndigheter som ingår i Samverkansgruppen för informationssäkerhet (Samfi) i uppdrag att utarbeta en samlad handlingsplan. Vidare har regeringen bl.a. gett MSB i uppdrag att genomföra utbildningsinsatser och att utarbeta en struktur för uppföljning av informationssäkerhetsarbetet inom den offentliga förvaltningen.

I budgetpropositionen beskriver regeringen vidare att man den 10 december 2020 beslutade om ett uppdrag till FRA, Försvarsmakten, MSB och Säkerhetspolisen att fördjupa samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter. Myndigheterna ska enligt uppdraget ha en nära samverkan med FMV, Polismyndigheten och Post- och telestyrelsen (PTS), som ska ges möjlighet att medverka i cybersäkerhetscentrets verksamhet. Det övergripande målet med det nationella cybersäkerhetscentret anges vara att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska

cyberhot och att minska sårbarheter. Regeringen anger vidare att cybersäkerhetscentrets verksamhet ska komma till bred nationell nytta inom såväl offentlig som privat verksamhet och göra Sverige säkrare genom att höja den samlade förmågan att möta cyberhoten och öka förmågan att effektivt stödja offentliga och privata aktörer. Verksamheten i centret ska utvecklas stegvis 2021–2023. Regeringen avser att under 2023 ta ställning till hur cybersäkerhetscentrets verksamhet fortsatt bör inriktas och bedrivas efter 2023.

Inom ramen för cybersäkerhetscentret ska myndigheterna enligt regeringsbeslutet (dnr Fö2019/01330)

- koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter
- förmedla råd och stöd avseende hot, sårbarheter och risker
- utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer inom cybersäkerhetsområdet.

Samverkan inom ramen för cybersäkerhetscentret ska utvecklas stegvis 2021–2023 för att

- samlokalisera relevanta förmågor från myndigheterna
- stötta vid hantering av cyberangrepp och andra it-incidenter samt upprätta en plan för samlad hantering på nationell nivå vid allvarliga cyberangrepp
- tillhandahålla anpassade och aggregerade lägesbilder och analyser avseende hot, sårbarheter och risker
- rikta och samordna varningar avseende hot och cyberangrepp
- samordna stödet till förebyggande skyddsåtgärder, exempelvis tekniska säkerhetsanalyser, och kartlägga verksamheters beredskap vid it-incidenter
- samordna och utgöra kontaktpunkt för internationella samarbeten på myndighetsnivå inom cybersäkerhetscentrets verksamhet
- verka för kunskaps-, kompetens- och informationsutbyte och samverkan med offentliga och privata aktörer, exempelvis avseende detektion, sårbarheter, hot, risker, analys, verktyg och metoder samt internationellt samarbete
- föra dialog med aktörer inom forsknings-, kunskaps- och kompetensuppbyggnad
- erbjuda kompetenshöjande insatser, exempelvis övningar och utbildningar för identifierade målgrupper.

Av budgetpropositionen framgår att myndigheterna inom ramen för samarbetet gemensamt publicerat tre externa rapporter: Cybersäkerhet i Sverige – hot, metoder, brister och beroenden, Cybersäkerhet i Sverige – rekommenderande skyddsåtgärder och Cybersäkerhet i Sverige – i skuggan av en pandemi.

I mars 2021 lämnade de ovannämnda myndigheterna en uppdaterad redovisning av den gemensamma handlingsplanen för myndigheternas arbete. Regeringen gör i budgetpropositionen bedömningen att den gemensamma handlingsplanen för informations- och cybersäkerhet ger värdefull information till

regeringen. Samverkan mellan de sju myndigheterna är nödvändig och viktig för att få en samlad bild. Regeringen bedömer att etableringen av ett nationellt cybersäkerhetscenter under 2021 är ett centralt och viktigt steg i det fortsatta arbetet med att stärka informations- och cybersäkerheten i Sverige.

Utredningen Ansvar, ledning och samordning inom civilt försvar (dir. 2018:79) fortsatte under 2020. I mars 2021 redovisade utredningen sitt betänkande Struktur för ökad motståndskraft (SOU 2021:25). Utredningen föreslår bl.a. inrättandet av nya beredskapssektorer och beredskapsområden, en indelning av landet i större geografiska områden för civil ledning och samordning samt ett övergripande ansvar för MSB för planeringen av civilt försvar. Enligt Regeringskansliet (Justitiedepartementet) planeras de delar som inte kräver lagändringar utan som regleras i förordning alltså beredskapsmyndigheter, sektorer, civilområden och MSB beslutas före sommaren 2022.

Utöver tio beredskapssektorer har utredningen identifierat fyra särskilda beredskapsområden som omfattar samhällsviktiga verksamheter och funktioner som är av särskild betydelse att upprätthålla i kris, höjd beredskap och då ytterst krig. Utredningens bedömning är att dessa områden bör vara en del av beredskapssystemet. Cybersäkerhet (i ett samarbete mellan Säkerhetspolisen, MSB, Försvarsmakten och FRA) identifieras som ett sådant område.

Utredningen delar Försvarsberedningens bedömning att ett systematiskt arbete med informations- och cybersäkerhet spelar en avgörande roll för att en trovärdig totalförsvarsförmåga ska kunna uppnås. Detta gäller hos såväl staten, kommunerna och regionerna som näringslivet. Det behöver finnas en nationell funktion med uppgift att stödja myndigheter och samhället i övrigt i arbetet med att förebygga och hantera angrepp inom informations- och kommunikationsområdet samt upprätthålla en aktuell lägesbild över samhällets digitala miljö. Verksamheten är viktig för det civila försvaret.

Utredningen föreslår alltså att cybersäkerhet ska vara ett särskilt beredskapsområde. Utredningen bedömer att det inte är möjligt att föreslå verksamheten som en beredskapssektor eftersom både Försvarsmakten och FRA ingår i arbetet med cybersäkerhetscentret samt att regeringen hittills inte har pekat ut någon samordnande myndighet för cybersäkerhetsområdet.

Det finns i dag ett etablerat samarbete och samverkan mellan myndigheterna inom cybersäkerhetsområdet genom bl.a. Samfi. Formerna för samverkan med de föreslagna beredskapssektorerna kommer att behöva byggas upp när dessa etablerats, enligt utredningen. Det behöver även etableras samverkansformer med de övriga särskilda beredskapsområden som föreslås.

Utskottets ställningstagande

En översyn av cybersäkerhetsområdet

Utskottet instämmer med regeringen i att flera åtgärder vidtagits de senaste åren för en förbättrad informations- och cybersäkerhet i samhället men att uppdraget långt ifrån är slutfört. Bland annat mot bakgrund av vad Försvarsberedningen uttryckte i sina rapporter Motståndskraft (Ds 2017:66) och Värnkraft

(Ds 2019:8), t.ex. om behovet av en högre grad av samordning på cybersäkerhetsområdet, välkomnar utskottet skapandet av det nya nationella cybersäkerhetscentret och framtagandet av en gemensam handlingsplan. Sammantaget finner utskottet att regeringen har vidtagit flera åtgärder för en förbättrad informations- och cybersäkerhet. Vidare ser utskottet fram emot beredningen av betänkandet från Utredningen om civilt försvar med dess förslag med bäring på området. Eftersom Försvarsberedningen dessutom tämligen nyligen kan sägas ha utrett cybersäkerhet och utmaningar förknippade med detta område finner utskottet sammantaget inte skäl att för tillfället vidta några ytterligare åtgärder i fråga om en översyn av cybersäkerhetsområdet. Motionerna 2021/22:3639 (M) yrkandena 1 och 2, 2021/22:3368 (M) yrkande 20, 2021/22:2531 (SD) yrkande 42 i denna del och 2021/22:2579 (SD) yrkande 17 i denna del avstyrks därmed.

Då samverkan med både privata och offentliga aktörer är satt att vara en central del i det nationella cybercentrets uppdrag och ambitionen är att satsa mer resurser på kunskapshöjande aktiviteter finner utskottet för tillfället inte heller skäl att vidta ytterligare åtgärder i fråga om civilsamhällets möjligheter att delta i utvecklingen av policyer som påverkar medborgarnas digitala rättigheter. Motion 2021/22:3245 (C) yrkande 24 avstyrks därmed.

Inrättandet av en it-haverikommission

Vikten av att utreda och dra lärdom av större it-relaterade incidenter kan inte underskattas. Utskottet konstaterar att regeringen gett cybersäkerhetscentret i uppdrag att bl.a. koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter, stötta vid hantering av cyberangrepp och andra it-incidenter samt upprätta en plan för samlad hantering på nationell nivå vid allvarliga cyberangrepp. Då denna samverkan inom ramen för cybersäkerhetscentret är tänkt att utvecklas stegvis 2021–2023 finner utskottet för närvarande inte skäl att vidta några ytterligare åtgärder när det gäller utredandet av allvarliga it-händelser. Motionerna 2021/22:3639 (M) yrkande 6, 2021/22:3227 (C) yrkande 22 och 2021/22:3245 (C) yrkande 20 avstyrks därmed.

Risker och sårbarheter

I fråga om hot-, sårbarhets- och riskbedömningar ingår det bl.a. också i det nya nationella cybersäkerhetscentrets uppgifter att förmedla råd och stöd i fråga om hot, sårbarheter och risker, att samordna stödet till förebyggande skyddsåtgärder, exempelvis tekniska säkerhetsanalyser, och att kartlägga verksamheters beredskap vid it-incidenter. Utskottet ser inte skäl att i detta tidiga skede av centret vidta några ytterligare åtgärder inom området. Motionerna 2021/22:3639 (M) yrkande 5, 2021/22:2934 (SD) yrkande 6, 2021/22:3245 (C) yrkandena 26 och 29, och 2021/22:624 (SD) avstyrks.

Cyberförsvar

Utskottets förslag i korthet

Riksdagen avslår motionsyrkanden om cyberförsvar.

Jämför reservation 8 (M, KD), 9 (SD), 10 (C), 11 (L), 12 (M, KD), 13 (C) och 14 (C).

Motionerna

Försvarsmaktens förmåga

Pål Jonson m.fl. (M) föreslår i kommittémotion 2021/22:3639 yrkande 10 att Sverige ska upprätta en cyberdoktrin för den defensiva och offensiva cyberförmågan. Cyberdoktrinen ska enligt motionärerna slå fast hur Sverige ser på principerna för användandet av den aktiva cyberförmågan.

I kommittémotion 2021/22:2531 yrkande 42 i denna del föreslår Roger Richthoff m.fl. (SD) att Sverige ska fortsätta att stärka sin förmåga att genomföra såväl defensiva som offensiva cyberoperationer.

Björn Söder m.fl. (SD) föreslår i kommittémotion 2021/22:2579 yrkande 17 i denna del att Sverige ska skaffa sig ett aktivt informationsteknologiskt försvar (aktiv cyberförmåga).

I kommittémotion 2021/22:3245 av Niels Paarup-Petersen m.fl. (C) föreslår motionärerna

- att Sverige tydligare än i dag ska uttala vilket land som står bakom cyberangrepp mot Sverige när det är möjligt att avgöra detta (yrkande 2)
- att Försvarsmaktens förmåga till både defensiva och offensiva cyberoperationer ska utvecklas (yrkande 12)
- att kopplingen mellan cyberförsvar och psykologiskt försvar ska utvecklas förmågemässigt (yrkande 13)
- att en utredning ska tillsättas för att se över ett eventuellt behov av att göra cyberförsvar till en egen försvarsgren (yrkande 15).

Joar Forssell m.fl. (L) lyfter i kommittémotion 2021/22:3998 yrkande 10 upp cyberhotet från Ryssland och anför att Sverige behöver en politik som bemöter både den militära hotbilden och underrättelsehotet.

Kompetensförsörjning

Pål Jonson m.fl. (M) föreslår i kommittémotion 2021/22:3639 yrkande 11 att användandet av tidvis tjänstgörande personal från näringslivet och från hemvärnet ska utvecklas för att stärka cyberförsvaret ytterligare. I yrkande 13, föreslår motionärerna att Försvarsmakten och Kungliga Tekniska högskolan (KTH) ska ges ett särskilt uppdrag att föreslå en process och struktur för att ta fram nya tekniska lösningar inom cyberförsvaret.

I kommittémotion 2021/22:3245 yrkande 10 framhåller Niels Paarup-Petersen m.fl. (C) att det bör övervägas att skapa ett cybervärn som står på två ben – ett ben för att bidra till att stärka samhällets förmåga att hantera stora cyberattacker och ett ben för att stå emot otillbörlig informationspåverkan under höjd beredskap och ytterst krig. Cybervärnet ska med andra ord också ha uppgifter inom det psykologiska försvaret.

I samma motion yrkande 11 framhålls vikten av fler cybervärnpliktiga för att stärka Försvarsmaktens egen kompetens men också för att stärka cyberkompetensen i samhället i stort.

Förfogandelagstiftning

Niels Paarup-Petersen m.fl. (C) föreslår i kommittémotion 2021/22:3245 yrkande 14 att en utredning tillsätts för att se över ett eventuellt behov av förfogandelagstiftning som träder i kraft vid höjd beredskap eller krig och som inkluderar digitala resurser för krigsföring i cyberdomänen.

Bakgrund och tidigare behandling

Försvarsmaktens förmåga

I betänkande 2020/21:FöU4 lade utskottet stor vikt vid att Sveriges cyberförmåga stärks och att samhällets cybersäkerhet förbättras. Att en cyberförsvarsförmåga hade etablerats av Försvarsmakten med stöd av FRA uttrycktes som centralt för att Sverige ska kunna skydda kritiska samhällsfunktioner och försvara sig mot cyberangrepp från kvalificerade motståndare. Ändringar i lagstiftningen och utökad tillsynsverksamhet angavs som andra exempel på redan vidtagna åtgärder som innebär ett starkare skydd för Sveriges säkerhet.

Utskottet uttryckte samtidigt det som mycket angeläget att den påbörjade utvecklingen fortsätter och att Sveriges förmåga på området stärks. Utskottet instämde därmed i regeringens bedömning att Sveriges cyberförsvarsförmåga bör stärkas ytterligare och att det inkluderar defensiva och offensiva operationer i cyberdomänen. Teknikutvecklingen på området går snabbt och utskottet delade regeringens mening att kontinuerlig forskning krävs för att bidra till att vidmakthålla och utveckla cyberförsvarsförmågan samt att kvalificerad personal behövs för att långsiktigt kompetensförsörja och stärka förmågan.

I likhet med regeringens syn, som den kommer till uttryck i försvarsinriktningspropositionen för 2021–2025 (prop. 2020/21:30), uttryckte utskottet att det krävs en stark säkerhetstjänst och försvarsunderrättelseförmåga för att kunna förebygga och identifiera hotande verksamhet, god förmåga att upptäcka, varna för och hantera intrång och angrepp samt ett starkt skydd av de mest skyddsvärda verksamheterna i samhället.

Kompetensförsörjning

I betänkande 2020/21:FöU4 uttryckte sig utskottet positivt till regeringens inriktning att Försvarsmakten ska samverka med andra berörda myndigheter och

planera för hur resurser ska kunna användas effektivt i olika situationer. Utskottet såg vidare positivt på inriktningen att hemvärnet även fortsättningsvis ska utföra viktiga uppgifter vid hanteringen av fredstida kriser.

I samma betänkande välkomnade utskottet också regeringens bedömning att en långsiktig samverkan mellan offentliga och privata aktörer på den centrala, regionala och lokala nivån behöver etableras. Likt regeringen uttryckte utskottet att det ansåg att Utredningen om civilt försvars uppdrag att föreslå en sektorsindelning för statliga myndigheter och vilka myndigheter som ska ges ett särskilt ansvar för krisberedskapen och civilt försvar i förlängningen bör skapa goda förutsättningar för arbetet med att utveckla och förtydliga samverkan med näringslivet på flera områden.

Utskottet instämde i det aktuella betänkandet i regeringens bedömning av behovet av att inrätta ett näringslivsråd under perioden 2021–2025 med syftet att upprätta ett ömsesidigt informationsutbyte och att ta fram en gemensam inriktning, planer och villkor för samverkan mellan offentliga och privata aktörer på samtliga nivåer.

I betänkande 2021/22:FöU1 välkomnade utskottet att grundutbildningen av cybersoldater hade påbörjats.

Pågående arbete

Försvarsmaktens förmåga

Av budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 6) framgår att det i försvarsbeslutet 2015 slogs fast att en cyberförsvarsförmåga behövde utvecklas och stärkas. År 2016 gav regeringen Försvarsmakten i uppdrag att med stöd av FRA påbörja arbetet med att analysera och utveckla cyberförsvarsförmågan inklusive att genomföra aktiva operationer i cybermiljön.

Regeringen uttrycker i budgetpropositionen att den avser att stärka och utveckla cyberförsvarsförmågan i enlighet med propositionen Totalförsvaret 2021–2025 (prop. 2020/21:30). Det inbegriper Försvarsmaktens förmåga att, med stöd av FRA, genomföra defensiva och offensiva operationer i cyberdomänen. Regeringen anser att arbetet med att förebygga, upptäcka och hantera cyberattacker är fortsatt prioriterat.

Det framgår vidare att Försvarsmakten, med stöd av FRA, har etablerat en cyberförsvarsförmåga, dvs. förmågan att genomföra såväl defensiva som offensiva operationer mot en kvalificerad motståndare i cybermiljön.

Kompetensförsörjning

Försvarsmakten har enligt budgetpropositionen bl.a. etablerat en militär virtuell träningsanläggning samt påbörjat grundutbildningen av cybersoldater. Ett trettiotal värnpliktiga har inlett befattningsutbildningen. Målsättningen är att utbilda 60 värnpliktiga per år.

Av budgetpropositionen framgår också att under 2020 inrättade Försvarsmakten Centrum för cyberförsvar och informationssäkerhet (CDIS) vid KTH.

CDIS bidrar till Försvarsmaktens möjlighet att få tillgång till utbildningar i forskningens framkant som stöd för Försvarsmaktens kompetensförsörjning och kompetensutveckling. Målsättningen med CDIS är att utveckla kunskap och skapa nya metoder, verktyg, koncept och tillämpningar inom området cyberförsvar och informationssäkerhet.

Det är regeringens bedömning att dessa bidrag till cyberförsvarsförmågan försvårar och höjer tröskeln för en aktör som överväger att angripa eller utöva påtryckningar mot Sverige eller svenska intressen.

I budgetpropositionen lyfter regeringen också fram att det militära försvaret är beroende av att ett antal viktiga samhällsfunktioner fungerar och att aktörer i det civila försvaret kan stödja Försvarsmakten för att den ska kunna lösa sina uppgifter vid höjd beredskap. Planeringen för det civila försvaret ska ske i samverkan mellan statliga myndigheter, kommuner, regioner, frivilligorganisationer, näringslivet m.fl. Regeringen anger att det militära och civila försvarets samverkan har ökat under försvarsbeslutsperioden och fortsatte att utvecklas under 2020. Arbetet med att integrera näringslivet i totalförsvarsplaneringen på samtliga nivåer har också påbörjats. Arbetet har till del utgått från förslag i Försvarsberedningens rapport Motståndskraft (Ds 2017:66) och slutrapporten Värnkraft (Ds 2019:8) samt betänkandet Näringslivets roll inom totalförsvaret (SOU 2019:51).

Vidare anger regeringen i samma proposition att den avser att verka för att näringslivet i ökad utsträckning involveras i arbetet med att säkerställa de viktigaste samhällsfunktionerna. Offentliga aktörer bör, i nära dialog med privata aktörer, bedöma behovet av förberedelser för att säkerställa en rimlig beredskap. Som ett led i att utveckla den offentlig-privata samverkan ska ett tvärsektoriellt näringslivsråd inrättas. Detta råd är planerat att tillsättas före sommaren 2022, enligt Regeringskansliet (Justitiedepartementet). Rådet ska bl.a. vara en plattform för informationsutbyte.

I propositionen Totalförsvaret 2021–2025 (prop. 2020/21:30) uttrycker regeringen att den delar Försvarsberedningens bedömning att personalbehovet inom det civila försvaret framför allt kommer att tillgodoses av anställd personal som i händelse av höjd beredskap tjänstgör med stöd av den allmänna tjänsteplikten. Även frivilliga har en viktig roll att fylla i personalförsörjningen för det civila försvaret. Regeringen anger vidare att det stora antalet privata aktörer som utför samhällsviktig verksamhet samt det över tid försämrade säkerhetspolitiska läget är två bidragande orsaker till att en översyn av personalförsörjningen inom det civila försvaret är angelägen. MSB fick i juli 2021 i uppdrag (dnr Ju2021/02771) att bedöma behovet av personalförstärkningar inom bevakningsansvariga myndigheter och andra berörda aktörer vid en situation med höjd beredskap och ytterst krig. En utgångspunkt för analysen av personalbehoven kan vara de områden som regeringen pekar ut som särskilt viktiga i totalförsvarspropositionen. Dessa är ordning och säkerhet, skydd av civilbefolkningen, hälso- och sjukvård, livsmedel och dricksvatten, finansiell beredskap, transporter, energiförsörjning samt elektroniska kommunikationer och post. MSB ska samarbeta med Försvarsmakten, Totalförsvarets plikt- och

prövningsverk samt andra relevanta aktörer i genomförandet av uppdraget. Uppdraget ska redovisas till Regeringskansliet (Justitiedepartementet) senast den 29 april 2022.

Förfogandelagstiftning

Av Försvarsberedningens rapport Värnkraft (Ds 2019:8) framgår hur förfogandelagen (1978:262) ger möjligheter för staten att förfoga över privat egendom och tjänster i syfte att tillgodose Försvarsmaktens behov av exempelvis försörjning. Genom förfogande kan fastigheter och annan egendom tas i anspråk och andra rättigheter till egendom, exempelvis servitut, upphävas eller begränsas. Ägare eller innehavare av produktionsmedel kan även behöva medverka till framställning av egendom för statens räkning.

Försvarsberedningen konstaterar också att regelverket för höjd beredskap och krig ger rättsliga förutsättningar för staten att ingripa i enskilda individers fri- och rättigheter samt förfoga över resurser som finns i näringslivet för att på så sätt få tillgång till personella och materiella resurser som kan gynna de samlade försvarsansträngningarna. Lagen (1994:1809) om totalförsvarsplikt ger t.ex. staten förutsättningar att genom tvångsmedel få tillgång till personal.

Utskottets ställningstagande

Försvarsmaktens förmåga

Vikten av att kunna möta nya hot och hotbilder kan inte underskattas. Utskottet välkomnar därför regeringens ambition att fortsätta prioritera att förebygga, upptäcka och hantera cyberattacker, vilket bl.a. innefattar Försvarsmaktens förmåga att med stöd av FRA m.fl. genomföra defensiva och offensiva operationer i cyberdomänen. Detta innebär viktiga steg mot att kunna försvåra och höja tröskeln för en aktör som överväger att angripa eller utöva påtryckningar mot Sverige eller svenska intressen. Möjligheten, och lämpligheten, att peka ut vem eller vilka som står bakom externa hot och påtryckningar får dock bedömas från fall till fall.

Utskottet ser positivt på det förmågearbete som regeringen, Försvarsmakten m.fl. bedriver och ser inte skäl att föreslå ytterligare åtgärder på området för tillfället. Motionerna 2021/22:3639 (M) yrkande 10, 2021/22:2531 (SD) yrkande 42 i denna del, 2021/22:2579 (SD) yrkande 17 i denna del, 2021/22:3245 (C) yrkandena 2, 12, 13 och 15, samt 2021/22:3998 (L) yrkande 10 avstyrks därmed.

Kompetensförsörjning

Utskottet önskar än en gång betona vikten av att tillgången på kvalificerad personal på cybersäkerhetsområdet tillgodoses genom bl.a. långsiktig kompetensförsörjning. Utskottet välkomnar därför att Försvarsmakten bl.a. har etablerat en militär virtuell träningsanläggning samt påbörjat en grundutbildning av cybersoldater.

Överlag ser utskottet positivt på regeringens inriktning att Försvarsmakten ska samverka med andra, t.ex. KTH och berörda myndigheter, och planera för hur resurser ska kunna användas effektivt vid olika situationer, inte minst på cybersäkerhetsområdet. Även inriktningen att hemvärnet ska kunna utföra viktiga uppgifter vid hanteringen av fredstida kriser och att näringslivet ska involveras i totalförsvarsplaneringen välkomnas i sammanhanget. Det är essentiellt att fortsätta strävandena att se till att varje enskild person gör bäst nytta där han eller hon placeras för totalförsvarets räkning. Totalförsvaret ska med andra ord ses som en helhet där de tillgängliga personalresurserna måste fördelas på ett rationellt sätt.

Resultatet av MSB:s uppdrag att bedöma behovet av personalförstärkningar inom bevakningsansvariga myndigheter och andra berörda aktörer vid en situation med höjd beredskap och ytterst krig emotses av utskottet. Även det snart tillsatta, tvärsektoriella näringslivsrådet torde kunna vara en resurs i fråga om kompetensförsörjning inom cybersäkerhetsområdet.

Utskottet ser av ovanstående skäl inte något behov av att vidta några ytterligare åtgärder för tillfället när det gäller försörjning av cyberkompetens ur Försvarsmaktens perspektiv. Motionerna 2021/22:3639 (M) yrkandena 11 och 13 samt 2021/22:3245 (C) yrkandena 10 och 11 avstyrks därmed.

Förfogandelagstiftning

Utskottet instämmer med Försvarsberedningen i att dagens regelverk för höjd beredskap och krig ger rättsliga förutsättningar för staten att ingripa i enskilda individers fri- och rättigheter, inklusive att förfoga över resurser som finns i näringslivet för att på så sätt få tillgång till personella och materiella resurser som kan gynna de samlade försvarsansträngningarna. Då utskottet inte ser något skäl att vidta några ytterligare åtgärder på området för tillfället avstyrks motion 2021/22:3245 (C) yrkande 14.

Samhällets förmågeutveckling

Utskottets förslag i korthet

Riksdagen avslår motionsyrkanden om samhällets förmågeutveckling på cybersäkerhetsområdet.

Jämför reservation 15 (M) och 16 (C).

Motionerna

Maria Stockhaus m.fl. (M) anför i kommittémotion 2021/22:3753 yrkande 12 att regeringen ska ta ledningen för att på ett operativt sätt stödja svenska myndigheters säkerhetsarbete.

Motionärerna föreslår vidare att ett fortbildningskrav inom informationssäkerhet införs för personer på ledande positioner inom den offentliga sektorn (yrkande 14).

I kommittémotion 2021/22:3245 av Niels Paarup-Petersen m.fl. (C) föreslår motionärerna

- att MSB:s och Säkerhetspolisens rekommendationer och s.k. best practices utvecklas, förtydligas, anpassas och sprids så att flera olika typer av organisationer får förutsättningar att följa rekommendationerna (yrkande 28)
- att kompetensen i samhället om cybersäkerhet, hot och risker ska breddas via civilsamhället (yrkande 31)
- att kompetensstrategier ska tas fram som höjer kunskapen om cybersäkerhet i offentlig sektor samt hos beslutsfattare (yrkande 34)
- att ett traineesystem ska skapas inom cybersäkerhetsområdet (yrkande 36)
- att det ska utredas om arbete med vissa tjänster ska förutsätta certifiering av kompetens inom cybersäkerhet (yrkande 38)
- att behovet av att stödja olika initiativ för att sprida information som höjer medvetenheten om cybersäkerhet ska lyftas fram (yrkande 39).

I kommittémotion 2021/22:3227 yrkande 25 föreslår Niels Paarup-Petersen m.fl. (C) att kunskapen om, och insatser mot, s.k. deep fakes och andra teknologiska möjligheter med samhällsstörande konsekvenser ska stärkas inom säkerhetsapparaten.

Elisabeth Falkhaven m.fl. (MP) föreslår i kommittémotion 2021/22:4197 yrkande 3 att cybersäkerheten ska stärkas inom offentlig sektor och särskilt samhällsviktiga delar av den privata sektorn.

I motion 2021/22:1078 av Edward Riedl (M) föreslås att den offentliga förvaltningens arbete med informationssäkerhet ska ses över då det under de senaste åren vid flera tillfällen framkommit att svenska myndigheters arbete med informationssäkerhet varit bristfällig.

Larry Söder (KD) föreslår i motion 2021/22:1394 att regeringen ger i uppdrag att utreda möjligheten att placera serverhallar för offentlig verksamhet inom Sveriges gränser.

Bakgrund

Tidigare behandling

I betänkande 2019/20:FöU7 uttryckte sig utskottet positivt om regeringens nationella strategi för samhällets informations- och cybersäkerhet inklusive det arbete som bedrivits sedan denna nationella strategi först publicerades. Utskottet lyfte särskilt fram att regeringen inom ramen för denna strategi avsåg att bl.a. verka för att öka tydligheten i myndighetsstyrningen och lyfta fram betydelsen av ett tillfredsställande informations- och cybersäkerhetsarbete internt på myndigheter, att ta fram en nationell modell för systematiskt arbete och att verka för att samverkan och informationsdelning ska kunna stärkas på

området. Betydelsen av att myndigheterna inom Samverkansgruppen för informationssäkerhet (Samfi) fortsätter att bidra till att stärka informations- och cybersäkerheten i landet underströks.

I betänkande 2020/21:FöU4 uttryckte utskottet likt regeringen att det systematiska arbetet med informations- och cybersäkerhet borde stärkas hos samtliga aktörer. Ökad rapportering av it-incidenter till MSB, anmälan av säkerhetshotande händelser och verksamhet till Försvarsmakten och Säkerhetspolisen samt ökat hänsynstagande till informations- och cybersäkerhetsperspektivet redan i anskaffningsfasen av it-system uttrycktes vara av stor vikt. För ett förstärkt totalförsvar uttrycktes det också som viktigt att myndigheter och organisationer har tillgång till säkra och robusta kommunikationstjänster och nätlösningar med höga säkerhetskrav.

I betänkande 2020/21:FöU6 uttryckte utskottet att arbetet med informations- och cybersäkerhet är något som bör vara ständigt pågående. Utskottet konstaterade vidare att samverkan mellan berörda myndigheter hade inletts under 2020 med anledning av det nationella cybersäkerhetscentret, vilket utskottet ställde sig positivt till, liksom MSB:s fortlöpande arbete inom området.

I betänkande 2021/22:FöU1 gjorde utskottet bedömningen att det fortfarande finns behov av att utveckla samhällets informations- och cybersäkerhet och ansåg att det var bekymmersamt att statliga myndigheters rapportering av it-incidenter hade minskat. Utskottet uttryckte att det avsåg att fortsätta att noga följa utvecklingen av det nya cybersäkerhetscentret till vilket flera myndigheter bidrar.

Pågående arbete

I budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 6) gör regeringen bedömningen att MSB arbetar aktivt för en ökad informationssäkerhet i samhället. Det nya föreskriftspaketet, utbildningsinsatser och arbetet med uppföljningsstrukturen är alla åtgärder som bidrar till en ökad förmåga inom området. Regeringen bedömer vidare att det nyligen inrättade cybersäkerhetscentret kommer att bidra till ökad samordning mellan myndigheterna på området. Det fortsatta arbetet inom ramen för den samlade informations- och cybersäkerhetshandlingsplanen är också viktigt för en väl fungerande samordning och för att uppnå målsättningarna i den nationella strategin för samhällets informations- och cybersäkerhet. Att statliga myndigheters rapportering av it-incidenter har minskat är dock bekymmersamt, menar regeringen, som anser att rapporteringen är viktig både för att öka myndigheternas egen förmåga och för att kunna inrikta arbetet med att utveckla informationssäkerheten i stort. Den rapportering som inkommer från leverantörer av samhällsviktiga och digitala tjänster, inom ramen för lagstiftningen utifrån EU:s direktiv om nätverks- och informationssystem (NIS), utgör också en viktig komponent i detta.

Av budgetpropositionen framgår att MSB i oktober 2020 gav ut ett föreskriftspaket inom informationssäkerhetsområdet. I paketet ingår uppdaterade

föreskrifter om informationssäkerhet och incidentrapportering och nya föreskrifter om säkerhetsåtgärder i informationssystem. Uppdateringarna innebär bl.a. tydligare krav på myndighetsledningar att inrikta, säkerställa resurser och följa upp informationssäkerhetsarbetet, nya krav på säkerhetsåtgärder rörande lokaler och personal samt att det blir enklare för myndigheterna att avgöra vad som ska incidentrapporteras. De nya föreskrifterna om säkerhetsåtgärder i informationssystem ställer minimikrav på vilka säkerhetsåtgärder en statlig myndighet ska ha på plats i den tekniska it-miljön.

MSB arbetade under 2020 med regeringsuppdraget att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen. MSB redovisade uppdraget den 1 mars 2021 och under maj–september 2021 prövades uppföljningsmodellen – som fått namnet Infosäkkollen – för första gången i skarpt läge. MSB mottog under perioden ca 300 svar från myndigheter, regioner och kommuner och påbörjade därefter ett arbete med att sammanställa och analysera resultaten. De organisationer som skickat in sina svar får en kompletterande återkoppling från MSB, som bl.a. inkluderar en jämförelse med liknande organisationer, och den 1 mars 2022 ska MSB redovisa en samlad bedömning till regeringen.

Av budgetpropositionen framgår också att MSB under 2020 arbetade med utbildningsinsatser gentemot offentlig sektor, i enlighet med det regeringsuppdrag som myndigheten fått, bl.a. genom framtagandet av en utbildning för myndighetschefer. MSB har också lanserat en ny version av webbutbildningen Digital informationssäkerhetsutbildning för alla (Disa). Vidare gav regeringen i december 2020 i uppdrag åt FRA, Försvarsmakten, MSB och Säkerhetspolisen att fördjupa samverkan inom cybersäkerhetsområdet genom inrättandet av ett nationellt cybersäkerhetscenter. Tillsammans med övriga myndigheter i Samfi har MSB uppdaterat handlingsplanen för informations- och cybersäkerhet för 2019–2022. Av den uppdaterade handlingsplanen framgår att myndigheterna vid flera tillfällen genomfört extern samverkan med representanter för branschorganisationer, standardiseringsorgan, myndigheter, företag, regioner och kommuner.

Av budgetpropositionen framgår också att FRA, i samverkan med Säkerhetspolisen, har tillgängliggjort ett tekniskt detekterings- och varningssystem (TDV) för fler av de mest skyddsvärda verksamheterna. Under 2020 ökade antalet myndigheter och statliga bolag som använder TDV med 70 procent. Förmågan att förebygga, upptäcka och hantera cyberattacker mot de mest skyddsvärda verksamheterna har stärkts ytterligare, enligt regeringen.

Regeringen beslutade i september 2019 att ge en särskild utredare i uppdrag att kartlägga och analysera statliga myndigheters behov av säker och kostnadseffektiv it-drift samt hur dessa behov tillgodoses. Utredaren skulle vidare analysera säkerhetsmässiga och rättsliga förutsättningar för samordnad statlig it-drift och lämna förslag på mer varaktiga former för sådan it-drift, om det bedömdes lämpligt ur ett säkerhetsperspektiv, och de författningsförslag som detta kräver. I sitt arbete skulle utredningen bl.a. beakta de krav som ställs mot

bakgrund av att planeringen för totalförsvaret har återupptagits. It-driftsutredningen överlämnade sitt delbetänkande Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering (SOU 2021:1) i januari 2021. Slutbetänkandet Säker och kostnadseffektiv it-drift – förslag till varaktiga former för samordnad statlig it-drift (SOU 2021:97) lämnades till Regeringskansliet (Infrastrukturdepartementet) den 15 december 2021. Betänkandet är ute på remiss. Remissvaren ska ha kommit in till Infrastrukturdepartementet senast den 21 mars 2022.

Som tidigare nämnts presenterade utredningen Ansvar, ledning och samordning inom civilt försvar (dir. 2018:79) sitt betänkande Struktur för ökad motståndskraft (SOU 2021:25) i mars 2021. Utöver tio beredskapssektorer har utredningen identifierat fyra särskilda beredskapsområden som omfattar samhällsviktiga verksamheter och funktioner som är av särskild betydelse att upprätthålla vid kris, höjd beredskap och krig. Utredningens bedömning är att dessa områden bör vara en del av beredskapssystemet. Cybersäkerhet (ett samarbete mellan Säkerhetspolisen, MSB, Försvarsmakten och FRA) identifieras som ett sådant område.

Cybersäkerhetsutredningen redogör i sitt slutbetänkande Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem (SOU 2021:63, juli 2021) bl.a. för nivån på informations- och cybersäkerheten i alla myndigheter och ger uttryck för att informations- och cybersäkerheten i statliga myndigheters verksamhet behöver stärkas. Åtgärder bör enligt utredningen därför vidtas som bidrar till att myndigheterna använder certifierade IKT-produkter, IKT-tjänster och IKT-processer i nätverks- och informationssystem i verksamheten om inte detta framstår som olämpligt eller omöjligt att genomföra. IKT står för informations- och kommunikationsteknik. Utredningen bedömer att MSB redan i dag har bemyndigande att i föreskrifter ställa ett sådant krav på statliga myndigheter. En sådan ordning kan även ligga till grund för det nationella arbete med hot-, sårbarhets- och riskbedömningar som utredningen föreslår ska genomföras. När remisstiden gått ut i början på februari kommer förslagen och remissvaren att beredas i vanlig ordning i Regeringskansliet.

Utskottets ställningstagande

Utskottet vidhåller, som det gjorde i betänkande 2020/21:FöU4, att det systematiska arbetet med informations- och cybersäkerhet bör stärkas än mer hos samtliga aktörer i samhället. Utskottet välkomnar därför det arbete som regeringen, enskilda myndigheter, Samfi och det nya nationella cybersäkerhetscentret bedriver till förmån för att stärka både den offentliga och den privata sektorns informations- och cybersäkerhet. Vidare pågår regeringens beredning av betänkanden från Utredningen om civilt försvar, Cybersäkerhetsutredningen och It-driftsutredningen, alla med bäring på området. Utskottet avser också att följa frågan om statliga myndigheters minskade rapportering av it-incidenter, vilket är bekymmersamt ur ett förmågeperspektiv, men ser ändå

inte skäl att för tillfället vidta några ytterligare åtgärder i fråga om detta eller inom området som behandlas i detta avsnitt i övrigt. Motionerna 2021/22:3753 (M) yrkandena 12 och 14, 2021/22:3245 (C) yrkandena 28, 31, 34, 36, 38 och 39, 2021/22:3227 (C) yrkande 25, 2021/22:4197 (MP) yrkande 3, 2021/22:1078 (M) och 2021/22:1394 (KD) avstyrks.

Samverkan med näringslivet

Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om samverkan med näringslivet.

Jämför reservation 17 (M).

Motionerna

Pål Jonson m.fl. (M) föreslår i kommittémotion 2021/22:3639 yrkande 7 att länken och samarbetet mellan staten och näringslivet ska fördjupas på cyberområdet. I samma motion yrkande 12 föreslås att FRA får ett utökat uppdrag att skydda samhällsviktiga företag från cyberattacker.

I kommittémotion 2021/22:3640 av Pål Jonson m.fl. (M) yrkande 16 anför motionärerna att åtgärder behöver vidtas dels för att tillvarata näringslivets resurser i händelse av kris och krig, dels för att skydda svenskt näringsliv från cyberhot. I yrkande 17 anför motionärerna att det behövs en översyn av hur samhällsviktiga svenska företag kan få stöd för att upptäcka och motverka spionage och attacker mot sin verksamhet.

Bakgrund

Tidigare behandling

I betänkandena 2019/20:FöU7, 2020/21:FöU4 och 2020/21:FöU7 betonade utskottet näringslivets roll i såväl krishantering som försörjningsberedskap. Vidare framhöll utskottet att en långsiktig samverkan mellan offentliga och privata aktörer på den centrala, regionala och lokala nivån i Sverige bör etableras.

Utskottet har även i betänkande 2020/21:FöU6 uttryckt att samverkan mellan staten och näringslivet inom cybersäkerhetsområdet är av stor vikt. Utskottet lyfte då att mycket av den samhällsviktiga verksamheten ägs och drivs av näringslivet. Utskottet noterade också att det pågår arbeten på flera håll, bl.a. genom inrättandet av det nya nationella cybersäkerhetscentret och genom olika samverkansprogram där det arbetas med frågan kring samverkan mellan staten och näringslivet, och såg därför inte något skäl att vidta några åtgärder.

I betänkande 2020/21:FöU4 välkomnade utskottet regeringens bedömning att en långsiktig samverkan mellan offentliga och privata aktörer på den centrala, regionala och lokala nivån behöver etableras. Likt regeringen ansåg utskottet att Utredningen om civilt försvars uppdrag att föreslå en sektorsindelning för statliga myndigheter och vilka myndigheter som ska ges ett särskilt ansvar för krisberedskapen och civilt försvar borde skapa goda förutsättningar för arbetet med att utveckla och förtydliga samverkan med näringslivet (SOU 2015:25 Struktur för ökad motståndskraft).

Pågående arbete

Enligt budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 6) ska all samhällsverksamhet kunna bedrivas under högsta beredskap. Riksdagen, regeringen, statliga myndigheter inklusive länsstyrelser, kommuner och regioner, näringsliv, frivilligorganisationer samt enskilda individer är alla delar av, och förutsätts bidra till, totalförsvaret. Arbetet med att integrera näringslivet i totalförsvarsplaneringen har påbörjats på samtliga nivåer. Arbetet har bl.a. utgått från förslag i Försvarsberedningens rapport Motståndskraft (Ds 2017:66), slutrapporten Värnkraft (Ds 2019:8) samt betänkandet Näringslivets roll inom totalförsvaret (SOU 2019:51).

Regeringen kommer enligt budgetpropositionen för 2022 att verka för att den svenska försörjningsberedskapen utvecklas och att näringslivet i ökad utsträckning involveras i arbetet med att säkerställa de viktigaste samhällsfunktionerna. Regeringen anser att det privata näringslivets involvering i planeringsarbetet bör öka. I nära dialog med privata aktörer bör offentliga aktörer bedöma behovet av förberedelser för att säkerställa en rimlig beredskap. För att utveckla samverkan mellan det offentliga och privata framgår det av budgetpropositionen att ett tvärsektoriellt näringslivsråd ska inrättas. Rådet ska bl.a. vara en plattform för informationsutbyte. Justitiedepartementet uppger att det tvärsektoriella näringslivsrådet är planerat att tillsättas före sommaren 2022.

Tillsammans med övriga myndigheter i Samfi har MSB enligt budgetpropositionen uppdaterat handlingsplanen för informations- och cybersäkerhet för 2019–2022. Av den uppdaterade handlingsplanen framgår att myndigheterna vid flera tillfällen genomfört extern samverkan med representanter för branschorganisationer, standardiseringsorgan, myndigheter, företag, regioner och kommuner.

Inom områden som exempelvis transportsektorn samt hälso- och sjukvården pågår i dag arbete med att utveckla och förtydliga samverkan med näringslivet. Regeringen uttrycker i proposition 2020/21:30 Totalförsvaret 2021–2025 att samverkan som sker områdes- och sektorsvis behöver stärkas ytterligare.

Inom ramen för det nyinrättade cybersäkerhetscentret ska de deltagande myndigheterna bl.a. koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter samt förmedla råd och stöd i fråga om

hot, sårbarheter och risker. Samverkan med den privata sektorn är också en viktig del av centrets uppdrag.

Enligt tidigare inrikesminister Mikael Dambergs svar på skriftlig fråga 2021/22:236 har regeringen en tät dialog med de ansvariga myndigheterna om verksamheten och den fortsatta inriktningen. Vidare uttryckte statsrådet att företag som verkar i Sverige har eget ansvar för sin motståndskraft mot cyberhot. Särskilda krav ställs på leverantörer av samhällsviktiga och digitala tjänster enligt lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster och på de som bedriver säkerhetskänslig verksamhet enligt säkerhetsskyddslagen (2018:585).

Regeringen gav år 2018 MSB i uppdrag att bidra till att öka små och medelstora företags och allmänhetens kunskaper om informationssäkerhet. Tillsammans med ett stort antal aktörer utformade MSB en informationskampanj, med vilken myndigheten nått ut brett enligt tidigare inrikesminister Dambergs svar på skriftlig fråga 2021/22:236.

Regeringen gav 2018 MSB i uppdrag att bidra till att öka små och medelstora företags och allmänhetens kunskaper om informationssäkerhet. Tillsammans med ett stort antal aktörer utformade MSB en informationskampanj, med vilken myndigheten nått ut brett enligt tidigare inrikesminister Dambergs svar på skriftlig fråga 2021/22:236.

I juni 2021 lanserade MSB en strategi för försörjningsberedskapen med fokus på samverkan med näringslivet. Strategin kan enligt MSB ses som ett ramverk för att utveckla det gemensamma arbetet för försörjningsberedskapen.

Utskottets ställningstagande

Utskottet vidhåller det som uttrycktes i betänkande 2020/21:FöU6 om att samverkan mellan staten och näringslivet inom cybersäkerhetsområdet är av stor vikt. Mycket av den samhällsviktiga verksamheten ägs och drivs av näringslivet i dag.

Utskottet vill i sammanhanget betona vikten av det systematiska arbetet med informations- och cybersäkerhet hos samtliga aktörer i samhället, såväl inom offentlig sektor som inom privat sektor. Informations- och cybersäkerhet angår sålunda hela samhället och samtliga aktörer behöver ta ansvar.

Utskottet välkomnar det arbete som regeringen, enskilda myndigheter, Samfi, det nya nationella cybersäkerhetscentret m.fl. bedriver till förmån för att stärka samverkan mellan den offentliga och den privata sektorn inom informations- och cybersäkerhet. Utskottet välkomnar även tillkomsten av det tvärsektoriella näringslivsrådet som har långsiktig samverkan med privata och offentliga aktörer som en central del i sitt uppdrag. Utskottet ser sammantaget inte skäl att vidta några ytterligare åtgärder i frågan. Motionerna 2021/22:3639 (M) yrkandena 7 och 12 samt 2021/22:3640 (M) yrkandena 16 och 17 avstyrks därmed.

Cybersäkerhet på universitet och högskolor

Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om cybersäkerhet på universitet och högskolor.

Jämför reservation 18 (M, KD).

Motionerna

I kommittémotion 2021/22:3640 anför Pål Jonson m.fl. (M) i yrkande 18 att de svenska underrättelsemyndigheterna bör få ett regeringsuppdrag att utveckla en strategi för hur svenska universitet och högskolor ska stärka sin säkerhet och kunna arbeta med screening i säkerhetskänslig forskning samt vid behov samarbeta med exempelvis Säkerhetspolisen, den militära underrättelse- och säkerhetstjänsten (Must) och FRA.

Enligt kommittémotion 2021/22:4161 av Pia Steensland m.fl. (KD) yrkande 32 bör underrättelsemyndigheterna få i uppdrag att utveckla en strategi för hur svenska universitet och högskolor ska stärka sin säkerhet och minska risken för spionage och stöld.

Bakgrund

Tidigare behandling

Utskottet har i yttrandena 2019/20:FöU5y och 2020/21:FöU5y betonat betydelsen av att ha en god förmåga att skydda näringsliv och forskning från industrispionage. I båda yttrandena uttryckte utskottet att de svenska underrättelsemyndigheterna spelar en stor roll i sammanhanget och att det är av vikt att relevanta myndigheter samverkar när det gäller underrättelseverksamhet och påverkanskampanjer. Utskottet bedömde i båda yttrandena att det bör göras noggranna överväganden innan nya uppdrag ges till berörda myndigheter med tanke på redan givna uppdrag och resursbehov. Utskottet underströk i yttrande 2020/21:FöU5y vikten av det som regeringen anfört i proposition 2020/21:60 om att fortsätta följa frågan om spionage och se över behovet av ytterligare åtgärder för att säkerställa att skyddsvärd verksamhet och kunskap vid universitet och högskolor inte riskerar att hamna i orätta händer.

Utskottet lyfte i 2020/21:FöU5y att det övergripande målet att totalförsvaret ska ha förmåga att försvara Sverige och värna vår säkerhet, frihet, självständighet och handlingsfrihet innefattar arbetet med att hantera en breddad hotbild, vilken även inkluderar hoten mot skyddsvärd verksamhet vid universitet och högskolor.

Vidare framhöll utskottet i betänkande 2020/21:FöU4 att det krävs en stark säkerhetstjänst och försvarsunderrättelseförmåga för att kunna förebygga och identifiera hotande verksamhet, god förmåga att upptäcka och hantera intrång samt ett starkt skydd av de mest skyddsvärda verksamheterna i samhället.

Samarbetet mellan FRA, Försvarsmakten och Säkerhetspolisen betonades ha ett betydande värde för de mest skyddsvärda verksamheterna i Sverige.

Pågående arbete

I det gemensamma regleringsbrevet för svenska universitet och högskolor för 2022 har samtliga universitet och högskolor fått i uppdrag att redogöra för hur de arbetar med informationssäkerhet. Berörda universitet och högskolor ska redogöra för hur de arbetar för att stärka sin informationssäkerhet och för hur de planerar för att möta framtida behov, bl.a. utifrån den ökade digitaliseringen i verksamheten. I redogörelsen ska det ingå en redovisning av hur lärosätena arbetar för att säkerställa informationssäkerheten vid forskning, undervisning och examination på distans.

Behovet av att beakta nationella säkerhetsaspekter i forskningsintensiva verksamheter framgår av regeringens Strategi för svensk rymdverksamhet (skr. 2017/18:259) respektive Nationell inriktning för artificiell intelligens (N 2018:14). I regeringens skrivelse Arbetet i frågor som rör Kina (skr. 2019/20:18) konstateras att ett stort ansvar vilar på universitet och högskolor och det forskningsintensiva näringslivet när det gäller värderingen och säkerställandet av skydd för svensk forskning.

I svar på skriftlig fråga 2020/21:1762 angav statsrådet Matilda Ernkrans att regeringen kommer att fortsätta följa frågan om spionage och se över behovet av ytterligare åtgärder i syfte att säkerställa att skyddsvärd verksamhet och kunskap vid universitet och högskolor inte riskerar att hamna i orätta händer.

Av Säkerhetspolisens årsbok för 2020 framgår att Säkerhetspolisen under året genomförde kunskapshöjande insatser på samhällsinstitutioner, inklusive universitet och högskolor, om hotet från statliga aktörer. Bland annat riktade Säkerhetspolisen under 2020 sig till säkerhetsskyddschefer och personal från universitet och högskolor.

Vidare anges i budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 16) att regeringen gett Vetenskapsrådet i uppdrag att finansiera forskning om cyber- och informationssäkerhet med 5 miljoner kronor (U2021/01515).

Utskottets ställningstagande

Utskottet anser, likt vad som anfördes i yttrandena 2019/20:FöU5y och 2020/21:FöU5y, att det är viktigt att Sverige har en god förmåga att skydda näringsliv och forskning från industrispionage, vilket även innefattar ett utvecklat informations- och cybersäkerhetsarbete. De svenska underrättelsemyndigheterna spelar en viktig roll i sammanhanget och det är centralt att relevanta myndigheter samverkar när det gäller bl.a. underrättelseverksamhet och påverkanskampanjer.

För att svenska högskolor och universitet ska kunna stärka sin informations- och cybersäkerhet är det av största vikt att det bedrivs ett strukturerat förebyggande arbete i samverkan med andra ansvariga myndigheter och att

andra åtgärder utifrån säkerhetsskyddslagen och övrig lagstiftning som myndigheter är skyldiga att följa efterlevs.

Utskottet ser positivt på att svenska universitet och högskolor i regleringsbrevet för 2022 fått i uppdrag att redovisa hur de arbetar med informationssäkerhet, och utskottet kommer att följa det arbetet. Också med anledning av regeringens övriga arbete samt Säkerhetspolisens och Vetenskapsrådets genomförda aktiviteter ser utskottet inte skäl att för tillfället vidta några ytterligare åtgärder på området. Motionerna 2021/22:3640 (M) yrkande 18 och 2021/22:4161 (KD) yrkande 19 avstyrks.

It-upphandlingar ur ett cybersäkerhetsperspektiv

Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om it-upphandlingar ur ett cybersäkerhetsperspektiv.

Jämför reservation 19 (M) och 20 (C).

Motionerna

Pål Jonson m.fl. (M) föreslår i kommittémotion 2021/22:3639 yrkande 9 att offentlig sektor ska kunna använda lagen om upphandling på försvars- och säkerhetsområdet (LUFS) i större utsträckning eftersom lagen om offentlig upphandling (LOU) kan vara ett problem vid offentliga aktörers upphandling av it-drift då frågor om cyber- och informationssäkerhet inte prioriteras lika högt som lägre pris.

I kommittémotion 2021/22:3245 yrkande 22 av Niels Paarup-Petersen m.fl. (C) framhåller motionärerna att tydligare krav när det gäller funktionalitet och säkerhet behöver ställas vid upphandlingar. I samma motion yrkande 23 föreslås att oberoende säkerhetsgenomgångar blir ett krav vid större upphandlingar. I samma motion yrkande 27 efterfrågas minimistandarder och funktionskrav för upphandling av samhällsviktig verksamhet.

Bakgrund

Tidigare behandling

I betänkande 2017/18:FöU4 gav utskottet stöd åt regeringens syn att stödet vid upphandling av säker elektronisk kommunikation och andra it-relaterade tjänster bör stärkas och att det är av vikt att de verksamheter som har behov av en hög nivå av driftssäkerhet inom kommunikationsnät och it-relaterade tjänster ställer krav på detta vid upphandling.

Vidare har utskottet i betänkande 2020/21:FöU4 uttryckt att förutsättningen för ett starkt cyberförsvar är att alla aktörer inom totalförsvaret har en god informations- och cybersäkerhet. Utskottet ansåg likt regeringen i proposi-

tionen Totalförsvaret 2021–2025 (prop. 2020/21:30) att det systematiska arbetet med informations- och cybersäkerhet bör stärkas hos samtliga aktörer. Vidare betonade utskottet att en ökad rapportering av it-incidenter till MSB, anmälan av säkerhetshotande händelser och verksamhet till Försvarsmakten och Säkerhetspolisen samt ökat hänsynstagande till informations- och cybersäkerhetsperspektivet redan i anskaffningsfasen av it-system är av stor vikt. För ett förstärkt totalförsvar uttrycktes det också som viktigt att myndigheter och organisationer har tillgång till säkra och robusta kommunikationstjänster och nätlösningar med höga säkerhetskrav.

Pågående arbete

I budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 6) redogör regeringen för bedömningen att MSB arbetar aktivt för en ökad informationssäkerhet i samhället. Det nya föreskriftspaketet, utbildningsinsatser och arbetet med uppföljningsstrukturen är alla åtgärder som bidrar till en ökad förmåga inom området. Regeringen bedömer vidare att det nyligen inrättade cybersäkerhetscentret kommer att bidra till ökad samordning mellan berörda myndigheter på området.

MSB beskriver i rapporten Upphandla informationssäkert – en vägledning hur aktörer inom offentlig sektor ska upphandla informationssäkert. Vägledningen ska vara ett stöd för hur krisberedskapsaspekter såsom kontinuitet, funktionalitet och leveransförmåga kan säkerställas vid upphandling till samhällsviktig verksamhet. Bland annat ger myndigheten exempel på standarder som kan användas vid upphandling av olika typer av tjänster.

I den samlade informations- och cybersäkerhetshandlingsplanen för 2019–2022 finns 77 åtgärder som MSB, FRA, FMV, Försvarsmakten, PTS, Polismyndigheten och Säkerhetspolisen enskilt, tillsammans eller i samverkan med andra aktörer avser att vidta för att höja informations- och cybersäkerheten i samhället. Samtliga 77 åtgärder i handlingsplanen ansluter till någon eller några av de sex strategiska prioriteringar som regeringen beslutat om i den nationella strategin för samhällets informations- och cybersäkerhet (skr. 2016/17:213). Åtgärderna syftar bl.a. till att stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter. Av handlingsplanen framgår att Säkerhetspolisen och Försvarsmakten under 2019–2022 ska ta fram nya vägledningar och utbildningsmaterial vilka kommer att omfatta informationssäkerhet och säkerhetsskyddade upphandlingar. Det framgår även att FMV ska medverka i svenska och internationella standardiseringsorgan och forum för att utveckla och förbättra standarder för kravställning och utvärdering av it-säkerhet och kryptografi.

Regeringen gav i november 2019 Upphandlingsmyndigheten i uppdrag att ge förstärkt stöd vid upphandlingar av samhällsviktig verksamhet samt varor och tjänster till sådan verksamhet. I uppdraget ingår att informera om och ge vägledning om de regler som kan aktualiseras vid upphandlingar så att leveranssäkerhet och krisberedskap säkerställs på ett systematiskt och strategiskt

sätt i upphandlande organisationers inköpsarbete. Uppdraget ska slutredovisas i myndighetens årsredovisning för 2021.

Statliga myndigheter som avser att genomföra en upphandling som innebär krav på säkerhetsskyddsavtal ska innan förfarandet inleds samråda med Säkerhetspolisen enligt 2 kap. 6 § säkerhetsskyddslagen. Innan samrådet kan ske ska verksamhetsutövaren genomföra en särskild säkerhetsskyddsbedömning.

Utskottets ställningstagande

Utskottet vill likt i betänkande 2017/18:FöU4 framhålla att stödet vid upphandling av säker elektronisk kommunikation och andra it-relaterade tjänster bör stärkas och att det är av vikt att de verksamheter som har behov av en hög nivå av driftssäkerhet inom kommunikationsnät och it-relaterade tjänster ställer krav på detta vid upphandling. Ett lågt pris bör med andra ord inte alltid styra inför upphandlingar. Utskottet noterar MSB:s arbete med att stödja aktörer inom offentlig sektor i informationssäker upphandling genom bl.a. utbildningar, handlingsplaner och vägledningar.

Utskottet välkomnar också uppdraget som Upphandlingsmyndigheten fått av regeringen att ge förstärkt stöd vid upphandlingar av samhällsviktig verksamhet och kommer att fortsätta att följa frågan.

Eftersom utskottet bedömer att regeringen redan verkar för att myndigheternas kompetens i upphandling av nätverk, produkter och system stärks på ett positivt sätt ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motionerna 2021/22:3639 (M) yrkande 9 och 2021/22:3245 (C) yrkandena 22, 23 och 27 avstyrks.

Internationella överenskommelser

Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om internationella överenskommelser.

Jämför reservation 21 (M) och 22 (C).

Motionerna

Pål Jonson m.fl. (M) anför i kommittémotion 2021/22:3639 yrkande 8 att regeringen bör främja ett djupare samarbete inom Norden och EU samt med Nato på cybersäkerhetsområdet.

I kommittémotion 2021/22:3245 yrkande 6 av Niels Paarup-Petersen m.fl. (C) föreslås förtroendeskapande åtgärder på det internationella cybersäkerhetsområdet.

Maria Nilsson (L) yrkar i motion 2021/22:2279 att regeringen ska verka för att det inrättas en cybersolidaritetspakt mellan demokratier. Cybersolidaritetspakten ska enligt motionären göra det mer kostsamt för angripare att genomföra attacker.

I motion 2021/22:2351 av Robert Hannah (L) yrkar motionären att regeringen ska verka för skapandet av en FN-konvention om cyberkrigföring. Motionären menar att en sådan FN-konvention skulle ge tydliga spelregler om cyberkrigföring och även skydda civila människor från kränkningar av civila eller mänskliga rättigheter.

Bakgrund

Tidigare behandling

Utskottet uttryckte i betänkande 2017/18:FöU4 vikten av internationellt samarbete för att främja informations- och cybersäkerheten eftersom den digitala utvecklingen är gränslös. Utskottet har även i yttrandena 2018/19:FöU3y, 2020/21:FöU3y samt 2020/21:FöU8y uttryckt vikten av EU:s arbete för förstärkt cybersäkerhet mot bakgrund av det snabbt växande hybridhot som utmanar säkerheten i Europa.

I utskottets betänkande 2017/18:FöU4 om den nationella strategin för samhällets informations- och cybersäkerhet ansåg utskottet likt regeringen att det är viktigt att Sverige verkar för att stärka sitt samlade agerande inom relevanta internationella samarbeten. Exempel på samarbeten som lyftes var FN och Nato och samarbeten med likasinnade länder, t.ex. de nordiska, för att stärka internationella samarbeten på området.

Pågående arbete

I budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 6) redogör regeringen för att det nordiska försvarssamarbetet, Nordic Defence Cooperation (Nordefco) fortsatte att utvecklas under 2020. Fokus under 2020 var enligt regeringen att stärka och utveckla samarbetet i fred, kris och konflikt inom överenskomna områden. Cybersäkerhet och de militära delarna av totalförsvaret var prioriterade samarbetsområden under 2020.

I budgetpropositionen redogörs även för de internationella övningar som genomförts med svenskt deltagande, såsom Cyber Storm och NATO Cyber Coalition.

För att stärka det internationella samarbetet inom cybersäkerhetsområdet uppger regeringen på sin webbplats att man bl.a. har ett pågående arbete i Organisationen för säkerhet och samarbete i Europa (OSSE) om förtroendeskapande åtgärder för hantering av cyberincidenter med säkerhetspolitiska återverkningar.

Av webbplatsen framgår också att arbete inom rådsarbetsgrupper och kommittéer inom EU genomförs kopplat till cybersäkerhetsområdet, t.ex. genom-

förandet av EU:s interna cybersäkerhetsarbete och det s.k. cybersäkerhetspaket som antogs 2017 samt genomförandet av EU:s externa cybersäkerhetsarbete i form av t.ex. EU:s diplomatiska verktygslåda, t.ex. genom antagande av en tematisk cybersanktionsregim och framtagande av gemensamma målsättningar för FN och globala processer. Dessutom sker bilaterala dialoger med länder i Norden, EU och på global nivå löpande.

I skrivelse 2016/17:213 uppger regeringen att man ska verka för att stärka internationella samarbeten kring cybersäkerhet och cyberförsvar för att hantera hot och sårbarheter, stärka internationella samarbeten kring tillämpningen av internationell rätt och förebyggande av konflikter, t.ex. genom etablering av frivilliga normer och förtroendeskapande åtgärder, samt främja ett öppet, fritt och säkert internet till stöd för mänskliga rättigheter och global utveckling.

Ett av det nya cybersäkerhetscentrets uppdrag är samordning och att utgöra en kontaktpunkt för internationella samarbeten på myndighetsnivå inom cybersäkerhetscentrets verksamhet.

Av MSB:s årsredovisning för 2020 framgår att MSB under 2020 utökade och fördjupade internationell samverkan med koppling till NIS-direktivet, bl.a. genom deltagande i ett ökat antal internationella arbetsgrupper.

Utskottets ställningstagande

Eftersom cyberhoten är oberoende av nationella gränser förutsätter arbetet med cybersäkerhet internationellt samarbete. Internationella samarbeten kring cybersäkerhet, tillika inom EU, är sålunda centrala för att hantera cyberhot och cyberangrepp. Utskottet noterar regeringens arbete med att stärka detta samarbete inom cybersäkerhetsområdet och ser också positivt på det nya cybersäkerhetscentrets uppdrag att samordna och utgöra en plattform för internationellt samarbete inom området.

Utskottet välkomnar bl.a. hur regeringen verkar för att stärka det internationella samarbetet inom Nato, FN och OSSE och med andra nordiska länder i fråga om cybersäkerhet. Också MSB har bidragit till att fördjupa den internationella samverkan kring cybersäkerhet. Sammanfattningsvis ser inte utskottet skäl att för tillfället vidta några ytterligare åtgärder på området. Motionerna 2021/22:3639 (M) yrkande 8, 2021/22:3245 (C) yrkande 6, 2021/22:2279 (L) och 2021/22:2351 (L) avstyrks.

Arbetet inom EU

Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om arbetet inom EU.
Jämför reservation 23 (M) och 24 (C).

Motionerna

Jessika Roswall m.fl. (M) föreslår i kommittémotion 2021/22:3775 yrkande 26 att regeringen ska verka för att EU:s cyberförsvar stärks.

I kommittémotion 2021/22:3245 yrkande 7 av Niels Paarup-Petersen m.fl. (C) föreslår motionärerna att EU ska ges en större roll i frågor som rör standarder för cybersäkerhet.

I samma motion yrkande 8 föreslås att regeringen ska verka för att EU får till uppgift att koordinera enskilda medlemsländers expertresurser inom cyberområdet om ett land utsätts för en omfattande cyberattack som det inte kan klara av själv och landets myndigheter ber om stöd.

I yrkande 25 i samma motion anförs att ny svensk lagstiftning måste ta hänsyn till den svenska konkurrenskraften, och begränsningar inom cybersäkerhetsområdet bör därför helst tas fram inom ramen för det gemensamma EU-samarbetet.

Bakgrund

Tidigare behandling

Utskottet har i bl.a. yttrande 2017/18:FöU1y framhållit vikten av EU-samarbeten för att möta globala utmaningar.

I betänkande 2017/18:FöU4 ställde sig utskottet bakom regeringens förslag till lag om informationssäkerhet för samhällsviktiga och digitala tjänster i syfte att genomföra EU:s s.k. NIS-direktiv (dvs. direktivet om nät- och informationssäkerhet). Utskottet ansåg i betänkandet att det är nödvändigt med samarbete både inom EU och internationellt för att främja informations- och cybersäkerheten eftersom den digitala utvecklingen är gränslös. I betänkandet instämde utskottet i regeringens bedömning att Sverige bör verka för att fortsätta sitt ledarskap inom EU på det digitala området och driva den digitala agendan framåt.

Utskottet noterade i betänkande 2020/21:FöU4 att regeringen arbetar aktivt med de insatser som görs inom EU för att stärka cybersäkerheten och att ett europeiskt kompetenscentrum för cybersäkerhet ska inrättas.

Regeringens förslag om kompletterande bestämmelser till EU:s cybersäkerhetsakt välkomnades av utskottet i betänkande 2020/21:FöU6. Genom cybersäkerhetsakten har EU sedan juni 2019 infört en gemensam certifieringsram som har som syfte att skapa förtroende samt öka tillväxten på cybersäker-

hetsmarknaden inom hela unionen. Vidare tillhandahålls en omfattande uppsättning regler, standarder och tekniska krav på produkter, tjänster och processer genom certifieringsramen.

I yttrande 2021/22:FöU2y lyfte utskottet vikten av att EU och Nato gemensamt ska kunna nyttja gemensamma resurser effektivt och på ett ändamålsenligt sätt kunna mobilisera resurser för att möta utmaningar på försvars- och säkerhetsområdet.

Utskottet ställde sig i yttrande 2020/21:FöU3y positivt till att kommissionen lyft fram förslaget om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum (COM(2018) 630).

Pågående arbete

Regeringen uppger i budgetpropositionen för 2022 (prop. 2021/22:1 utg.omr. 6) att arbetet med att stärka både den digitala och den fysiska infrastrukturen inom EU är angeläget. Regeringen anser att målsättningar kring cybersäkerhet bör vara högt ställda.

Regeringen följde enligt budgetpropositionen för 2022 under 2020 utvecklingen av EU-kommissionens arbete med försvarsfrågor, inklusive inrättandet av ett generaldirektorat för försvarsindustri och rymd samt det generella arbetet inom EU med hanteringen av hybridhot och cybersäkerhet.

Av budgetpropositionen framgår vidare att regeringen har för avsikt att etablera ett nationellt samordningscenter på MSB kopplat till Europeiska kompetenscentret för cybersäkerhet inom näringsliv, teknik och forskning (ECCC). Samordningscentret ska kunna inrättas vid myndigheten under 2022 enligt regeringsuppdraget till MSB. ECCC kommer att vara EU:s huvudorgan för investeringar i cybersäkerhetsforskning, cybersäkerhetsteknik och industriell utveckling av cybersäkerhet samt för genomförande av projekt och initiativ tillsammans med nätverket av nationella samordningscenter. EU-organet kommer också att ge expertstöd, utfärda vägledningar och dela kunskap inom cybersäkerhetsområdet.

Sedan den 28 juni 2021 är bestämmelserna om cybersäkerhetscertifiering i Europaparlamentets och rådets förordning (EU) 2019/881 tillämpliga i Sverige. I lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt och förordningen (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt finns bestämmelser om bl.a. nationell myndighet för cybersäkerhetscertifiering, tillsyn och sanktioner. Syftet med det nya regelverket är att skapa förutsättningar för att inom EU uppnå en hög nivå på cybersäkerhet i produkter, tjänster och processer inom området informations- och kommunikationsteknik. Regeringen bedömer att det fortsatta arbetet på EU-nivå behöver ske i samarbete mellan berörda myndigheter och aktörer i näringslivet.

EU arbetar med två lagstiftningsförslag för att stärka cybersäkerheten inom unionen, ett uppdaterat direktiv för att bättre skydda nätverks- och informationssystem (NIS 2) samt ett nytt direktiv om kritiska enheters resiliens (CER). NIS-direktivet infördes 2016 som den allra första lagstiftningsåtgärden inom EU med syftet att öka samarbetet mellan medlemsländerna i fråga om cybersäkerhet. Genom direktivet fastställdes säkerhetsrelaterade skyldigheter för leverantörer av samhällsviktiga tjänster (inom kritiska sektorer som t.ex. energi och transport) och leverantörer av digitala tjänster. I december 2020 föreslog kommissionen ett reviderat NIS-direktiv (NIS 2) som skulle ersätta direktivet från 2016. I december 2021 antog Europeiska rådet en allmän riktlinje om det nya NIS 2-direktivet. Det franska ordförandeskapet räknar med intensiva trepartssamtal under de första tre månaderna enligt Regeringskansliet. Trepartsförhandlingarna om CER-direktivet inleds i januari/februari 2022. Från mars månad planerar det franska ordförandeskapet för två till tre förhandlingsmöten per månad.

Den 23 juni 2021 lade kommissionen fram en vision om att bygga upp en ny gemensam cyberenhet (Joint Cyber Unit) för att hantera det ökande antalet allvarliga cyberincidenter som påverkar offentliga tjänster, företag och allmänheten i hela EU. Den gemensamma cyberenheten syftar till att sammanföra resurser och expertis inom EU och dess medlemsländer för att effektivt förebygga, avskräcka och reagera på storskaliga cyberincidenter och cyberkriser. Den gemensamma cyberenheten kommer att fungera som en plattform för att säkerställa EU:s samordnade insatser vid storskaliga cyberincidenter och cyberkriser samt för att erbjuda hjälp med att återhämta sig från sådana attacker. Målet är att den gemensamma cyberenheten inleder sin Verksamhet senast den 30 juni 2022 och att den är fullt utbyggd ett år senare, senast den 30 juni 2023.

EU:s cybersäkerhetsstrategi är vidare ett centralt inslag inom EU:s digitala framtid. Cybersäkerhetsstrategin är en del i ett paket av åtgärder som syftar till att förbättra resiliensen i såväl den digitala som den fysiska infrastrukturen hos den offentliga och privata sektorn och unionen i dess helhet. I strategin finns också förslag som ska stärka EU:s verktygslåda för cyberdiplomati för att förebygga och motverka cyberhot och cyberkriser, särskilt sådan verksamhet som påverkar kritisk infrastruktur. Dessutom föreslås en ny arbetsgrupp där cyberrelaterad underrättelseinformation ska kunna delas.

Utskottets ställningstagande

Eftersom cybersäkerhetshoten är gränsöverskridande och med tanke på de ständigt ökande komplexa angreppen, anser utskottet att det är av stor vikt att kunna bemöta cyberhot på ett samordnat sätt inom EU. Det är därför angeläget att se över och utveckla resurser och system för att stärka kapaciteten att gemensamt inom unionen kunna hantera cyberincidenter och cyberkriser. Utskottet är positivt till kommissionens vision om en gemensam cyberenhet som

syftar till att sammanföra resurser och expertis inom EU och dess medlemsländer för att effektivt förebygga, avskräcka och reagera på storskaliga cyberincidenter. Alla berörda aktörer i EU måste vara beredda att agera kollektivt vid cyberincidenter. Vidare noterar utskottet att regeringen arbetar med de aktiviteter som bedrivs inom EU för att stärka cybersäkerheten och att ett europeiskt kompetenscentrum för cybersäkerhet ska inrättas. Utskottet anser att det är viktigt att denna utveckling fortsätter och kommer även fortsättningsvis att följa regeringens och EU:s arbete med dessa frågor. Utskottet ser inte skäl att för tillfället vidta några ytterligare åtgärder. Motionerna 2021/22:3775 (M) yrkande 26 och 2021/22:3245 (C) yrkandena 7, 8 och 25 avstyrks.

Reservationer

1. En översyn av cybersäkerhetsområdet, punkt 1 (M, KD)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M), Mikael Oscarsson (KD) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2021/22:3368 av Viktor Wärnick m.fl. (M) yrkande 20 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 1 och 2 samt
avslår motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del,
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del och
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 24.

Ställningstagande

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

På ett antal områden finns det en stor förbättringspotential. Det behövs ett samlat grepp kring hur Sverige kan stärka och kontinuerligt arbeta med cybersäkerhet. Etablerandet av det nya cybersäkerhetscentret är en viktig byggsten i detta arbete.

Vi vill därför initiera en större utredning som ska stödja och utveckla en svensk cybersäkerhetsstrategi. Utredningen bör ha en bred ansats och utgå från 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. Utredningen ska kontinuerligt stärka en skarp svensk cybersäkerhetsstrategi som utgör en del av den svenska nationella säkerhetsstrategin.

Vi föreslår sålunda att regeringen ska genomföra en översyn av cybersäkerhetsområdet med tydliga delredovisningar och att Sverige ska få en ny cyberstrategi. Vi vill i sammanhanget understryka vikten av ett starkt försvar mot yttre påverkan och att det brådskar med att den nya myndigheten för psykologiskt försvar och det nya cybersäkerhetscentret kommer till stånd och blir fullt verksamma.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

2. En översyn av cybersäkerhetsområdet, punkt 1 (SD)

av Roger Richthoff (SD), Caroline Nordengrip (SD) och Per Söderlund (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del och
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del och
avslår motionerna
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 24,
2021/22:3368 av Viktor Wärnick m.fl. (M) yrkande 20 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 1 och 2.

Ställningstagande

Spridningen av informationsteknik har varit en mycket viktig del i globaliseringen som knutit samman länder på ett sådant sätt att man i dag har omedelbar tillgång till hela världen. Informationsteknologin kan dock användas för både positiva och negativa ändamål. Spionerи och regelrätta cyberattacker över nätet har blivit vardag. Militär underrättelsetjänst, terrorister och organiserad brottslighet kommer att fortsätta att använda sig av informationsteknologi i allt högre utsträckning, inte minst för att det är billigt och svårspårbart och man når hela världen. Detta gör det allt viktigare att vidta adekvata åtgärder för att skydda och försvara vitala nationella intressen mot cyberhot. Vi föreslår därför att en samordnande myndighet ges i uppdrag att ansvara för att den offentliga sektorn skyddas mot cyberangrepp.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

3. En översyn av cybersäkerhetsområdet, punkt 1 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 24 och
avslår motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del,
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del,
2021/22:3368 av Viktor Wärnick m.fl. (M) yrkande 20 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 1 och 2.

Ställningstagande

Det offentliga är bara en liten del av det svenska samhället. Ska Sverige ha ett bättre cybersäkerhetsskydd är det alltså inte bara det offentliga Sverige som behöver ett bättre skydd. Det gäller också för näringslivet, civilsamhället och inte minst den enskilda medborgaren. För den enskilda medborgaren är den avgörande insatsen en ökad säkerhetsmedvetenhet.

När det kommer till cybersäkerhet är det avgörande att säkra att staten arbetar för att försvara medborgarnas rättigheter, inte utarmar dem. Jag föreslår därför att civilsamhället ska inkluderas i utvecklingen av policyer som påverkar medborgarnas digitala rättigheter.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

4. Inrättandet av en it-haverikommission, punkt 2 (M, C)

av Pål Jonson (M), Jan R Andersson (M), Daniel Bäckström (C), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2021/22:3227 av Niels Paarup-Petersen m.fl. (C) yrkande 22,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 20 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 6.

Ställningstagande

Sårbarheten i den digitala infrastrukturen är uppenbar med återkommande lagbrott, läckor och avbrott. It-störningar i samhällsviktig verksamhet, såväl offentlig som privat, kan få mycket långtgående konsekvenser för samhällets funktionalitet. För att förbättra säkerheten föreslår vi därför att det inom den

verksamhet som grundlagts genom bl.a. genomförandet av EU:s direktiv om nätverks- och informationssystem (NIS), den nya säkerhetsskyddslagen och EU:s dataskyddsförordning (GDPR) ska skapas en it-haverikommission, förslagsvis som en vidareutveckling av CERT-SE, dvs. Sveriges nationella it-incidentcentrum (Computer Security Incident Response Team, CSIRT), och detta i samband med utvecklingen av det nya cybersäkerhetscentret. Denna kommission ska ansvara för att analysera incidenter, skapa rekommendationer och sprida råd, riktlinjer och information om nödvändiga förbättringar i system såväl inom den offentliga sektorn som inom kritiska privata sektorer. It-haverikommissionen bör kunna utfärda tvingande åtgärder.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

5. Risker och sårbarheter, punkt 3 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 3 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 5 och
avslår motionerna
2021/22:624 av Markus Wiechel och Björn Söder (båda SD),
2021/22:2934 av Jimmy Ståhl m.fl. (SD) yrkande 6 och
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 26 och 29.

Ställningstagande

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 det systematiska informationssäkerhetsarbetet och 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 gemensamma hot-, sårbarhets- och riskbedömningar samt skyddsprofiler kan tas fram till stöd för kravställning på IKT-produkter, IKT-tjänster och IKT-processer som ska användas i nätverks- och informationssystem i säkerhetskänslig verksamhet. IKT står för informations- och kommunikationsteknik.

Vi anser att det utifrån de allvarliga brister som har konstaterats är prioriterat att gå vidare med utredningens förslag rörande hot-, sårbarhets- och riskbedömningar, vilka kan fungera som stöd för kravställning, och föreslår därför att regeringen ska ge FMV i uppdrag att i samråd och samverkan med framför allt de myndigheter som ingår i det nationella cybersäkerhetscentret arbeta vidare med de förslag som utredningen Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem tagit fram rörande hot-, sårbarhets- och riskbedömningar.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

6. Risker och sårbarheter, punkt 3 (SD)

av Roger Richthoff (SD), Caroline Nordengrip (SD) och Per Söderlund (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 3 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:2934 av Jimmy Ståhl m.fl. (SD) yrkande 6 och
avslår motionerna
2021/22:624 av Markus Wiechel och Björn Söder (båda SD),
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 26 och 29 samt
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 5.

Ställningstagande

Viss infrastruktur är särskilt känslig för dataintrång eftersom särskilt känslig information om medborgare, militär, politisk ledning m.m. kan hamna i orätta händer. Syftet med ett dataintrång kan variera. Alla företag kan drabbas av förluster eller stölder av it-information. Det kan ske fysiskt på plats, genom digitala angrepp utifrån eller via interna misstag. All kommunikation måste därför klassas som osäker även om en anläggning är digitalt fysiskt åtskild från omvärlden. Det uppstår också extraordinära problem om nationer utstuderat använder sina egna bolag, sin befolkning eller auktoritet till att illegalt inhämta it-information utanför sin egen nationsgräns. Lösningen ligger i att försvåra otillåtna intrång och skapa hinder som är fysiska, digitala och juridiska, men även diplomatiska. Då viss it-infrastruktur är särskilt sårbar för dataintrång föreslår vi därför att säkerhetsrutinerna för sådan infrastruktur ses över.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

7. Risker och sårbarheter, punkt 3 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 3 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 26 och 29 samt avslår motionerna
2021/22:624 av Markus Wiechel och Björn Söder (båda SD),
2021/22:2934 av Jimmy Ståhl m.fl. (SD) yrkande 6 och
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 5.

Ställningstagande

Utländsk makt bedriver kartläggningsverksamhet mot Sverige och de testar på olika sätt våra system inklusive sårbarheter i vår infrastruktur. Vi måste därför utgå från att informationen redan finns hos främmande makt. Att någon annan kan sitta på en samlad information om sårbarheter och svagheter i vår digitala infrastruktur men inte vi som land är en stor försvars- och säkerhetspolitisk utmaning för oss. Uppenbart riskerar det kraftigt att begränsa vårt lands handlingsfrihet vid en stor cyberattack som påverkar samhällsviktig verksamhet. Jag föreslår därför att regeringen ska ge i uppdrag åt Post- och telestyrelsen (PTS) att genomföra en utredning om sårbarheterna i fibernät och noder för att få en nationell lägesbild. En kartläggning behöver göras tillsammans med näringslivet som äger mycket av infrastrukturen.

Då bl.a. vattenrening, elförsörjning och andra helt grundläggande delar av samhällets infrastruktur i dag är digitaliserade och därmed sårbara för attacker, sårbarheterna inte testas på ett strukturerat sätt och en överblick över sårbarheterna saknas föreslår jag att infrastrukturen sårbarhetstestas löpande.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

8. Försvarsmaktens förmåga, punkt 4 (M, KD)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M), Mikael Oscarsson (KD) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 10 och
avslår motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del,
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 2, 12, 13 och 15 samt
2021/22:3998 av Joar Forssell m.fl. (L) yrkande 10.

Ställningstagande

Ett trovärdigt cyberförsvar handlar om förmågan att skydda de egna it-systemen från angrepp, men även om att cyberförsvaret ska ha förmågan att slå tillbaka mot en potentiell angripare – en s.k. aktiv cyberförmåga. Det finns en bred politisk enighet kring att Sverige ska ha en offensiv förmåga på cyberområdet, men denna förmåga ger också upphov till svåra frågor. Den aktiva cyberförmågan kräver att det tas fram ett förhållningssätt för hur, var och när den i så fall ska användas. Vi föreslår därför att regeringen ska verka för att det upprättas en cyberdoktrin för den defensiva och offensiva cyberförmågan.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

9. Försvarsmaktens förmåga, punkt 4 (SD)

av Roger Richthoff (SD), Caroline Nordengrip (SD) och Per Söderlund (SD).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del och
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del och
avslår motionerna
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 2, 12, 13 och 15,
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 10 och
2021/22:3998 av Joar Forssell m.fl. (L) yrkande 10.

Ställningstagande

Informationsteknologi kan användas för både positiva och negativa ändamål. Spionerі och regelrätta cyberattacker över nätet har blivit vardag i dag. Stormakterna, med Ryssland, USA och Kina i spetsen, satsar stort på att bygga upp sina resurser för cyberkrigföring, spionage och övervakning. Militär underrättelsetjänst, terrorister och organiserad brottslighet kommer att använda sig av informationsteknologi i allt högre utsträckning, inte minst för att det är billigt och svårspårbart och man når hela världen.

Detta gör det allt viktigare att vidta adekvata åtgärder för att skydda och försvara vitala nationella intressen mot cyberhot. Detta blir särskilt viktigt när större delen av samhället är helt beroende av fungerande informationsteknologi. Särskilt viktigt är att skydda betalsystem, energiförsörjning och transporter. Vi föreslår därför att Sverige ska fortsätta att stärka sin förmåga att genomföra såväl defensiva som offensiva cyberoperationer.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

10. Försvarsmaktens förmåga, punkt 4 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 2, 12, 13 och 15 samt
avslår motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del,
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del,
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 10 och
2021/22:3998 av Joar Forssell m.fl. (L) yrkande 10.

Ställningstagande

Jag instämmer i Försvarsmaktens syn att kärnan i arbetet med att förstärka cyberförsvarsförmågan är utökad kapacitet till defensiva och offensiva cyberoperationer mot kvalificerade motståndare i cyberdomänen. Cyberoperationer är en lika självklar del i modern krigföring som mark-, sjö- och luftoperationer och är därmed en naturlig del av det nationella försvaret av Sverige och svenska intressen. Jag föreslår därför att Försvarsmaktens förmåga till både defensiva och offensiva cyberoperationer ska utvecklas.

Sedan 2020 utbildar Försvarsmakten värnpliktiga cybersoldater i samarbete med KTH där värnplikten beskrivs. Det är angeläget att cybersoldaterna på sikt blir fler. För att belysa ett eventuellt behov av att stärka cyberfrågornas vikt i Försvarsmakten vill jag därför också föreslå att det utreds om det finns ett behov av att införa ytterligare en försvarsgren jämte armén, flygvapnet och marinen, nämligen en som hanterar cyberförsvaret av Sverige.

Vidare vill jag understryka kopplingarna mellan infrastruktur och psykologiskt försvar och att samhällets totala försvarsförmåga avgörs på en digital arena där frågorna hänger ihop. Sverige attackeras varje dag digitalt och det är på tiden att vi får förmågor som motsvarar hotet. Jag föreslår därför att kopplingen mellan cyberförsvar och psykologiskt försvar ska utvecklas förmågemässigt.

Avslutningsvis vill jag understryka att det är många länder som har en förmåga att utföra cyberangrepp, ofta med hög uthållighet och samordningsförmåga. Både Ryssland och Kina genomför koordinerade antagonistiska handlingar mot Sverige och kan använda sig av stora resurser för att nå sina målsättningar. Den som har tid, kompetens och resurser kan ta sig in i alla delar av internet. Och de som gör det är andra länders säkerhetstjänster, underrättelsetjänster och försvarsmakter. Ingen skillnad görs mellan civilt och militärt eller offentligt och privat. Det betyder att alla är en potentiell måltavla. Storskaligheten i attackerna kan vara svår att stå emot också för den bäste. För andra är attacken helt omöjlig att ens upptäcka innan det är för sent. Jag föreslår därför att regeringen ska verka för att tydligare än i dag uttala vilket land som står bakom cyberangrepp mot Sverige när man väl vet vem eller vilka som står bakom dessa.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

11. Försvarsmaktens förmåga, punkt 4 (L)

av Allan Widman (L).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 4 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3998 av Joar Forssell m.fl. (L) yrkande 10 och
avslår motionerna
2021/22:2531 av Roger Richthoff m.fl. (SD) yrkande 42 i denna del,
2021/22:2579 av Björn Söder m.fl. (SD) yrkande 17 i denna del,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 2, 12, 13 och 15 samt
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 10.

Ställningstagande

Det pågår en massiv desinformationskampanj på internet i den ryska regeringens regi. Det sprids dimridåer, mer eller mindre trovärdiga, om vad som händer i omvärlden. Bakom detta ligger ett tvådelat syfte: internt i Ryssland handlar det om att skapa stöd för sittande regims agerande, externt bidrar det till att vilseleda opinion och beslutsfattare. Målet är att det ska bli svårare att lita på någonting över huvud taget. Säkerhetspolisen uppger att Ryssland bedriver ett psykologiskt krig mot Sverige. Därtill är det ställt utom allt tvivel att ryska aktörer utgör ett omfattande cyberhot mot svenska intressen. Det är mycket sannolikt att det var ryska grupper som låg bakom ransomware-attacken mot svenska Coop. Till detta kan läggas industrispionage osv. Med anledning av cyberhotet från Ryssland föreslår jag att Sverige ska främja en politik som bemöter såväl den militära hotbilden som underrättelsehotet.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

12. Kompetensförsörjning, punkt 5 (M, KD)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M), Mikael Oscarsson (KD) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 5 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 11 och 13 samt
avslår motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 10 och 11.

Ställningstagande

Vi anser att behovet av att resurssätta och kompetensförsörja det svenska cyberförsvaret kommer att bli en viktig framtidsfråga. Försvarsmakten kommer inte fullt ut att kunna konkurrera med det privata näringslivet när det gäller löner. Därför måste Försvarsmakten dels fortsätta att vidareutveckla möjligheten att själv utbilda cybersoldater, 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 det näringslivets totalförsvarsråd som Försvarsberedningen föreslagit som det försvarsindustriråd som vårt parti tidigare föreslagit.

Det finns en stor potential att utnyttja dem 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 föreslår vi ska undersökas vidare. I förlängningen skulle detta kunna leda till etablerandet av digitala hemvärnsförband och en frivillig försvarsorganisation med koppling till cyberförmåga.

Ett effektivt och kompetent cyberförsvar är också 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 det tekniska detekterings- och varningssystem (TDV) som används av FRA.

Vi anser därför att Försvarsmakten ska ges ökade möjligheter att genom innovationsupphandling 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. Vi föreslår därför att Försvarsmakten och KTH ges ett särskilt uppdrag att ta fram förslag på hur en process och struktur skulle kunna se ut för att ta fram nya tekniska lösningar inom cyberförsvaret.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

13. Kompetensförsörjning, punkt 5 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 5 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 10 och 11 samt avslår motion
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 11 och 13.

Ställningstagande

Alla i Sverige ska kunna bidra till totalförsvaret, också om ens intresse och kompetens i huvudsak inte finns inom det traditionellt militära området, dvs. armén, flygvapnet och marinen. Samhällets förmåga att stå emot och återhämta sig från cyberattacker måste bli bättre. Jag föreslår därför att det ska övervägas att skapa ett cybervärn som står på två ben, ett ben för att bidra till att stärka samhällets förmåga att hantera stora cyberattacker och ett ben för att stå emot otillbörlig informationspåverkan under höjd beredskap och ytterst krig. Med andra ord ska cybervärnet också ha uppgifter inom det psykologiska försvaret. På så sätt kan vi också tydliggöra sambandet mellan cyberförsvar och psykologiskt försvar. Cybervärnet ska utgöra en aktiv del av totalförsvaret

med kompetens som kan nyttjas av olika aktörer som själva saknar tillräcklig sådan. Det blir en förstärkningsresurs på samma sätt som vissa andra kritiska resurser som frivilliga redan utgör inom ramen för de frivilliga försvarsorganisationernas arbete.

Vidare föreslår jag att de cybervärnpliktiga ska bli fler för att stärka Försvarsmaktens egen kompetens men också för att stärka cyberkompetensen i samhället i stort.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

14. Förfogandelagstiftning, punkt 6 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 6 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 14.

Ställningstagande

Under höjd beredskap och krig har staten stora befogenheter att beslagta och förfoga över Sveriges privatägda industri, privatpersoners fordon och andra resurser som fysiskt kan behövas i en krigssituation. Syftet med förfogandelagstiftningen är att stärka Sveriges förmåga att hantera och motstå krig utan att staten måste äga all materiel själv. Var och en är en del av totalförsvaret i Sverige. Förfogandelagstiftningen är baserad på fysiska enheter i en materiell värld. Men i och med att krigsarenan har utvecklats till att också omfatta en digital värld är i dag inte bara fysiska utan även digitala resurser avgörande för statens förmågor. Lagen om elektronisk kommunikation ger vissa möjligheter kopplat till själva näten, men det är oklart om dessa skrivningar räcker i dagens läge. Jag föreslår därför att regeringen ser över behovet av en uppdatering av förfogandelagstiftningen för att också inkludera digitala resurser för krigföring i cyberdomänen.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

15. Samhällets förmågeutveckling, punkt 7 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 7 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3753 av Maria Stockhaus m.fl. (M) yrkandena 12 och 14 samt
avslår motionerna
2021/22:1078 av Edward Riedl (M),
2021/22:1394 av Larry Söder (KD),
2021/22:3227 av Niels Paarup-Petersen m.fl. (C) yrkande 25,
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 28, 31, 34, 36, 38 och 39 samt
2021/22:4197 av Elisabeth Falkhaven m.fl. (MP) yrkande 3.

Ställningstagande

Svenska myndigheter uppvisar sedan många år brister på cybersäkerhetsområdet. Myndigheternas säkerhetsarbete har generellt inte hållit jämna steg med digitaliseringen och det är därför viktigt att det finns en tydlig ledning i det arbetet. Vi föreslår därför att regeringen ska ta ledningen för att på ett operativt sätt stödja myndigheternas säkerhetsarbete.

En del av de ovan nämnda bristerna beror på bristfällig kunskap om vilka viktiga uppgifter myndigheter har i sitt förvar och hur de ska hanteras. Ska vi klara omställningen till ett digitalt samhälle krävs en tydlig kompetensförsörjning och utveckling av ledningen inom den offentliga sektorn. Vi föreslår därför att det ska införas ett fortbildningskrav inom informationssäkerhetsområdet för personer på ledande positioner i offentlig sektor.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

16. Samhällets förmågeutveckling, punkt 7 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 7 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2021/22:3227 av Niels Paarup-Petersen m.fl. (C) yrkande 25 och
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 28, 31, 34, 36, 38 och 39 samt
avslår motionerna
2021/22:1078 av Edward Riedl (M),
2021/22:1394 av Larry Söder (KD),
2021/22:3753 av Maria Stockhaus m.fl. (M) yrkandena 12 och 14 samt
2021/22:4197 av Elisabeth Falkhaven m.fl. (MP) yrkande 3.

Ställningstagande

Det saknas i dag kompetens och förståelse för den digitala hotbilden mot Sverige, både i det politiska systemet, i näringslivet och på bredden i samhället. Det saknas med andra ord kompetens för att kunna minska det ständigt vidgade glapp som finns mellan en accelererande digitalisering och en god cybersäkerhet. Både det politiska systemet, den offentliga sektorn och allmänheten ligger i mångt och mycket efter i förståelsen för den faktiska hotbilden. Åtgärderna och skyddet är inte heller dimensionerade för den hotbild vi ser. Att stärka kompetensen inom cybersäkerhetsområdet handlar inte enbart om att få fram fler specialister i it-säkerhet. Cybersäkerhet är mycket mer än en it-fråga; det är en kulturfråga, menar jag. Jag anser att det behövs kompetensstrategier för bredden och spetsen i samhället som höjer kunskapen hos enskilda medborgare, inom offentlig sektor och näringsliv såväl som hos beslutsfattare, inklusive den politiska nivån.

Jag föreslår därför

- att kompetensstrategier ska tas fram som höjer kunskapen om cybersäkerhet i offentlig sektor samt hos beslutsfattare
- att kompetensen i samhället om cybersäkerhet, hot och risker ska breddas via civilsamhället
- att ett traineesystem ska skapas inom cybersäkerhetsområdet
- att behovet av att stödja olika initiativ för att sprida information som höjer medvetenheten om cybersäkerhet ska lyftas fram
- att MSB:s och Säkerhetspolisens rekommendationer och s.k. best practices ska utvecklas, förtydligas, anpassas och spridas så att flera olika typer av organisationer får förutsättningar att följa rekommendationerna
- att det ska utredas om arbete med vissa tjänster ska förutsätta certifiering av kompetens inom cybersäkerhetsområdet
- att kunskapen om, och insatser mot, s.k. deep fakes och andra teknologiska möjligheter med samhällsstörande konsekvenser ska stärkas inom säkerhetsapparaten.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

17. Samverkan med näringslivet, punkt 8 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 8 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2021/22:3639 av Pål Jonson m.fl. (M) yrkandena 7 och 12 samt
2021/22:3640 av Pål Jonson m.fl. (M) yrkandena 16 och 17.

Ställningstagande

Vi anser att det finns ett flertal områden inom cybersäkerhet som behöver stärkas i Sverige. Det handlar bl.a. om kompetensförsörjning, större och effektivare satsningar på forskning inom akademin samt bättre samarbetsstrukturer med näringslivet. En bra samverkan mellan staten och näringslivet är en förutsättning 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 i dag hos det privata näringslivet. Detta gäller inte minst på cyberområdet. Vi anser därför att det är centralt att länken offentligt–privat fördjupas på cyberområdet för att stärka svensk säkerhet brett. I princip all produktutveckling inom cybersäkerhetsområdet sker inom det privata näringslivet, och den teknikkompetens som finns bland dessa företag är ofta högre än den som finns på statliga myndigheter. 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.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

18. Cybersäkerhet på universitet och högskolor, punkt 9 (M, KD)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M), Mikael Oscarsson (KD) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 9 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motionerna
2021/22:3640 av Pål Jonson m.fl. (M) yrkande 18 och
2021/22:4161 av Pia Steensland m.fl. (KD) yrkande 32.

Ställningstagande

Det svenska näringslivet och den fria forskningen drabbas i dag av spionage och industriella stölder som går att knyta till den kinesiska staten. Det är av yttersta vikt att Sverige kan skydda näringslivet, i synnerhet innovativa teknikföretag. Det hot som svenska underrättelsemyndigheter beskriver är mycket oroande, inte minst när svensk teknologisk kompetens kan ha en militär användbarhet. Vi vill därför att regeringen ger underrättelsemyndigheterna i uppdrag att utveckla en strategi för hur svenska universitet och högskolor ska stärka sin säkerhet och kunna arbeta med screening i säkerhetskänslig forskning samt vid behov samarbeta med exempelvis Säkerhetspolisen, den militära underrättelse- och säkerhetstjänsten (Must) och FRA.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

19. It-upphandlingar ur ett cybersäkerhetsperspektiv, punkt 10 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 10 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 9 och
avslår motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 22, 23 och 27.

Ställningstagande

Utredningen om informations- och cybersäkerhet i Sverige (SOU 2015:23) har konstaterat att lagen om offentlig upphandling (LOU) kan vara ett problem vid offentliga aktörers upphandling av it-drift eftersom lägre pris prioriteras högre än cyber- och informationssäkerhet. Vi vill därför att offentliga aktörer ska kunna använda sig av lagen 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 myndigheter att ställa krav utifrån nödvändiga säkerhetshänsyn. Vi anser däremot att LOU även fortsättningsvis ska användas där det går men föreslår att upphandlingskompetensen när det gäller cybersäkerhet stärks.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

20. It-upphandlingar ur ett cybersäkerhetsperspektiv, punkt 10 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 10 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 22, 23 och 27 samt
avslår motion
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 9.

Ställningstagande

Det saknas i dag krav på digital säkerhet, vilket gör det svårt för bl.a. kommuner och regioner att ställa krav på säkerhet i sin egen digitaliseringsresa. Dels finns kunskapen inte inom den interna organisationen, dels ställer olika kommuner olika krav, vilket försvårar för företag att utveckla produkter och delta med ”standardsäkerhetsprodukter” i upphandlingar. Branschorganisationer önskar att det införs standarder då det skulle göra det lättare att utveckla produkter som är användbara för fler, vilket de kan göra ekonomisk vinst på och spara tid på i upphandlingsprocesser. Jag föreslår därför att det tas fram minimistandarder och funktionskrav för samhällsviktig verksamhet. Att även den digitala infrastrukturen omfattas av funktionskrav är viktigt.

Vid stora och samhällsviktiga it- och digitaliseringsupphandlingar måste såväl köpare som leverantör ha kompetens att kravställa respektive leverera säkra system. Jag föreslår att oberoende säkerhetsgenomgångar blir ett krav vid större upphandlingar. På så vis kan samhället undvika en lång rad allvarliga digitala säkerhetsbrister och stärka it-konsulternas fokus på säkerhet.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

21. Internationella överenskommelser, punkt 11 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 11 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 8 och
avslår motionerna
2021/22:2279 av Maria Nilsson (L),
2021/22:2351 av Robert Hannah (L) och
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 6.

Ställningstagande

Vi anser att regeringen bör främja ett djupare samarbete inom Norden och EU samt med Nato på cybersäkerhetsområdet. För att stärka cyberförsvaret bedrivs bl.a. projekt inom ramen för den europeiska försvarsfonden. Sverige bör bedriva ett aktivt arbete för att kunna få del av de medlen. MSB har fått i uppdrag att förbereda för att bli nationellt samordningscenter kopplat till Europeiska kompetenscentret för cybersäkerhet. Dessa kompetenscenter bör arbeta parallellt med cybersäkerhet och cyberförsvar.

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 i ljuset av den exponentiella ökningen av cyberattacker. Sverige bör samarbeta med Nato i så stor utsträckning som möjligt när det gäller cyberförsvar. Vi har redan nu representation på Natos kompetenscentrum i Tallinn och Sverige har deltagit i komplexa Natoledda övningar som Locked Shields där det svenska bidraget lett till stor framgång.

Vi anser vidare att de nordiska länderna bör samordna och öva sina nationella it-incidentcentrum (Computer Emergency Response Team, CERT) gemensamt och intensifiera samarbetet kring utbyggnaden av 5G inklusive de säkerhetsaspekter som är kopplade till detta arbete.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

22. Internationella överenskommelser, punkt 11 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 11 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkande 6 och
avslår motionerna
2021/22:2279 av Maria Nilsson (L),
2021/22:2351 av Robert Hannah (L) och
2021/22:3639 av Pål Jonson m.fl. (M) yrkande 8.

Ställningstagande

Det saknas i dag förtroendeskapande mekanismer inom ramen för det internationella cybersäkerhetssamarbetet. Tidigare har det länge funnits många sådana inom exempelvis nedrustningsområdet. På samma sätt som Sverige varit aktivt i det arbetet bör regeringen verka för att det skapas liknande mekanismer för cybersäkerhet. Kostnaden för aggressiva statsunderstödda cyberaktiviteter mot Sverige måste höjas, och det rejält. Det är en del av vårt lands motståndskraft att kunna agera när vi och våra demokratiska grannländer utsätts, i fred, krig och allt däremellan.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

23. Arbetet inom EU, punkt 12 (M)

av Pål Jonson (M), Jan R Andersson (M), Jörgen Berglund (M) och Alexandra Anstrell (M).

Förslag till riksdagsbeslut

Vi anser att förslaget till riksdagsbeslut under punkt 12 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3775 av Jessika Roswall m.fl. (M) yrkande 26 och
avslår motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 7, 8 och 25.

Ställningstagande

Behovet av europeisk samverkan inom cyberområdet är stort. Sverige som är ett ledande land inom digitalisering bör axla en större roll och regeringen borde vara pådrivande i frågan. Den offentliga sektorns robusthet och myndigheternas förmåga att effektivt reagera på cyberattacker behöver förbättras. Vi vill se att regeringen tydligare satsar på utbildning och kompetens och att innovationskraften stärks genom europeiska samarbeten. Regeringen bör vidare stärka arbetet med att bekämpa desinformation och cyberattacker inom EU som syftar till att störa våra demokratiska processer och undergräva förtroendet för våra institutioner. Åtgärdsplanen mot desinformation ger bra vägledning i det arbetet. Det handlar om att stärka samarbetet för att upptäcka, förebygga och bekämpa angrepp och samtidigt stärka motståndskraften mot dessa hot. Vi föreslår att regeringen ska verka för att EU:s cyberförsvar stärks.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

24. Arbetet inom EU, punkt 12 (C)

av Daniel Bäckström (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 12 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion
2021/22:3245 av Niels Paarup-Petersen m.fl. (C) yrkandena 7, 8 och 25 samt avslår motion
2021/22:3775 av Jessika Roswall m.fl. (M) yrkande 26.

Ställningstagande

Regeringen bör verka för en koordineringsmekanism inom EU vid storskaliga cyberattacker. På samma vis som EU för exempelvis skogsbränder får till uppgift att koordinera enskilda medlemsländers expertresurser, borde liknande uppgift kunna tillämpas inom cyberområdet om ett land utsätts för en omfattande cyberattack som det inte kan hantera på egen hand. Precis som i räddningstjänstsamarbetet inom EU (civilskyddssamarbetet) ska det vara frivilligt att anmäla nationella resurser, och man ska vid varje enskilt tillfälle kunna välja om man vill bidra eller inte. På samma sätt som inom civilskyddssamarbetet hade EU också kunnat ha medfinansieringsresurser för att bygga upp sådana nationella kompetenser som EU samlat saknar. Sverige skulle vid behov kunna bidra till en sådan solidarisk cyberpolitik genom att både självständigt och inom ramen för EU:s civila krishanteringsmekanism bygga upp ett världsledande digitalt katastrofteam som kan tillhanda kommunikativ infrastruktur i

kriser, naturliga kriser såväl som sådana som skapats av cyberangrepp eller krig.

Frågan om att ge EU en större roll i frågor som rör standarder för cybersäkerhet bör drivas av regeringen. När internationella regler och standarder saknas blir också samarbete mellan länder svårare, både förebyggande, kapacitetsbyggande och responsivt. Mer samarbete krävs i frågan. Allt fler länder har en uttalad syn på hur man vill att det internationella samarbetet utvecklas samt vilka normer och standarder som ska inkluderas i ett internationellt regelverk för cybersäkerhet dock inte Sverige. Mer måste göras för att Sverige ska kunna påverka och driva utvecklingen på den internationella arenan. Jag anser vidare att ny lagstiftning måste ta hänsyn till svensk konkurrenskraft och begränsningar bör helst tas fram inom EU-samarbetet.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

BILAGA

Förteckning över behandlade förslag

Motioner från allmänna motionstiden 2021/22

2021/22:624 av Markus Wiechel och Björn Söder (båda SD):

Riksdagen ställer sig bakom det som anförs i motionen om en bredare granskning av svenskarnas användning av teknik från länder som kan anses utgöra säkerhetshot och tillkännager detta för regeringen.

2021/22:1078 av Edward Riedl (M):

Riksdagen ställer sig bakom det som anförs i motionen om att se över offentlig förvaltnings arbete med informationssäkerhet och tillkännager detta för regeringen.

2021/22:1394 av Larry Söder (KD):

Riksdagen ställer sig bakom det som anförs i motionen om att utreda möjligheten till att offentlig verksamhets serverbehov byggs upp inom Sveriges gränser och tillkännager detta för regeringen.

2021/22:2279 av Maria Nilsson (L):

Riksdagen ställer sig bakom det som anförs i motionen om att inrätta en cybersolidaritetspakt och tillkännager detta för regeringen.

2021/22:2351 av Robert Hannah (L):

Riksdagen ställer sig bakom det som anförs i motionen om att Sverige ska verka för skapandet av en FN-konvention om cyberkrigföring och tillkännager detta för regeringen.

2021/22:2531 av Roger Richthoff m.fl. (SD):

42. Riksdagen ställer sig bakom det som anförs i motionen om cyberförsvar och tillkännager detta för regeringen.

2021/22:2579 av Björn Söder m.fl. (SD):

17. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige bör skaffa sig ett aktivt informationsteknologiskt försvar (aktiv cyberförmåga) och att en samordnande myndighet bör ansvara för att den offentliga sektorn skyddas mot angrepp genom tillräckligt skydd och tillräcklig kompetens och tillkännager detta för regeringen.

2021/22:2934 av Jimmy Ståhl m.fl. (SD):

6. Riksdagen ställer sig bakom det som anförs i motionen om säkerhetsrutiner för viss it-infrastruktur och tillkännager detta för regeringen.

2021/22:3227 av Niels Paarup-Petersen m.fl. (C):

22. Riksdagen ställer sig bakom det som anförs i motionen om en it-haverikommission och tillkännager detta för regeringen.
25. Riksdagen ställer sig bakom det som anförs i motionen om teknologiska möjligheter med samhällsstörande konsekvenser och tillkännager detta för regeringen.

2021/22:3245 av Niels Paarup-Petersen m.fl. (C):

2. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige tydligare än i dag när vi blir utsatta för omfattande cyberangrepp bör uttala vilket land som står bakom när attribuering är möjlig, och detta tillkännager riksdagen för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om förtroendeskapande åtgärder inom cyberområdet och tillkännager detta för regeringen.
7. Riksdagen ställer sig bakom det som anförs i motionen om att EU bör få en större roll i frågor som rör standarder kring cybersäkerhet, och detta tillkännager riksdagen för regeringen.
8. Riksdagen ställer sig bakom det som anförs i motionen om en EU-koordineringsmekanism vid storskaliga cyberattacker och tillkännager detta för regeringen.
10. Riksdagen ställer sig bakom det som anförs i motionen om cybervärn och tillkännager detta för regeringen.
11. Riksdagen ställer sig bakom det som anförs i motionen om cybervärnpliktiga och tillkännager detta för regeringen.
12. Riksdagen ställer sig bakom det som anförs i motionen om utveckling av Försvarsmaktens förmåga till både defensiva och offensiva cyberoperationer och tillkännager detta för regeringen.
13. Riksdagen ställer sig bakom det som anförs i motionen om att utveckla kopplingen mellan cyberförsvar och psykologiskt försvar och tillkännager detta för regeringen.
14. Riksdagen ställer sig bakom det som anförs i motionen om att tillsätta en utredning om behovet av förfogandelagstiftning inom cyberområdet som träder i kraft vid höjd beredskap eller krig och tillkännager detta för regeringen.
15. Riksdagen ställer sig bakom det som anförs i motionen om att tillsätta en utredning för att se över ett eventuellt behov av att göra cyberförsvar till en egen försvarsgren och tillkännager detta för regeringen.
20. Riksdagen ställer sig bakom det som anförs i motionen om it-haverikommission och tillkännager detta för regeringen.

22. Riksdagen ställer sig bakom det som anförs i motionen om att tydligare kravställningar gällande funktionalitet och säkerhet behöver ställas vid upphandlingar och tillkännager detta för regeringen.
23. Riksdagen ställer sig bakom det som anförs i motionen om att oberoende säkerhetsgenomgångar bör bli ett krav vid större upphandlingar och tillkännager detta för regeringen.
24. Riksdagen ställer sig bakom det som anförs i motionen om att civilsamhället bör inkluderas i utvecklingen av policyer som påverkar medborgarnas digitala rättigheter och tillkännager detta för regeringen.
25. Riksdagen ställer sig bakom det som anförs i motionen om att ny lagstiftning måste ta hänsyn till svensk konkurrenskraft och begränsningar bör helst tas fram inom EU-samarbetet och tillkännager detta för regeringen.
26. Riksdagen ställer sig bakom det som anförs i motionen om att uppdra åt PTS att genomföra en utredning om sårbarheterna i fibernät och noder för att få en nationell lägesbild, och detta tillkännager riksdagen för regeringen.
27. Riksdagen ställer sig bakom det som anförs i motionen om att ta fram minimistandarder och funktionskrav för samhällsviktig verksamhet och tillkännager detta för regeringen.
28. Riksdagen ställer sig bakom det som anförs i motionen om att MSB:s/Säpos rekommendationer och best practices utvecklas, förtydligas, anpassas och sprids så att flera olika typer av organisationer har förutsättningar att följa rekommendationerna, och detta tillkännager riksdagen för regeringen.
29. Riksdagen ställer sig bakom det som anförs i motionen om löpande sårbarhetstestning av kritisk infrastruktur och tillkännager detta för regeringen.
31. Riksdagen ställer sig bakom det som anförs i motionen om att bredda kompetensen i samhället om cybersäkerhet, hot och risker via civilsamhället och tillkännager detta för regeringen.
34. Riksdagen ställer sig bakom det som anförs i motionen om kompetensstrategier för att säkerställa en miniminivå av kunskap inom cybersäkerhet i offentlig sektor samt fördjupade och obligatoriska utbildningar för beslutsfattare och tillkännager detta för regeringen.
36. Riksdagen ställer sig bakom det som anförs i motionen om traineesystem inom cybersäkerhet och tillkännager detta för regeringen.
38. Riksdagen ställer sig bakom det som anförs i motionen om behov av att utreda om arbete med vissa tjänster ska förutsätta certifiering av kompetens inom cybersäkerhet och tillkännager detta för regeringen.
39. Riksdagen ställer sig bakom det som anförs i motionen om behov av att stödja olika initiativ för att sprida information och medvetenhet om cybersäkerhet och tillkännager detta för regeringen.

2021/22:3368 av Viktor Wärnick m.fl. (M):

20. Riksdagen ställer sig bakom det som anförs i motionen om om vikten av ett starkt försvar mot påverkan och att det brådskar med att de nya myndigheterna för psykologiskt försvar och cybersäkerhet kommer till stånd och blir fullt verksamma, och detta tillkännager riksdagen för regeringen.

2021/22:3639 av Pål Jonson m.fl. (M):

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.
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.

2021/22:3640 av Pål Jonson m.fl. (M):

16. Riksdagen ställer sig bakom det som anförs i motionen om att skydda näringslivet och tillkännager detta för regeringen.
17. Riksdagen ställer sig bakom det som anförs i motionen om en översyn av hur samhällsviktiga svenska företag kan få stöd för att upptäcka och motverka spionage och attacker mot sin verksamhet och tillkännager detta för regeringen.
18. Riksdagen ställer sig bakom det som anförs i motionen om behovet av att skydda svenska universitet och högskolor och tillkännager detta för regeringen.

2021/22:3753 av Maria Stockhaus m.fl. (M):

12. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör ta ledningen för att på ett operativt sätt stödja myndigheternas säkerhetsarbete och tillkännager detta för regeringen.
14. Riksdagen ställer sig bakom det som anförs i motionen om att införa ett fortbildningskrav inom informationssäkerhet för personer på ledande positioner i offentlig sektor och tillkännager detta för regeringen.

2021/22:3775 av Jessika Roswall m.fl. (M):

26. Riksdagen ställer sig bakom det som anförs i motionen om förstärkning av EU:s cyberförsvar och tillkännager detta för regeringen.

2021/22:3998 av Joar Forssell m.fl. (L):

10. Riksdagen ställer sig bakom det som anförs i motionen om cyberhotet från ryska aktörer och tillkännager detta för regeringen.

2021/22:4161 av Pia Steensland m.fl. (KD):

32. Riksdagen ställer sig bakom det som anförs i motionen om att stärka säkerheten och minska risken för spionage och immateriell stöld vid svenska lärosäten och tillkännager detta för regeringen.

2021/22:4197 av Elisabeth Falkhaven m.fl. (MP):

3. Riksdagen ställer sig bakom det som anförs i motionen om att stärka cybersäkerheten i offentlig sektor och särskilt samhällsviktiga delar av den privata sektorn och tillkännager detta för regeringen.

Tryck: Elanders Sverige AB, Vällingby 2022