



# Nationell strategi för samhällets informations- och cybersäkerhet

---

## Sammanfattning

Utskottet föreslår att riksdagen lägger skrivelse 2016/17:213 till handlingarna.

I skrivelsen redogör regeringen för att det finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. Den aktuella nationella strategin för samhällets informations- och cybersäkerhet är ett uttryck för regeringens övergripande prioriteringar och syftar till att utgöra en plattform för Sveriges fortsatta utvecklingsarbete inom området. Huvudsyftena med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Regeringen vill genom strategin även stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten. Strategin omfattar därmed hela samhället, dvs. statliga myndigheter, kommuner och landsting, företag, organisationer och privatpersoner. Av strategin framgår regeringens målsättningar och vad den avser att verka för.

Utskottet ser positivt på regeringens nationella strategi, som kommer att bidra till att skapa långsiktiga förutsättningar för informations- och cybersäkerheten för hela det svenska samhället.

I anslutning till detta ärende behandlas också motionsyrkanden om informations- och cybersäkerhet från den allmänna motionstiden 2017/18.

Utskottet avstyrker samtliga motionsyrkanden med hänvisning till pågående arbete.

I betänkandet finns 15 reservationer (M, SD, C, L, KD).

### *Behandlade förslag*

Skrivelse 2016/17:213 Nationell strategi för samhällets informations- och cybersäkerhet.

16 yrkanden i följdmotioner.

Ett tjugotal yrkanden i motioner från allmänna motionstiden 2017/18.

# Innehållsförteckning

Utskottets förslag till riksdagsbeslut.....	3
Redogörelse för ärendet .....	6
Ärendet och dess beredning.....	6
Bakgrund .....	6
Utskottets överväganden.....	9
En systematisk och samlad ansats i arbetet med informations- och cybersäkerhet.....	9
Säkerheten i nätverk, produkter och system .....	17
Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter.....	19
Förebygga och bekämpa it-relaterad brottslighet .....	20
Främjande av kunskap och kompetensutveckling .....	21
Stärkt samarbete på EU-nivå och internationellt .....	23
Skrivelsen .....	25
Reservationer .....	26
1. En generell förstärkning av informations- och cybersäkerheten, punkt 1 (M, C, L, KD).....	26
2. Åtgärder för en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet, punkt 2 (M) .....	27
3. Översyn av de regelverk som styr kommunernas krav på informations- och cybersäkerhet, punkt 3 (M, C, L, KD).....	28
4. Sanktioner, punkt 4 (M, C, L, KD).....	28
5. Samverkan, punkt 5 (M, C, L, KD) .....	29
6. Ny myndighet för cybersäkerhet, punkt 6 (KD) .....	30
7. Säkerheten i nätverk, produkter och system, punkt 7 (M, C, L, KD) ...	31
8. Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter, punkt 8 (M).....	32
9. Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter, punkt 8 (C) .....	33
10. Förebygga och bekämpa it-relaterad brottslighet, punkt 9 (M, C, L, KD).....	34
11. Främjande av kunskap och kompetensutveckling, punkt 10 (M) .....	34
12. Främjande av kunskap och kompetensutveckling, punkt 10 (SD).....	35
13. Främjande av kunskap och kompetensutveckling, punkt 10 (C) .....	36
14. Stärkt samarbete på EU-nivå och internationellt, punkt 11 (M, C, L, KD).....	37
15. Stärkt samarbete på EU-nivå och internationellt, punkt 11 (SD).....	38
<i>Bilaga</i>	
Förteckning över behandlade förslag .....	40
Skrivelsen .....	40
Följdmotionerna .....	40
Motioner från allmänna motionstiden 2017/18 .....	41

# Utskottets förslag till riksdagsbeslut

## 1. En generell förstärkning av informations- och cybersäkerheten

Riksdagen avslår motionerna

2017/18:226 av Daniel Bäckström (C) yrkande 3,

2017/18:639 av Penilla Gunther (KD),

2017/18:1133 av Edward Riedl (M),

2017/18:3220 av Allan Widman m.fl. (L, M, C, KD) yrkande 7,

2017/18:3765 av Daniel Bäckström m.fl. (C) yrkande 23 och

2017/18:3833 av Jessica Rosencrantz m.fl. (M) yrkande 48.

*Reservation 1 (M, C, L, KD)*

## 2. Åtgärder för en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

Riksdagen avslår motionerna

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 1,

2017/18:2343 av Stig Henriksson m.fl. (V) yrkande 3,

2017/18:3005 av Sofia Fölster (M),

2017/18:3221 av Hans Wallmark m.fl. (M) yrkandena 2, 3 och 5,

2017/18:3222 av Hans Wallmark m.fl. (M) yrkande 31 och

2017/18:3566 av Ulf Kristersson m.fl. (M) yrkande 21.

*Reservation 2 (M)*

## 3. Översyn av de regelverk som styr kommunernas krav på informations- och cybersäkerhet

Riksdagen avslår motion

2017/18:226 av Daniel Bäckström (C) yrkande 1.

*Reservation 3 (M, C, L, KD)*

## 4. Sanktioner

Riksdagen avslår motionerna

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 3 och

2017/18:2343 av Stig Henriksson m.fl. (V) yrkande 4.

*Reservation 4 (M, C, L, KD)*

## 5. Samverkan

Riksdagen avslår motionerna

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 6 och

2017/18:3222 av Hans Wallmark m.fl. (M) yrkande 26.

*Reservation 5 (M, C, L, KD)*

**6. Ny myndighet för cybersäkerhet**

Riksdagen avslår motionerna

2017/18:306 av Mikael Oscarsson m.fl. (KD) och

2017/18:3827 av Mikael Oscarsson m.fl. (KD) yrkande 41.

*Reservation 6 (KD)*

**7. Säkerheten i nätverk, produkter och system**

Riksdagen avslår motionerna

2017/18:341 av Hans Wallmark m.fl. (M) yrkandena 2 och 4 samt

2017/18:3221 av Hans Wallmark m.fl. (M) yrkande 4.

*Reservation 7 (M, C, L, KD)*

**8. Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter**

Riksdagen avslår motionerna

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 5,

2017/18:2017 av Mikael Jansson m.fl. (SD) yrkande 80,

2017/18:3331 av Björn Söder m.fl. (SD) yrkande 17 och

2017/18:3765 av Daniel Bäckström m.fl. (C) yrkande 16.

*Reservation 8 (M)*

*Reservation 9 (C)*

**9. Förebygga och bekämpa it-relaterad brottslighet**

Riksdagen avslår motion

2017/18:226 av Daniel Bäckström (C) yrkande 2.

*Reservation 10 (M, C, L, KD)*

**10. Främjande av kunskap och kompetensutveckling**

Riksdagen avslår motionerna

2017/18:226 av Daniel Bäckström (C) yrkande 4,

2017/18:353 av Roger Richtoff m.fl. (SD) yrkande 1 och

2017/18:3221 av Hans Wallmark m.fl. (M) yrkande 6.

*Reservation 11 (M)*

*Reservation 12 (SD)*

*Reservation 13 (C)*

**11. Stärkt samarbete på EU-nivå och internationellt**

Riksdagen avslår motionerna

2017/18:226 av Daniel Bäckström (C) yrkande 5,

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 7,

2017/18:353 av Roger Richtoff m.fl. (SD) yrkandena 2 och 3,

2017/18:431 av Robert Hannah (L),

2017/18:446 av Robert Hannah (L),

2017/18:2017 av Mikael Jansson m.fl. (SD) yrkande 81,

2017/18:3331 av Björn Söder m.fl. (SD) yrkande 18 och

2017/18:3684 av Annie Lööf m.fl. (C) yrkande 35.

*Reservation 14 (M, C, L, KD)*

*Reservation 15 (SD)*

## **12. Skrivelsen**

Riksdagen lägger skrivelse 2016/17:213 till handlingarna.

Stockholm den 7 december 2017

På försvarsutskottets vägnar

*Allan Widman*

Följande ledamöter har deltagit i beslutet: Allan Widman (L), Hans Wallmark (M), Peter Jeppsson (S), Lena Asplund (M), Alexandra Völker (S), Mikael Jansson (SD), Jan R Andersson (M), Kent Härstedt (S), Daniel Bäckström (C), Anders Schröder (MP), Lotta Olsson (M), Paula Holmqvist (S), Lotta Johnsson Fornarve (V), Mikael Oscarsson (KD), Mattias Ottosson (S) och Lena Emilsson (S).

# Redogörelse för ärendet

## Ärendet och dess beredning

Regeringen anger att det finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. Den aktuella nationella strategin för samhällets informations- och cybersäkerhet är ett uttryck för regeringens övergripande prioriteringar och syftar till att vara en plattform för Sveriges fortsatta utvecklingsarbete inom området.

Justitie- och inrikesminister Morgan Johansson redogjorde bl.a. för regeringens arbete med informations- och cybersäkerhetsfrågor i utskottet den 17 oktober 2017.

Generaldirektörerna för Säpo och för Försvarets radioanstalt (FRA) samt chefen för den militära säkerhets- och underrättelsetjänsten (Must) informerade utskottet om myndigheternas cybersäkerhetsarbete den 23 november 2017.

Förutom följdmotioner till skrivelsen behandlas i betänkandet även motionsyrkanden om informations- och cybersäkerhet från den allmänna motionstiden 2017/18.

## Bakgrund

### Behovet av en strategi

Regeringen understryker i skrivelsen att digitaliseringen är ett globalt fenomen som påverkar i stort sett alla delar av vårt samhälle. Digitaliseringen är en av vår tids största förändringar, och den snabba utvecklingen av informations- och kommunikationsteknologi har stor inverkan på vår framtid. Det medför stora möjligheter, men också risker. Hur vi hanterar de risker som följer av digitaliseringen har stor betydelse för vår förmåga att upprätthålla och stärka både vårt välstånd och vår säkerhet. Alla behöver ta sitt ansvar för informations- och cybersäkerhetsfrågor för att Sverige ska uppnå en effektiv och säker hantering av information, anför regeringen.

Regeringen anser också att utmaningarna inom informations- och cybersäkerhetsområdet delas med andra länder. De strategiska lösningarna måste därför även utvecklas genom internationell samverkan och dialog kring förebyggande åtgärder, både inom EU och i andra internationella organ.

Genom ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet kan den fortsatta digitaliseringen av samhället säkerställas, samtidigt som man också hävdar Sveriges säkerhet och nationella intressen såsom mänskliga fri- och rättigheter och samhällets funktionalitet, menar regeringen. Ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet är också en viktig förutsättning för svensk tillväxt och konkurrenskraft och en

nödvändighet för att näringslivet ska kunna utveckla och tillhandahålla konkurrenskraftiga varor och tjänster. För att höja informations- och cybersäkerheten finns det ett behov av att alla berörda parter i högre grad samverkar mot gemensamma målsättningar. Mot denna bakgrund har regeringen beslutat att ta fram en nationell strategi för samhällets informations- och cybersäkerhet. Strategin är ett uttryck för regeringens övergripande prioriteringar och syftar till att vara en plattform för Sveriges fortsatta utvecklingsarbete inom området.

## Definitioner

Med informations- och cybersäkerhet avses i skrivelsen en uppsättning säkerhetsåtgärder för bevarande av konfidentialitet, riktighet och tillgänglighet av information. Med konfidentialitet avses att obehöriga inte ska kunna ta del av informationen. Med riktighet menas att informationen inte förändras, manipuleras eller förstörs på ett obehörigt sätt. Med tillgänglighet menas att behöriga ska kunna ha tillgång till informationen på det sätt och vid den tidpunkt som tjänsterna erbjuder. För informationssäkerhet som avser digital information används i skrivelsen även begreppet cybersäkerhet. I skrivelsen används begreppen beroende av sitt sammanhang, där exempelvis cybersäkerhetsbegreppet är vanligt förekommande i en internationell kontext.

## Utgångspunkter

Strategin för samhällets informations- och cybersäkerhet har sin utgångspunkt i målen för Sveriges säkerhet, anför regeringen: att värna befolkningens liv och hälsa, liksom samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter (prop. 2008/09:140, bet. 2008/09:FöU10, rskr. 2008/09:292). Strategin har även sin utgångspunkt i det it-politiska målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter (prop. 2011/12:1, bet. 2011/12:TU1, rskr. 2011/12:87).

Strategin för samhällets informations- och cybersäkerhet bygger på och konkretiserar de inriktningar för informations- och cybersäkerheten som regeringen anger i den nationella säkerhetsstrategin och i digitaliseringsstrategin (N2017/03643/D).

I dag finns bestämmelser om informationssäkerhet i olika regelverk. Informationssäkerhet är en av tre grundläggande säkerhetsskyddsåtgärder enligt säkerhetsskyddslagen (1996:627). Lagstiftningen gäller för de mest skyddsvärda verksamheterna i samhället och innebär långtgående krav på olika skyddsåtgärder. För övriga statliga myndigheter gäller de krav på informationssäkerheten som framgår av förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap. Bestämmelser om informationssäkerhet finns även i arkivlagen (1990:782), personuppgiftslagen (1998:204) och lagen (2003:389) om elektronisk kommunika-

tion. Utöver dessa författningar finns myndighetsföreskrifter som reglerar informationssäkerhet inom ett flertal sektorer.

Flera författningar som reglerar informationssäkerhet kommer att förändras eller tillkomma inom de kommande åren, anger regeringen. Det pågår för närvarande en översyn av säkerhetsskyddslagstiftningen med förslag om att bl.a. utvidga lagens tillämpningsområde för att uppnå ett bättre skydd för Sveriges säkerhet (SOU 2015:25). Europaparlamentets och rådets direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen (NIS-direktivet), som ska vara genomfört i svensk lagstiftning senast i maj 2018, anger bl.a. en skyldighet för alla medlemsstater att anta en nationell strategi för säkerhet i nätverk och informationssystem. En annan EU-lag, Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning), kommer att börja tillämpas i maj 2018 och innebär högre krav på hanteringen av personuppgifter.

Flera utredningar och granskningar inom informations- och cybersäkerhetsområdet har de senaste åren pekat på brister i förhållande till dagens hot och risker. Bland annat har Riksrevisionen granskat informationssäkerheten i statsförvaltningen (RiR 2016:8 och RiR 2014:23). Även betänkandet Informations- och cybersäkerhet i Sverige innehåller ett flertal förslag på informations- och cybersäkerhetsområdet (SOU 2015:23). I den försvarspolitiska inriktningspropositionen bedömde regeringen att Sveriges samlade förmåga att förebygga, motverka och aktivt hantera konsekvenser av civila och militära hot, händelser, attacker och angrepp i cybermiljön måste utvecklas och förstärkas (prop. 2014/15:109).



# Utskottets överväganden

## En systematisk och samlad ansats i arbetet med informations- och cybersäkerhet

### Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet, dvs. yrkandena om en generell förstärkning av området, åtgärder för en systematisk och samlad ansats, översyn av regelverk, sanktioner, samverkan och en ny myndighet för cybersäkerhet. Utskottet hänvisar till pågående arbete.

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

### Skrivelsen

Regeringen anger inledningsvis att det finns ett stort behov av att utveckla samhällets informations- och cybersäkerhet. Den aktuella nationella strategin för samhällets informations- och cybersäkerhet är ett uttryck för regeringens övergripande prioriteringar och syftar till att vara en plattform för Sveriges fortsatta utvecklingsarbete inom området. Huvudsyftena med strategin är att bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Regeringen vill genom strategin även stödja de insatser och det engagemang som redan finns i samhället för att stärka informations- och cybersäkerheten. Strategin omfattar därmed hela samhället, dvs. statliga myndigheter, kommuner och landsting, företag, organisationer och privatpersoner.

För att sårbarheter ska minska och för att målen för Sveriges säkerhet och it-politik ska kunna främjas är det regeringens bedömning att man i arbetet med samhällets informations- och cybersäkerhet framför allt behöver prioritera att

- säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet
- öka säkerheten i nätverk, produkter och system
- stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter
- öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet
- öka kunskapen och främja kompetensutvecklingen
- stärka det internationella samarbetet.

För var och en av dessa prioriteringar ställer regeringen i skrivelsen upp ett antal målsättningar och anger en inriktning för hur målsättningarna ska nås.

För att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet och för att bedriva ett systematiskt informations-säkerhetsarbete anger regeringen målsättningarna att statliga myndigheter, kommuner, landsting, företag och andra organisationer ska ha kännedom om hot och risker, ta ansvar för sin informationssäkerhet och bedriva ett systematiskt informationssäkerhetsarbete och att det ska finnas en nationell modell till stöd för ett systematiskt informationssäkerhetsarbete.

Regeringen ska därför verka för att öka tydligheten i myndighetsstyrningen och lyfta betydelsen av ett tillfredsställande informationssäkerhetsarbete internt på myndigheterna, och verka för att förutsättningarna förbättras för samhällets olika aktörer när det gäller att bedriva ett systematiskt informationssäkerhetsarbete och göra mer enhetliga bedömningar av hot, risker och säkerhetsåtgärder, genom att en nationell modell för systematiskt informationssäkerhetsarbete tas fram.

Regeringen menar vidare att en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet kräver att samverkan och informationsdelning på informations- och cybersäkerhetsområdet stärks.

Regeringen ska därför verka för att samverkan mellan myndigheter med särskilda uppgifter på informations- och cybersäkerhetsområdet stärks och för att ändamålsenlig informationsdelning och samverkan mellan privata och offentliga aktörer säkerställs.

Ytterligare en målsättning är att det ska finnas en ändamålsenlig tillsyn som skapar förutsättningar för en ökad informations- och cybersäkerhet i samhället.

Regeringen ska därför verka för att säkerhetsskyddslagstiftningen bättre möter de förändrade kraven på säkerhetsskydd inom informationssäkerhetsområdet, bl.a. genom ett adekvat system för sanktioner och en effektiv tillsyn, att NIS-direktivet genomförs effektivt, att det etableras en adekvat styrning och tillsyn av säkerheten i nätverk och informationssystem i samhällsviktig verksamhet för vissa aktörer inom de utpekade sektorerna och att behovet av ytterligare åtgärder för att utveckla tillsynen av informationssäkerheten i hela samhället bevakas.

## **Bakgrund och tidigare behandling**

I samband med Riksrevisionens rapport om informationssäkerhetsarbete på nio myndigheter och regeringens påföljande skrivelse underströk utskottet i betänkande 2016/17:FöU8, på samma sätt som Riksrevisionen gjort i sin rapport, att man i statsförvaltningen hanterar mycket information som är skyddsvärd och att ett seriöst arbete med informationssäkerhet bör ha som mål att all skyddsvärd information ska vara tillgänglig, riktig, konfidentiell och spårbar. Eftersom informationssäkerhet är en fråga som berör all personal i en myndighet bör en allomfattande kultur skapas för att minimera riskerna för störningar i olika samhällsfunktioner. Utskottet fann likt tidigare att alla myndigheters

roll och ansvar i arbetet borde framhållas, både ur ett ansvars- och ur ett samverkansperspektiv.

Av dessa skäl fann utskottet det därför oroande att Riksrevisionen i sin nyligen genomförda granskning av nio myndigheter funnit att arbetet med informationssäkerhet på de granskade myndigheterna ”ligger på en nivå som är märkbart under vad som är tillräckligt” och – att döma av Riksrevisionens tidigare rapporter – inte ser ut att ha utvecklats i tillräcklig grad över tid. Även Myndigheten för samhällsskydd och beredskap (MSB) underströk i sin nationella risk- och förmågebedömning för 2016 (publikationsnummer MSB1012) att myndigheter behöver utveckla arbetet med sin informations- och cybersäkerhet.

Utskottet fann dock att regeringens arbete med att ta fram en nationell strategi för samhällets informations- och cybersäkerhet i närtid var lovtvårt och att detta förhoppningsvis kunde innebära ett bättre stöd till myndigheterna i informationssäkerhetsarbetet och en starkare styrning från regeringen gentemot myndigheterna men också samhället i stort. Utskottet ansåg att detta var nödvändigt för att kunna hantera hot eller risker från exempelvis stater, statsunderstödda aktörer, terrorister och organiserad brottslighet samt fel och störningar som inte orsakas av antagonister utan beror på mjuk- eller hårdvarufel, processbrister, bristande kvalitetskontroll, slarv, missbedömningar eller rena olycksfall. Regeringen borde bedriva arbetet skyndsamt, ansåg utskottet.

Inom ramen för det övergripande strategiarbetet såg utskottet också fram emot regeringens utredning som skulle lämna förslag på hur NIS-direktivet borde genomföras i svensk rätt samt beredningen av betänkandet En ny säkerhetsskyddslag (SOU 2015:25) som innehåller förslag om hur säkerhetsskyddsregleringen bör reformeras. Dessa var viktiga pusselbitar i sammanhanget, underströk utskottet.

På grundval av detta pågående arbete ansåg utskottet det därför inte motiverat att vidta ytterligare åtgärder, och föreslog sålunda att riksdagen lade skrivelse 2016/17:42 Riksrevisionens rapport om informationssäkerhetsarbete på nio myndigheter till handlingarna och att samtliga motionsyrkanden i ärendet skulle avslås.

Ur ett mer militärt perspektiv ansåg utskottet i betänkande 2016/17:FöU3 att cyberfrågorna var av stor vikt och att Sverige måste se dessa med ett strategiskt och långsiktigt perspektiv. Behovet av en svensk cyberförmåga hade flera gånger behandlats av utskottet. Utskottet stod fast vid tidigare bedömning att grunden i en robust cyberförsvarsförmåga bör vara att kunna skydda samhällsviktiga funktioner och sådana system som är vitala för totalförsvaret mot antagonistiska it-angrepp från kvalificerade statliga och statsunderstödda aktörer. Utskottet lade fortfarande stor vikt vid att Sverige borde kunna genomföra aktiva operationer i cybermiljön och välkomnade därför att regeringen hade gett Försvarsmakten i uppdrag att med stöd av FRA analysera och redovisa hur förmågan att utföra aktiva operationer i cybermiljön kunde utvecklas.

Utskottet delade motionärernas syn på behovet av ett aktivt cyberförsvar men bedömde samtidigt, mot bakgrund av vad regeringen anfört om det pågående arbetet, att det inte fanns behov av ytterligare åtgärder på området. Samtliga motionsyrkanden avstyrktes därför.

## **Motionerna**

### *En generell förstärkning av informations- och cybersäkerheten*

Allan Widman m.fl. (L, M, C, KD) föreslår i motion 2017/18:3220 att det bör ses över hur skyddet för samhällsviktig infrastruktur och verksamhet kan stärkas, detta bl.a. mot bakgrund av det stora antalet it-attacker mot svenska myndigheter och Transportstyrelsens agerande när de lade ut hanteringen av mycket känslig information på entreprenad (yrkande 7).

I följdmotion 2017/18:226 anför Daniel Bäckström (C) att en god informations- och cybersäkerhet är mycket viktig men att arbetet behöver utvecklas ordentligt. Regeringen tar viktiga steg i den nationella strategin för samhällets informations- och cybersäkerhet men når inte riktigt ända fram för att skrivelsen ska göra skäl för sitt namn, menar motionären, som bl.a. föreslår i yrkande 3, tillika i motion 2017/18:3765 (yrkande 23), att Sverige bör förbereda sig bättre och mer resolut för det förändrade säkerhetsläget. Motionärerna föreslår därför, mot bakgrund av Transportstyrelsens hantering av känsliga it-uppgifter och många kommuners avsaknad av ett systematiskt arbete med informations-säkerhet, att åtgärder bör vidtas för att säkra it-hanteringen och stärka it- och cybersäkerheten generellt men inte minst för de verksamheter – privata och offentliga – som äger och driver samhällsviktig verksamhet eller infrastruktur eller i övrigt hanterar frågor som rör rikets säkerhet.

Penilla Gunther (KD) föreslår i motion 2017/18:639 att det bl.a. mot bakgrund av det stora antalet cyberattacker som sker varje dag – inte minst mot svenska intressen – och händelserna kring Transportstyrelsens hantering av it-system bör tas ett helhetsgrepp om cybersäkerheten för infrastrukturen i Sverige.

I motion 2017/18:3833 anför Jessica Rosencrantz m.fl. (M) att det blir allt vanligare med it-angrepp mot samhällsviktig infrastruktur. Motionärerna föreslår därför att it-infrastrukturen i hela landet bör ha ett skydd som svarar upp mot det försämrade säkerhetspolitiska läget (yrkande 48).

Edward Riedl (M) föreslår i motion 2017/18:1133 att myndigheternas arbete med informationssäkerhet bör ses över eftersom det på senare tid framkommit att deras arbete med informationssäkerhet är bristfälligt.

### *Åtgärder för en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet*

Hans Wallmark m.fl. (M) anför i följdmotion 2017/18:341 att en väl fungerande informations- och cybersäkerhet är helt grundläggande för att samhället ska kunna fungera såväl i fred som i kris och krig. Under de senaste åren har

flera granskningar pekat på allvarliga brister i säkerhetsskyddsarbetet hos både offentliga och privata aktörer. Under det senaste året har även bristerna i säkerhetsskyddet åskådliggjorts genom ett antal omfattande cyberangrepp. Motionärerna anser inte heller att Regeringskansliet – så som det är organiserat för närvarande – klarar av att hantera säkerhetsskyddsfrågor som berör rikets säkerhet på ett adekvat sätt. Regeringens skrivelse kan mer liknas vid en vision än en strategi, och skrivelsen saknar besked om hur målsättningarna i strategin ska uppnås och med vilka medel, menar motionärerna. Mot den bakgrunden föreslås därför i yrkande 1, tillika i motion 2017/18:3566 yrkande 21 av Ulf Kristersson m.fl. (M) och i motion 2017/18:3221 yrkande 2 av Hans Wallmark m.fl. (M), att ansvaret för it-säkerheten bör samlas och tydliggöras, t.ex. genom inrättandet av ett myndighetsråd.

För att kunna möta risker och hot ska Sverige ha en god krisberedskap föreslår Hans Wallmark m.fl. (M) vidare i motion 2017/18:3221 att det bör skapas en utredningsgrupp som analyserar regelverk och processer för it-säkerhet hos myndigheter och i ett andra steg föreslår relevanta åtgärder (yrkande 3) och att kraven på it-säkerhet hos leverantörer och ägare till större it-system bör ses över (yrkande 5).

Hans Wallmark m.fl. (M) anför i motion 2017/18:3222 att de attacker som skett mot it-system på senare år innebär ett stort hot mot samhällets funktionalitet såväl i fred som i händelse av kris och konflikt. Motionärerna föreslår därför att det kontinuerligt bör tas fram och utvecklas nationella strategier och strukturer för cybersäkerhet (yrkande 31). Motionärerna menar att säkerhetskrisen hos Transportstyrelsen tydligt visat på vikten av att skärpa arbetet med it- och cybersäkerhet i Sverige.

I motion 2017/18:3005 föreslår Sofia Fölster (M) att rutinerna för it-säkerhet i Regeringskansliet och vid svenska myndigheter bör ses över, detta mot bakgrund av att det framkommit att stora mängder sekretessbelagd information som handhas av Transportstyrelsen läckt ut och potentiellt spridits till främmande makt. Även regeringens handläggning av ärendet kan ifrågasättas, anför motionären.

Stig Henriksson m.fl. (V) anför i motion 2017/18:2343 att informationssäkerhetsarbetet inom staten under lång tid har varit alltför dåligt. Motionärerna förslår att regeringen bör återkomma under mandatperioden med en strategi för statens informations- och cybersäkerhet utifrån SOU 2015:23 (yrkande 3).

### *Översyn av de regelverk som styr kommunernas krav på informations- och cybersäkerhet*

Daniel Bäckström (C) anför i följdmotion 2017/18:226 att det är minst lika viktigt som en nationell modell för systematisk informationshantering att det finns tydlig styrning, lagar och regler som gör att aktörer måste beakta, ta hänsyn till och arbeta med systematisk informationssäkerhet i sin verksamhet. Skrivelsen tycks i huvudsak vara inriktad på statliga myndigheter, och ofta saknas resonemang om hur statsmaktens regelstyrning när de gäller informa-

tionssäkerhet kan tydliggöras för aktörer som inte är statliga myndigheter, menar motionären som vidare hävdar att det är uppenbart att dagens regelverk inte är tillräckligt för att få exempelvis kommuner att arbeta systematiskt med informationssäkerhet. Motionären föreslår därför att det bör ses över om de befintliga regelverk som styr kommunernas krav på informations- och cybersäkerhet, inklusive tillsyn, är tillräckliga eller behöver tydliggöras (yrkande 1).

### *Sanktioner*

Hans Wallmark m.fl. (M) föreslår i följdmotion 2017/18:341 att ett sanktions-system för överträdelse mot säkerhetsskyddslagen snarast bör införas för att få till stånd en välfungerande informations- och cybersäkerhet (yrkande 3).

I motion 2017/18:2343 anför Stig Henriksson m.fl. (V) att informationssäkerhetsarbetet inom staten under lång tid har varit alltför dåligt. Motionärerna föreslår att regeringen bör fastställa en tidsplan för när målen i strategin ska vara uppfyllda och överväga sanktionsmöjligheter för de myndigheter som inte uppfyller godtagbara krav på informations- och cybersäkerhet (yrkande 4).

### *Samverkan*

Hans Wallmark m.fl. (M) föreslår vidare i följdmotion 2017/18:341 att det görs en särskild översyn av hur samverkan med näringslivet kan förbättras för att åstadkomma en välfungerande informations- och cybersäkerhet (yrkande 6).

I motion 2017/18:3222 anför Hans Wallmark m.fl. (M) också att de attacker som skett mot it-system på senare år innebär ett stort hot mot samhällets funktionalitet såväl i fred som i händelse av kris och konflikt. Motionärerna föreslår därför att ett nätverk med frivilliga it-expertiser från privat och offentlig sektor bör skapas för att motverka hotet (yrkande 26).

### *Ny myndighet för cybersäkerhet*

Mikael Oscarsson m.fl. (KD) föreslår i följdmotion 2017/18:306, liksom i motion 2017/18:3827 yrkande 41, att en myndighet bör inrättas för cybersäkerhet. Motionärerna anser att för att möta aktuella problem på området, inklusive de problem som tas upp i skrivelsen, räcker regeringens förslag på åtgärder inte särskilt långt.

## **Utskottets ställningstagande**

Utskottet ser positivt på regeringens nationella strategi för samhällets informations- och cybersäkerhet för att kunna uppnå och bevara konfidentialitet, riktighet och tillgänglighet av information.

Den nationella och internationella digitalisering som sker i dag går i rasande fart och för inte bara med sig möjligheter till utveckling. Det finns alltför många exempel på hur obehöriga aktörer kommit åt eller fått möjligheter att

komma åt känslig information. Inte minst Riksrevisionens granskningar har visat på att informationssäkerheten hos svenska myndigheter inte utvecklats tillräckligt under ett antal år. Utskottet ser det därför som välkommet att en strategi på området presenterats av regeringen. Den kommer att bidra till att skapa långsiktiga förutsättningar för informations- och cybersäkerheten för hela det svenska samhället. Utskottet ser fram emot ytterligare konkretiseringar av de förslag på målsättningar och åtgärder som redan finns på nedanstående och prioriterade områden samt den uppdatering av strategin som är aviserad av regeringen till 2018.

När det gäller *en generell förstärkning av informations- och cybersäkerheten, specifika åtgärder för en systematisk och samlad ansats i arbetet och en översyn av de regelverk som styr kommunernas krav på området* anser utskottet i enlighet med regeringen att den aktuella strategin är själva basen för att kunna säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet. Utskottet ser därför positivt på att regeringen inom ramen för denna strategi avser att bl.a. verka för att öka tydligheten i myndighetsstyrningen och lyfta betydelsen av ett tillfredsställande informationssäkerhetsarbete internt på myndigheter, att ta fram en nationell modell för systematiskt informationssäkerhetsarbete samt att verka för att samverkan och informationsdelning kan stärkas på området. Utskottet anser också att regeringens intention att verka för att säkerhetsskyddslagstiftningen bättre möter de förändrade kraven på säkerhetsskydd inom informationssäkerhetsområdet är välkommet, bl.a. genom ett adekvat system för sanktioner och en effektiv tillsyn, att NIS-direktivet genomförs effektivt och att det etableras en adekvat styrning och tillsyn av säkerheten i nätverk och informationssystem i samhällsviktig verksamhet.

Utskottet ser med anledning av den presenterade strategin inte skäl att vidta ytterligare åtgärder för tillfället vad gäller att skapa en systematisk och samlad ansats utan avstyrker motionerna 2017/18:226 (C) yrkandena 1 och 3, 2017/18:341 (M) yrkande 1, 2017/18:639 (KD), 2017/18:1133 (M), 2017/18:2343 (V) yrkande 3, 2017/18:3005 (M), 2017/18:3220 (L, M, C, KD) yrkande 7, 2017/18:3221 (M) yrkandena 2, 3, och 5, 2017/18:3222 (M) yrkande 31, 2017/18:3566 (M) yrkande 21, 2017/18:3765 (C) yrkande 23 samt 2017/18:3833 (M) yrkande 48.

Vad gäller *sanktioner* framgår det av skrivelsen att regeringen den 23 mars 2017 gav en särskild utredare i uppdrag att bl.a. utreda och föreslå ett system med sanktioner i säkerhetsskyddslagstiftningen (dir. 2017:32). Utredaren ska också genomföra en översyn av bestämmelserna om tillsyn enligt säkerhetsskyddslagen och lämna förslag om hur en ändamålsenlig tillsyn över säkerhetskänslig verksamhet ska vara utformad. Utredningen ska redovisas i maj 2018.

Utskottet ser vikten av att tillsyn kan kombineras med sanktionsmöjligheter men ser inte skäl att vidta ytterligare åtgärder för tillfället i väntan på utredningens resultat och avstyrker därför motionerna 2017/18:341 (M) yrkande 3 och 2017/18:2343 (V) yrkande 4.

I fråga om *samverkan* redovisar regeringen i skrivelsen flera goda exempel på samverkan på informationssäkerhetsområdet i Sverige. Samverkansgruppen för informationssäkerhet (SAMFI) spelar t.ex. en viktig roll genom att verka för säker informationstillgång i samhället. Regeringen ser dock ett behov av en utvecklad och fördjupad myndighetssamverkan för att höja informations- och cybersäkerheten i samhället. Ett exempel på detta behov är att ett antal nya myndigheter kommer att få nya uppgifter på informations- och cybersäkerhetsområdet när NIS-direktivet genomförs i svensk lagstiftning genom en proposition under våren 2018. På informations- och cybersäkerhetsområdet finns också flera exempel på plattformar för privat-offentlig samverkan. Utskottet anser liksom regeringen att det är viktigt att samverkan utvecklas utifrån ett helhetsperspektiv. Det är positivt att regeringen avser att verka ytterligare för att samverkan mellan myndigheter med särskilda uppgifter på informations- och cybersäkerhetsområdet stärks och för att en ändamålsenlig informationsdelning och samverkan mellan privata och offentliga aktörer säkerställs.

Eftersom regeringen, förutom den aviserade propositionen, också uttrycker att strategin efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motionerna 2017/18:341 (M) yrkande 6 och 2017/18:3222 (M) yrkande 26 avstyrks.

När det gäller förslaget om *en ny myndighet för cybersäkerhet* anser utskottet i grunden att arbetet med informationssäkerhet är ett ansvar för hela samhället och alla aktörer. I enlighet med den vedertagna ansvarsprincipen bör berörda aktörer ansvara för att identifiera och möta informationspåverkan inom sina respektive ansvarsområden. Utskottet instämmer med regeringen om att det i sammanhanget är särskilt viktigt med samverkan och en gemensam riktning för arbetet på området, för ingen kan lösa säkerhetsutmaningarna ensam. Även om den enskilda organisationen ytterst ansvarar för att hantera sin information är det i dagsläget enligt utskottet viktigare att förbättra förutsättningarna att bedriva ett systematiskt och samordnat informationssäkerhetsarbete än att skapa en för ändamålet särskild myndighet, något som inte bedöms som kostnadseffektivt eller ändamålsenligt. Utskottet anser alltså att det fortsätta arbetet bör bedrivas inom befintliga myndighetsstrukturer och bygga på samverkan. SAMFI spelar redan i dag en viktig roll genom att verka för säker informationstillgång i samhället. NIS-direktivets genomförande i svensk rätt kommer också att ställa ytterligare samverkanskrav. En gemensam modell för systematiskt informationssäkerhetsarbete bör kunna öka samverkan inom området eftersom en sådan kan göra det enklare för organisationer att möta relevanta krav och styra sitt informationssäkerhetsarbete samtidigt som expert- och tillsynsmyndigheternas kompetens används mer effektivt, vilket också regeringen anger i skrivelsen.



Eftersom regeringen dessutom uttrycker att strategin efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motionerna 2017/18:306 (KD) och 2017/18:3827 (KD) yrkande 41 avstyrks.

## Säkerheten i nätverk, produkter och system

### Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om säkerheten i nätverk, produkter och system. Utskottet hänvisar till pågående arbete.

Jämför reservation 7 (M, C, L, KD).

### Skrivelsen

För att öka säkerheten i nätverk, produkter och system och skapa en säker infrastruktur för elektronisk kommunikation anger regeringen målsättningarna som att elektroniska kommunikationer ska vara effektiva, säkra och robusta samt kunna tillgodose användarnas behov av att elektronisk kommunikation i Sverige ska vara tillgänglig oberoende av funktioner utanför landets gränser, och att tillsynsmyndighetens behov av att kunna vidta adekvata åtgärder ska kunna säkerställas.

Regeringen ska därför verka för att elektroniska kommunikationsnät byggs på ett sådant sätt att de kan fungera oberoende av funktioner i andra länder, att aktörer inom allmän ordning, säkerhet, hälsa och försvar har tillgång till moderna, säkra och robusta kommunikationslösningar, att myndigheternas kompetens i fråga om upphandling av nätverk, produkter och system stärks, att myndigheterna vid upphandlingar säkerställer att hänsyn tas till säkerhetsaspekter och att Post- och telestyrelsens (PTS) förutsättningar att verka för en hög nivå av nät- och informationssäkerhet inom sektorn för elektronisk kommunikation stärks.

Tillgången till säkra kryptosystem för it- och kommunikationslösningar ska vidare motsvara behoven i samhället. Regeringen ska därför verka för att en nationell strategi och åtgärdsplan för säkra kryptosystem genomförs.

För att säkerheten i industriella informations- och styrsystem ska öka ska regeringen verka för att företag och myndigheter som äger eller arbetar med samhällsviktig verksamhet där industriella informations- och styrsystem ingår får stöd i sitt arbete med att stärka informationssäkerheten och att företag med verksamhet inom t.ex. verkstads- och processindustri där industriella informations- och styrsystem fyller viktiga funktioner får utvecklade förutsättningar till stöd för att stärka sitt arbete med informationssäkerhet.

## Motionerna

Hans Wallmark m.fl. (M) föreslår i följdmotion 2017/18:341 yrkande 2, liksom i motion 2017/18:3221 yrkande 4, att möjligheten att använda lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet i större utsträckning bör ses över. I motion 2017/18:341 föreslås också att behovet av ett svenskt myndighetsmoln bör utredas (yrkande 4).

## Utskottets ställningstagande

Utskottet instämmer med regeringen i att det är nödvändigt för att öka säkerheten i nätverk, produkter och system samt för att skapa en säker infrastruktur för elektronisk kommunikation att bl.a. verka för att elektroniska kommunikationsnät byggs på ett sådant sätt att de kan fungera oberoende av funktioner i andra länder och att aktörer inom allmän ordning, säkerhet, hälsa och försvar har tillgång till moderna, säkra och robusta kommunikationslösningar. Regeringen uttrycker bl.a. att den avser att verka för att en nationell strategi och åtgärdsplan för säkra kryptosystem genomförs, vilket utskottet ger sitt stöd åt.

Eftersom strategin enligt regeringen efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motion 2017/18:341 (M) yrkande 4 om behovet av ett svenskt myndighetsmoln avstyrks.

Utskottet ger vidare stöd åt regeringens syn att stödet vid upphandling av säker elektronisk kommunikation och andra it-relaterade tjänster bör stärkas och att det är viktigt att de verksamheter som har behov av en hög nivå av driftssäkerhet inom kommunikationsnät och it-relaterade tjänster ställer krav på detta vid upphandling.

Eftersom regeringen uttrycker att den ska verka för att myndigheternas kompetens i fråga om upphandling av nätverk, produkter och system stärks och att myndigheterna vid upphandlingar säkerställer att hänsyn tas till säkerhetsaspekter ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motionerna 2017/18:341 (M) yrkande 2 och 2017/18:3221 (M) yrkande 4 avstyrks därmed.

## Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter

### Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter. Utskottet hänvisar till pågående arbete.

Jämför reservation 8 (M) och 9 (C).

### Skrivelsen

I fråga om att stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter anger regeringen att målsättningarna är att förmågan ska förbättras, att berörda aktörer ska kunna agera samordnat för att hantera cyberattacker och andra allvarliga it-incidenter och att det ska finnas ett utvecklat cyberförsvar för Sveriges mest skyddsvärda verksamheter med en förstärkt militär förmåga att möta och hantera angrepp från kvalificerade motståndare i cyberrymden.

Regeringen ska därför verka för att det finns en samordnad planering mellan myndigheterna i händelse av en cyberattack eller annan allvarlig it-incident, att verksamheter i behov av kontinuerlig bevakning och med särskilda behov av skydd får tillgång till ett sensor- eller detekterings- och varningssystem samt att ett effektivt och sömlöst cyberförsvar med förmågan att förebygga, upptäcka och hantera cyberangrepp – både för militär och för civil verksamhet – fortsätter att utvecklas och förstärkas, vilket även inkluderar att Försvarsmakten utvecklar sin förmåga att försvara Sverige mot kvalificerade angripare i cyberrymden.

### Motionerna

Hans Wallmark m.fl. (M) föreslår i följdmotion 2017/18:341 att en inriktning eller doktrin bör tas fram för när, var och hur en aktiv svensk cyberförmåga ska kunna användas (yrkande 5).

I motion 2017/18:3765 anför Daniel Bäckström m.fl. (C) att Sverige måste förbereda sig bättre och mer resolut för det förändrade säkerhetsläget. Motionärerna föreslår därför att åtgärder bör vidtas, t.ex. med hjälp av frivilliga försvarsorganisationer, för att kunna möta hybridhot i form av påverkanskampanjer såväl som cyberattacker (yrkande 16).

Mikael Jansson m.fl. (SD) föreslår i motion 2017/18:2017 yrkande 80, liksom Björn Söder m.fl. (SD) gör i motion 2017/18:3331 yrkande 17, att Sverige bör skaffa ett aktivt informationsteknologiskt försvar (aktiv cyberförmåga) som bör hålla svenska myndigheter med en standardplattform för datahantering, och kan förhindra dataintrång hos svenska myndigheter. Ett sådant it-försvar bör vara en underavdelning i en ny civilförsvarsmyndighet.

## Utskottets ställningstagande

Utskottet lägger stor vikt vid att Försvarsmakten utvecklar sin förmåga att försvara Sverige mot kvalificerade angripare i cyberrymden. Utskottet ger stöd åt regeringens intention att verka för ett effektivt cyberförsvar med förmågan att förebygga, upptäcka och hantera cyberangrepp, både för militär och för civil verksamhet. Att det finns en samordnad planering mellan myndigheter och andra aktörer i händelse av en cyberattack eller annan allvarlig it-incident och att verksamheter i behov av kontinuerlig bevakning och med särskilda behov av skydd får tillgång till ett sensor- eller detekterings- och varningssystem ser utskottet också som en viktig förutsättning för en god svensk informations säkerhet.

Eftersom regeringen uttrycker att strategin efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motionerna 2017/18:341 (M) yrkande 5, 2017/18:2017 (SD) yrkande 80, 2017/18:3331 (SD) yrkande 17 och 2017/18:3765 (C) yrkande 16 avstyrks.

## Förebygga och bekämpa it-relaterad brottslighet

### Utskottets förslag i korthet

Riksdagen avslår motionsyrkandet om att förebygga och bekämpa it-relaterad brottslighet. Utskottet hänvisar till pågående arbete.

Jämför reservation 10 (M, C, L, KD).

## Skrivelsen

Vad gäller att öka möjligheterna att förebygga och bekämpa it-relaterad brottslighet anger regeringen målsättningarna till att de brottsbekämpande myndigheterna ska ha beredskap och förmåga att bekämpa it-relaterade brott på ett effektivt och ändamålsenligt sätt och att arbetet med att förebygga it-relaterade brott ska utvecklas.

Regeringen ska därför verka för att lagstiftningen är anpassad för att effektivt kunna motverka den it-relaterade brottsligheten, att de brottsbekämpande myndigheterna ges förutsättningar att – med hänsyn till skydd av den personliga integriteten och rättssäkerheten – upprätthålla sin förmåga att inhämta information, att de brottsbekämpande myndigheterna säkerställer en adekvat organisation och tillräckliga resurser för att effektivt kunna förebygga och bekämpa den it-relaterade brottsligheten samt att de brottsbekämpande myndigheterna systematiskt arbetar för att utveckla kompetens och arbetsmetoder för att förebygga och bekämpa it-relaterad brottslighet. Regeringen ska också verka för att medvetenheten och kunskapen ökar hos andra aktörer än de

brottsbekämpande om hur de kan bidra i arbetet med att förebygga it-relaterade brott samt att det internationella samarbetet mot it-relaterad brottslighet förstärks i syfte att bidra till en ökad lagföring i Sverige.

### **Motionen**

Daniel Bäckström (C) föreslår i följdmotion 2017/18:226 att regeringens strategi bör kompletteras med ambitioner och förslag för att motverka den ökade trenden med cyberbaserat industriellt ekonomiskt spionage, detta för att arbetet med en god informations- och cybersäkerhet ska kunna utvecklas ordentligt (yrkande 2).

### **Utskottets ställningstagande**

Regeringens intention att verka för att lagstiftningen är anpassad för att effektivt kunna motverka it-relaterad brottslighet och för att de brottsbekämpande myndigheterna ges förutsättningar att – med hänsyn till skydd av den personliga integriteten och rättssäkerheten – upprätthålla sin förmåga att inhämta information får stöd av utskottet. Detta inkluderar en adekvat organisation och tillräckliga resurser för att effektivt kunna förebygga och bekämpa den it-relaterade brottsligheten inklusive cyberbaserat industriellt ekonomiskt spionage.

Eftersom strategin enligt regeringen efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motion 2017/18:226 (C) yrkande 2 avstyrks.

## **Främjande av kunskap och kompetensutveckling**

### **Utskottets förslag i korthet**

Riksdagen avslår motionsyrkandena om främjande av kunskap och kompetensutveckling. Utskottet hänvisar till pågående arbete.

Jämför reservation 11 (M), 12 (SD) och 13 (C).

### **Skrivelsen**

Regeringen anger i sin skrivelse att för att öka kunskapen och främja kompetensutvecklingen är målsättningarna att kunskapen i samhället som helhet om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka och att kunskapen hos enskilda användare av digital teknik om de mest angelägna sårbarheterna och behoven av säkerhetsåtgärder ska öka.

Regeringen ska därför verka för att berörda myndigheter utvecklar arbetet med att genomföra och stödja kartläggningar och utredningar om sårbarheter och lämpliga säkerhetsåtgärder i samhället samt verka för att höja människors

kunskap om sårbarheter och lämpliga säkerhetsåtgärder som var och en kan vidta för att skydda sig.

Ytterligare en målsättning är att det ska bedrivas högre utbildning samt forskning och utveckling av hög kvalitet om informations- och cybersäkerhet och säkerhet på it- och telekomområdet i Sverige.

Regeringen ska därför verka för att lärosäten, industriforskningsinstitut, näringsliv och offentlig sektor samverkar för att öka nyttiggörande och innovation inom informations- och cybersäkerhetsområdet, och för att informations- och cybersäkerhet ska beaktas i samtliga strategiska samverkansprogram.

I fråga om övningsverksamhet är målsättningen att det regelbundet ska genomföras både tvärssektoriella och tekniska informations- och cybersäkerhetsövningar för att stärka Sveriges förmåga att hantera konsekvenserna av allvarliga it-incidenter.

Regeringen ska därför verka för att förmågan att hantera allvarliga it-incidenter upprätthålls genom en samordnad övningsverksamhet.

## Motionerna

Roger Richtoff m.fl. (SD) välkomnar i följdmotion 2017/18:353 att regeringen lägger fram ett förslag till en nationell strategi på cybersäkerhetsområdet då den utveckling som ägt rum inom svenska myndigheter har lett till att man i flera fall har fattat beslut som i mycket hög grad har lett till att informations-säkerheten har satts på spel. Motionärerna menar dock att det finns problematiska inslag i den föreslagna strategin och föreslår därför att behovet av myndighetsintern it-säkerhetskompetens bör ses över (yrkande 1).

I följdmotion 2017/18:226 föreslår Daniel Bäckström (C) att det bör tas fram strategier för ett generellt kompetenslyft i fråga om informations- och cybersäkerhet och säkerhetsskydd för att arbetet ska kunna utvecklas ordentligt (yrkande 4).

Hans Wallmark m.fl. (M) föreslår i motion 2017/18:3221 att möjligheten att stärka medborgarnas kunskap om it-säkerhet bör ses över, detta för att man ska kunna möta olika risker och hot i samhället (yrkande 6).

## Utskottets ställningstagande

Utskottet anser likt regeringen att det är nödvändigt att främja kunskaps- och kompetensutvecklingen på informationssäkerhetsområdet i samhället och ger därför stöd åt regeringens intention att verka för att berörda myndigheter utvecklar arbetet med att genomföra och stödja kartläggningar och utredningar om sårbarheter och lämpliga säkerhetsåtgärder i samhället. Utskottet ger också sitt stöd åt regeringens intention att verka för att människors kunskap höjs om sårbarheter och lämpliga säkerhetsåtgärder som var och en kan vidta för att skydda sig.

Eftersom regeringen uttrycker att strategin efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att

de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motionerna 2017/18:226 (C) yrkande 4, 2017/18:353 (SD) yrkande 1 och 2017/18:3221 (M) yrkande 6 avstyrks.

## Stärkt samarbete på EU-nivå och internationellt

### Utskottets förslag i korthet

Riksdagen avslår motionsyrkandena om stärkt samarbete på EU-nivå och internationellt. Utskottet hänvisar till pågående arbete.

Jämför reservation 14 (M, C, L, KD) och 15 (SD).

### Skrivelsen

I fråga om EU-samarbetet och det internationella samarbetet uttrycker regeringen målsättningen att sådana samarbeten kring cybersäkerhet ska stärkas inom ramen för målsättningen om ett globalt, tillgängligt, öppet och robust internet som präglas av frihet och respekt för mänskliga rättigheter.

Regeringen ska därför verka för att stärka Sveriges samlade agerande som aktör inom relevanta internationella processer (inom bl.a. FN, EU, Organisationen för säkerhet och samarbete i Europa och i partnerskapet med Nato) och i samarbeten med likasinnade länder (i Norden, närområdet, inom EU och med globala partner), att motverka tendenser till fragmentering av internet och begränsning av globala flöden samt att motverka en statsledd förvaltning av internet och värna de icke-statliga aktörernas roller och ansvar. Regeringen ska också verka för att stärka internationella samarbeten kring cybersäkerhet och cyberförsvar för att hantera hot och sårbarheter, att stärka internationella samarbeten kring tillämpningen av internationell rätt och förebyggande av konflikter, t.ex. genom etablering av frivilliga normer och förtroendeskapande åtgärder samt att främja ett öppet, fritt och säkert internet till stöd för mänskliga rättigheter och global utveckling.

Cybersäkerhet ska främjas inom ramen för ambitionen att värna fria flöden till stöd för innovation, konkurrenskraft och samhällsutveckling, anger regeringen vidare.

Regeringen ska därför verka för att fortsätta Sveriges ledarskap inom EU på det digitala området och driva den digitala agendan framåt, genom att fullborda den digitala inre marknaden, genom att vara drivande i diskussioner om framtidsfrågor och genom att EU aktivt och offensivt motverkar digital protektionism samtidigt som legitima allmänna ändamål som dataskydd och nationell säkerhet respekteras.

Regeringen uttrycker avslutningsvis i skrivelsen att säkerhetsutmaningarna inte kommer att kunna lösas en gång för alla. Teknik- och hotutvecklingen innebär att informations- och cybersäkerhetsområdet förändras och utvecklas i snabb takt. Detta återspeglas bl.a. i förändrade regler och krav på EU-nivå och internationellt. Strategin måste ha en flexibilitet och kunna anpassas till

de snabba omvärldsförändringarna och är därför inte tidssatt utan kommer att behöva uppdateras vid behov. Regeringens avsikt är att genomföra en första sådan uppdatering 2018 i syfte att anpassa strategin till de nya bestämmelser och övriga konsekvenser som genomförandet av NIS-direktivet i svensk rätt kommer att innebära.

### **Motionerna**

Hans Wallmark m.fl. (M) föreslår i följdmotion 2017/18:341 att en tydlig svensk linje för det internationella arbetet med it-säkerhet bör tas fram (yrkande 7).

I följdmotion 2017/18:226 föreslår Daniel Bäckström (C) att regeringen bör verka för att EU får en större och tydligare roll vad gäller cybersäkerhet för att arbetet ska kunna utvecklas ordentligt (yrkande 5).

Annie Lööf m.fl. (C) anför i motion 2017/18:3684 att Sverige ska ha en så god motståndskraft som möjligt för att upptäcka och stå emot cyberattacker och olaga intrång. Motionärerna föreslår därför att Sverige bör driva att minimikraven för informationssäkerhet i alla EU:s medlemsländer höjs eftersom inget system är starkare än sin svagaste länk (yrkande 35).

I följdmotion 2017/18:353 föreslår Roger Richtoff m.fl. (SD) att Sverige inte bör göra sig beroende av EU för att kunna upprätthålla en tillräckligt hög säkerhet på den digitala arenan (yrkande 2), samt att EU:s arbete i fråga om lokaliseringskrav bör motverkas av Sverige då grundprincipen bör vara att det är de enskilda medlemsstaterna som avgör vilka krav man kan ställa på företag när det gäller lagring av data eftersom det är staterna som avgör vilka behov som måste finnas inom landets gränser (yrkande 3).

Mikael Jansson m.fl. (SD) anför i motion 2017/18:2017 yrkande 81, liksom Björn Söder m.fl. (SD) gör i motion 2017/18:3331 yrkande 18, att det nordiska samarbetet bör öka inom en rad frågor på försvars- och säkerhetsområdet. Ett sådant försvarssamarbete i fred med nordiska och även baltiska grannar skulle syfta till att spara pengar genom kostnadsdelning. Motionärerna föreslår därför att Sverige bör undersöka möjligheterna till ett nordiskt säkert internet baserat på svenska mikrosatelliter.

I motionerna 2017/18:431 och 2017/18:446 föreslår Robert Hannah (L) att Sverige bör verka för skapandet av en FN-konvention om cyberkrigföring. Motionären anför att Sverige bör verka för gemensamma spelregler som skyddar individer, företag och stater från it-angrepp under både freds- och krigstid.

### **Utskottets ställningstagande**

Utskottet har flera gånger uttryckt vikten av samarbete inom EU inom olika områden och anser att det är nödvändigt med samarbete inom EU och internationellt också för att främja informations- och cybersäkerheten eftersom den digitala utvecklingen är gränslös. Utskottet instämmer med regeringen om att Sverige bör verka för att fortsätta Sveriges ledarskap inom EU på det digitala



området och driva den digitala agendan framåt. Likt regeringen anser utskottet att det också är viktigt att Sverige verkar för att stärka sitt samlade agerande som aktör inom andra relevanta internationella processer, t.ex. FN och i partnerskapet med Nato och i samarbeten med likasinnade länder, t.ex. de nordiska, för att stärka internationella samarbeten på området.

Eftersom strategin enligt regeringen efter behov kommer att följas av specifika uppdrag och andra styrande åtgärder till berörda myndigheter för att de angivna målsättningarna ska kunna nås ser utskottet inte skäl att vidta några ytterligare åtgärder för tillfället. Motionerna 2017/18:226 (C) yrkande 5, 2017/18:341 (M) yrkande 7, 2017/18:353 (SD) yrkandena 2 och 3, 2017/18:431 (L), 2017/18:446 (L), 2017/18:2017 (SD) yrkande 81, 2017/18:3331 (SD) yrkande 18, samt 2017/18:3684 (C) yrkande 35 avstyrks.

## Skrivelsen

### **Utskottets förslag i korthet**

Riksdagen lägger skrivelse 2016/17:213 Nationell strategi för samhällets informations- och cybersäkerhet till handlingarna.

### **Utskottets ställningstagande**

Med det som anförts ovan föreslår utskottet att riksdagen lägger skrivelsen till handlingarna.

# Reservationer

## 1. En generell förstärkning av informations- och cybersäkerheten, punkt 1 (M, C, L, KD)

av Allan Widman (L), Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD).

### *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

2017/18:226 av Daniel Bäckström (C) yrkande 3,

2017/18:3220 av Allan Widman m.fl. (L, M, C, KD) yrkande 7 och

2017/18:3765 av Daniel Bäckström m.fl. (C) yrkande 23 och

bifaller delvis motionerna

2017/18:639 av Penilla Gunther (KD),

2017/18:1133 av Edward Riedl (M) och

2017/18:3833 av Jessica Rosencrantz m.fl. (M) yrkande 48.

### *Ställningstagande*

Vi föreslår att det bör ses över hur skyddet av samhällsviktig infrastruktur och verksamhet kan stärkas i Sverige, detta bl.a. mot bakgrund av det stora antalet it-attacker som skett mot svenska myndigheter och Transportstyrelsens agerande när man lade ut hanteringen av mycket känslig information på entreprenad. Cyberinfrastrukturen i hela landet bör därför ha ett skydd som svarar upp mot det försämrade säkerhetspolitiska läget, och det bör tas ett helhetsgrepp i denna fråga.

Vi föreslår sålunda, också mot bakgrund av många kommuners avsaknad av ett systematiskt arbete med informationssäkerhet, att åtgärder bör vidtas för att säkra it-hanteringen och stärka it- och cybersäkerheten generellt men inte minst för de verksamheter – privata och offentliga – som äger och driver samhällsviktig verksamhet eller infrastruktur eller i övrigt hanterar frågor som rör rikets säkerhet.

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

## 2. Åtgärder för en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet, punkt 2 (M)

av Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M) och Lotta Olsson (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  
2017/18:341 av Hans Wallmark m.fl. (M) yrkande 1,  
2017/18:3221 av Hans Wallmark m.fl. (M) yrkandena 2, 3 och 5,  
2017/18:3222 av Hans Wallmark m.fl. (M) yrkande 31 och  
2017/18:3566 av Ulf Kristersson m.fl. (M) yrkande 21 och  
avslår motionerna  
2017/18:2343 av Stig Henriksson m.fl. (V) yrkande 3 och  
2017/18:3005 av Sofia Fölster (M).

### *Ställningstagande*

Under de senaste åren har flera granskningar pekat på allvarliga brister i säkerhetsskyddsarbetet hos både offentliga och privata aktörer. Säkerhetskrisen hos Transportstyrelsen har tydligt visat på vikten av att skärpa arbetet med it- och cybersäkerhet i Sverige, anser vi. Under det senaste året har även bristerna i säkerhetsskyddet åskådliggjorts genom ett antal omfattande cyberangrepp.

Vi anser inte att Regeringskansliet på ett adekvat sätt klarar av att hantera säkerhetsskyddsfrågor som rör rikets säkerhet utan att regeringens skrivelse mer kan liknas vid en vision än en strategi. Skrivelsen saknar även besked om hur målsättningarna i strategin ska uppnås och med vilka medel.

De attacker som skett mot it-system på senare år innebär ett stort hot mot samhällets funktionalitet såväl i fred som i händelse av kris och konflikt. Vi föreslår därför att nationella strategier och strukturer för cybersäkerhet kontinuerligt bör utvecklas.

Då en väl fungerande informations- och cybersäkerhet är grundläggande för att samhället ska kunna fungera såväl i fred som i kris och krig föreslår vi bl.a. att ansvaret för it-säkerheten bör samlas och tydliggöras, t.ex. genom inrättandet av ett myndighetsråd.

Vi föreslår vidare att det bör skapas en utredningsgrupp som analyserar regelverk och processer för it-säkerhet hos myndigheter och i ett andra steg föreslår relevanta åtgärder. Dessutom bör kraven på it-säkerhet hos leverantörer och ägare till större it-system ses över.

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

### **3. Översyn av de regelverk som styr kommunernas krav på informations- och cybersäkerhet, punkt 3 (M, C, L, KD)**

av Allan Widman (L), Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD).

#### *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

2017/18:226 av Daniel Bäckström (C) yrkande 1.

#### *Ställningstagande*

Vi anser att regeringen tar viktiga steg i den nationella strategin för samhällets informations- och cybersäkerhet men inte riktigt når ända fram för att skrivelsen ska göra skillnad för sitt namn. För oss är det uppenbart att dagens regelverk inte är tillräckligt för att få exempelvis kommuner att arbeta systematiskt med informationssäkerhet, och vi föreslår därför att det bör ses över om de befintliga regelverk som styr kommunernas krav på informations- och cybersäkerhet, inklusive tillsyn, är tillräckliga eller behöver tydliggöras.

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

### **4. Sanktioner, punkt 4 (M, C, L, KD)**

av Allan Widman (L), Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD).

#### *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

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 3 och avslår motion

2017/18:2343 av Stig Henriksson m.fl. (V) yrkande 4.

### *Ställningstagande*

I fråga om ett sanktionssystem kopplat till säkerhetsskyddslagen saknas i dag sanktionsmöjligheter mot den aktör som har brutit mot säkerhetsskyddslagens bestämmelser om informations- och cybersäkerhet. Detta är en brist som måste åtgärdas, anser vi. Det räcker inte med att det finns relevanta bestämmelser om säkerhetskänslig verksamhet. För att skapa en större tyngd i lagstiftningen måste den även innehålla en möjlighet att vidta sanktioner mot dem som bryter mot bestämmelserna. För närvarande pågår ett utredningsarbete (dir. 2017:32) när det gäller möjligheten att införa ett sanktionssystem kopplat till säkerhetsskyddslagen. Utredningen ska presentera sina förslag senast den 1 maj 2018.

Vi föreslår att ett sanktionssystem för överträdelse mot säkerhetsskyddslagen snarast bör införas för att få till stånd en väl fungerande informations- och cybersäkerhet.

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

### **5. Samverkan, punkt 5 (M, C, L, KD)**

av Allan Widman (L), Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD).

### *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 motionerna  
2017/18:341 av Hans Wallmark m.fl. (M) yrkande 6 och  
2017/18:3222 av Hans Wallmark m.fl. (M) yrkande 26.

### *Ställningstagande*

Samhällets funktionalitet är i dag starkt beroende av näringslivet för att betalningsströmmar, elförsörjning och informationsflöden ska fungera, bara för att ta några exempel.

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

Regeringens nationella strategi för samhällets informations- och cybersäkerhet innehåller dock inga konkreta förslag på hur samverkan med näringslivet kan förbättras och hur samhällets it-säkerhet som helhet kan dra nytta av den teknikkompetens som finns på området i Sverige.

Vi föreslår därför att en särskild översyn av hur samverkan med näringslivet kan förbättras bör göras för att åstadkomma en väl fungerande informations- och cybersäkerhet samt att ett nätverk med frivilliga it-experter från privat och offentlig sektor bör skapas för att motverka hoten.

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

## **6. Ny myndighet för cybersäkerhet, punkt 6 (KD)**

av Mikael Oscarsson (KD).

### *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 motionerna

2017/18:306 av Mikael Oscarsson m.fl. (KD) och

2017/18:3827 av Mikael Oscarsson m.fl. (KD) yrkande 41.

### *Ställningstagande*

Vårt samhälle, liksom de flesta samhällen i världen, är och blir alltmer beroende av informationsteknik. Cyberangrepp kan leda till mycket omfattande följder för samhället, i vissa avseenden lika förödande som ett angrepp med konventionella vapen. Till skillnad från konventionella angrepp kan det vara utomordentligt svårt att identifiera vem som står bakom ett cyberangrepp. Hot om cyberangrepp kan dessutom utnyttjas i utpressningssyfte, inte bara mot företag och organisationer utan även mot regeringar. Jag anser att samhället därför måste ha en god förmåga att såväl möta direkta angrepp som avskräcka en eventuell angripare. Det kan bara ske på samma arena som hotet uppträder – cyberarenan. Det finns i dag sex myndigheter i Sverige som har ett av regeringen utsett ansvar för informationssäkerheten i samhället. Dessa myndigheter ingår i Samverkansgruppen för informationssäkerhet (SAMFI). Samverkan skulle underlättas om den hanterades av en för ändamålet utpekad organisation. En sådan organisation skulle också ha en viktig roll genom att kunna ge råd till de företag, myndigheter och organisationer vars verksamhet är starkt beroende av fungerande it-system. Jag föreslår därför att det bör inrättas en myndighet för cybersäkerhet.

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

## **7. Säkerheten i nätverk, produkter och system, punkt 7 (M, C, L, KD)**

av Allan Widman (L), Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD).

### *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 motionerna

2017/18:341 av Hans Wallmark m.fl. (M) yrkandena 2 och 4 samt

2017/18:3221 av Hans Wallmark m.fl. (M) yrkande 4.

### *Ställningstagande*

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

Vi föreslår därför att regeringen bör se över hur offentliga aktörer ska kunna använda sig av lagen (2011:1029) om upphandling på försvars- och säkerhetsområdet (LUFSS) i större utsträckning. LUFSS innehåller till skillnad från LOU bestämmelser om bl.a. informationssäkerhet och stärker därmed möjligheterna för bl.a. myndigheter att ställa krav utifrån nödvändiga säkerhetskänsligheter.

Frågan om en gemensam statlig molntjänst för myndigheternas it-drift har lyfts av flera aktörer. Tidigare under året redovisade Statens servicecenter ett förslag om att en statlig molntjänst bör införas där merparten av de statliga myndigheternas it-drift bör samordnas. Enligt utredningen skulle en statlig molntjänst hantera många av de utmaningar som finns när det gäller myndigheternas it-drift. Det skulle innebära samordningsvinster och i förlängningen besparingar för myndigheterna, en förenkling för myndigheterna och viktigast av allt – it-säkerheten och driftssäkerheten skulle förstärkas kraftigt. Även FRA har förordat en molntjänst för Sveriges myndigheter och de statliga bolagen.

Vi vill även lyfta fram möjligheten att en statlig molntjänst skulle minska den Stockholmskoncentration som i dag finns inom myndigheternas it-drift och därmed skapa kvalificerade arbetstillfällen på andra platser i Sverige och dessutom minska sårbarheten vid t.ex. ett större strömavbrott i Stockholmsområdet.

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

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

## **8. Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter, punkt 8 (M)**

av Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M) och Lotta Olsson (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 motion

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 5 och avslår motionerna

2017/18:2017 av Mikael Jansson m.fl. (SD) yrkande 80,

2017/18:3331 av Björn Söder m.fl. (SD) yrkande 17 och

2017/18:3765 av Daniel Bäckström m.fl. (C) yrkande 16.

### *Ställningstagande*

I regeringens inriktningsproposition för försvaret beskrivs den svenska cyberförmågan. Inriktningspropositionen bygger på den försvarsuppgörelse som träffades i april 2015 mellan Moderaterna, Centerpartiet och Kristdemokraterna samt Socialdemokraterna och Miljöpartiet. I den står bl.a. att ”i det nya osäkrare säkerhetspolitiska läget är försvarsunderrättelse- och cyberförsvarsförmåga centralt. Grunden för denna förmåga är att kunna skydda vitala system från angrepp. För det krävs att även kunna genomföra aktiva operationer i cybermiljön”.

Sverige ska med andra ord ha en aktiv (offensiv) förmåga att genomföra cyberattacker mot andra aktörer. Konceptet med en aktiv cyberförmåga är dock inte oproblemiskt och kräver att centrala frågor om hur, när och var förmågan ska kunna användas besvaras. Rättsläget när det gäller huruvida krigets lagar och internationell rätt är tillämplbara på cyberkrigföring är oklart även om dessa lagar rent generellt ska tillämpas teknikneutralt baserat bl.a. på principerna om proportionalitet om urskiljning. Aktiv cyberförmåga är dessutom ett instrument som kan ha långtgående konsekvenser på samhällets funktionalitet hos det land som utsätts för det. Vissa menar därmed att det är att jämställa med massförstörelsevapen. Ytterst handlar den aktiva cyberförmågan om att hindra andra aktörer från att genomföra cyberangrepp mot samhällsviktig verksamhet eftersom Sverige då har en förmåga till vedergällning. Men för att denna förmåga ska vara effektiv och inte behöva användas krävs det att den kommuniceras på ett tydligt och vederhäftigt sätt.



Vi föreslår därför att regeringen bör återkomma med en inriktning eller doktrin för när, var och hur den aktiva cyberförmågan eventuellt ska användas. Alternativt bör detta bli föremål för ett kompletterande uppdrag för Försvarsberedningen i syfte att uppnå en bred politisk samsyn i frågan.

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

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

## **9. Förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter, punkt 8 (C)**

av Daniel Bäckström (C).

### *Förslag till riksdagsbeslut*

Jag 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 motion

2017/18:3765 av Daniel Bäckström m.fl. (C) yrkande 16 och avslår motionerna

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 5,

2017/18:2017 av Mikael Jansson m.fl. (SD) yrkande 80 och

2017/18:3331 av Björn Söder m.fl. (SD) yrkande 17.

### *Ställningstagande*

Jag anser att Sverige måste förbereda sig bättre och mer resolut för det förändrade säkerhetsläget. Jag ser bl.a. att det finns ett behov av att bättre kunna möta hybridhot i form av t.ex. påverkanskampanjer och cyberattacker och tror att det kan finnas ett mervärde i att det finns frivilliga försvarsorganisationer som kan hantera det moderna samhällets sårbarheter inom it och desinformation. På så sätt kan man också nå människor som annars inte skulle söka sig till totalförsvaret. Detta är bra för folkförankringen. Jag föreslår därför att åtgärder bör vidtas, t.ex. med hjälp av frivilliga försvarsorganisationer, för att kunna möta hybridhot i form av påverkanskampanjer såväl som cyberattacker.

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

## **10. Förebygga och bekämpa it-relaterad brottslighet, punkt 9 (M, C, L, KD)**

av Allan Widman (L), Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD).

### *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 motion

2017/18:226 av Daniel Bäckström (C) yrkande 2.

### *Ställningstagande*

Regeringen tar viktiga steg i den nationella strategin för samhällets informations- och cybersäkerhet men når inte riktigt ända fram för att skrivelsen ska göra skäl för sitt namn, anser vi. Det brottsförebyggande perspektivet finns med, men det saknas ambitioner och konkreta förslag för att motverka den ökande trenden av cyberbaserat industriellt ekonomiskt spionage. FRA har identifierat att statsunderstödda cyberaktiviteter mot Sverige inte enbart riktar sig mot föremål som strikt befinner sig inom ramen för nationell säkerhet (försvar m.m.) utan även är riktade mot industrin, forskningen samt kritisk infrastruktur. Vi föreslår därför att regeringens strategi bör kompletteras med ambitioner och förslag för att motverka den ökade trenden med cyberbaserat industriellt ekonomiskt spionage, detta för att arbetet med en god informations- och cybersäkerhet ska kunna utvecklas ordentligt.

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

## **11. Främjande av kunskap och kompetensutveckling, punkt 10 (M)**

av Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M) och Lotta Olsson (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

2017/18:3221 av Hans Wallmark m.fl. (M) yrkande 6 och

avslår motionerna  
2017/18:226 av Daniel Bäckström (C) yrkande 4 och  
2017/18:353 av Roger Richtoff m.fl. (SD) yrkande 1.

### *Ställningstagande*

Vid t.ex. överbelastningsattacker använder sig angripare ofta av kapade datorer som kan tillhöra privatpersoner, myndigheter eller företag. Detta sätter fingret på en viktig problematik. Vilket ansvar går det att lägga på en enskild användare eller ägare till en dator eller server eller på den som är ansvarig för it-säkerheten på ett företag eller en myndighet? Vi anser att det finns ett behov av att höja medvetenheten hos allmänheten om vad man som enskild användare kan göra för att försvåra att ens it-utrustning används i brottsliga syften. Dessutom skulle detta också kunna sätta ribban för vilket ansvar som är möjligt att utkräva. Vi föreslår därför att möjligheten att stärka medborgarnas kunskap om it-säkerhet bör ses över.

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

## **12. Främjande av kunskap och kompetensutveckling, punkt 10 (SD)**

av Mikael Jansson (SD).

### *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

2017/18:353 av Roger Richtoff m.fl. (SD) yrkande 1 och  
avslår motionerna  
2017/18:226 av Daniel Bäckström (C) yrkande 4 och  
2017/18:3221 av Hans Wallmark m.fl. (M) yrkande 6.

### *Ställningstagande*

Jag välkomnar att regeringen lägger fram ett förslag till en nationell strategi på cybersäkerhetsområdet. Den utveckling som har ägt rum inom svenska myndigheter har uppenbarligen lett till att man i flera fall har fattat beslut som i mycket hög grad har lett till att informationssäkerheten har satts på spel. När den nya strategin nu antas är det alltså ett välkommet steg i rätt riktning. Tyvärr går det ändå att se att det finns problematiska inslag i regeringens föreslagna strategi, anser jag. Regeringens skrivningar öppnar för att man även i framti-

den kommer att kunna göra misstag av den typ som nyligen har skett på Transportstyrelsen. Det är inte lämpligt att enbart fokusera strategin på möjligheter till extern upphandling av elektronisk kommunikation eftersom detta alltid är ett riskmoment som kan leda till säkerhetsläckor. Det är därför min uppfattning att svenska myndigheter som är beroende av en hög grad av drifts- och informationssäkerhet i högre grad än i dag bör kunna förlita sig på att ha tillräcklig it-kompetens inom den egna myndigheten, alternativt vid en för ändamålet ansvarig myndighet. Jag föreslår därför att behovet av myndighetsintern it-säkerhetskompetens bör ses över.

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

### **13. Främjande av kunskap och kompetensutveckling, 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

2017/18:226 av Daniel Bäckström (C) yrkande 4 och avslår motionerna

2017/18:353 av Roger Richtoff m.fl. (SD) yrkande 1 och

2017/18:3221 av Hans Wallmark m.fl. (M) yrkande 6.

#### *Ställningstagande*

Jag anser att det för ett framgångsrikt informationssäkerhetsarbete krävs förståelse för frågan i en organisations alla funktioner. Ett generellt kunskapslyft om informationssäkerhet och säkerhetsskydd behövs inom de flesta organisationer. Regeringen lyfter fram forskning och högre utbildning inom informationssäkerhetsområdet, vilket är bra men långt ifrån tillräckligt. Det saknas en helhetssyn i den nationella strategin. Det hade varit önskvärt om regeringen också hade kommit med förslag på hur en generell kunskapsförhöjning ska kunna ske. Hur enskilda förhåller sig till säkerheten kring information är ytterst viktigt för att kunna upprätthålla ett gott skydd, men det är tveksamt om de insatser som bedrivs av ett fåtal myndigheter i dag för att öka individens kunskap verkligen är tillräckliga. Jag föreslår därför att det bör tas fram strategier för ett generellt kompetenslyft i fråga om informations- och cybersäkerhet och säkerhetsskydd för att arbetet ska kunna utvecklas ordentligt.

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

#### **14. Stärkt samarbete på EU-nivå och internationellt, punkt 11 (M, C, L, KD)**

av Allan Widman (L), Hans Wallmark (M), Lena Asplund (M), Jan R Andersson (M), Daniel Bäckström (C), Lotta Olsson (M) och Mikael Oscarsson (KD).

##### *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 motionerna

2017/18:226 av Daniel Bäckström (C) yrkande 5,

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 7 och

2017/18:3684 av Annie Lööf m.fl. (C) yrkande 35 och avslår motionerna

2017/18:353 av Roger Richtoff m.fl. (SD) yrkandena 2 och 3,

2017/18:431 av Robert Hannah (L),

2017/18:446 av Robert Hannah (L),

2017/18:2017 av Mikael Jansson m.fl. (SD) yrkande 81 och

2017/18:3331 av Björn Söder m.fl. (SD) yrkande 18.

##### *Ställningstagande*

It-frågor är per definition internationella och gränsöverskridande. Våra it-system i Sverige är sammankopplade med system i andra länder i ett globalt nätverk. Detta skapar stora möjligheter att ha kontakt och handla med hela världen, men det exponerar oss även för globala hot. Det kan röra sig om en lång rad aktörer som av olika orsaker vill skada Sverige och svenska intressen. På grund av den gränsöverskridande dimensionen i it-frågorna är det internationella samarbetet för att stärka it-säkerheten centralt. För svenskt vidkommande måste vi ha en tydlig position kring hur vi ser på frågorna och hur vi vill agera i internationella forum. Det kräver att Sverige kan definiera vad vi anser vara mest skyddsvärt, var de främsta samarbetsvinsterna finns och med vilka aktörer Sverige vill samverka. Regeringen säger sig vilja verka för ett starkare internationellt samarbete på detta område men klargör inte hur den avser att driva dessa frågor inom olika organisationer eller vad den vill åstadkomma. Vi föreslår därför att regeringen bör ta fram en tydlig svensk linje i det internationella arbetet med it-säkerhet.

Vi hade gärna också sett tydligare resonemang och förslag om hur regeringen vill att EU ska utvecklas på cyberområdet. Nätverks- och informationssystem, och internet i synnerhet, spelar en viktig roll för rörligheten för varor, tjänster och personer inom EU. Eftersom så mycket är sammanlänkat kan också små avbrott snabbt bli stora och påverka inte bara enskilda människor i

vardagen utan också enskilda länder och EU som helhet. Effektiva åtgärder för att förstärka säkerheten i nätverks- och informationssystemen förutsätter åtgärder på EU-nivå. Även i det operativa arbetet med att hantera cyberkriser kan det finnas anledning att stärka det europeiska samarbetet. Vi föreslår därför att regeringen bör verka för att EU får en större och tydligare roll vad gäller cybersäkerhet för att arbetet ska kunna utvecklas ordentligt. Vi föreslår också att Sverige bör driva att minimikraven för informationssäkerhet i alla EU:s medlemsländer höjs eftersom inget system är starkare än sin svagaste länk.

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

## **15. Stärkt samarbete på EU-nivå och internationellt, punkt 11 (SD)**

av Mikael Jansson (SD).

### *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 motionerna

2017/18:353 av Roger Richtoff m.fl. (SD) yrkandena 2 och 3,

2017/18:2017 av Mikael Jansson m.fl. (SD) yrkande 81 och

2017/18:3331 av Björn Söder m.fl. (SD) yrkande 18 och

avslår motionerna

2017/18:226 av Daniel Bäckström (C) yrkande 5,

2017/18:341 av Hans Wallmark m.fl. (M) yrkande 7,

2017/18:431 av Robert Hannah (L),

2017/18:446 av Robert Hannah (L) och

2017/18:3684 av Annie Lööf m.fl. (C) yrkande 35.

### *Ställningstagande*

Jag är förespråkare av att Sverige på sikt lämnar EU och anser det därför inte rimligt att vårt land bygger upp alltför långtgående och djupa samarbeten på områden som är känsliga. Informationssäkerhets- och cybersäkerhetsområdet måste betraktas som ett sådant med hänvisning till att alltmer av den internationella politikens försök till påverkan, precis som konstateras i skrivelsen, involverar området i olika former. På samma sätt som Sverige har ett eget militärt försvar föreslår jag att Sverige inte bör göra sig beroende av EU för att kunna upprätthålla en tillräckligt hög säkerhet på den digitala arenan.

Jag anser också att regeringen har fel när det gäller bekämpandet av det man kallar digital protektionism. Jag föreslår därför att EU:s arbete med lokaliseringskrav bör motverkas av Sverige då grundprincipen bör vara att det är

de enskilda medlemsstaterna som avgör vilka krav man kan ställa på företag när det gäller lagring av data eftersom det är staterna som avgör vilka behov som måste finnas inom landets gränser.

Det nordiska samarbetet bör öka inom en rad frågor på försvars- och säkerhetsområdet, anser jag vidare. Ett sådant försvarssamarbete i fred med nordiska och även baltiska grannar skulle syfta till att spara pengar genom kostnadsdelning. Jag föreslår därför att Sverige bör undersöka möjligheterna till ett nordiskt, säkert internet baserat på svenska mikrosatelliter.

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

BILAGA

## Förteckning över behandlade förslag

### Skrivelsen

Regeringens skrivelse 2016/17:213 Nationell strategi för samhällets informations- och cybersäkerhet.

### Följdmotionerna

*2017/18:226 av Daniel Bäckström (C):*

1. Riksdagen ställer sig bakom det som anförs i motionen om att se över om de befintliga regelverk som styr kommunernas krav på informations- och cybersäkerhet, inklusive tillsyn, är tillräckliga eller behöver tydliggöras, och detta tillkännager riksdagen för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att strategin behöver kompletteras med ambitioner och förslag för att motverka den ökade trenden med cyberbaserat industriellt ekonomiskt spionage, och detta tillkännager riksdagen för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att åtgärder behöver vidtas för att säkra it-hantering och stärka it- och cybersäkerheten generellt men inte minst för de verksamheter, privata och offentliga, som äger och driver samhällsviktig verksamhet eller infrastruktur eller i övrigt hanterar frågor som rör rikets säkerhet, och detta tillkännager riksdagen för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att ta fram strategier för ett generellt kompetenslyft avseende informations- och cybersäkerhet och säkerhetsskydd och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om att EU bör få en större och tydligare roll vad gäller cybersäkerhet, och detta tillkännager riksdagen för regeringen.

*2017/18:306 av Mikael Oscarsson m.fl. (KD):*

Riksdagen ställer sig bakom det som anförs i motionen om att införa en myndighet för cybersäkerhet och tillkännager detta för regeringen.

*2017/18:341 av Hans Wallmark m.fl. (M):*

1. Riksdagen ställer sig bakom det som anförs i motionen om att samla och tydliggöra ansvaret för it-säkerheten och tillkännager detta för regeringen.



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

*2017/18:353 av Roger Richtoff m.fl. (SD):*

1. Riksdagen ställer sig bakom det som anförs i motionen om behovet av myndighetsintern kompetens i it-säkerhet inom landet och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om samarbete när det gäller cyberförsvar och cybersäkerhet inom EU och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om EU:s arbete mot lokaliseringskrav och tillkännager detta för regeringen.

## Motioner från allmänna motionstiden 2017/18

*2017/18:431 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.

*2017/18:446 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.

*2017/18:639 av Penilla Gunther (KD):*

Riksdagen ställer sig bakom det som anförs i motionen om att det behöver tas ett helhetsgrepp om cybersäkerheten för landets infrastruktur och tillkännager detta för regeringen.

*2017/18:1133 av Edward Riedl (M):*

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

*2017/18:2017 av Mikael Jansson m.fl. (SD):*

80. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige bör skaffa ett aktivt informationsteknologiskt försvar (aktiv cyberförmåga) (avsnitt 26.1.3) och tillkännager detta för regeringen.
81. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige bör undersöka möjligheterna till ett nordiskt, säkert internet baserat på svenska mikrosatelliter (avsnitt 8.1 och 11.7) och tillkännager detta för regeringen.

*2017/18:2343 av Stig Henriksson m.fl. (V):*

3. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen under mandatperioden bör återkomma med en strategi för statens informations- och cybersäkerhet utifrån SOU 2015:23 och tillkännager detta för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att regeringen bör fastställa en tidsplan för när målen i strategin ska vara uppfyllda och överväga sanktionsmöjligheter för de myndigheter som inte uppfyller godtagbara krav på informations- och cybersäkerhet, och detta tillkännager riksdagen för regeringen.

*2017/18:3005 av Sofia Fölster (M):*

Riksdagen ställer sig bakom det som anförs i motionen om att se över rutinerna för it-säkerhet i Regeringskansliet och svenska myndigheter och tillkännager detta för regeringen.

*2017/18:3220 av Allan Widman m.fl. (L, M, C, KD):*

7. Riksdagen ställer sig bakom det som anförs i motionen om att se över hur skyddet för samhällsviktig infrastruktur och verksamhet kan stärkas och tillkännager detta för regeringen.

*2017/18:3221 av Hans Wallmark m.fl. (M):*

2. Riksdagen ställer sig bakom det som anförs i motionen om att samla och tydliggöra ansvaret för it-säkerheten och tillkännager detta för regeringen.
3. Riksdagen ställer sig bakom det som anförs i motionen om att skapa en utredningsgrupp som analyserar regelverk och processer för it-säkerhet hos myndigheter och i ett andra steg föreslår relevanta åtgärder, och detta tillkännager riksdagen för regeringen.
4. Riksdagen ställer sig bakom det som anförs i motionen om att se över möjligheten att använda lagen om upphandling på försvars- och säkerhetsområdet i större utsträckning och tillkännager detta för regeringen.
5. Riksdagen ställer sig bakom det som anförs i motionen om att se över krav på it-säkerhet hos leverantörer och ägare till större it-system och tillkännager detta för regeringen.
6. Riksdagen ställer sig bakom det som anförs i motionen om att se över möjligheten att stärka medborgarnas kunskap om it-säkerhet och tillkännager detta för regeringen.

*2017/18:3222 av Hans Wallmark m.fl. (M):*

26. Riksdagen ställer sig bakom det som anförs i motionen om att skapa ett nätverk med frivilliga it-experter från privat och offentlig sektor och tillkännager detta för regeringen.
31. Riksdagen ställer sig bakom det som anförs i motionen om att kontinuerligt ta fram och utveckla nationella strategier och strukturer för cybersäkerhet och tillkännager detta för regeringen.

*2017/18:3331 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 tillkännager detta för regeringen.
18. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige bör undersöka möjligheterna till ett krypterat datanätverk för de nordiska länderna baserat på svenska mikrosatelliter och tillkännager detta för regeringen.

*2017/18:3566 av Ulf Kristersson m.fl. (M):*

21. Riksdagen ställer sig bakom det som anförs i motionen om att samla och tydliggöra ansvaret för it-säkerheten och tillkännager detta för regeringen.

*2017/18:3684 av Annie Lööf m.fl. (C):*

35. Riksdagen ställer sig bakom det som anförs i motionen om att Sverige ska driva att minimikraven för informationssäkerhet i alla EU:s medlemsländer höjs eftersom inget system är starkare än sin svagaste länk, och detta tillkännager riksdagen för regeringen.

*2017/18:3765 av Daniel Bäckström m.fl. (C):*

16. Riksdagen ställer sig bakom det som anförs i motionen om att kunna möta hybridhot i form av påverkanskampanjer såväl som cyberattacker och tillkännager detta för regeringen.
23. Riksdagen ställer sig bakom det som anförs i motionen om behov av att vidta åtgärder för att stärka it- och cybersäkerheten i de verksamheter – privata och offentliga – som äger och driver samhällsviktig verksamhet och infrastruktur eller i övrigt hanterar frågor som rör rikets säkerhet, och detta tillkännager riksdagen för regeringen.

*2017/18:3827 av Mikael Oscarsson m.fl. (KD):*

41. Riksdagen ställer sig bakom det som anförs i motionen om en myndighet med ansvar för Sveriges cybersäkerhet och tillkännager detta för regeringen.

*2017/18:3833 av Jessica Rosencrantz m.fl. (M):*

48. Riksdagen ställer sig bakom det som anförs i motionen om att it-infrastrukturen i hela landet ska ha ett skydd som svarar upp mot det försämrade säkerhetspolitiska läget och tillkännager detta för regeringen.