En granskningsrapport från Riksrevisionen

Regeringens styrning av samhällets informations- och cybersäkerhet

– både brådskande och viktig

RiR 2023:8

RIKSREVISIONEN

Riksrevisionen är en myndighet under riksdagen med uppgift att granska statliga myndigheter och verksamheter. Vi bedriver både årlig revision och effektivitetsrevision. Genom ett grundlagsskyddat oberoende har Riksrevisionen ett starkt mandat och är en viktig del av riksdagens kontrollmakt som bidrar till förbättringar och demokratisk insyn.

Denna rapport har tagits fram inom effektivitetsrevisionen, vars uppgift är att granska hur effektiv den statliga verksamheten är. Vi lämnar även rekommendationer för att förbättra den granskade verksamheten. Effektivitetsgranskningar lämnas direkt till riksdagen som bereder dem tillsammans med en svarsskrivelse från regeringen.

Riksrevisionen

RiR 2023:8
ISBN 978-91-7086-659-3
ISSN 1652-6597
Omslagets originalfoto: Plattform
Tryck: Riksdagstryckeriet, Stockholm 2023

Beslutad: 2023-04-13
Diarienummer: 3.1.1-2022-0145
RiR 2023:8

Till: Riksdagen

Härmed överlämnas enligt 9 § lagen (2002:1022) om revision av statlig verksamhet m.m. följande granskningsrapport:

Regeringens styrning av samhällets informations- och cybersäkerhet

– både brådskande och viktig

Riksrevisionen har granskat regeringens styrning av samhällets informations- och cybersäkerhet. Resultatet av granskningen redovisas i denna granskningsrapport. Den innehåller slutsatser och rekommendationer som avser regeringen och Regeringskansliet.

Riksrevisor Helena Lindberg har beslutat i detta ärende. Revisionsdirektör Marcus Pettersson har varit föredragande. Enhetschef Jesper Antelius, revisionsdirektör Helena Fröberg och revisor Ylva Ericsson har medverkat i den slutliga handläggningen.

Helena Lindberg

Marcus Pettersson

För kännedom

Regeringskansliet; Finansdepartementet, Försvarsdepartementet, Landsbygds- och infrastrukturdepartementet, Klimat- och näringslivsdepartementet, Justitiedepartementet, Socialdepartementet, Utbildningsdepartementet och Utrikesdepartementet

Riksrevisionen

Riksrevisionen

Innehåll

Sammanfattning

Digitaliseringen har slagit igenom i alla samhällssektorer på alla nivåer. Det ökar behovet av informations- och cybersäkerhet. Cybersäkerhetshotet sägs också öka. Ansvaret för att hantera riskerna, hoten och sårbarheterna samt öka säkerheten är delat, både inom Regeringskansliet och mellan myndigheter. I regeringens informations- och cybersäkerhetsstrategi beskrivs ett antal målsättningar för arbetet. Sex år efter dess införande finns det fortfarande problem inom strategins samtliga områden.

Riksrevisionen har därför granskat om regeringens arbete för att stärka Sveriges informations- och cybersäkerhet har varit effektivt. Riksrevisionens övergripande slutsats är att regeringens arbete inom området inte har varit det. Den centrala bristen är avsaknad av strategiska avvägningar och prioriteringar som inriktar informations- och cybersäkerhetsarbetet. Ett tydligt exempel på brister i strategiska avvägningar är hur Sverige arbetar med frågorna i och gentemot EU. Arbetet i EU bedrivs i hög takt och om Sverige inte är med och påverkar det arbetet tidigt är risken stor att det internationella regelverket inte gynnar svenska intressen i samma utsträckning som annars hade varit möjligt.

Regeringen har inte heller tagit fram eller implementerat den nationella strategin för samhällets informations- och cybersäkerhet enligt internationell bästa praxis. Enligt Riksrevisionen saknar strategin en tydlig vision, uppföljningsbara målsättningar, ansvariga för att genomföra åtgärder och tilldelade resurser för arbetet. I avsaknad av en tydlig politik på området arbetar departementen och myndigheterna utifrån sina respektive mål och prioriteringar. Det gör det svårt att säkerställa att de insatser som görs är rätt insatser för Sveriges samlade informations- och cybersäkerhet, liksom att insatserna genomförs på ett effektivt sätt. Det riskerar att leda till att de åtgärder som vidtas inte får effekt, men också till ett ineffektivt resursutnyttjande.

Regeringens styrning har därför i mångt och mycket utgått från separata sakfrågor som inte har värderats eller rangordnats utifrån vad som gynnar Sverige som helhet. Regeringskansliet har försökt få till bättre sammanhållning i arbetet genom att skapa interdepartementala arbetsgrupper och uppdra åt ett antal myndigheter att skapa ett nationellt cybersäkerhetscenter (NCSC). Riksrevisionens bedömning är att det inte har lett till en ökad förmåga att prioritera insatser utifrån Sveriges samlade behov på informations- och cybersäkerhetsområdet, eller till en långsiktig, strategisk, holistisk och sammanhållen styrning av området. Bristerna har enligt Riksrevisionen lett till en svag styrning av informations- och

cyberssäkerhetsområdet från regeringens sida. Det har också hindrat progression i arbetet med samhällets informations- och cyberssäkerhet.

Informationsutbyte är viktigt för att kunna arbeta mot samma mål och samordna insatser. Riksrevisionens bedömning är att utbyte av information, både inom det offentliga och mellan det offentliga och det privata, i nuläget inte fungerar effektivt. Myndigheterna producerar i dagsläget flera olika och delvis överlappande lägesrapporter, men en rapport som ger överblick saknas. Näringslivet upplever sig inte få tillräcklig information från det offentliga, och uppfattar det som att myndigheterna inte är intresserade av att ta emot information från dem. Även övrig samverkan med näringslivet har varit svår att få till. Exempelvis involverades näringslivet i begränsad omfattning både i framtagandet av strategin och i uppbyggnaden av NCSC. Sammantaget riskerar detta leda till att Regeringskansliet och myndigheterna inte får en god förståelse för näringslivets behov, vad företagen kan bidra med eller en bra lägesbild av de viktigaste riskerna och hoten mot Sverige i cybermiljön. Utbyte av information är behäftat med vissa legala, tekniska och kulturella utmaningar. Det är därför viktigt att Regeringskansliet och myndigheterna hittar strukturer för att hantera de utmaningarna.

Rekommendationer

Riksrevisionen lämnar följande rekommendationer till regeringen:

- Skapa en strategisk, holistisk och långsiktig inriktning för arbetet med informations- och cybersäkerhet. Inriktningen bör omfatta en analys av de nationella strategiska utmaningarna, avvägningar och prioriteringar samt resurstilldelning och handlingsplan för genomförandet. Arbetet bör involvera berörda intressenter.
- Säkerställ en samlad styrning med tydlig ansvarsfördelning, tillräcklig kompetens och effektiva former för samordning av informations- och cybersäkerhetsfrågorna i Regeringskansliet.
- Identifiera hinder för informationsutbyte och se till att det finns strukturer som medger det informationsutbyte som är nödvändigt mellan myndigheter såväl som mellan det offentliga och det privata för att arbetet med samhällets informations- och cybersäkerhet ska fungera effektivt.
- Se över det nationella informations- och cybersäkerhetscentrets uppdrag, mandat och organisatoriska hemvist för att säkerställa dess bidrag till hela samhällets informationssäkerhet såväl som cybersäkerhet.

1 Inledning

1.1 Motiv till granskning

Digitaliseringen har slagit igenom i alla samhällssektorer på alla nivåer. Det ökar behovet av informations- och cybersäkerhet. Cybersäkerhetshotet sägs öka[1], men insynen i risk- och hotbilden samt existerande sårbarheter är begränsad. Konsultföretaget PwC har konstaterat att svenska företag drabbas av cyberattacker i högre utsträckning än motsvarande nordiska företag och att trenden är ökande.[2] Riskerna och hoten är dock svåra att uppskatta och definiera. Mörkertalet är stort på området; attacker som förekommer eller avvärjs, liksom brister som identifieras, blir inte alltid publika. Alla intrång identifieras inte heller. Myndigheten för samhällsskydd och beredskap (MSB) konstaterade i sin årsrapport att stora delar av den offentliga förvaltningen inte arbetar systematiskt med sin informationssäkerhet och att det behövs en generell satsning på att stärka det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.[3]

Enligt beräkningar från EU var kostnaderna för cyberattacker på den globala ekonomin 5,5 miljarder euro under 2020. Enligt Europaparlamentet går skadorna som orsakas av cyberattacker bortom ekonomi och hotar EU:s demokratiska grunder såväl som samhällets grundläggande funktioner. Nödvändiga tjänster och viktiga sektorer som transport, energi, hälsa och finans har blivit alltmer beroende av digitala teknologier. Detta, tillsammans med ett ständigt ökande antal fysiska objekt uppkopplade till nätet kan få stora konsekvenser och kan göra cybersäkerhet till en fråga om liv och död.[4]

Ansvaret för att hantera riskerna, hoten och sårbarheterna samt öka säkerheten är delat, både inom Regeringskansliet och mellan myndigheter. Vissa departement och myndigheter kan sägas vara centrala för arbetet, men är samtidigt inte de enda

1 Säkerhetspolisen (Säpo), *Årsbok 2022*, 2023; Försvarsmakten/Must, *Årsöversikt 2022*, 2023; Försvarets radioanstalt (FRA), *Årsrapport 2022,* 2023 visar att cyberhotet ökar allt mer. FRA konstaterar att ”hotbilden mot Sverige är både bredare och mer komplex än tidigare, och angreppen har intensifierats”. Försvarets radioanstalt, Årsrapport 2020, 2021, s. 29.

2 PwC, *Nordic Cyber Crime Survey 2020,* 2020.

3 Myndigheten för samhällsskydd och beredskap, *När kriget kom nära: årsrapport it-incidentrapportering 2022*, 2023, s. 14.

4 Europaparlamentet, ”Cybersäkerhet: vikten av att minska kostnaderna för cyberattacker”, hämtad 2022-06-08.

som arbetar med frågorna.[5] Det nationella informations- och cybersäkerhetsarbetet är uppdelat i olika, delvis överlappande, ansvarsområden, både på departements- och på myndighetsnivå. Försvarsdepartementet och Justitiedepartementet kan sägas vara centrala. Men även Utrikesdepartementet, Näringsdepartementet, Infrastrukturdepartementet, Utbildningsdepartementet, Finansdepartementet och Socialdepartementet är involverade. Inom varje departement deltar dessutom flera olika enheter i arbetet. Det har dock saknats en sammanhållande funktion inom Regeringskansliet som säkerställer en holistisk styrning avseende informations- och cybersäkerhet. Däremot finns interdepartementala grupper på handläggar-, chefstjänstemanna-, huvudmanna-, och statssekreterarnivå som diskuterar frågorna.[6]

Det delade ansvaret på Regeringskansliet speglas även hos myndigheterna. Försvarets radioanstalt (FRA), Säkerhetspolisen (Säpo), Försvarsmakten, Myndighetens för samhällsskydd och beredskap (MSB), Polismyndigheten, Post- och telestyrelsen (PTS) och Försvarets materielverk (FMV) kan sägas vara de centrala myndigheterna på området. Ingen av dem har däremot ett övergripande ansvar. Regeringens styrning av dem hanteras av tre olika departement och de arbetar mot olika övergripande mål inom sina respektive politikområden. Detta skapar en risk för att regeringens och myndigheternas åtgärder inte är koherenta.[7] Sedan 1990-talet har det vid ett flertal tillfällen[8] framförts synpunkter kring att informations- och cybersäkerhet är en tvärsektoriell fråga som kräver en samlad styrning. Frågans tvärsektoriella natur i kombination med vår förvaltningsmodell med fristående myndigheter ställer stora krav på Regeringskansliets beredningsförmåga. Riksrevisionen identifierade 2014[9] problem kopplade till Regeringskansliets bristande förmåga att bereda frågor rörande informationssäkerhet på ett samlat sätt. Regeringens informations- och cybersäkerhetsstrategi[10] formulerar ett antal strategiska prioriteringar för arbetet. Sex år efter införandet tycks det fortfarande finnas problem inom samtliga av strategins områden. Det är därför angeläget att granska regeringens strategi såväl som åtgärderna för att förverkliga den.

---

5 Exempelvis kan Justitiedepartementet och Försvarsdepartementet sägas vara mer centrala även om många andra som Infrastrukturdepartementet och Utrikesdepartementet också har viktiga roller. Bland myndigheterna är främst sju myndigheter centrala; FRA, Säkerhetspolisen (Säpo), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB), Polismyndigheten, Post- och telestyrelsen (PTS) och Försvarets materielverk (FMV).

6 Intervju Regeringskansliet 11.

7 Se Statskontoret *Regeringens styrning i tvärsektoriella frågor - En studie om erfarenheter och utvecklingsmöjligheter*, 2022, s. 11f.

8 Se exempelvis bet.1995/96:TU19, SOU 2001:41, SOU 2005:71 eller SOU 2015:23.

9 Riksrevisionen, *Informationssäkerheten i den civila statsförvaltningen, RiR 2014:23.*

10 Skr. 2016/17:213.

1.2 Övergripande revisionsfråga och avgränsningar

Vår övergripande revisionsfråga är: Har regeringens arbete för att stärka Sveriges informations- och cybersäkerhet varit effektivt?

Vi utgår från två delfrågor:

1. Är den nationella informations- och cybersäkerhetsstrategin effektivt utformad?
2. Har regeringen implementerat den nationella informations- och cybersäkerhetsstrategin på ett effektivt sätt?

Med implementering avses i det här fallet att man aktivt arbetar med att genomföra strategin och dess åtgärder ur ett livscykelperspektiv. Det innebär att man löpande utvärderar och arbetar med ständiga förbättringar för att nå målen i strategin.

Fokus i granskningen är på regeringens och Regeringskansliets (Statsrådsberedningen, Försvarsdepartementet, Justitiedepartementet, Utrikesdepartementet, Finansdepartementet, Utbildningsdepartementet, Näringsdepartementet, Infrastrukturdepartementet och Socialdepartementet) arbete. För att följa styrningen och få en bild av eventuella behov som myndigheterna har framfört till regeringen och hur regeringen har hanterat dessa berörs även vissa myndigheter av granskningen. De myndigheter som i huvudsak är föremål för styrningen och förser regeringen med underlag är de sju myndigheter som samverkar i det nationella cybersäkerhetscentret (NCSC), det vill säga FRA, Säpo, Försvarsmakten, MSB, Polismyndigheten, PTS och FMV.[11]

Regeringskansliets arbete med informations- och cybersäkerhet tar sin utgångspunkt i förordningen (1996:1515) med instruktion för Regeringskansliet. Enligt den hade Justitiedepartementet fram till årsskiftet 2022/23 ansvar för förvaltnings- och lagstiftningsärenden om informations- och cybersäkerhet, i den mån sådana ärenden inte hör till något annat departement. Numera har Försvarsdepartementet det ansvaret. Begreppet ”cybersäkerhet” fördes in i förordningen hösten 2022, dessförinnan angavs endast ”informationssäkerhet”. Därtill ansvarar varje departement för informations- och cybersäkerhetsfrågor inom

[11] Regeringsuppdraget om att inrätta NCSC gavs till fyra myndigheter (FRA, Försvarsmakten, MSB och Säpo). Dessa ska enligt uppdraget samråda och inhämta synpunkter från ytterligare tre myndigheter (FMV, Polismyndigheten och PTS), vilka med tiden även har involverats i centrets samverkan. Uppdraget avseende centret har inte förändrats avseende vilka myndigheter som omfattas. Däremot har myndigheterna själva exempelvis skapat en utökad ledningsgrupp där de tre tillkommande myndigheterna ingår. Arbetet i centret involverar även det alla sju myndigheter.

sitt ansvarsområde utan att det särskilt anges i förordningen. Den omständigheten att ansvaret för informations- och cybersäkerhetsfrågor är spritt på flera departement är skälet till att Regeringskansliet under årens lopp på olika sätt har samordnat arbetet med sådana frågor. Samordningsarbetet är alltså ett komplement till det sedvanliga linjearbetet.

De problemindikationer som låg till grund för beslut om att inleda granskning rörde i huvudsak regeringens och Regeringskansliets förmåga att bereda och styra informations- och cybersäkerhetsområdet ur ett strategiskt perspektiv. Granskningens huvudsakliga inriktning har därför varit innehållet i regeringens styrning snarare än hur styrningen har genomförts gentemot varje enskild myndighet. Det innebär i sin tur att det arbete som sker ”i linjen” på respektive departement i huvudsak inte har varit föremål för granskning och därmed beskrivs i begränsad omfattning i rapporten.

Granskningen har inte omfattat myndigheternas eller Regeringskansliets interna informations- och cybersäkerhet. Eftersom strategin beslutades 2017 avser granskningen i huvudsak perioden 2017–2022.

1.3 Bedömningsgrunder

Den övergripande utgångspunkten för granskningen är målen för Sveriges säkerhet: att värna befolkningens liv och hälsa, liksom samhällets funktionalitet, samt förmågan att upprätthålla grundläggande värden som demokrati, rättssäkerhet och mänskliga fri- och rättigheter.[12] Informations- och cybersäkerhetsstrategin har även sin utgångspunkt i det it-politiska målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[13]

Regeringen har uttryckt uppfattningen att ”informations- och cybersäkerhetsarbete är en nödvändig verksamhet för att värna kvaliteten och effektiviteten hos samhällets funktioner och en förutsättning för att digitaliseringens möjligheter ska kunna tas tillvara”.[14] Något som även försvarsutskottet har ställt sig bakom.[15] Vidare konstaterade regeringen i försvarsbeslutet 2015 att den samlade svenska förmågan att förebygga, motverka och aktivt hantera konsekvenserna av civila och militära hot, händelser, attacker och angrepp i cybermiljön måste utvecklas och förstärkas.[16]

12 Prop. 2008/09:140, bet. 2008/09:FöU10, rskr. 2008/09:292.
13 Prop. 2011/12:1, bet. 2011/12:TU1, rskr. 2011/12:87.
14 Skr. 2016/17:213, s. 6. Har behandlats av riksdagen i bet. 2017/18:FÖU4.
15 Skr. 2016/17:213, s. 6. Har behandlats av riksdagen i bet. 2017/18:FÖU4, s.10.
16 Prop. 2014/15:109, bet. 2014/15:FöU11, rskr. 2014/15:251.

Försvarsutskottet har understrukit vikten av samverkan och en gemensam riktning för arbetet på cybersäkerhetsområdet eftersom ingen kan lösa säkerhetsutmaningarna ensam[17] och har instämt i regeringens och Försvarsberedningens bedömning att en högre grad av samordning behövs på cybersäkerhetsområdet.[18] Utskottet förutsatte att regeringen säkerställer att Regeringskansliet har en ändamålsenlig organisationsstruktur för att hantera frågor kopplade till informations- och cybersäkerhet.[19]

En gemensam modell för systematiskt informationssäkerhetsarbete borde enligt utskottet 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 därmed skulle användas mer effektivt.[20] Samverkan bör också inkludera näringslivet,[21] och utskottet har påpekat vikten av att det finns en samordnad planering mellan myndigheter och andra aktörer i händelse av en cyberattack eller annan allvarlig it-incident.[22] Utskottet har också uttryckt att det är nödvändigt med internationellt samarbete för att främja informations- och cybersäkerheten eftersom den digitala utvecklingen är gränslös.[23]

Även Försvarsberedningen har framfört behov av koordinering och helhetsperspektiv. De mest skyddsvärda verksamheterna bedrivs inte solitärt utan är beroende av funktionalitet och säkerhet inom andra verksamheter. Arbetet med skydd för de mest skyddsvärda verksamheterna kan därför enligt beredningen inte bedrivas isolerat, utan måste ske koordinerat med det samlade arbetet med samhällets informations- och cybersäkerhet.[24]

Avseende styrningen av statsförvaltningen har regeringen framfört att den bör vara långsiktig, strategisk, helhetsinriktad, sammanhållen, verksamhetsanpassad och tillitsbaserad. Det innebär bland annat att regeringen ska vara tydlig med vilken inriktning myndigheternas verksamhet ska ha, men att detaljstyrning och onödig administration bör undvikas. Ordningen förutsätter en bra uppföljning av myndigheternas resultat och verksamhet och att regeringen ingriper om den bedömer att myndigheterna inte sköter sina uppgifter på ett ändamålsenligt sätt.[25]

17 Bet. 2017/18:FöU14, s. 11.
18 Bet. 2020/21:FöU4, s. 48.
19 Bet. 2020/21:FöU4, s. 49.
20 Bet. 2017/18:FöU4, s. 16.
21 Bet. 2020/21:FöU6, sid 15-16.
22 Bet. 2017/18:FöU6, s. 20.
23 Bet. 2017/18:FöU14, s. 10.
24 Ds 2017:66, s. 115.
25 Prop 2020/21:1 UO 2, s. 58; bet.2020/21:FiU1; rskr.2020/21:63.

Operationaliserade bedömningsgrunder för delfråga ett

Bedömningsgrunden för delfråga ett utgår dels från de övergripande uttalandena ovan, dels från internationell bästa praxis.

Som internationell bästa praxis utgår vi i huvudsak från Enisas (European Union Agency for Network and Information Security) Good Practice Guide för att ta fram, implementera och arbeta med en nationell cybersäkerhetsstrategi ur ett livscykelperspektiv.[26] Avseende framtagandet av strategin rekommenderar Enisa att man:

- bestämmer vision, omfattning, målsättningar och prioriteringar
- använder ett riskbaserat tillvägagångsätt
- inventerar nuvarande politik, lagstiftning och förmågor
- tar fram en tydlig lednings- och styrningsstruktur
- identifierar och involverar intressenter
- etablerar betrodda strukturer för informationsdelning
- tar fram en plan för implementering av strategin samt följer upp och utvärderar den.

För att en strategi på informations- och cybersäkerhetsområdet ska utgöra ett effektivt styrinstrument anser Riksrevisionen, utöver vad som framförs ovan, att den även bör omfatta:

- en analys som definierar den strategiska utmaningen och dess natur
- en vägledande policy för att hantera den strategiska utmaningen
- en uppsättning sammanhängande åtgärder designade för att förverkliga den vägledande policyn[27]
- avvägningar och prioriteringar
- utpekade resurser för att uppnå målen.

---

26 Enisa, NCSS *Good Practice Guide. Designing and Implementing National Cyber Security Strategies*, 2016.

27 Rumelt beskriver de olika delarna av en strategi med hjälp av hur en läkare arbetar. Utmaningen består av en patients olika reaktioner och symptom samt patientens medicinska historik. Läkaren ställer sedan en klinisk diagnos för att komma fram till en lämplig behandlingsmetod vilket jämförs med policy/handlingsprogram. Läkarens ordination avseende eventuell diet, behandling eller medicinering utgör slutligen en uppsättning sammanhängande åtgärder designade för att förverkliga den vägledande policyn/handlingsprogrammet. Rumelt, Richard, *Good strategy/bad strategy: The difference and why it matters*, 2011.

En strategi utan tilldelade resurser, i synnerhet finansiella, har på informations- och cybersäkerhetsområdet ett begränsat värde som styrinstrument.[28] Huruvida finansieringen utgörs av dedikerade medel i myndigheternas befintliga anslag eller av nya medel är av mindre betydelse. Det viktiga är att strategin faktiskt pekar ut prioriteringar och resurssättning i förhållande till de mål som ska uppnås.[29]

I diskursen kring nationella cybersäkerhetsstrategier diskuteras fem dilemman och fem perspektiv som kräver olika former av avvägningar sinsemellan.[30] Inom dessa perspektiv och dilemman finns två huvudsakliga spänningsområden mellan civilt och militärt respektive underrättelse/kontraspionage och brottsbekämpning. Perspektiven kan vara olika gällande målsättningar, organisation och underliggande värden och uppfattningar[31] och påverka hur man ser på öppenhet, hotaktörens motiv, om man agerar passivt eller offensivt gentemot en hotaktör/brottsling samt informationsdelning. Därför är det av vikt att ta skillnaderna i syn på omgivningen mellan olika aktörer i beaktande när man tar fram en nationell cybersäkerhetsstrategi.[32]

Operationaliserade bedömningsgrunder för delfråga två

För att bedöma implementeringen av strategin använder Riksrevisionen de femton områden som Enisa anser bör ingå som en del av implementeringen. De femton områdena kopplar också till de sex strategiska prioriteringarna i den nationella informations- och cybersäkerhetsstrategin enligt nedan (de strategiska prioriteringarna står i fetstil och områdena i kursiv stil):

1. **Säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet**
    a. *Ta fram en nationell cyberkontinuitetsplan*
    b. *Etablera privat-offentliga samarbeten*
    c. *Institutionalisera samarbeten mellan myndigheter*

28 Klimburg, Alexander (red.), *National cyber security framework manual*, 2012, s. 110.
29 Klimburg, Alexander (red.), *National cyber security framework manual*, 2012, s. 110.
30 Dilemmana är stimulans av ekonomin kontra att förbättra nationell säkerhet, modernisering av kritisk infrastruktur kontra skyddet av kritisk infrastruktur, privat sektor kontra offentlig sektor, dataskydd kontra informationsdelning och till sist yttrandefrihet kontra politisk stabilitet. Perspektiven å sin sida är det militära, att motverka cyberbrottslighet, underrättelse och kontraspionage, skyddet av nationell kritisk infrastruktur och krisberedskap samt cyberdiplomati och styrningen av internet (se Klimburg, Alexander (red.), *National cyber security framework manual*, 2012, s. 31ff).
31 Klimburg, Alexander (red.), *National cyber security framework manual*, 2012, s. 86.
32 Klimburg, Alexander (red.), *National cyber security framework manual*, 2012, s. 88.

2. **Öka säkerheten i nätverk, produkter och system**
    a. *Skydda kritisk infrastruktur*
    b. *Etablera en grundnivå/baseline för säkerhetsåtgärder*
    c. *Skapa incitament för den privata sektorn att investera i säkerhetsåtgärder*
3. **Stärka förmågan att förebygga, upptäcka och hantera cyberattacker och andra it-incidenter**
    a. *Genomför cybersäkerhetsövningar*
    b. *Etablera mekanismer för incidentrapportering*
    c. *Etablera en förmåga att hantera incidenter*
4. **Stärka förmågan att förebygga och bekämpa it-relaterad brottslighet**
    a. *Vidta åtgärder för att motverka it-relaterad brottslighet*
5. **Öka kunskapen och främja kompetensutvecklingen**
    a. *Höj användares medvetandenivå (avseende informations- och cybersäkerhetshot)*
    b. *Stärk möjligheterna till kompetensutveckling och utbildning*
    c. *Främja forskning och innovation kopplat till informations- och cybersäkerhet*
6. **Stärka det internationella samarbetet**
    a. *Samarbeta internationellt*

Ett av Enisas områden, att *skapa balans mellan säkerhet och integritet- och dataskydd*, faller däremot inte naturligt in under ett av de sex fokusområdena. Men genom att arbeta med Enisas punkter kan regeringen alltså implementera den nationella strategin.

I bedömningen av regeringens arbete utgår Riksrevisionen från att regeringen bör vidta åtgärder i någon utsträckning inom de olika områdena. Åtgärderna behöver ges resurser och det ska vara tydligt hur de är tänkta att bidra till genomförandet av strategin. Riksrevisionen anser vidare att regeringen måste följa upp och utvärdera åtgärdernas effekter löpande för att kunna genomföra ständiga förbättringar.

1.4 Metod och genomförande

Granskningen har genomförts av en projektgrupp bestående av Marcus Pettersson (projektledare), Helena Fröberg och Ylva Ericsson. Företrädare för Regeringskansliet (Finansdepartementet, Försvarsdepartementet, Infrastrukturdepartementet, Justitiedepartementet, Näringsdepartementet,

Socialdepartementet Utbildningsdepartementet och Utrikesdepartementet), FRA, Försvarsmakten, MSB, Polismyndigheten och Säpo har fått tillfälle att faktagranska och i övrigt lämna synpunkter på ett utkast till granskningsrapport.

Granskningens iakttagelser är baserade på dokumentstudier och intervjuer. För att besvara granskningsfrågorna har vi dels gått igenom underlag från framtagandet av den nationella informations- och cybersäkerhetsstrategin liksom strategin i sig, dels gått igenom den faktiska styrning som har riktats till myndigheterna genom instruktioner, regleringsbrev och uppdrag liksom tilldelning av medel. Utöver det har vi kartlagt utredningsdirektiv och lagändringar på området. För att göra en bedömning av hur myndigheterna har arbetat med att genomföra regeringens styrning har vi tagit del av skriftliga underlag i form av interna inriktningar, uppdrag och återrapportering.

Vi har tagit del av material från beredningar inom Regeringskansliet. Även återrapporteringar och underlag från myndigheterna såsom lägesanalyser, påtalanden om brister, förbättringsförslag, önskemål om styrning, samt material från dialoger med myndigheterna har studerats. Detta har givit en bild av hur beredningarna har gått till och vilka som har varit delaktiga, liksom vilken information regeringens beslut baseras på, om myndigheterna får gehör, och om frågor har beretts men sedan inte resulterat i någon åtgärd. Vi har även tagit del av underlag från de interdepartementala grupper där informations- och cybersäkerhet diskuterats. Det skriftliga materialet har kompletterats med intervjuer med Regeringskansliet och myndigheterna för att få en djupare förståelse för processerna och för att kunna förklara eventuella brister i regeringens styrning. Riksrevisionen har i granskningen genomfört cirka 70 intervjuer. Av dessa har 42 intervjuer (40 respondenter) genomförts med myndigheter.[33] 16 av intervjuerna (23 respondenter) har genomförts med Regeringskansliet.[34] Övriga intervjuer har genomförts med personer från näringslivet eller andra organisationer.

---

[33] Polismyndigheten fem intervjuer och sju respondenter, Försvarsmakten fjorton intervjuer och tolv respondenter, Säkerhetspolisen nio intervjuer och elva respondenter, Myndigheten för samhällsskydd och beredskap sju intervjuer och fyra respondenter, Försvarets radioanstalt sex intervjuer och 6 respondenter och Försvarets materielverk två intervjuer och en respondent.

[34] Statsrådsberedningen en intervju och en respondent, Utrikesdepartementet fyra intervjuer och fyra respondenter, Näringsdepartementet två intervjuer och en respondent, Justitiedepartementet tre intervjuer och två respondenter, Utbildningsdepartementet en intervju och tre respondenter, Socialdepartementet en intervju och fem respondenter, Försvarsdepartementet tre intervjuer och sex respondenter och tidigare Infrastrukturdepartementet en intervju och två respondenter.

Avseende handlingar, arbetsmaterial och övrigt skriftligt underlag från myndigheterna har Riksrevisionen tagit del av cirka tvåhundra dokument hos främst FRA, Säpo, MSB och Försvarsmakten. Hos FRA har Riksrevisionen tagit del av hela den akt som myndigheten har sammanställt och diarieför avseende arbetet med att förbereda, inrätta och driva arbetet i det Nationella cybersäkerhetscentret. Riksrevisionen har tagit del av tillgängliga protokoll avseende möten inom GD-gruppen såväl som den strategiska ledningsgruppen inom ramen för Nationellt cybersäkerhetscenter.

Riksrevisionen har även tagit del av samtliga tillgängliga protokoll (cirka 15 protokoll) från mötena i den interdepartementala grupp (ida-gruppen) som tidigare Infrastrukturdepartementet ansvarade för. Avseende underlag kopplat till den statssekreterargrupp som knöts till ida-gruppen under Infrastrukturdepartementet har Riksrevisionen tagit del av totalt cirka 40 dokument av arbetsmaterial fördelat på fem departement.[35] Utöver dessa dokument har Riksrevisionen även tagit del av promemorior och powerpointpresentationer som har tagits fram inom arbetet knutet till ida-gruppen under Infrastrukturdepartementet såväl som underlag som togs fram av den informella ida-gruppen under Justitiedepartementet. Riksrevisionen har även begärt in och tagit del av ungefär 190 underlag rörande den ordinarie myndighetsstyrningen som departementen har genomfört.

Arbetet med strategiska frågor kopplat till informations- och cybersäkerhet i Regeringskansliet har under granskningsperioden löpande bedrivits av ett begränsat antal personer. Enligt Riksrevisionens bedömning uppskattningsvis 10–15 handläggare, och 10–15 huvudmän eller chefstjänstemän samt utöver det ett tiotal statssekreterare. Riksrevisionen bedömer utifrån ovan angivna att det underlag som har inhämtats i granskningen är tillräckligt för att stödja de iakttagelser och slutsatser som presenteras i granskningsrapporten.

35 Dessa var Försvarsdepartementet, tidigare Infrastrukturdepartementet, Justitiedepartementet, Näringsdepartementet och Utrikesdepartementet.

2 Regeringens arbete med att ta fram den nationella informations- och cybersäkerhetsstrategin

Kapitlet beskriver regeringens och Regeringskansliets arbete med att ta fram den nationella informations- och cybersäkerhetsstrategin och iakttagelser av hur strategin är utformad. Det är uppdelat utifrån Enisas bästa praxis, som är del av granskningens bedömningsgrunder. Kapitlet besvarar delfråga ett:

Är den nationella informations- och cybersäkerhetsstrategin effektivt utformad?

Enligt Riksrevisionen ska en effektiv strategi behandla ett antal frågeställningar[36] och innehålla:

- en analys som definierar den strategiska utmaningen och dess natur
- en vägledande policy för att hantera den strategiska utmaningen
- en uppsättning sammanhängande åtgärder designade för att förverkliga den vägledande policyn
- avvägningar och prioriteringar
- utpekade resurser för att uppnå målen.

Utifrån bedömningsnormernas beskrivning av vad som kännetecknar en effektiv strategi, och då särskilt på informations- och cybersäkerhetsområdet är Riksrevisionens bedömning att regeringens strategi brister på de flesta punkterna. Den har brister inom i stort sett samtliga av de frågeställningar som Enisa anser bör behandlas i en strategi. Den uppfyller heller inte de kriterier som Riksrevisionen bedömer krävs i form av analys av strategiska utmaningar, prioriteringar och avvägningar, utpekade resurser samt sammanhängande åtgärder.

[36] Bestämma vision, omfattning, målsättningar och prioriteringar; använda ett riskbaserat tillvägagångsätt; inventera nuvarande politik, lagstiftning och förmågor; bestämma en tydlig lednings- och styrningsstruktur; identifiera och involverar intressenter, etablera betrodda strukturer för informationsdelning samt innefatta implementeringsplan, uppföljning och utvärdering.

2.1 Strategin saknar analys av strategiska utmaningar och tydliga prioriteringar

Riksrevisionens bedömer att regeringens strategi saknar vad som utmärker en bra strategi på ett flertal punkter. Den utgör därför inte det styrinstrument som skulle behövas på informations- och cybersäkerhetsområdet.

Den svenska informations- och cybersäkerhetsstrategin ska utgöra en plattform för Sveriges fortsatta arbete, stötta aktörer i deras cybersäkerhetsarbete och skapa ett mer samlat arbete på området. Strategin omfattar hela samhället. Tanken är att den ska bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet. Regeringen pekar på kopplingar till såväl den nationella säkerhetsstrategin som digitaliseringsstrategin och det it-politiska målet att Sverige ska vara bäst i världen på att använda digitaliseringens möjligheter.[37] Strategins övergripande målsättning har därmed en ansats att vara bred och heltäckande.

Strategin innehåller tre kapitel. Den första delen behandlar frågor om behovet av en strategi och utgångspunkterna för Sveriges informations- och cybersäkerhet. Den andra delen beskriver sex fokusområden som enligt regeringen utgör strategiska prioriteringar. Den tredje delen redogör för hur regeringen tänker sig att följa upp strategin. De sex prioriteringarna är:

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

Under dessa presenteras sedan totalt tretton olika målsättningar kopplade till de strategiska prioriteringarna. En stor del av målsättningarna utgörs av ospecifika skrivningar i form av att samverkan ska stärkas, säkerheten ska öka eller förmågan ska förbättras. Även om en sådan oprecis målformulering skulle kunna användas för att mäta en förändring så saknas det en tydlig utgångspunkt för hur nivån såg

[37] Skr. 2016/17:213.

ut på de flesta olika områden som berörs i strategin när den presenterades. Det innebär att en bedömning av hur ett område har utvecklats blir svår att genomföra och den blir subjektiv. Att använda sig av oprecisa kriterier innebär även att styrsignalen blir svag.

Regeringen nämner på ett antal ställen kortfattat varför informations- och cybersäkerhet är viktigt, exempelvis för att slå vakt om grundläggande värden och mål i samhället eller för verksamheter för att nå upp till kvalitets- och effektivitetskrav. Men det går inte att hitta någon tydlig vision i form av ett önskat framtida tillstånd. I stället blir de tretton målsättningarna det som kommer närmast att vara en vision.[38]

Strategin är i flera delar otydlig gällande såväl vilka aktörer och sektorer som är tänkta att påverkas och hur. Det finns även otydligheter avseende hur olika målsättningar och aktiviteter är tänkta att påverka samhället, ekonomin och medborgarna i stort. Regeringen ger uttryck för att strategin omfattar hela samhället i form av statliga myndigheter, kommuner, landsting, företag, organisationer och privatpersoner.[39] Det saknas dock i stort resonemang om målsättningar eller åtgärder kopplat till olika aktörer eller sektorer. De resonemang som förs är i huvudsak generiska och aktörslösa vad avser både utförare och vem som ska gynnas av eventuella åtgärder.

Strategin innehåller heller inte någon egentlig analys kring de strategiska utmaningarna. Den innehåller beskrivningar av olika problem, exempelvis att digitalisering och därmed kravet på säkerhet ökar, att informationssäkerhetens komplexitet, gränsöverskridande karaktär och snabba utvecklingstakt kräver en effektiv samverkan samt att antagonister blir mer och mer sofistikerade. Sådana problembeskrivningar utgör enligt Riksrevisionen inte en analys av den strategiska utmaningen. I avsnittet kring behovet av en gemensam nationell modell finns vissa resonemang som har karaktären av analys, exempelvis att regelverk kan vara överlappande och eventuellt motstridiga, att ansvarsområden kan vara överlappande, eller att det kanske finns luckor mellan dem. Fler sådana resonemang saknas dock i huvudsak i strategin. En analys av de strategiska utmaningarna bör enligt Riksrevisionen peka ut vad som inte fungerar i det svenska samhället avseende informations- och cyberssäkerhet och orsakerna till problemen.

---

38 MSB har i faktagranskningen framfört att strategin saknar en tydlig bild av vad strategin ska omhänderta och att strategin inte adresserar varför den finns, och vilken roll cybersäkerhetsarbetet kan och ska ha i den samlade krisberedskapen. Se Myndigheten för samhällsskydd och beredskap, *Föredragnings-PM Faktagranskning Riksrevisionens rapport om samhällets informations- och cybersäkerhet*, 2023.

39 Skr. 2016/17:213, s. 6.

Strategin innehåller inte heller beskrivningar av avvägningar eller prioriteringar utan utgörs mer av en uppräkning av målsättningar. Detta trots att ett flertal aktörer som är tänkta att samverka har delvis skilda synsätt och prioriteringar.[40] Avseende vägledande policy/handlingsprogram kan regeringens så kallade strategiska prioriteringar och skrivningar kring vad regeringen ska verka för ses som ett uttryck för policy. Som nämnts beskrivs de dock vagt. Eftersom det saknas en tydlig analys kring de strategiska utmaningarna blir det svårt att bedöma i vilken utsträckning det är lämpliga fokusområden för att lösa problemen. Strategin innehåller inte heller någon redogörelse för vilka resurser som ska tillgängliggöras för att uppnå målsättningarna.

Slutligen konstaterar Riksrevisionen att strategin inte innehåller någon uppsättning sammanhängande åtgärder designade för att förverkliga den vägledande policyn. I samband med att strategin presenterades gav regeringen även ett antal myndigheter totalt fyra olika uppdrag.[41] Det var först i och med ett uppdrag att ta fram en handlingsplan för att förverkliga strategins målsättningar 2018 som det presenterades konkreta åtgärder med en mer uttalad koppling till själva strategin.[42] Handlingsplanen bygger på åtgärder som myndigheterna redan genomförde utifrån instruktion, regleringsbrev och regeringsuppdrag. Handlingsplanen utgör därmed snarare en redovisning av åtgärder som myndigheterna genomför baserad på annan styrning än styrning som kommer av strategin. Strategin och handlingsplanen utgör inte formell styrning gentemot myndigheterna. Myndigheternas resurstilldelning görs i stället utifrån den formella styrningen i instruktion, regleringsbrev och regeringsuppdrag. Riksrevisionen har vid ett flertal tillfällen påpekat att signaler som regeringen skickar på ett annat sätt än vad regeringen anser vara formell styrning innebär att dessa signaler ”hamnar sist i kön”.[43]

---

40 Detta avser såväl myndigheter eller organisationer som olika departement. Säpo, FRA och Försvarsmakten/Must kan ses som underrättelsemyndigheter som åtminstone initialt kan ha intresse av att följa och kartlägga en aktör snarare än att offentliggöra information. MSB utgör exempel på en myndighet som har ett motstående intresse att snabbt sprida information om händelsen för att förhindra att flera organisationer drabbas. Säkerhetspolisen och Försvarsmakten är inte underrättelsemyndigheter per definition. Säkerhetspolisen är en säkerhetstjänst och hos Försvarsmakten är det bara den delen av myndigheten som utgörs av Must som kan benämnas som en ”underrättelsemyndighet”. Delar av Säkerhetspolisens verksamhet och den delen av Försvarsmakten som utgörs av Must fungerar dock i praktiken i mångt och mycket som underrättelsemyndigheter och därför benämns de som underrättelsemyndigheter i granskningsrapporten.

41 Regeringsuppdrag Ju2017/05787/SSK, regeringsuppdrag Ju2017/05789/SSK, regeringsuppdrag Ju2017/05788/SSK och regeringsuppdrag Ju2017/05786/L4.

42 Regeringsbeslut Ju2018/03737/SSK.

43 Se exempelvis Riksrevisionen, *Livsmedels- och läkemedelsförsörjning: samhällets säkerhet och viktiga samhällsfunktioner* RiR 2018:6.

I praktiken innebär detta att de åtgärder myndigheterna har genomfört på området inte styrs av målsättningarna i strategin. Flera myndighetsföreträdare uppger att strategin har haft liten eller ingen påverkan på vilka åtgärder myndigheterna genomför. Det gäller såväl åtgärder inom varje myndighet som åtgärder som vidtas eller skulle kunna vidtas i samverkan mellan myndigheter.[44] Underlag som Riksrevisionen har tagit del av angående det interna arbetet i Regeringskansliet tyder på att samma problematik återfinns i avvägningarna mellan olika departement i Regeringskansliet.[45] En av Riksrevisionens iakttagelser är att Regeringskansliet diskuterar och vidtar åtgärder utan att utgångspunkten är informations- och cybersäkerhetsstrategin och dess målsättningar.

2.2 Framtagandet av strategin genomfördes inte utifrån ett riskbaserat tillvägagångssätt

Riksrevisionens bedömning är att regeringen och Regeringskansliet inte har haft ett riskbaserat tillvägagångssätt vid framtagandet av strategin. En konsekvens av det är att det inte går att avgöra om de föreslagna fokusområden är de som är viktigast att prioritera.

Enligt Enisas bästa praxis är det centralt att utgå från ett riskbaserat tillvägagångssätt i framtagandet av strategin. I regeringens strategi används begreppet risk frekvent. Regeringen betonar vikten av att utgångspunkten för samhällets aktörer i arbetet med informations- och cybersäkerhet ska vara ett strukturerat och riskbaserat arbete. Vad gäller arbetet med framtagandet av strategin eller hur regeringen har kommit fram till de strategiska prioriteringarna saknas beskrivningarna eller resonemang kring risk helt.

Det finns flera olika nationella bedömningar av hot, risker och sårbarheter som Regeringskansliet skulle kunna ha som utgångspunkt vid framtagande av strategin.[46] Ett exempel är Myndigheten för samhällsskydd och beredskaps nationella risk- och förmågebedömning som syftar till att inrikta och utveckla krisberedskapen och civilt försvar. Den bedömningen är ett exempel på en möjlig utgångspunkt för arbetet med att ta fram strategin och göra avvägningar och prioriteringar. Den nationella risk- och förmågebedömningen eller liknande bedömningar omnämns dock inte i strategin. Av de underlag vi har tagit del av och

44 Intervju Försvarsmakten 1 och 3; intervju Försvarets radioanstalt 1; intervju MSB 3.

45 Minnesanteckningar från Regeringskansliets arbetsmaterial 2.

46 Exempelvis Försvarsmaktens perspektivstudier, Försvarsmakten/Musts årsöversikt, Försvarets radioanstalts årsrapport och Säkerhetspolisens årliga lägesbild om hoten mot Sverige.

de intervjuer vi har genomfört med tjänstemän på Regeringskansliet har det heller inte framkommit något som tyder på att den nationella risk- och förmågebedömningen eller liknande exempel har varit en utgångspunkt. Det finns heller inget underlag som tyder på att man på något uttryckligt sätt har haft en riskbaserad utgångspunkt i sitt arbete med framtagandet av strategin. Om handläggarna har resonerat utifrån en riskbaserad utgångspunkt så återspeglas det inte i strategin eller i underlag.

2.3 Strategins inventering av nuvarande politik, lagstiftning och förmågor är otillräcklig

Riksrevisionens bedömer att strategin inte innehåller någon inventering av nuvarande politik, lagstiftning eller förmågor.[47] Det innebär att det inte går att få en bild av om nuvarande politik, lagstiftning och förmågor är tillräckliga för att uppnå eftersträvad målbild, och om så inte är fallet vilka åtgärder som behöver vidtas.

I strategin redogör regeringen kortfattat för ett antal lagar och förordningar som innehåller bestämmelser om informationssäkerhet. Man nämner även att det finns myndighetsföreskrifter som reglerar informationssäkerhet inom ett flertal sektorer. Vidare omnämns ett antal författningar och områden som kommer att beröras av förändrad lagstiftning såväl som ett antal utredningar och rapporter som har pekat på brister eller problem på området.[48] Under den strategiska prioriteringen att säkerställa en systematisk och samlad ansats i arbetet med informations- och cybersäkerhet framför regeringen att en prioriterad målsättning är att det tas fram en nationell modell för systematiskt informationssäkerhetsarbete.[49] Regeringen lyfter fram att en sådan modell syftar till att utgöra en gemensam plattform för det systematiska informationssäkerhetsarbetet och kan samordna och samla regelverk, metoder, verktyg, utbildningar med mera på myndighetsnivå på ett lättillgängligt sätt. Modellen kan enligt regeringen bidra till en mer sammanhållen styrningen och öka samverkan inom området.[50] Här pekar regeringen således på att det finns problem med lagstiftning och styrning, möjliga målkonflikter eller överlappande mandat såväl som en risk för att frågor inte omhändertas som en konsekvens av oklar ansvarsfördelning. Just detta möjliga problem är enligt Enisa skälet till att man bör göra en djupgående inventering av politik, lagstiftning och förmågor. En

47 Här avses i första hand den eventuella politik som fanns vid tillfället för framtagandet. Om man arbetar med ständiga förbättringar bör strategin även uppdateras löpande i de fall politiken förändras.

48 Skr. 2016/17:213, s. 7.

49 Skr. 2016/17:213, s. 11.

50 Skr. 2016/17:213, s. 12.

sådan inventering kan ligga till grund för valet av åtgärder och prioriteringar i det fortsatta arbetet. Utöver dessa övergripande och oprecisa skrivningar redogör regeringen inte för någon mer omfattande inventering av politik, lagstiftning eller förmågor. Det går därför inte utifrån strategin att få en djupare förståelse kring ”ekosystemet” för informations- och cybersäkerhet i Sverige.

Behovet av samordning uppges kvarstå än idag. I utredningen *Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem* konstaterar utredaren att det nationella informations- och cybersäkerhetsarbetet alltjämt är uppdelat i olika, delvis överlappande ansvarsområden, både på departements- och på myndighetsnivå.[51] Bristerna medför enligt utredningen betydande utmaningar i arbetet för såväl offentliga som enskilda verksamhetsutövare. Det krävs därför åtgärder som kan ge offentliga och enskilda aktörer förutsättningar att kunna uppnå en tillräcklig grad av informations- och cybersäkerhet i verksamheten. Det närmare behovet av ytterligare reglering samt tydligare styrning och samordning av arbetet med samhällets informations- och cybersäkerhet bör därför enligt utredaren utredas i särskild ordning.[52] Riksrevisionen delar utredningens uppfattning att det kan finnas ett behov av ytterligare reglering samt tydligare styrning och samordning.

2.4 Strategin saknar en tydlig lednings- och styrningsstruktur

Riksrevisionens bedömning är att strategin i huvudsak inte tillför något avseende vem som ansvarar för vad och på vilket sätt. De problem som i strategin lyfts avseende otydligheter rörande ansvarsförhållanden adresseras inte på något sätt.

I den första versionen av informations- och cybersäkerhetsstrategin saknades det skrivningar om lednings- och styrningsstruktur. Som en följd av NIS-direktivet uppdaterade regeringen strategin 2018.[53] Syftet var att utveckla och tydliggöra ansvar och roller för genomförandet av strategin i en styrningsram.[54] Styrningsramen beskrivs som ett ramverk som definierar roller och ansvar hos aktörer som deltar i genomförandet av strategin.[55] Syftet med en tydlig

51 SOU 2021:63, s. 360f.

52 SOU 2021:63, s. 360.

53 Skr. 2016/17:213, bilaga: Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet.

54 Skr. 2016/17:213, bilaga: Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet, s. 39.

55 Skr. 2016/17:213, bilaga: Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet.

styrningsram anges först och främst vara att skapa fördjupad samverkan kring de aktiviteter som genomförs för att höja informations- och cybersäkerheten i samhället. Med det åsyftas aktiviteter som i många fall behöver genomföras i samverkan och som påverkar fler aktörer än den egna organisationen. Vidare anges att styrningsramen ska bidra till en överblick över vilka aktörer som bidrar till genomförandet av strategin.[56]

Avseende ansvar framgår att:

- regeringen har ansvar för strategin
- justitieministern och inrikesministern är de statsråd i regeringen som har ansvar för att samordna genomförandet och uppföljning av strategin
- Regeringskansliet har i uppdrag att stödja regeringen i dess uppgift att styra riket och förverkliga sin politik
- varje departement ansvarar för att löpande utveckla aktiviteter för att nå målsättningarna i strategin.[57]

Utöver ovan utpekade punkter använder sig regeringen inte av begreppet ansvar, vilket enligt Riksrevisionens bedömning är centralt i en tydlig lednings- och styrningsstruktur. Under rubriken Statliga myndigheter beskriver regeringen att vissa myndigheter har uppgifter eller uppdrag som syftar till att höja informations- och cybersäkerheten och man nämner vissa myndigheter som har specifika uppdrag. Man nämner också att alla statliga myndigheter under regeringen ska analysera om det finns sårbarheter eller risker inom myndighetens ansvarsområde som synnerligen allvarligt kan försämra myndighetens förmåga till verksamhet inom området.[58] Avseende fortsättningen skriver regeringen att uppdrag från regeringen för att höja samhällets informations- och cybersäkerhet kommer att riktas till såväl Samfi-myndigheterna[59] som andra myndigheter. Regeringen uttrycker även en avsikt att verka för att koordinera alla uppdrag och uppgifter till

56 Skr. 2016/17:213, s. 40.

57 Skr. 2016/17:213, s. 41f.

58 Skr. 2016/17:213, s. 42.

59 Samverkansgruppen för informationssäkerhet (Samfi). Gruppen bestod av Myndigheten för samhällsskydd och beredskap (MSB), Post- och telestyrelsen (PTS), Polismyndigheten, Försvarets radioanstalt (FRA), Säkerhetspolisen (Säpo), Försvarets materielverk (FMV)/Sveriges Certifieringsorgan för IT-säkerhet (CSEC), Försvarsmakten /Militära underrättelse- och säkerhetstjänsten (Must). Samfi var ett samverkansforum som skapades 2003 av dåvarande Krisberedskapsmyndigheten (KBM). Forumet hade inget eget mandat utan arbete och åtgärder genomfördes av de samverkande myndigheterna var och en för sig. Samverkan var frivillig.

statliga myndigheter.[60] För att genomföra det internationella arbetet är det enligt regeringen av vikt att agera samstämmigt och effektivt. För att uppnå det krävs en förbättrad överblick över ett stort antal internationella processer som innefattar politiska, legala och tekniska aspekter. Det förutsätter i sin tur enligt regeringen samverkan och informationsdelning såväl mellan berörda myndigheter som i förhållande till Regeringskansliet.[61]

Under rubriken en tydligare roll för samverkansgruppen för informationssäkerhet betonar regeringen behovet av en fördjupad samverkan mellan myndigheterna i Samfi. Myndigheterna sägs utgöra en kanal och mottagare för frågeställningar som rör olika typer av aktiviteter som övriga aktörer i samhället bedriver för att höja informations- och cybersäkerheten. Regeringen betonar även vikten av att myndigheterna delar information om sin samverkan med andra aktörer för att undvika överlappande arbete eller att centrala behov inte tillgodoses.[62]

Regeringen beskriver vidare att man har gett myndigheterna i Samfi i uppdrag att ta fram en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. Handlingsplanen ska utgöra en samlad redovisning av vilka åtgärder Samfi-myndigheterna på eget initiativ planerar att vidta för att höja informations- och cybersäkerheten i samhället inom ramen för sina befintliga ansvarsområden. De planerade åtgärderna ska utgå från målen i regeringens strategi.[63]

Regeringen anför också att ett effektivt genomförande av strategin kräver att myndigheterna i så stor utsträckning som möjligt samordnar sitt arbete. Det innebär enligt regeringen att myndigheterna i sin egen planering och prioritering av verksamheten, när så är relevant för myndigheten, ska beakta arbetet med handlingsplanen för att ta tillvara effektivitets- och kvalitetsnyttor i arbetet med hela samhällets informations- och cybersäkerhet. Regeringen anser även att myndigheterna på ett systematiskt sätt bör inhämta idéer och råd och i övrigt samverka med andra relevanta aktörer som kan bidra i arbetet. Företag anges som särskilt viktiga i det hänseendet liksom myndigheter, kommuner, landsting, Sveriges kommuner och landsting (numera Sveriges kommuner och regioner) och andra organisationer.[64]

60 Skr. 2016/17:213, s. 42.
61 Skr. 2016/17:213, s. 42.f.
62 Skr. 2016/17:213, s. 43.
63 Skr. 2016/17:213, s. 43.
64 Skr. 2016/17:213, s. 44.

Strategin beskriver i begränsad omfattning vilka aktörer som ansvarar för vilka frågor.[65] De tydligaste utpekandena avseende ansvar gäller regeringen samt Regeringskansliet och olika departement. Regeringen lyfter att varje enskild organisation ska bedriva sitt arbete i enlighet med ansvarsprincipen och gällande regelverk. Arbetet ska bedrivas systematiskt och självständigt, men med stöd av de aktiviteter som genomförs inom styrningsramen. Utöver det adresserar regeringen Samfi-myndigheterna som grupp eller myndigheterna över lag med olika önskemål eller förhoppningar, men tydlighet kring vem som ska göra vad och på vilket sätt saknas i stort sett.

Skrivningarna om ansvar, uppdrag och tillvägagångssätt är generella och oprecisa. Exempel på sådana formuleringar är: ”när så är relevant ska myndigheten beakta”, ”bör inhämta”, ”i övrigt samverka” och ”myndigheterna bör inhämta idéer och råd”.[66]

2.5 Intressenter involverades inte tillräckligt i framtagandet

Arbetet med framtagandet av strategin har enligt Riksrevisionens bedömning involverat ett fåtal potentiella intressenter och då endast i en begränsad omfattning. Om strategin inte har en bred förankring och involverar en bredd avseende samhällsaktörer så är risken stor att den inte heller beaktar hela samhällets behov. Det riskerar även att försvåra det samarbete mellan den offentliga och den privata sektorn som regeringen beskriver som viktigt.

År 2016 fick Justitiedepartementet i uppgift att ta fram en nationell strategi för samhällets cyber- och informationssäkerhet. Inom departementet var det enheten för samordning av samhällets krisberedskap (SSK) som fick uppdraget, som grundades dels på NISU-utredningen,[67] dels på framtagandet och införandet av NIS-direktivet. Enligt EU:s NIS-direktiv ska medlemsstaterna ha en nationell strategi för säkerhet i nätverks- och informationssystem som fastställer strategiska mål och konkreta politiska åtgärder som ska genomföras.[68]

65 Intervju Försvarsmakten 2 och 6.
66 Skr. 2016/17:213.
67 SOU 2015:23.
68 Direktiv (EU) 2016/1148, artikel 7.

Arbetet med att ta fram strategin beskrivs av handläggarna på SSK som ett lagarbete och genomfördes med stöd av en interdepartemental arbetsgrupp (ida-grupp) med representanter från åtta departement.[69] Inledningsvis hade SSK ett antal möten med personer från andra departement för att diskutera innehållet i strategin innan de gick vidare med att ta fram texter. Av intervjuer med Regeringskansliet framgår att framtagandet av strategin i huvudsak har varit ett arbete som involverat ett fåtal tjänstemän från de åtta departement som deltog i ida-gruppen år 2017. Strukturen för strategin var dels inspirerad av strategier i andra länder, dels av de ingående departementens ansvarsområden och respektive departements viktigaste frågor. Enligt handläggarna på Justitiedepartementet byggde även andra länder upp sina initiala strategier på ett liknande sätt med ett antal viktiga områden. Arbetet hämtade även inspiration från det strategiarbete som tidigare hade genomförts i Samfi, varför även myndighetsperspektivet syns i delar av strategin. De olika departementen skrev olika avsnitt i strategin medan Justitiedepartementet ansvarade för att få ihop helheten.

Det fanns en ambition att ta in externa synpunkter och förslag, och kontakt med myndigheter förekom. Hur mycket myndigheterna involverades varierade mellan departementen. Vissa myndigheter var med och tog fram texter till strategin, medan andra snarare lämnade synpunkter på ett utkast till strategin. Försvarsmyndigheterna verkar dock ha blivit involverade i arbetet med de underlag som Försvarsdepartementet har tagit fram och Försvarsmakten uppger att man har fått gehör för de synpunkter och viktiga frågor som myndigheten lyfte i dialogen med Försvarsdepartementet.[70]

Samtidigt som ambitionen att ta in synpunkter utanför Regeringskansliet fanns uppger handläggarna att det var många frågor att reda ut internt. Justitiedepartementet bedömde vid tidpunkten för framtagandet att Regeringskansliet inte var moget för att inhämta externa synpunkter.[71] Inför framtagandet av strategin höll dock inrikesministern och närings- och innovationsministern ett rundabordssamtal om hur informations- och cybersäkerheten i Sverige kan stärkas för ett mer konkurrenskraftigt näringsliv och

69 Gruppen var inte en formell ida-grupp utan deltagandet baserades på frivillighet hos ett antal tjänstemän på olika departement som arbetade med informationssäkerhetsfrågor. *Arbetsgrupper och andra osjälvständiga organ inom Regeringskansliet,* SB PM 2021:2.

70 Intervju Försvarsmakten 1.

71 Intervju Regeringskansliet 6.

robust samhälle.[72] Man bad de inbjudna att fundera utifrån temat och att ta med sig tankar och idéer om:

- Vilka är de viktigaste utmaningarna och möjligheterna som ni ser för er egen del, för näringslivet och för samhällets informations- och cybersäkerhet?
- Vilka åtgärder ser ni som mest prioriterade för att bemöta dessa utmaningar och möjligheter? Nationellt, inom EU samt internationellt?
- Vilka långsiktiga målsättningar bör Sverige arbeta mot på informations- och cybersäkerhetsområdet?

Efter samtalet skickade ett fåtal företag också in skriftliga synpunkter. Valet av representanter till samtalet uppges av tjänstemännen på Justitiedepartementet ha baserats på en förfrågan till MSB kring lämpliga deltagare och på förslag från andra departement.

Det finns inget underlag som Riksrevisionen har fått ta del av som tyder på att man har genomfört någon form av intressentanalys, åtminstone inte i någon formell mening.

2.5.1 Regeringen uttryckte inte någon uppfattning kring strukturer för informationsdelning

Regeringen har i strategin inte förtydligat på vilket sätt man anser att samverkan och informationsdelning ska ske. Det framgår inte om regeringen anser att samverkan ska ske i nuvarande forum eller om det behöver skapas andra eller kompletterande forum. Det framgår heller inte i vilken form eller på vilket sätt och i vilket syfte informationsdelningen ska ske. En tydligare inriktning kring vad som förväntades och på vilket sätt resultatet skulle uppnås hade enligt Riksrevisionens bedömning kunnat underlätta myndigheternas arbete med informationsdelning.

Regeringen nämner Samfi, Samverkansforumet Nationell samverkan till skydd mot allvarliga it-hot (NSIT) och Nationella telesamverkansgruppen (NTSG). Regeringen nämner även ett antal forum som MSB har tagit initiativ till och ansvarar för nämligen:

- FIDI-SCADA: forum för att dela information om säkerhet i informations- och styrsystem (Industrial Control Systems, ICS).

---

[72] De organisationer som bjöds in var Näringslivets säkerhetsdelegation, Ericsson, SAAB, Telia, Basefarm, Vattenfall, ABB, Tieto, CGI, Tele2, SAS, Volvo Cars, Intel, Nasdaq/OMX, IBM, Prevas, Atsec, Tutus, Advenica, Klarna, SEB, Säkerhets- och försvarsföretagen (SOFF), Myndigheten för samhällsskydd och beredskap, Post- och telestyrelsen, Försvarsmakten.

- FIDI-Vård och omsorg: forum för att stärka och förbättra informationssäkerhet inom hälso- och sjukvårdssektorn.
- FIDI-Drift: forum för att dela information inom it-driftsektorn.
- FIDI-Telekom: forum för teleoperatörer om operativa och tekniska frågor med incidentnära fokus.
- FIDI-Finans: forum för att diskutera informationssäkerhetsfrågor inom den finansiella sektorn.

Förutom dessa forum som regeringen nämner har det efter att strategin presenterades tillkommit ett antal ytterligare forum. MSB har exempelvis i uppdrag att leda ett samarbetsforum där tillsynsmyndigheterna inom NIS-området och Socialstyrelsen ingår.[73] Tillsammans med tillsynsmyndigheterna och Socialstyrelsen arrangerar MSB även regelbundna privat-offentliga samverkansforum.[74] Deltagarna kommer från de branschorganisationer som representerar leverantörer av samhällsviktiga och digitala tjänster. Syftet är att främja informationsdelning och att sammanställa vilka behov av övrigt stöd som finns.[75] Säkerhetspolisen och Försvarsmakten har ett liknande uppdrag avseende ett samarbetsforum för tillsynsmyndigheter inom säkerhetsskyddsområdet.[76]

I regeringens informations- och cyberssäkerhetsstrategi finns under rubriken Samverkan och informationsdelning exempel på ett antal samverkansplattformar för informationsdelning såväl mellan myndigheter som mellan offentliga och privata aktörer.[77] Regeringen anger att det finns ett behov av en utvecklad och fördjupad myndighetssamverkan såväl som att fortsätta utveckla informationsdelningen gällande risker, hot och säkerhetsåtgärder i syfte att skyddet snabbt ska kunna anpassas hos fler aktörer.[78] Regeringen skriver att man ska verka för en ökad samverkan samt en ändamålsenlig informationsdelning.[79] Strategin innehåller dock inga resonemang eller beskrivningar om möjliga problem med dagens samverkan och informationsdelning. Det finns inte heller något resonemang kring hur regeringen ser på de samverkansplattformar som omnämns och om det i huvudsak är genom dessa plattformar som samverkan och informationsdelning ska ske.

---

73 21 § förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.
74 MSB genomför även en årlig konferens riktad till samtliga NIS-leverantörer.
75 MSB, *MSB:s roll och ansvar inom NIS*, 2021, s. 11.
76 Regeringsbeslut Ju2021/01245.
77 I huvudsak de forum som nämns ovan i texten.
78 Skr. 2016/17:213, s. 14.
79 Skr. 2016/17:213, s. 14.

2.6 Strategins utformning och plan för implementering främjar inte ständiga förbättringar

Skrivningarna i strategin är enligt Riksrevisionen otydliga kring hur den ska implementeras, följas upp och utvärderas. I handlingsplanen redogör myndigheterna för eventuella effekter av vidtagna åtgärder men bedömningarna är vaga och utgörs mer av en beskrivning av möjliga effekter snarare än faktiskt observerade effekter. En mer omfattande utvärdering ska ske först 2023. Utöver kompletteringen av strategin 2018 har det heller inte skett några förändringar eller korrigeringar. Riksrevisionens bedömning är därför att regeringen inte har arbetat med strategin på ett sätt som innebär ständiga förbättringar.

I strategin fanns det ursprungligen inga skrivningar om hur strategin skulle implementeras och endast begränsade skrivningar om hur och av vem den skulle följas upp och utvärderas.[80] Justitie- och inrikesministern pekades ut som det statsråd i regeringen som har ansvar för att samordna genomförandet och uppföljningen av strategin. Samtidigt anges att övriga statsråd ansvarar för genomförande och uppföljning av strategin inom ramen för respektive departements ansvarsområden. Regeringen skriver även att man avser att regelbundet begära in redovisningar av arbetet med informations- och cybersäkerhet hos de statliga myndigheterna.[81]

I praktiken har Regeringskansliet hanterat uppföljningen genom den informella ida-gruppen för informationssäkerhet där man på mötena gick bordet runt och lät alla berätta vad de gjorde för att genomföra strategin. Tanken var att mötena skulle fungera som regelbundna påminnelser och avstämningar för att hålla arbetet med att genomföra strategin vid liv. Justitiedepartementet skickade utöver detta, vid fyra tillfällen, ut frågor till alla departement med önskemål att lista alla avslutade och pågående projekt kopplade till strategin. Man hade från Justitiedepartementets sida avsikten att strategin ”blev verkstad” snarare än att komma på nya initiativ. Det var dock upp till varje departement att bestämma vilka konkreta åtgärder man ville vidta för att genomföra strategin.[82]

2019 tog en nytillsatt samordnare på Statsrådsberedningen över samordningen av frågorna. Justitiedepartementet fortsatte däremot ansvara för uppföljningen av strategin. Det fanns dock inte något större intresse för strategin på Statsrådsberedningen. Statsrådsberedningen hade inte heller något uttryckligt

80 Skr. 2016/17:213, s. 35.
81 Skr. 2016/17:213, s. 41f.
82 Intervju Regeringskansliet 6.

ansvar för att genomföra någon specifik del i strategin, utan det ansvaret vilade på departementen och uppföljningsansvaret på Justitiedepartementet.[83]

Inom ramen för uppdraget att ta fram en handlingsplan genomförde dock myndigheterna åtgärder för att uppnå de målsättningar som redovisas i strategin. Åtgärderna är strukturerade utifrån strategins fokusområden och pekar ut vilken/vilka myndigheter som har ansvar för genomförandet och vilka myndigheter som eventuellt deltar i genomförandet. Handlingsplanen innehåller även en kvalitativ bedömning av vilka effekter åtgärderna bedöms ha inneburit.[84] Bedömningen innehåller inga nyckeltal/uttryckliga resultatmått eller kvantitativa bedömningar utan utgörs i huvudsak av vaga beskrivningar som att saker ska öka, förstärkas, förbättras, utgöra förutsättningar för eller liknande. Beskrivningarna möjliggör därmed inte några djupare bedömningar av resultat i förhållande till insats. Nyttan med handlingsplanen utifrån hur arbetet med den är organiserat bedöms av flera myndigheter som låg.[85] [86] FRA har exempelvis framfört att handlingsplanen i stället blir en sammanställning av de enskilda myndigheternas verksamhetsplaner.[87]

83 Intervju Regeringskansliet 6.

84 Handlingsplanen upprättades för första gången 1 mars 2019 och den uppdateras årligen med nya åtgärder som myndigheterna avser att genomföra samt en bedömning av vilka effekter som tidigare års åtgärder bedöms ha åstadkommit.

85 Intervju MSB 2.

86 MSB har i faktagranskningen framfört att myndigheternas ambitionsnivå när det gällde att nyttja handlingsplanen för att fördjupa samverkan skilde sig. Se Myndigheten för samhällsskydd och beredskap, *Föredragnings-PM Faktagranskning Riksrevisionens rapport om samhällets informations- och cybersäkerhet*, 2023.

87 Handling från FRA till Fö/SUND daterad 2018-05-07.

3 Åtgärder för att implementera strategin

Kapitlet beskriver regeringens, Regeringskansliets och myndigheternas arbete med att implementera strategin. Kapitlet besvarar delfråga två:

Har regeringen implementerat den nationella informations- och cybersäkerhetsstrategin effektivt?

Bedömningsgrunden utgår från de femton områden[88] som Enisa pekat ut som viktiga att arbeta med för att implementera nationella informations- och cybersäkerhetsstrategier. Enligt Riksrevisionen bör regeringen vidta åtgärder i någon utsträckning inom de olika områdena. Åtgärderna behöver även prioriteras inbördes, ges resurser samt vara koherenta utifrån hur de är tänkta att bidra till att implementera strategin. Riksrevisionen konstaterar vidare att regeringen måste följa upp och utvärdera åtgärdernas effekter löpande för att kunna genomföra ständiga förbättringar.

Sammantaget har regeringens arbete för att implementera strategin inte varit effektivt i alla avseenden. Regeringen har vidtagit ett flertal åtgärder för att implementera strategin. Det har handlat om uppdrag till ett sextiotal myndigheter, lagändringar, tilldelning av finansiella medel och deltagande i internationella sammanslutningar. Åtgärderna är dock spridda över tid och tycks inte direkt utgå från en långsiktig och strategisk tanke om hur strategin ska implementeras. Riksrevisionens iakttagelse är att åtgärderna snarare genomförs för att lösa aktuella problem än för att genomföra strategin. Regeringen har varit olika aktiv inom de olika områdena som Enisa har identifierat och har för vissa av dem inte vidtagit några åtgärder alls. Även för områden där flera åtgärder har vidtagits har resultaten hittills varit svaga. Trots att Regeringskansliet har uppmärksammats på att önskade resultat inte har uppnåtts lyser åtgärder för att uppnå bättre resultat med sin frånvaro.

---

88 De är: ta fram en nationell cyberkontinuitetsplan, skydda kritisk infrastruktur, genomföra cybersäkerhetsövningar, etablera en grundnivå/baseline för säkerhetsåtgärder, etablera mekanismer för incidentrapportering, höja användares medvetandenivå (avseende informations- och cybersäkerhetshot), stärka möjligheterna till kompetensutveckling och utbildning, etablera en förmåga att hantera incidenter, vidta åtgärder för att motverka it-relaterad brottslighet, samarbeta internationellt, etablera privat-offentliga samarbeten, skapa balans mellan säkerhet och integritet- och dataskydd, institutionalisera samarbeten mellan myndigheter, främja forskning och innovation kopplat till informations- och cybersäkerhet, skapa incitament för den privata sektorn att investera i säkerhetsåtgärder.

3.1 Regeringen har inte vidtagit några direkta åtgärder för fyra av områdena

Inom ett av områdena har regeringen inte vidtagit några åtgärder alls, och inom tre har regeringen i huvudsak vidtagit indirekta åtgärder.

För området *genomföra cybersäkerhetsövningar* har regeringen inte vidtagit några åtgärder gentemot myndigheterna. Myndigheterna har däremot ändå dels genomfört, dels deltagit i övningar både nationellt och internationellt[89] [90], men inget tyder på att strategin har varit vägledande för att detta skulle ske. Riksrevisionen delar Kungliga Ingenjörsvetenskapsakademiens (IVA) uppfattning att det som saknas och som behövs i Sverige är en sammanhållen övnings- och teststrategi för cyberdomänen. Enligt IVA kan ett nationellt övnings- och testramverk bidra till strukturerade och mätbara resultat som ger värdefulla underlag och rekommendationer till beslutsfattare. Resultaten kan också användas för att identifiera förbättringsområden inom den nationella informations- och cybersäkerhetsstrategin.[91]

Vad gäller att *ta fram en nationell cyberkontinuitetsplan* förekommer olika uppdrag som syftar till att öka kunskapen om risker, hot, sårbarheter och behov. Sådan kunskap kan i sin tur bidra till att öka beredskapen och användas till att utveckla kontinuitetsplaner. Men uttryckliga uppdrag om att ta fram en kontinuitetsplan har inte förekommit.[92] Det är främst Försvarsmakten och MSB som har fått uppdrag om att kartlägga risker, hot och behov,[93] men även andra myndigheter har fått uppdrag på dessa teman.[94] De sju myndigheterna som samverkar i centret fick 2018 också i uppdrag att ta fram en samlad informations- och cybersäkerhetshandlingsplan för 2019–2022.[95] Åtgärden att ta fram en nationell

---

89 För en heltäckande bild av vilka övningar som har genomförts se Wiktorin, *Cyberförsvaret – en introduktion*, 2022, s. 98f.

90 MSB har även tagit fram en nationell strategi för systematisk övningsverksamhet, se *Nationell strategi för systematisk övningsverksamhet. För krisberedskap och civilt försvar*, 2020.

91 IVA, *Cybersäkerhet för ökad konkurrenskraft*, 2022, s. 33.

92 I regeringsuppdraget om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter anges dock att samverkan inom ramen för cybersäkerhetscentret ska utvecklas stegvis 2021–2023 inom bland annat stöd vid hanteringen av cyberangrepp och andra it-incidenter samt upprättande av en plan för samlad hantering på nationell nivå vid allvarliga cyberangrepp. Se regeringsbeslut Fö2019/01330.

93 Se bilaga ”Riktlinjer för den militära säkerhetstjänsten” till Försvarsmaktens regleringsbrev, 2017–2022; regleringsbrev för MSB 2017; regeringsbeslut Ju2019/03058/SSK, Ju2019/02421/SSK; regeringsbeslut Ju2017/05789/SSK.

94 Se exempelvis regeringsbeslut I2020/01087/D; regeringsbeslut Ju2017/05787/SSK; regeringsbeslut Ju2022/02143.

95 Regeringsbeslut Ju2018/03737/SSK.

kontinuitetsplan för cyberområdet återfinns dock varken i strategin eller i handlingsplanen.[96] Nationella beredskapsplaner finns exempelvis för hanteringen av en kärnteknisk olycka, för foder- och livsmedelskedjan och för Sveriges elförsörjning men inte för informations- och cybersäkerhet. Sedan den 1 oktober 2022 finns utpekade statliga myndighet som ansvarar för att leda arbetet med att samordna åtgärder inom en beredskapssektor vid fredstida krissituationer och höjd beredskap.[97] För beredskapssektorn elektroniska kommunikationer och post är Post- och telestyrelsen (PTS) sektorsansvarig myndighet.[98] Av PTS föreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster framgår bland annat att leverantörer av digital infrastruktur ska dokumentera sin kontinuitetsplanering[99], men Riksrevisionen konstaterar att reglering som ställer krav på en nationell kontinuitetsplan för cyberområdet saknas.

Enisa menar också att man bör *etablera en grundnivå/baseline för säkerhetsåtgärder*. Centermyndigheterna har både innan och efter att NCSC bildades försökt ta fram en nationell modell för systematiskt informationssäkerhetsarbete. Den ska underlätta för aktörer att göra mer enhetliga bedömningar av risker, hot och säkerhetsåtgärder,[100] vilket enligt Riksrevisionen skulle bidra till att skapa en grundnivå för säkerhetsåtgärder. Centermyndigheterna har däremot inte lyckats komma överens och någon modell har därför inte tagits fram. Regeringen har uttryckt intresse för att en modell ska tas fram, men har inte lämnat ett uppdrag eller vidtagit andra åtgärder för att säkerställa det (se avsnitt 3.1.1.).[101] Det närmaste en grundnivå/baseline som finns idag är MSB:s föreskrifter om systematiskt informationssäkerhetsarbete.[102] Vad gäller näringslivet finns det i NIS-regelverket krav på privata aktörer (NIS-leverantörer) att vidta säkerhetsåtgärder för att höja säkerheten i sina informationssystem.

---

96 Intervju Försvarsmakten 1.

97 I utredningen som låg till grund för förändringen föreslogs att informations- och cybersäkerhetsfrågorna skulle hanteras i ett särskilt tvärsektoriellt beredskapsområde för cybersäkerhet, vilket dock inte genomfördes. Se SOU 2021:25.

98 Förordningen (2022:524) om statliga myndigheters beredskap.

99 PTSFS 2021:3.

100 Bet. 2017/18:FöU4, s. 8.

101 Minnesanteckningar från möte i ida-gruppen för informationssäkerhetsfrågor 2018-01-26; Gemensam beredning 2018-05-07 av regeringsbeslut om: uppdrag att ta fram och genomföra en gemensam informations- och cybersäkerhetshandlingsplan för åren 2019–2022; Skr. 2016/17:213.

102 Se Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6); Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7); Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8).

Vissa av myndigheternas uppgifter och uppdrag berör området ändå, även om de inte per se etablerar en grundnivå. Exempelvis står FMV för certifiering av it-säkerhetsprodukter,[103] vilket kan bidra till en viss nivå av säkerhet. Utöver detta har MSB fått i uppdrag att vidta vissa åtgärder för att förbereda genomförandet av direktivet för nätverk och informationssystem EU 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen. Upphandlingsmyndigheten har fått i uppdrag att redovisa vilket stöd som ges avseende kravställning på informationssäkerhet vid offentlig upphandling.[104]

Slutligen, avseende området *skapa incitament för den privata sektorn att investera i säkerhetsåtgärder,*[105] har regeringen också i huvudsak vidtagit indirekta åtgärder. Incitament har framförts som ett viktigt styrmedel. Bland annat har det sagts att på den nationella nivån är cybersäkerhet *en fråga om implicit koordinering av många aktörer: det vill säga lagar, marknader, normer och andra mekanismer som skalar bättre. Här blir insikter i informationssäkerhetsekonomi avgörande – ett klokt sätt att uppnå implicit koordinering är nämligen … att den som har möjlighet att åtgärda ett cybersäkerhetsproblem i görligaste mån också ges incitament att göra det. Med sådana kloka incitament minskar behovet av explicit och centraliserat samarbete. Därför kan ganska små interventioner som justerar incitament få stor effekt på ett lands cybersäkerhet. Men denna sorts resonemang saknas i stor utsträckning i regeringens strategi, vilket är en brist, eftersom koordinering genom incitament troligen är det mest effektiva sättet att öka samhällets cybersäkerhet.*[106]

Regeringen har konstaterat att för att informations- och cybersäkerheten i samhället ska öka krävs att fler aktörer i både offentlig och privat sektor i högre utsträckning prioriterar och avsätter resurser för att höja säkerheten i sina verksamheter.[107] Regeringens insatser på området har dock fokuserat på den offentliga sektorn.[108] Att offentlig sektor investerar kan dock i förlängningen leda till att även privat sektor ser nyttan av att investera.

---

103 § 5 förordningen (2007:854) med instruktion för Försvaret materielverk.

104 Regeringsbeslut Ju2017/05786/L4; regeringsbeslut Fi2017/03257/DF; regleringsbrev för Upphandlingsmyndigheten 2018.

105 Detta benämns i akademin informationssäkerhetsekonomi (eng. information security economics eller economics of information security).

106 Franke, *Cybersäkerhet för en uppkopplad ekonomi*, 2020, s. 50.

107 Prop 2019/20:1 UO 6, s. 76.

108 Digg har tillsammans med Statskontoret fått i uppdrag att ta fram förslag på utvecklad styrning av digitala investeringar i offentlig sektor (regeringsbeslut I2020/00420/DF), och regeringen har också tagit fram en ägarpolicy för statliga bolag som betonar vikten av att de bedriver utvecklingsarbete. Näringsdepartementet, *Statens ägarpolicy och principer för bolag med statligt ägande 2020,* 2020.

3.1.1 Nationell modell – fördjupande exempel på en fråga där regeringen inte vidtagit åtgärder

Ett exempel på ett område som regeringen ansett viktigt men där den inte vidtagit åtgärder för att nå efterfrågat resultat är arbetet med en gemensam nationell modell för systematisk informations- och cybersäkerhet. Denna syftar till att underlätta för aktörer att göra mer enhetliga bedömningar av risker, hot och säkerhetsåtgärder. Även om behovet av en nationell modell uttrycktes redan 2015, och sågs som en central åtgärd av regeringen, så står man inte närmare en lösning idag än vad man gjorde då.

Utgångspunkten för arbetet med en nationell modell kan härledas till MSB och en inspiration utifrån Norges arbete med informations- och cybersäkerhet. Under NISU-utredningen försåg MSB utredaren med material och tankar kring en nationell modell.[109] När utredningen presenterade sitt förslag var en gemensam nationell modell för informationssäkerhet en av de centrala åtgärderna som föreslogs. Efter NISU-utredningen uppstod ett vakuum avseende denna.[110] Därför startade Samfi en arbetsgrupp under 2016.[111] Gruppen delredovisade sitt arbete under 2017. Samma år presenterade regeringen den nationella informations- och cybersäkerhetsstrategin, där en gemensam nationell modell var en central åtgärd för att uppnå regeringens målsättningar. I juli 2018 antydde regeringen att man skulle återkomma med ett uppdrag till de centrala myndigheterna om nationell modell och i november 2018 höll Regeringskansliet en myndighetshearing med Samfi-myndigheterna om frågan. Vid hearingen ställde sig samtliga myndigheter positiva till att skapa en nationell modell mot bakgrund av att arbetet hitintills inte varit samordnat. Flera av dem efterfrågade också en tydlig styrning från regeringen gällande detta.[112] MSB efterfrågade ett regeringsuppdrag till myndigheterna att i samverkan med andra ta fram en modell. FRA efterfrågade ett regeringsuppdrag till samtliga berörda myndigheter. FRA hade även framfört synpunkter kring nationell modell till Försvarsdepartementet vid ett tidigare tillfälle och myndigheten ansåg att regeringen borde ge ett mer stringent uppdrag om att skapa en nationell modell.[113]

---

109 Intervju MSB 4.

110 Vakuumet bestod i att alla visste att regeringen önskade en gemensam modell men ingen visste om man skulle ta fram den, vem som skulle ta fram den, hur man skulle ta fram den eller vad den skulle innefatta.

111 Intervju MSB 4.

112 FRA, minnesanteckningar från hearing.

113 Handling från FRA till Fö/SUND daterad 2018-05-07.

Trots avsaknad av regeringsuppdrag startade Samfi 2019 en förstudie om nationell modell. I juni 2020 avbröts arbetet efter oenighet i Samfi om vad arbetsgruppen skulle leverera. Deltagarna i arbetsgruppen hade olika syn på vad arbetet skulle innefatta och vad olika termer innebar. Exempelvis hade man olika syn på klassningsmodeller[114] och begreppet systematiskt informationssäkerhetsarbete och om fokus skulle riktas mot cyberangrepp eller om ett allriskperspektiv skulle anläggas. Det fanns också osäkerhet kring vilken produkt det handlade om och dess status; MSB ansåg att resultatet skulle tas hem och förankras hos respektive myndighet medan övriga myndigheter menade att ett förslag från en expertgrupp var det bästa alternativet. Arbetsgruppen kom bara till principnivå i förstudien.

I januari 2021 återupptogs arbetet med en förstudie inom ramen för NCSC. Oenigheten och svårigheterna har dock fortsatt. Arbetet förenklades dock genom att det hanterades inom ramen för centrets styrstruktur och avgränsades, i enlighet med centrets uppgift, till systematiskt cybersäkerhetsarbete. Efter att förstudien slutfördes har arbetet pausats i avvaktan på att myndigheterna i NCSC ska besluta om hur arbetet ska tas vidare.[115]

3.2 Åtta av femton områden har tillförts budget

För de åtta områdena *etablera en grundnivå/baseline för säkerhetsåtgärder, skydd av kritisk infrastruktur, stärk möjligheterna till kompetensutveckling och utbildning, samarbeta internationellt, institutionalisera samarbetet mellan myndigheter, etablera mekanismer för incidentrapportering, höj användares medvetandenivå (avseende informations- och cybersäkerhetsrisker och hot)* respektive *främja forskning och innovation* har regering och riksdag till viss del avsatt särskilda medel. Uppdrag och åtgärder inom övriga sju områden ska genomföras inom befintligt anslag. Utöver riktade medel för åtgärder inom Enisas områden har vissa myndigheter fått riktade medel för att stärka sin egen informations- och cybersäkerhet.[116] I flera av de myndigheter som har berörts av granskningen är det svårt att se hur mycket resurser myndigheterna satsar på verksamhet som är tänkt att stärka informations-

114 Informationsklassning innebär att man värderar organisationens informationstillgångar utifrån de interna och externa krav på konfidentialitet, riktighet och tillgänglighet som kommit fram i analysfasen. Kraven konkretiseras genom gradering av informationstillgångarna i olika nivåer, ofta kallade konsekvensnivåer. Kraven på skydd verkställs sedan genom att man kopplar adekvata säkerhetsåtgärder till varje konsekvensnivå. Se Myndigheten för samhällsskydd och beredskap, ”Metodstöd för systematiskt informationssäkerhetsarbete”.

115 Myndigheten för samhällsskydd och beredskap, *Föredragnings-PM Faktagranskning Riksrevisionens rapport om samhällets informations- och cybersäkerhet*, 2023.

116 Se exempelvis e-post Regeringskansliet 1.

och cybersäkerheten i Sverige. Det beror på att myndigheterna inte skär sin verksamhet på det sättet. Medel som har annonserats för insatser på informations- och cybersäkerhetsområdet i budgetpropositioner har heller inte alltid varit öronmärkta i regleringsbreven, utan har gått in i myndigheternas ramanslag. Strategin eller handlingsplanen innefattar inte någon resurssättning. Detta i kombination med bristen på utvärdering av vilka effekter som uppnås innebär att det inte går att avgöra om resurserna används effektivt. Företrädare för MSB har dock gett uttryck för att den totala resurstilldelningen på området är för låg.[117]

Vad gäller *grundnivå för säkerhetsåtgärder* har FMV en särskild anslagspost för evaluering och certifiering av IT-säkerhetsprodukter. Den ökar kontinuerligt under perioden 2017–2022, från knappt 14 mnkr till drygt 14 mnkr. 2022 fick FMV också en ny anslagspost för nationell tillsyn av cybersäkerhetscertifiering om 9,5 mnkr.[118]

För *skydd av kritisk infrastruktur* har PTS en särskild anslagspost för driftsäker och tillgänglig kommunikation som har ökat under den granskade perioden, från 126 mnkr 2017 till 1 561 mnkr 2022. PTS fick också 10 mnkr 2018 för att stärka det civila försvaret inom elektroniska kommunikationer.[119] Ingen av PTS två poster är dock specifikt för cybersäkerhet och har fokus på fredstida hot och påfrestningar. PTS, Säpo och Transportstyrelsen har vidare aviserats tillskott för ökat arbete som en följd av den nya säkerhetsskyddslagen i budgetpropositionerna för 2018 och 2019. Dessutom aviserade regeringen i budgetpropositionen för 2018, utgiftsområde 6, ytterligare medel till FRA (10 mnkr årligen för skydd mot angrepp) och MSB (40 mnkr för informationssäkerhet och psykologiskt försvar). Medlen öronmärktes dock inte i regleringsbreven utan gick in i deras respektive ramanslag.[120] I tillägg till det tilldelades MSB i vårändringsbudgeten för 2018 ytterligare 7 mnkr för nya uppgifter med anledning av NIS-direktivet.[121] Inte heller dessa medel öronmärktes i regleringsbrevet.[122] Även andra myndigheter, såsom Finansinspektionen, har fått pengar för ökad tillsyn som tillskott till deras respektive ramanslag.[123] Regeringen aviserade i budgetpropositionen för 2020, utgiftsområde 6, också en intern omfördelning av Försvarsmaktens medel för att genomföra åtgärder inom cyberförsvar, informationssäkerhet och särskilda insatser

117 Intervju MSB 1.
118 Regleringsbrev för FMV 2017–2022. Den nya anslagsposten skulle enligt budgetpropositionen ha varit 14 mnkr.
119 Regleringsbrev för PTS 2017–2022.
120 E-post Regeringskansliet 2; e-post Regeringskansliet 4.
121 Prop. 2017/18:99, s. 55.
122 Se regleringsbrev för MSB 2018–2019.
123 Prop. 2022/23:1 UO2, s. 30f.

om totalt 370 mnkr över tre år. Det går dock inte att se de omflyttningarna i regleringsbrevet; den anslagspost som skulle öka har inte ökat med de summor som nämnts. Försvarsdepartementet menar att omflyttningar har gjorts som planerat, men att de inte går att se på grund av andra förändringar i anslagen.[124]

Områdena om *forskning* och *kompetensutveckling* har tilldelats Försvarshögskolan (FHS) och Vetenskapsrådet. FHS har aviserats 5 mnkr 2018 respektive 2019 för utbyggnad av civila utbildningar. Medlen har gått in som en höjning av ramanslaget för grundutbildning.[125] Vetenskapsrådet har tilldelats 20 mnkr för forskning om informations- och cybersäkerhet samt 10 mnkr för forskning om digitaliseringens samhälleliga konsekvenser.[126] Likaså har området *höj användares medvetandenivå* tillförts 40 mnkr genom MSB gör att genomföra en informationskampanj riktad mot allmänheten.[127] Medlen öronmärktes dock inte i myndighetens regleringsbrev.[128]

MSB tilldelades också 15 mnkr för att stärka CERT-SE[129] inom området *etablera mekanismer för incidentrapportering*, som inte heller de öronmärktes i regleringsbrevet.[130]

Även medlen som främjar *internationellt samarbete* berör forskning och kompetensutveckling genom att utgöra medlemsavgift på 25 mnkr årligen till det europeiska projektet High performance computing.

Av medel som inte har egna anslagsposter har området *institutionalisera samarbeten mellan myndigheter* tilldelats mest resurser. Det handlar om uppdraget att etablera NCSC. Försvarsmakten, FRA, Säpo och MSB har 2021 och 2022 fått öronmärkta medel för centret och Fortifikationsverket har också fått medel för en lokal för NCSC. Försvarsmakten har fått 10 mnkr årligen för NCSC. FRA och MSB har fått 15 mnkr respektive 20 mnkr vardera 2021 respektive 2022. Säpo aviserades 10 mnkr i budgetpropositionen för 2021, men någon summa nämns inte i myndighetens öppna regleringsbrev.

124 E-post Regeringskansliet 3.
125 Se prop. 2017/18:1 UO 16; regleringsbrev för Försvarshögskolan 2018 och 2019.
126 Regleringsbrev för Vetenskapsrådet 2021 och 2022.
127 Prop. 2021/22:99, s. 169.
128 Se regleringsbrev för MSB 2022.
129 Prop. 2021/22:99, s. 169.
130 Se regleringsbrev för MSB 2022.

Tabell 1 Medel avsatta för åtgärder, per myndighet och år

	2017	2018	2019	2020	2021	2022
Försvarsmakten					10 000 (NCSC)	10 000 (NCSC)
FMV	13 950	14 071	14 198	14 430	14 224	14 394 9 500 (tillsyn)
FRA		10 000 årligen i ramanslag			15 000 (NCSC)	20 000 (NCSC)
MSB		47 000 ramanslag			15 000 (NCSC)	20 000 (NCSC) 55 000 ramanslag
PTS			5 200 för tillsyn (NIS)			
Säpo					10 000 (NCSC)	10 000 (NCSC)
Fortifikationsverket						900 000 (NCSC lokaler)
Vetenskapsrådet					5 000	15 000 + 10 000
FHS		5 000	5 000			
Medlemsavgift HPC			25 000	25 000	25 000	25 000
Transportstyrelsen		2 000	2 000 9 000	4 000	4 000	

Anm.: Summor i tusen kronor. Tabellen inkluderar inte medel som har tilldelats myndigheter för att stärka den egna informations- och cybersäkerheten.
Källa: Budgetpropositioner och regleringsbrev för åren 2017–2022.

3.3 Svaga resultat av vidtagna åtgärder

Även på områden där regeringen har vidtagit ett flertal åtgärder är resultaten av dem otydliga eller svaga.

Regeringen har gett flest uppdrag inom områdena *skydda kritisk infrastruktur* och *höj användares medvetandenivå*. Det är däremot svårt att säga vad det har haft för effekt på implementeringen av den nationella informations- och cybersäkerhetstrategin. Vad gäller *skydd av kritisk infrastruktur* har myndigheterna haft både stående och tillfälliga uppdrag som rör området och regeringen har också

initierat utredningar och föreslagit lagstiftningsförändringar.[131] Initiativen har ofta föranletts av förändringar i omvärlden såsom EU-initiativ, framkomsten av ny teknik eller ändrade hotbilder snarare än sprungna ur på förhand medvetna och strategiska avvägningar och prioriteringar. Åtgärderna för att *höja medvetandenivå* har i stort handlat om informationskampanjer, utbildningar och att ge stöd och råd. Dessa har riktat sig till det offentliga, det privata näringslivet, samt allmänheten.[132]

Även inom området *vidta åtgärder för att motverka it-relaterad brottslighet* har regeringen vidtagit relativt sett många åtgärder. Inom den punkten har det däremot i huvudsak handlat om olika lagändringar som ska underlätta polisens arbete.[133] De lagändringarna kopplar också till punkten *skapa balans mellan säkerhet och integritet- och dataskydd*. Polismyndigheten har också stärkt sin utredningsorganisation genom att inrätta ett nationellt och sju regionala (ett i varje polisregion) it-brottscentrum, så kallade SC3 respektive RC3. Utvecklingen av de regionala centrumen har däremot gått långsamt och det har varit svårt att få personal med rätt kompetens på plats. För komplexa cyberbrott råder det brist på utredare och det råder ständig brist på it-forensiker.[134] Denna organisatoriska förstärkning har däremot inte styrts av regeringen utan av Polismyndigheten.

Även områdena som kopplar till *utbildning, kompetensutveckling* och *forskning* har tillsammans fått en del uppmärksamhet. Regeringen har gett uppdrag, skrivit överenskommelser, tilldelat budget och lyft vikten av frågorna i budgetpropositioner.[135] Trots detta upplever både myndigheter och företag att det

---

131 Se exempelvis stående uppdrag i regleringsbreven för Försvarsmakten, FRA, Säpo och MSB för åren 2017–2022 och i förordningen (2007:951) med instruktion för Post- och telestyrelsen och förordningen (2014:1103) med instruktion för Säkerhetspolisen; regeringsbeslut Fi2017/03084/DF; regeringsbeslut I2019/0414/D U; regeringsbeslut Fi2022/01168.

132 Se exempelvis regeringsbeslut Ju2017/05789/SSK.; regeringsbeslut Ju2017/05788/SSK; regeringsbeslut Ju2018/01866/SSK; regeringsbeslut Ju2018/02265/SSK; regeringsbeslut Ju2019/03057/SSK; regeringsbeslut Ju2022/01292; 4 § förordningen (2007:951) med instruktion för Post- och telestyrelsen.

133 Se exempelvis Regleringsbrev för Polismyndigheten 2017 och 2022; regeringsbeslut Ju2020/00378/PO; SOU 2017:75 Datalagring - brottsbekämpning och personlig integritet; SOU 2017:89; SOU 2017:100; prop. 2018/19:96. Regeringen säger sig också bereda ratificering av Europarådets konvention om it-relaterad brottlighet.

134 Riksrevisionen, *Internetrelaterade sexuella övergrepp mot barn – stora utmaningar för polis och åklagare* RiR 2021:25; Riksrevisionen, *It-relaterad brottslighet – polis och åklagare kan bli effektivare* RiR 2015:21; intervju Polismyndigheten 1.

135 Se prop 2016/17:1 UO 22; prop 2017/18:1 UO 22; prop. 2019/20:1 UO 6, 16 och 22; prop. 2020/21:1 UO 22; prop. 2021/22:1 UO 22 och 16; regleringsbrev för Polismyndigheten 2017; regeringsbeslut Ju2020/00378/PO; regeringsbeslut Ju2022/02042; regeringsbeslut Ju2018/05292 (delvis), Ju2021/02005; regeringsbeslut I2019/01963/D U; regleringsbrev för Vetenskapsrådet för 2021 och 2022; regeringsbeslut Ju2021/03097.

fortfarande råder brist på relevant kompetens.[136] Kungl. Krigsvetenskapsakademien har framfört att en av de stora bristerna med koppling till kompetensförsörjning är att det inte finns ett ramverk bestående av en nationell kompetensförsörjningsstrategi och plan för hur vi ska resurssätta mot behoven på området. Ett sådant ramverk skulle kunna skapa en gemensam bild av vilken kompetens som krävs för en viss roll (befattning) och även en bild av vilka behov som finns och hur väl täckta de är i form av utbildningar.[137]

3.3.1 NCSC – exempel på åtgärd med svagt resultat

NCSC:s uppdrag

NCSC upprättades genom ett regeringsbeslut i december 2020. Arbetet och förberedelserna för centret hade dock pågått under drygt två år före det.[138] Regeringens strategi för informations- och cybersäkerhet betonade ett behov av ökad samverkan, såväl för Samfi-myndigheterna som för samhället över lag. Avsikten att skapa ett center uttrycktes officiellt första gången i regeringsförklaringen 2019. Myndigheterna som sedan fick i uppdrag att inrätta det tog under hösten 2019 gemensamt fram ett förslag på vilket sätt en fördjupad samverkan i form av ett cybersäkerhetscenter skulle kunna genomföras.

Det uppdrag myndigheterna sedan fick i december 2020 innebar att:

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

Samverkan inom ramen för cybersäkerhetscentret skulle utvecklas stegvis 2021–2023 inom följande områden:

- samlokalisering av relevanta förmågor från myndigheterna

136 Se exempelvis Schwarz, Åsa ”Kompetensbristen inom cybersäkerhet skenar”, hämtad 2022-05-23, 4c Strategies, ”Kompetensbristen inom cybersäkerhet – en nationell utmaning”, hämtad 2022-05-23; Oltsik, J, *The Life and Times of Cybersecurity Professionals 2020,* ESG, ISSA, 2020; möte Säpo 1 och 2; möte Försvarets radioanstalt 1.

137 Wiktorin, *Cyberförsvar – en introduktion,* 2022, s. 110f.

138 Myndigheterna påbörjade arbetet redan innan man fick uppdrag att genomföra förberedelser.

- stöd vid hanteringen av cyberangrepp och andra it-incidenter samt upprättande av en plan för samlad hantering på nationell nivå vid allvarliga cyberangrepp
- tillhandahållande av anpassade och aggregerade lägesbilder och analyser avseende hot, sårbarheter och risker
- riktade och samordnade varningar avseende hot och cyberangrepp
- samordning av stödet till förebyggande skyddsåtgärder, exempelvis tekniska säkerhetsanalyser och kartläggning av verksamheters beredskap vid it-incidenter
- samordning av, och utgöra kontaktpunkt för, internationella samarbeten på myndighetsnivå inom cybersäkerhetscentrets verksamhet
- kunskaps-, kompetens- och informationsutbyte och samverkan med offentliga och privata aktörer, exempelvis avseende detektion, sårbarheter, hot, risker, analys, verktyg och metoder samt internationellt samarbete
- dialog med aktörer inom forsknings-, kunskaps- och kompetensuppbyggnad
- erbjudande av kompetenshöjande insatser, exempelvis övningar och utbildningar för identifierade målgrupper.[139]

NCSC i jämförelse med center i andra länder

Det svenska centret skiljer sig från hur sådana har organiserats i flera andra länder. Vi har tittat på hur elva[140] andra västländer har organiserat sitt arbete. Det är vanligt att bilda ett center för att hantera cybersäkerhetsfrågor, åtta av elva länder har gjort det. De tre[141] som inte har ett center har i stället gett en specifik myndighet, som också arbetar med andra frågor, ansvar för området. Undantaget är möjligen USA där ansvaret tycks något mer uppdelat än i de andra länderna. Ett av länderna som har bildat ett center har gjort centret till en egen myndighet,[142] medan de andra har lagt det antingen under en annan myndighet eller under ett departement.[143] Det svenska centret ligger varken under en specifik myndighet eller under ett

139 Regeringsbeslut Fö2019/01330.

140 Finland, Norge, Danmark, Tyskland, Frankrike, USA, Storbritannien, Nya Zeeland, Australien, Nederländerna och Kanada.

141 USA, Tyskland och Frankrike.

142 Kanada.

143 Nederländerna och Nya Zeeland har placerat sina center under ett departement, Danmark och Norge under en säkerhetsmyndighet, Australien och Storbritannien under en signalspaningsmyndighet och Finland under en myndighet med ett bredare ansvar. Se SOU 2021:63, s. 261–350.

departement, och är inte heller en egen myndighet. Även om fyra myndigheter delar på ansvaret för centret ska samverkan ske mellan sju myndigheter. Det ska skapa förutsättningar för myndigheterna att fortsätta arbeta med sina respektive ansvarsområden men överbrygga eventuella överlappningar och gap i ansvar. En sådan konstruktion riskerar att skapa en tungrodd organisation, speciellt eftersom beslut fattas i konsensus.[144] Den risken har enligt Riksrevisionen förverkligats då det har tagit lång tid för centret att komma framåt i de flesta frågor som det jobbar med.

Arbetet har kantats av svårigheter

Centret har fram till dess att man anställde en chef i september 2021 bedrivits i projektform. Det har funnits en projektorganisation med uppdrag att arbeta med utformandet av centret, och de deltagande myndigheterna har bildat arbetsgrupper för att hantera olika sakfrågor. Arbetet i grupperna inom centret har kantats av svårigheter. Deltagare i grupperna beskriver det som att man har försökt ensa och få samman olika myndighetskulturer och att bygga förtroende mellan såväl myndigheter som enskilda individer. Våra intervjuer och underlag som vi har tagit del av ger en bild av att otydligheten avseende uppdrag, ansvar, genomförande och förväntningar har gjort det svårt att komma framåt i arbetet. Arbetet med att hitta en permanent lokal är ett exempel. Eftersom de deltagande myndigheterna har haft olika syn på hur centret ska drivas och vilken verksamhet som ska ”flyttas in” har de inte kunnat enas om säkerhetskrav för fastigheten. Arbetsgruppen har presenterat ett stort antal förslag. Myndigheterna var även vid ett tillfälle överens om en lokal, men arbetet tog ny riktning när nya krav inkom sent i processen.

Andra problem har att göra med att NCSC inte är en myndighet utan en samverkanskoalition mellan ett antal myndigheter. Det har enligt företrädare för centret försvårat upphandling och diarieföring.[145] Problemen visar sig även kring centrets huvuduppgifter, informationsdelning och lägesbild.

Informationsdelningen har inte fungerat fullt ut

En del av regeringens uppdrag var att centret skulle utgöra en nationell plattform för samverkan och informationsutbyte med privata och offentliga aktörer. Frågan om informationsutbyte har varit svår att hantera och arbetet har fortskridit i små steg. Problemen har varit både juridiska, kulturella och kommit sig av bristande systemstöd.

144 Möte Säkerhetspolisen 1 och 2; möte Försvarets radioanstalt 1.
145 Intervju Chefen för Nationellt cybersäkerhetscenter 1.

Tre av de fyra myndigheterna som har ett huvudansvar i centret är underrättelsemyndigheter.[146] Dessa myndigheter är av legala och kulturella skäl ofta restriktiva i sin informationsdelning. En underrättelsemyndighet kan vara förhindrad att dela information med andra aktörer på grund av sekretess eller överenskommelser med samarbetspartner i andra länder. En alltför extensiv informationsdelning riskerar också att röja inhämtningsmetoder och källor. Även om det inte finns legala hinder att dela information bygger informationsdelning i underrättelsevärlden på förtroende.[147] Information behandlas dessutom som en handelsvara, det vill säga man utbyter information om man anser att man får någonting i gengäld. Innan NCSC bildades fanns ett samarbete och informationsutbyte i form av NSIT (Nationell samverkan till skydd mot allvarliga IT-hot) mellan Säkerhetspolisen, Försvarsmakten och FRA. NSIT pausades och avbröts i samband med att NCSC bildades.[148] Ett samarbete liknande det som bedrevs inom NSIT har fortsatt inom ramen för NCSC men MSB, som inte är en underrättelsemyndighet, har i flera avseenden inte inkluderats i det samarbetet

NCSC har heller inte lyckats få fram ett gemensamt system för att dela information som omfattas av sekretess. Skälen uppges vara juridiska och upphandlingsmässiga eftersom centret inte är en myndighet.[149] Det innebär i sin tur att informationsdelningen måste hanteras manuellt mellan handläggare. Informationsdelning mellan myndigheterna är därmed fortfarande svårt.

Vad avser informationsdelning mellan statliga myndigheter och näringslivet har utmaningen varit ännu större. När centret bildades framförde företrädare för näringslivet vikten av att tidigt inkludera näringslivet i dess arbete. Man påpekade att om ambitionen är att NCSC ska stödja näringslivet så måste näringslivet involveras från början för att delge sina behov, samt tydliggöra hur de kan bistå. En struktur skapar en kultur och om vissa aktörer utelämnas från början kommer denna kultur att institutionaliseras.[150] Man framförde vidare vikten av att centret inte blir ett ”svart hål” dit information förmedlas från olika aktörer och inget

146 Säkerhetspolisen och Försvarsmakten är inte underrättelsemyndigheter per definition. Säkerhetspolisen är en säkerhetstjänst och hos Försvarsmakten är det bara den delen av myndigheten som utgörs av Must som kan benämnas som en ”underrättelsemyndighet”. Delar av Säkerhetspolisens verksamhet och den delen av Försvarsmakten som utgörs av Must fungerar dock i praktiken i mångt och mycket som underrättelsemyndigheter och därför benämns de som underrättelsemyndigheter i granskningsrapporten.

147 Intervju Försvarsmakten 5.

148 Försvarsmaktens faktagranskning av Riksrevisionens rapportutkast.

149 Intervju Chefen för Nationellt cybersäkerhetscenter 1.

150 SOFF, *Näringslivets syn på Sveriges kommande nationella cybersäkerhetscenter*, skrivelse till Regeringskansliet 20-04-23, s. 2.

kommer ut till samhällets övriga aktörer. Delgivning av information till samhällets aktörer, både privata och offentliga, var enligt näringslivet av största betydelse. Näringslivets uppfattning var därför att säkerställandet av samverkan mellan stat och näringsliv inom ramen för det nya centret var centralt.[151] Riksrevisionen konstaterar att staten fram till idag inte involverat näringslivet i utvecklingen av NCSC i någon betydande omfattning.

Utifrån näringslivets perspektiv har staten inte heller etablerat ett effektivt informationsutbyte inom ramen för NCSC. Enligt IVA finns det tillgång till information kring cybersäkerhetsfrågor över lag, men det är oklart hur den ska utformas och spridas för att bli användbar för företag inom olika branscher och av olika storlek.[152] Tjänsteföretagen uppger att det saknas tillgång till kvalificerad hotbildsbedömning och tillräcklig inriktning från myndigheternas sida.[153] Nio av tio företag uppger i Tjänsteföretagens undersökning att man idag inte samarbetar med myndigheter avseende cybersäkerhet. Ett antal tjänsteföretag upplever bristande intresse från myndigheterna att utveckla ett närmare samarbete, samt till viss del bristande förståelse hos myndigheterna om vad företagen tillhandahåller som är av vikt för samhället.[154] NCSC inledde under hösten 2022 ett pilotprojekt med finanssektorn. Syftet är att inleda ett strategiskt samarbete och utveckla former för informationsdelning mellan centermyndigheterna och sektorn. Riksrevisionen har dock inte fått ta del av några underlag som visar konkreta effekter av projektet.[155] Företrädare för vissa av myndigheterna i NCSC uttrycker att näringslivet har för högt ställda förväntningar, exempelvis att näringslivet har en övertro på att bara man får ta del av underrättelseinformation så kommer problemen att lösa sig.[156]

En ytterligare fråga är i vilken form, hur och i vilken omfattning information ska utbytas mellan olika aktörer i Sverige. Det finns inga entydiga riktlinjer,

---

151 SOFF, *Skrivelse med anledning av pågående arbete kring ett nationellt center för informations- och cybersäkerhet*, Stockholm 19 juni 2019.

152 IVA, *Cybersäkerhet för ökad konkurrenskraft*, 2022, s. 29f.

153 Almega, *Tjänsteföretagen och Stärkt cybersäkerhet i Sverige*, 2022, s. 13.

154 Almega, *Tjänsteföretagen och Stärkt cybersäkerhet i Sverige*, 2022, s. 17–18.

155 MSB har i faktagranskningen framfört följande: NCSC:s finansforum hade under 2022 två möten där riktlinjer för informationsdelning beslutades och sedan dess har informationsdelning från MSB/CERT-SE skett. Forumet hade första mötet i december. De två första mötena handlade om ”vad” (syfte antogs) och ”hur” (medlemsriktlinjerna antogs). Nu har tre arbetsgrupper tillsatts och arbetet påbörjats ”på riktigt”. Mot denna bakgrund kan arbetet sägas gå relativt fort sett från starten för lite drygt tre månader sedan, Se Myndigheten för samhällsskydd och beredskap, *Föredragnings-PM Faktagranskning Riksrevisionens rapport om samhällets informations- och cybersäkerhet*, 2023.

156 Intervju Säkerhetspolisen 1, 2 och 3; intervju Chefen för Nationellt cybersäkerhetscenter 1.

definitioner eller bestämmelser kring vilken information som ska delas eller hur den ska vara utformad. Inom vissa områden, exempelvis incidentrapportering enligt NIS och avseende statliga myndigheter, finns kriterier för hur incidentrapportering ska ske och vad den ska innehålla. Men det saknas ett standardiserat koncept för informationsdelning på informations- och cybersäkerhetsområdet. Detta kan jämföras med exempelvis USA där man har skapat en standard för informationsutbyte.[157] Avsaknaden av ett standardiserat koncept har påverkat och försvårat arbetet med att skapa nödvändiga informationsutbyten, såväl mellan myndigheter i centret som mellan myndigheter och privata aktörer.

Gemensam lägesbild tog tid att ta fram

Vad gäller arbetet med lägesbild har myndigheterna arbetat med frågan sedan NCSC bildades. Ett sådant arbete bedrevs tidigare också inom ramen för NSIT där myndigheterna arbetade fram rutiner och ställningstaganden kring hur information ska delas dem emellan. Trots att arbetet bedrivits under lång tid hade NCSC svårt att leverera en lägesbild under våren 2022 när en sådan efterfrågades av Regeringskansliet. Riksrevisionens tolkning är att regeringen i sitt uppdrag har efterfrågat att myndigheterna genom centret ska kunna leverera en ensad lägesbild på en viss sekretessnivå beroende på situation. Eftersom myndigheterna hanterar information på olika sekretessnivå och därför kan vara förhindrade att lämna över den fullständiga informationen obearbetad krävs ett arbete kring hur de ska bearbeta sin information för att kunna dela den och sätta ihop den med andra informationsmängder.[158] Oförmågan att leverera den efterfrågade lägesbilden uppges från vissa av myndigheterna bero på den korta tiden, en helg, centret fick på sig att leverera.[159] Riksrevisionen har svårt att avgöra om förfrågan var rimlig eller ej utifrån ett tidsperspektiv. Vi bedömer dock att möjligheterna att svara upp mot förfrågan hade varit större om myndigheterna effektivt hade undersökt vilka som skulle kunna komma att efterfråga en lägesbild, vilken förväntan som fanns och vad myndigheterna behövde göra för att kunna dela information mellan sig.

---

157 Se mer på Information Sharing and Analysis Organization Standards Organization:s webbsida.

158 Det brukar benämnas som ”tear lining” i betydelsen att information som står under ett faktiskt streck i ett underrättelsedokument har förberetts och bearbetats för att kunna delas. Central Intelligence Agency (CIA), ”Producing Timely Tailored Finished Intelligence: Writing for the Consumer”, hämtad 2023-01-30.

159 Intervju MSB 5; intervju Försvarets radioanstalt 2; intervju Försvarsmakten 4; intervju Säkerhetspolisen 2.

3.4 Få åtgärder inom centrala områden

Regeringen har varit relativt passiv även inom områden som har identifierats som viktiga, som att främja ökad rapportering av it-incidenter och att vara proaktiv på det internationella planet.

Att förebygga, upptäcka och hantera *it-incidenter* är ett eget tema i den nationella strategin och två punkter i Enisas lista. Regeringen har uppmärksammat att kunskapen om it-incidenter behöver öka,[160] men har inte vidtagit specifika åtgärder för att främja rapporteringen. Som nämnts tidigare är incitament viktiga. Anmälan av it-incidenter är ett område där incitament saknas. Det finns en mekanism för incidentrapportering i form av Cert.se som ligger på MSB. Statliga myndigheter samt NIS-leverantörer ska rapportera incidenter till MSB, men andra aktörer kan också rapportera på frivillig basis.[161] I förhållande till befintlig incidentrapportering har regeringen gett MSB och Polismyndigheten ett gemensamt uppdrag om att ta fram rutiner för vidarerapportering från MSB till Polismyndigheten om incidenter som uppstått på grund av brottslig verksamhet. MSB har motsatt sig en sådan vidarebefordran till polisens utredande verksamhet eftersom det automatiskt skulle leda till polisutredningar. Det skulle enligt MSB i sin tur kunna påverka viljan att rapportera incidenter negativt eftersom de drabbade organisationer som av olika anledningar väljer att inte polisanmäla då inte heller kommer att incidentrapportera. Det valda upplägget har inte någon motsvarighet i andra jämförbara länder.[162] MSB menar att det redan är svårt att se till att incidenter rapporteras. Detta leder till ett stort mörkertal och riskerar ge en otillräcklig lägesbild. Representanter från privat sektor menar att många avstår från att polisanmäla incidenter eftersom brotten ändå inte klaras upp.[163] Regeringen har ändå, i enlighet med Polismyndighetens begäran, gett uppdrag om utökad samverkan vad gäller rapporterade it-incidenter.[164]

Däremot har regeringen gett vissa uppdrag om att förebygga och hantera it-incidenter. MSB har fått två uppdrag, 2018 och 2022, om att utveckla eller stärka

160 Prop. 2018/19:1 UO 6, s. 74.

161 MSB, ”It-incidentrapportering för statliga myndigheter”, hämtad 2023-02-08. MSB ska enligt sin instruktion ha en sådan funktion, se § 11b förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

162 Se Myndigheten för samhällsskydd och beredskap, *Föredragnings-PM Faktagranskning Riksrevisionens rapport om samhällets informations- och cybersäkerhet*, 2023.

163 Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2022-05-19:1.

164 Justitiedepartementet, *Information till PM om vissa it-incidenter*, PM från L4, riktad till chefsleden uppåt i Ju; regeringsbeslut Ju2016/05127.

sitt arbete med att förebygga och hantera it-incidenter.[165] Uppdragen har inte kombinerats med några särskilda medel. Enligt uppdraget att bilda NCSC ska centret koordinera arbetet med att förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter. Centermyndigheterna har haft svårt att få till också denna del av uppdraget. De har dock pekat på att de i samband med valet 2022 bedrev ett intensivt koordineringsarbete som gav goda resultat och faktisk effekt.[166]

Slutligen lyfts vikten av *internationellt samarbete* både i den nationella strategin och av Enisa. Utrikesdepartementet (UD) ansvarar bland annat för Sveriges förbindelser med andra länder och internationella organisationer. Departementet representerar Sverige vid internationella möten och framför då Sveriges ståndpunkter. Företrädare för UD upplever dock att det svenska arbetet internationellt inom informations- och cybersäkerhet är reaktivt och inte proaktivt. De menar att detta beror både på bristande resurser och bristande organisation, både inom Regeringskansliet och i samarbetet med myndigheterna. Spelreglerna för det som sker på nationell nivå sätts till stor del på den internationella nivån.[167] Bristen på proaktivitet innebär då att Sverige i mindre utsträckning än vad som kanske vore önskvärt påverkar området i riktning med svenska intressen.[168]

Även myndigheterna är delvis delaktiga i det internationella arbetet på sina områden. FMV, MSB och Försvarsmakten har det exempelvis som stående inslag i sina regleringsbrev.[169] Det har också förekommit tillfälliga uppdrag till myndigheterna avseende internationell samverkan. MSB fick 2021 exempelvis i uppdrag att förbereda sig att bli nationellt samordningscenter kopplat till det europeiska kompetenscentret för cybersäkerhet inom näringsliv, forskning och teknik.[170] Efter att förberedelserna var genomförda fick MSB i uppdrag att utgöra ett sådant nationellt samordningscenter.[171] MSB bedriver ett omfattande internationellt arbete inom ramen för NIS-direktivet och deltar i medlemsstaternas

165 Regleringsbrev för MSB 2018; regeringsbeslut Ju2022/02219.

166 Intervjuer med företrädare för myndigheter i NCSC hösten 2022.

167 Se Myndigheten för samhällsskydd och beredskap, ”Aktuella EU-regleringar för informations- och cybersäkerhetsområdet”.

168 Minnesanteckningar från arbetsmaterial inför möte i statssekreterargruppen för digitalisering och cybersäkerhetsfrågor 2020-09-30; intervju Regeringskansliet 10. Se även kap. 4.

169 Regleringsbrev för FMV 2017–2022; Bilaga ”Riktlinjer för den militära säkerhetstjänsten” till regleringsbrev för Försvarsmakten 2017–2022. MSB är behörig myndighet för den offentligt reglerade tjänsten (PRS) inom det europeiska satellitnavigeringsprogrammet (Galileo) i enlighet med Rådets beslut 1104/2011/EU, MSBs regleringsbrev för budgetåret 2022

170 Regeringsbeslut Ju2021/03097.

171 11 c § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

samordningsgrupper både på policy[172] och teknisk[173] nivå. Myndigheten driver och deltar även i arbetsgrupper i flera centrala frågor inför NIS2 som incidentrapportering, leveranskedjor, dimensionerande hotbild, säkerhetsåtgärder med flera.[174]

3.5 Åtgärder som regeringen inte har vidtagit eller som har vidtagits sent i granskningsperioden

Informations- och cybersäkerhet är ett omfattande område som sträcker sig från en kabel som grävts av till cyberspionage eller gråzonsoperationer från främmande makt. Även om det säkerhetspolitiska läget har förändrats och kräver ett ökat fokus på antagonistiska hot, går det inte att bortse från den vardagliga informationssäkerheten. Inrättandet av NCSC beskrivs ibland som lösningen på alla problem som rör informations- och cybersäkerhet. Även ett fullt fungerande och operativt center löser dock bara en delmängd av problemen kopplade till informations- och cybersäkerhet.[175] Centrets övergripande uppdrag är att motverka antagonistiska cyberhot.[176] Alla myndigheter har bidragit till informationsdelning i centret genom att dela med sig av information om incidenter, sårbarheter och samhällskonsekvenser. MSB har dock framfört att övriga centermyndigheter företrädesvis har intresserat sig för denna information i de fall den rört angrepp som misstänks ha utförts av statsunderstödda aktörer, eller i vissa fall, grupper av kvalificerade cyberbrottslingar.[177] [178] Regeringskansliet har i faktagranskningen framfört till Riksrevisionen att centrets uppgifter inte enbart ska omfatta

---

172 NIS-samarbetsgruppen som är medlemsstaternas högsta beslutsfattande organ för myndigheter som implementerar NIS-direktivet. Under första halvåret 2023, d v s under Sveriges ordförandeskap i EU:s ministerråd, är myndigheten orförande.

173 EU:s CSIRT-nätverk (för tekniskt samarbete kring incidenthantering) och CyCLONe-nätverk (för bedömning av samhällskonsekvenser av it-incidenter och information till bl a ministerrådet och EU:s European External Action Service).

174 Se Myndigheten för samhällsskydd och beredskap, *Föredragnings-PM Faktagranskning Riksrevisionens rapport om samhällets informations- och cybersäkerhet*, 2023.

175 Intervju MSB 5.

176 Regeringsbeslut Fö2019/01330.

177 Myndigheten för samhällsskydd och beredskap, *Föredragnings-PM Faktagranskning Riksrevisionens rapport om samhällets informations- och cybersäkerhet*, 2023.

178 FRA har framfört till Riksrevisionen att många skyddsåtgärder mot antagonistiska och icke-antagonistiska incidenter är desamma. Däremot är angrepp från antagonistiska hot potentiellt mycket värre. Därmed är det den antagonistiska hotbilden som måste vara dimensionerande för cybersäkerhetsarbetet. Genom detta skapas till stor del skyddsåtgärder även mot icke antagonistiska hot men framför allt kompetens att hantera hela hotskalan.

cyberangrepp utan även andra it-incidenter.[179] [180] Riksrevisionen bedömer att inriktningen om att även omfatta andra it-incidenter inte har fått genomslag i centrets verksamhet.

Riksrevisionens uppfattning är att en god cybersäkerhet förmodligen inte går att uppnå om den inte vilar på en god informationssäkerhetsgrund. Undersökningar och rapporter pekar på bristande informationssäkerhet hos en rad organisationer i Sverige idag.[181] Det kan därför vara av intresse att peka på ett par problem som regeringen antingen inte har adresserat eller adresserat väldigt sent.

Ett sådant område är sensorsystem.[182] FRA har ett sensorsystem, TDV, som erbjuds till de statliga myndigheter och statliga företag som bedöms bedriva verksamhet som är av betydelse för Sveriges säkerhet. FRA erbjuder även rådgivning och stöd till samma krets. FRA har under flera år framfört till Regeringskansliet att myndigheten borde få möjlighet att erbjuda stöd till fler aktörer. Först i juni 2022 genomförde regeringen en ändring som möjliggör för FRA att vända sig även till privata aktörer.[183] Givet att den största delen av den samhällskritiska infrastrukturen idag återfinns inom det privata näringslivet är det svårt att förstå varför det har tagit så lång tid för regeringen att genomföra FRA:s förslag.
I samband med att FRA ursprungligen fick uppdraget menade regeringen att det inom den statliga sfären behöver finnas en hög teknisk kompetens och tekniska resurser för avancerat stöd i informationssäkerhetsfrågor och vid attacker. Det framfördes dock synpunkter på att FRA inte skulle konkurrera med det privata näringslivet, vilka regeringen instämde med. Samtidigt påpekade regeringen att säkerhetsskyddskraven väger tungt när det gäller samhällsviktiga funktioner, varför staten har ett ansvar att säkerställa att kompetens som denna finns på nationell nivå.[184]

---

179 Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet,* 2023.

180 Försvarsmakten och Säkerhetspolisen har dock i faktagranskningen uppgivit att begreppet andra it-incidenter kan behöva förtydligas. Försvarsmakten har framfört att det i uppdragsbeskrivningen står att myndigheterna som samverkar genom cybersäkerhetscentret ska bidra till verksamheten inom ramen för sina befintliga uppgifter. Den fördjupade samverkan inom cybersäkerhetscentret ska inte ta över det ansvar som ligger på de ingående myndigheterna och andra aktörer.

181 Se exempelvis MSB, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen,* 2022.

182 Sensorsystem läser innehållet i datatrafik för att upptäcka skadlig kod och intrång.

183 Förordning om ändring i förordningen (2007:937) med instruktion för Försvarets radioanstalt, SFS 2022:776, 9 juni 2022.

184 Prop. 2001/02:158, s 109–110.

Även MSB har vid ett flertal tillfällen framfört förslag på att införa sensorsystem till en bredare krets än den FRA erbjuder det till, bland annat till NIS-leverantörer[185]. Myndigheten har dock inte fått gehör för sitt förslag hos regeringen trots ett flertal påstötningar.[186]

Ett ytterligare exempel på svårigheter att få mandat eller medel för åtgärder är MSB:s arbete med Infosäkkollen.[187] [188] Enligt MSB har myndigheten både haft svårt för att få gehör för att få uppdraget såväl som att få det finansierat.[189]

En åtgärd som har föreslagits av ett flertal intressenter under lång tid är bildandet av en haverikommission avseende informations- och cybersäkerhetsincidenter.[190] IVA lyfter exempelvis att det behövs en kommission som hanterar incidenter och ”haverier” relaterade till cybersäkerhet. Kommissionen skulle genom analys, diskussion, råd och rekommendationer skapa möjligheter för olika aktörer att dra nytta av erfarenheter från inträffade angrepp och upptäckta sårbarheter.[191] Riksrevisionen konstaterar att det finns ett behov av strukturer som möjliggör informationsdelning och lärande från incidenter i högre utsträckning än vad som sker idag.[192] Riksrevisionen har däremot inte granskat på vilket sätt och i vilken form ett sådant utbyte bäst sker.

Ett ytterligare problemområde är den bristande samordningen av initiativ och åtgärder som vidtas. Ett exempel är regeringsuppdraget till Länsstyrelserna att regelbundet redovisa regionala lägesbilder till Regeringskansliet om hur den ryska invasionen av Ukraina påverkar det svenska samhället.[193] En aspekt av lägesbilden

185 Se MSB m.fl., *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – redovisning mars 2022*, 2022, s. 57.

186 Intervju MSB 1.

187 Regeringsbeslut Ju2019/03058/SSK, Ju2019/02421/SSK.

188 Infosäkkollen är ett verktyg som stödjer uppföljning och förbättring av systematiskt informationssäkerhetsarbete i kommuner, regioner och statliga myndigheter. Med verktyget kan organisationen själv undersöka vilken nivå arbetet befinner sig på och hur det kan utvecklas. Resultatet ger underlag för planering och prioritering, och med regelbundna uppföljningar kan utvecklingen följas över tid. Myndigheten för samhällsskydd och beredskap, ”Infosäkkollen”, hämtad 2023-03-09.

189 Intervju MSB 2.

190 Computer Sweden, ”Kritik mot regeringens utredning om it-säkerhet: För mycket myndighetsfokus, hämtad 2023-02-07; Motion till riksdagen 2021/22:3245 av Niels Paarup-Petersen m.fl. (C), Cybersäkerhet och cyberförsvar, Motion 2021/22:3639 av Pål Jonson m.fl. (M).

191 IVA, *Cybersäkerhet för ökad konkurrenskraft*, 2022, s. 31.

192 Exempel på problem i dagens strukturer är att det saknas tydliga incitament för näringslivet att dela med sig av information kring incidenter och man upplever också att det offentliga har svårt att garantera anonymitet om vilket företag som har varit föremål för incidenten om man lämnar över information.

193 Länsstyrelserna, ”Uppdrag till länsstyrelserna att redovisa regionala lägesbilder till Regeringskansliet”, hämtad 2023-02-07.

omfattar cyberperspektivet. Samtidigt har MSB arbetat med Infosäkkollen på uppdrag av regeringen.[194] Trots att uppdragen till stor del omfattar samma aktörer och samma frågor har det inte skett någon koordinering mellan uppdragen på Regeringskansliet. MSB ville efter förfrågan från projektgruppen hos Länsstyrelserna dela med sig av resultatet av sitt arbete men blev stoppade från att göra det av Justitiedepartementet.[195] Länsstyrelserna och MSB har dock samverkat kring metodfrågor och analys av det material som länsstyrelserna hämtade in.[196]

194 Regeringsbeslut Ju2019/03058/SSK, Ju2019/02421/SSK.

195 Intervju MSB 2 och 3.

196 Se Myndigheten för samhällsskydd och beredskap svar kring faktagranskning, *Promemoria Tidslinje över samarbetet med länsstyrelserna kring uppdraget om att ta fram en lägesbild över kommunernas cybersäkerhet*, 2023.

4 Regeringskansliets arbete med samhällets informations- och cybersäkerhet

I kapitel 2 och 3 har Riksrevisionen konstaterat brister i regeringens styrning för att stärka samhällets informations- och cybersäkerhet. Eftersom Regeringskansliet bereder regeringens beslut har vi valt att studera Regeringskansliets arbetssätt, organisation och resurser närmare för att försöka hitta förklaringar till bristerna.

Samhällets informations- och cybersäkerhetsfrågor spänner över ett flertal sakområden och under granskningsperioden var Statsrådsberedningen och nio departement[197] ansvariga för olika aspekter av frågan. Då det i allt högre utsträckning finns ett behov av att hantera dessa frågor samlat[198] finns enligt Riksrevisionens bedömning skäl att belysa hur Regeringskansliet arbetar med informations- och cybersäkerhetsområdet.

Riksrevisionens konstaterar att Regeringskansliets valda arbetsmetoder, organisering och avsatta resurser inte har varit tillräckliga för att styra området på ett strategiskt sätt. Om regeringen och Regeringskansliet hade åstadkommit en strategisk styrning på området hade, enligt Riksrevisionens bedömning, förmodligen nivån på informations- och cybersäkerhet i Sverige varit högre än vad den är idag.

4.1 Regeringskansliets arbetsmetoder har inte säkerställt strategisk styrning av informations- och cyberssäkerhetsområdet

Riksrevisionens bedömning är att Regeringskansliet har försökt samordna samhällets informations- och cybersäkerhetsfrågor internt, men hittills inte har

197 Finansdepartementet, Försvarsdepartementet, Infrastrukturdepartementet, Justitiedepartementet, Miljödepartementet, Näringsdepartementet, Socialdepartementet, Utbildningsdepartementet och Utrikesdepartementet. Fram till 2023-01-01 hade Justitiedepartementet ansvar för förvaltningsärenden inom informations- och cybersäkerhet i den mån sådana ärenden inte hörde till något annat departement. Därefter tog Försvarsdepartementet över det ansvaret. Statsrådsberednings ansvar omfattar bland annat förvaltningsärenden som gäller regeringen, Regeringskansliet, kommittéväsendet och europeiska integrationsfrågor av horisontell karaktär. Förordning (1996:1515) med instruktion för Regeringskansliet.

198 Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-05-25:2.

lyckats fullt ut.[199] Enligt Riksrevisionen har Regeringskansliets arbete med informations- och cybersäkerhetsfrågor i mångt och mycket utgått från preferenser i de enskilda sakområdena som sedan samordnats med övriga berörda departement. Det gäller exempelvis den nationella informations- och cybersäkerhetsstrategin där olika departement ansvarade för att skriva olika avsnitt.[200] Det finns också exempel när samtliga berörda departement inte blivit involverade i beredning av informations- och cyberssäkerhetsärenden. Ett departement drev en svensk position i EU i cirka ett år utan att informera övriga departement, vilket blev problematiskt då samtliga svenska politiska perspektiv inte omhändertogs i den svenska linjen.[201]

För att underlätta samordningen av informations- och cybersäkerhetsfrågorna har interdepartementala arbetsgrupper (ida-grupper) skapats. Syftet var att träffas regelbundet för diskussioner och erfarenhetsutbyte,[202] vilket med tiden kompletterades med en vilja om att samordna och inrikta frågorna.[203] För samhällets informations- och cybersäkerhet har grupper, formella såväl som informella, med mer eller mindre tydligt uttalade uppdrag funnits både före och under Riksrevisionens granskningsperiod. Olika delar av Regeringskansliet har varit ansvariga för att sammankalla dessa ida-grupper. Den informella ida-grupp som Justitiedepartementet samlade bestod av tjänstemän på i huvudsak handläggarnivå medan ida-gruppen Infrastrukturdepartementet ansvarade för år 2020 till 2022 samlade personer på chefs- och huvudmannanivå. Till ida-gruppen som Infrastrukturdepartementet ansvarade för knöts en statssekreterargrupp och en tjänstemannagrupp. Den sistnämna gruppen bestod av handläggare. Tabellen nedan ger en beskrivning av grupperna över tid.

199 Regeringskansliet har även framfört bristerna i *PM Informations- och cybersäkerhet – aktörers ansvar och eventuella luckor i upplägg och hantering,* 2022.

200 Intervju Regeringskansliet 6 och 11; möte Regeringskansliet 1; intervju Försvarsmakten 1.

201 Intervju Regeringskansliet 10.

202 Intervju Regeringskansliet 6.

203 Minnesanteckningar från arbetsmaterial från statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet, *PPT Cyber/Digitalisering – Förslag, process arbetssätt*, 2020-06-12.

Tabell 2 Regeringskansliets interdepartementala arbetsformer för digitalisering, cyber- och informationssäkerhet över tid

År	Interdepartemental arbetsform	Sammankallande samt övriga deltagare i Regeringskansliet	Centrala leveranser
2017	Informell ida-grupp	Justitiedepartementet Fi/Fö/UD/M/Nä/Soc/Ku/Ju	
2018	Informell ida-grupp	Justitiedepartementet Fi/Fö/UD/M/Nä/Soc/Ku/Ju	
2019 januari till våren 2020	Ida-grupp	Statsrådsberedningen Fö/Ju/UD/Nä/Infra/Soc	
2020, senvår	Statssekreterar-, ida- och tjänstemannagrupp	Infrastrukturdepartementet Fö/Ju/UD/Nä/Infra/SB/Soc/U	
2021	Statssekreterar-, ida- och tjänstemannagrupp	Som ovan + M och Fi	Strategiska promemorior
2022	Statssekreterar-, ida- och tjänstemannagrupp	Som ovan	Strategiska promemorior

Källa: Skriftliga underlag från Regeringskansliet. Riksrevisionens bearbetning.

Under första delen av Riksrevisionens granskningsperiod sammankallade Justitiedepartementet den informella ida-gruppen för informationssäkerhet.[204] Den arbetade med att ta fram en nationell strategi för samhällets informations- och cybersäkerhet.[205] Statsrådsberedningen tog över ansvaret för att sammankalla en interdepartemental grupp gällande informations- och cybersäkerhet år 2019.[206] Under det dryga året Statsrådsberedningen var sammankallande framgick av regeringsförklaringen att ett nationellt center skulle upprättas för att öka informations- och cybersäkerheten och ett regeringsbeslut fattades om att fyra myndigheter skulle påbörja förberedelserna för ett sådant center.[207] Statsrådsberedningen började samla Regeringskansliets tvärsektoriella frågor inom informations- och cybersäkerhet och skrev promemorior om dessa. Statsrådsberedningens arbetet framstod då alltmer som beredning av ärenden inom informations- och cybersäkerhet[208], vilket enligt Regeringskansliets

204 Ida-gruppen var under denna period inte formellt beslutad varför den omnämns som en informell ida-grupp.
205 Skr. 2016/17:213.
206 Intervju Regeringskansliet 7.
207 Regeringsförklaringen 21 januari 2019; regeringsbeslut Fö2019/01330.
208 Intervju Regeringskansliet 7.

arbetsordning är departementens uppgift.[209] Infrastrukturdepartementet fick ett formellt uppdrag att ansvara för en interdepartemental grupp gällande digitaliserings- och cyberfrågor i början av år 2020 och kom i gång med arbetet under senvåren 2020.[210] Till denna ida-grupp, som främst bestod av chefstjänstemän och huvudmän, knöts en statssekreterargrupp och en tjänstemannagrupp (handläggare) som skulle utföra olika arbetsuppgifter. Syftet med att tillföra en statssekreterargrupp var att få ett politiskt och strategiskt helhetsperspektiv på cyberfrågorna. Initiativen hitintills ansågs inte ha tillgodosett behovet av en tydlig inriktning och samordning av dessa frågor.[211] Kunskapsuppbyggnad i Regeringskansliet och ökad förståelse för de andra departementens perspektiv var andra mål med ida-grupperna.[212]

Av uppdraget från Statsrådsberedningen till Infrastrukturdepartementet framgår bland annat att en statssekreterargrupp inrättas för att få ett politiskt och strategiskt helhetsperspektiv på cyberfrågorna. En ida-grupp skulle bistå statssekreterargruppen i dess arbete med att stärka samordningen i Regeringskansliet av cyberfrågor som var av strategisk betydelse. Cyberfrågorna omfattar bland annat den fortsatta digitaliseringen av samhället, innovation, Sveriges säkerhet och nationella intressen, svensk tillväxt och konkurrenskraft. Förväntade resultat av arbetet var att:

- departementen tar ett större ansvar för cyberfrågorna
- de strategiska cyberfrågorna som ska samordnas identifieras
- det tas ett samlat grepp om cyberfrågornas olika aspekter där olika intressen balanseras genom en tydlig inriktning och samordning
- denna inriktning och samordning ska möjliggöra en högre prioritet för frågorna inom Regeringskansliet och förbättra förutsättningarna för svenskt inflytande och deltagande i internationellt samarbete genom att en mer enhetlig linje hålls. Inte minst behöver departementens arbete på EU-nivå inom cyberområdet samordnas på ett bättre sätt.[213]

---

209 Förordning (1996:1515) med instruktion för Regeringskansliet.

210 Intervju Regeringskansliet 9.

211 Minnesanteckningar från arbetsmaterial från statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet, *PPT Cyber/Digitalisering – Förslag, process arbetssätt*, 2020-06-12.

212 Minnesanteckningar från arbetsmaterial från statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet, *PPT Cyber/Digitalisering – Förslag, process arbetssätt*, 2020-06-12.

213 Minnesanteckningar från Regeringskansliets arbetsmaterial 1.

Statssekreterargruppen enades om följande arbetsprocess för det interdepartementala arbetet gällande digitaliserings- och cyberfrågor. Varje statssekreterarmöte utgick från ett strategiskt område med ett antal beredda beslutspunkter som underlag för diskussion. Efter att statssekreterargruppen diskuterat frågan lämnades eventuellt en beställning till ida-gruppen. Ida-gruppen gav Infrastrukturdepartementet i uppdrag att ta fram underlag, exempelvis strategiska promemorior, med stöd av tjänstemannanätverket. Underlagen bereddes i och godkändes av ida-gruppen innan de presenterades i och godkändes av statssekreterargruppen. Statsekreterargruppsmötena skulle mynna ut i ett antal strategiska positionspromemorior innehållandes bland annat talepunkter och språkregler inom digitalisering och cybersäkerhet som statssekreterargruppen kunde driva och kraftsamla kring inför EU-ordförandeskapet.[214] Dessa skulle dock inte ta över gemensam beredning av ärenden.[215]

Ett antal strategiska frågor som behövde samordnas[216] mellan departementen identifierades och beskrevs i promemorior på olika teman.[217] En av Riksrevisionens iakttagelser är att i flera av promemoriorna har informations- och cybersäkerhet beaktats i begränsad omfattning.[218] Riksrevisionen konstaterar också att ett flertal av promemoriorna beskriver teman på övergripande nivå och inte tar sig an de

214 Minnesanteckningar från Regeringskansliets arbetsmaterial 2.

215 Minnesanteckningar från arbetsmaterial från statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2020-09-30; minnesanteckningar från arbetsmaterial från möte i ida-gruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-04-23.

216 Regeringskansliet har i faktagranskningen framfört att de frågor som valdes ut skulle berörda minst två av följande aspekter: digitalisering av samhället, innovation, Sveriges säkerhet och nationella intressen, svensk tillväxt samt konkurrenskraft. Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023.

217 Tjänstemannagruppen fick uppdrag att skriva promemorior av statssekreterargruppen via ida-gruppen, men det förekom även att statssekreterargruppen formulerade uppdrag till tjänstemannagruppen. Intervju Regeringskansliet 9.

218 *PM Strategisk inriktning för hälsodata, e-hälsa och digital infrastruktur*, 2022-05-04; *PM Artificiell intelligens*, 2021-03-10*; PM om data*, 2021-03-30 samt *PM om gemensamma initiativ*; minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-05-25:1.

delar av uppdraget som omfattar samordning, inriktning eller framtagande av svenska handlingslinjer.[219] [220]

Regeringskansliet har framfört att nyttan med de interdepartementala mötena och promemoriorna främst har varit att hitta gemensamma grunder och inriktning, öka förståelsen för att digitalisering behöver kombineras med cybersäkerhet och höja kunskapsnivån i statssekreterar- respektive ida-gruppen. Flera uppger även att grupperna har underlättat informationsutbytet mellan departementen och möjliggjort att frågor som berör flera departement har identifierats och diskuterats. Vissa menar att de underlättat beredningen av regeringsärenden.[221] Dessa nyttor beskrivs dock som svårkvantifierade. För att en promemoria skulle godkännas av statssekreterargruppen behövde de inte nå konsensus som i Regeringskanslets ordinarie beredningsprocesser, utan det räckte med att vara ”tillräckligt” överens om innehållet. Innebörden av att vara tillräckligt överens framgår varken av skriftliga underlag eller intervjuer med representanter från Regeringskansliet. Fördelar med att promemoriorna inte mynnar ut i regeringsbeslut är att det ger en möjlighet för deltagarna att pröva sig fram utan att det direkt leder till skarpa åtgärder. Samtidigt skapar det en osäkerhet kring promemoriornas status och därmed hur de kan användas.[222] Riksrevisionen konstaterar att produkterna inte är samordnade på ett sådant sätt att de kan användas för att inrikta digitaliserings-

---

219 Förväntan/krav på leverans enligt uppdraget från Statsrådsberedningen till Infrastrukturdepartementet var bland annat att ta ett samlat grepp om cyberfrågornas olika aspekter där olika intressen balanserades genom en tydlig inriktning och samordning. Denna inriktning och samordning skulle möjliggöra en högre prioritet för frågorna inom Regeringskansliet och förbättra förutsättningarna för svenskt inflytande och deltagande i internationellt samarbete genom att en mer enhetlig linje skulle hållas. Inte minst behöver departementens arbete på EU-nivå inom cyberområdet samordnas på ett bättre sätt. Minnesanteckningar från Regeringskansliets arbetsmaterial 1.

220 Regeringskansliet har i faktagranskningen skrivit att det finns exempel på hur teman beskrivna i promemorior mynnat ut i styrning. Som exempel anger Regeringskansliet promemorian om digital suveränitet som utgjorde grunden för Sveriges ställningstagande i olika EU-fora i den frågan. Ett annat exempel som Regeringskansliet uppger är slutsatsen att Sverige bör kandidera till Internationella teleunionens verkställande råd, vilket gjordes och resulterade i att Sverige valdes in. Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023.

221 Regeringskansliet har i faktagranskningen förmedlat att den samlade benämningen av statssekreterar-, ida- och tjänstemannagruppen är samordningsgruppen och att flera deltagare i samordningsgruppen har uttryckt att arbetet underlättat gemensamberedningar. Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023. Samordningsgruppen har inte förekommit i de underlag som Riksrevisionen tagit del av under granskningen.

222 Intervju Regeringskansliet 5 och 6; Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-02-18.

eller cybersäkerhetsfrågorna, vilket var ett av de förväntade resultaten enligt uppdraget från Statsrådsberedningen till Infrastrukturdepartementet. Inriktning och styrning har fortsatt skett i de ordinarie beredningsprocesserna.

Andra menar att det interdepartementala arbetet har föga eller inget mervärde. Status på tjänstemannagruppens promemorior beskrivs som oklar och att de sällan eller aldrig använts som underlag i beredning av regeringsärenden. Det har också funnits utmaningar med att hitta skrivningar som alla har kunnat enas om och ibland har ståndpunkter uteslutits utan förklaring. Säkerhetsaspekterna har av ett departement beskrivits som ett filter som läggs på i efterhand i digitaliseringsarbetet. Två departement har lyft i underlag till statssekreterargruppen att vissa promemorior inte cirkulerats med alla i tjänstemannagruppen innan möten i statssekreterargruppen, vilket har lett till att vissa relevanta perspektiv inte belysts.[223] [224] Promemoriorna skulle kunna ha använts för att styra strategiskt, exempelvis som underlag till regeringsuppdrag eller till framtagande av svenska positioner i EU- eller andra internationella sammanhang.[225] Två anledningar till att så inte har skett är att de strategiska ståndpunkter som de interdepartementala grupperna varit överens om inte dokumenterats skriftligt och att samtliga berörda departement inte alltid nått samsyn kring promemoriornas innehåll.[226]

Riksrevisionen bedömer att det interdepartementala arbetet kring digitalisering, cyber- och informationssäkerhet har haft ett mervärde inom Regeringskansliet i form av förbättrat informationsutbyte och ökad kunskap. Riksrevisionen konstaterar dock att Regeringskansliets arbetsmetoder gällande samhällets informations- och cybersäkerhet däremot inte räckt hela vägen fram för att lösa ut centrala målkonflikter eller styra strategiskt på området.

---

223 Intervju Regeringskansliet 6; minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2020-12-18, 2022-08-26:1 och 2.

224 Regeringskansliet har uppgett i faktagranskningen att detta i så fall varit helt i enlighet med hierarkierna mellan grupperna om hur arbetet grupperna emellan var fördelat. Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023.

225 Intervju Regeringskansliet 11.

226 Intervju Regeringskansliet 6 och 9; minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2022-08-26: 2.

4.2 Regeringskansliets förmåga inom informations- och cyberssäkerhet räcker inte till

Jämfört med motsvarigheter i andra europeiska länder har Regeringskansliet relativt sett få personella resurser som arbetar med informations- och cybersäkerhet. Pandemin har inneburit ett ökat fokus på digitaliserings-, cyber- och informationssäkerhetsfrågor och representanter för Regeringskansliet menar att personalresurserna inte räcker till. Resurs- och tidsbrist är ett återkommande tema vid intervjuer med representanter i de interdepartementala grupperna för digitaliserings- och cyberfrågor och tjänstemannagruppen uppges vara särskilt tungt belastad.[227] De tjänstemän på Regeringskansliet som under granskningsperioden deltog i ida-grupperna återfanns på nio departement. Ett flertal av dem hade samhällets cyber- och informationssäkerhet som en av sina huvuduppgifter och hade mer tid att ta sig an frågorna ur ett strategiskt perspektiv.[228] Riksrevisionen bedömer dock att interaktion mellan tjänstemän som arbetar strategiskt med informations- och cybersäkerhetssäkerhetsfrågor och tjänstemän som kommer i kontakt med frågorna mer sällan, exempelvis myndighetshandläggare, skulle behöva ske i större utsträckning. Det skulle minska risken för glapp i kunskapsöverföringen dem emellan.

Framtagande av promemorior i tjänstemannagruppen beskrivs som resurskrävande samtidigt som deras syfte och användbarhet har begränsat mervärde då de inte är direkt användbara i regeringens styrning. I de flesta fall deltar samma personer i det interdepartementala arbetet som i Regeringskansliets ordinarie beredningsprocesser. Deltagare i tjänstemannagruppen har ställts sig frågande till arbetsinsatsens mervärde; den är i flera fall omfattande och tidskrävande samtidigt som vissa uppgifter redan utförs parallellt i linjen på tjänstemannanivå. Det gäller exempelvis prioriteringar inför EU-ordförandeskapet.[229] Riksrevisionen konstaterar att Regeringskansliet har anammat en komplex organisation och metod för arbetet med strategiska informations- och cybersäkerhetsfrågor utan att tillföra ytterligare personal, budget eller, gällande de interdepartementala grupperna, tydligt mandat. Riksrevisionen bedömer därmed att Regeringskansliets personella resurser inte har nyttjats på ett effektivt sätt.

---

227 Intervju Regeringskansliet 9 och 10; minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-05-25:1, 2021-09-15 samt 2022-03-18.

228 Intervju Regeringskansliet 6, 7 och 8.

229 Intervju Regeringskansliet 6 och 10; minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2022-08-26:2; minnesanteckningar från Regeringskansliets arbetsmaterial 3.

Enligt Riksrevisionens bedömning är Regeringskansliets förmåga att identifiera och ta fram lämpliga uppdrag till sina respektive myndigheter över lag god. Långsiktigheten saknas dock och vissa uppdrag är otydliga och inte helt anpassade till vad som ska uppnås. Ett exempel är uppdraget om fördjupad samverkan inom ramen för NCSC. Myndighetsrepresentanter menar att det är svårt att bygga infrastruktur med utgångspunkt i tillfälliga uppdrag och tidsbegränsade ekonomiska medel.[230] [231] Riksrevisionen konstaterar att Regeringskansliets förmåga inte har varit tillräcklig för att bedöma vad som krävs för en fungerande samverkan inom NCSC.

Granskningen visar att Regeringskansliet inte heller ser till Sveriges sammantagna intressen i centrala uppdrag som syftar till att stärka samhällets informations- och cybersäkerhet. Ett centralt regeringsuppdrag för att nå målen i den nationella informations- och cyberssäkerhetsstrategin är det som gick till myndigheterna som samverkar i cybersäkerhetscentret om att ta fram en samlad handlingsplan. Uppdraget ger få möjligheter att föreslå andra åtgärder än de som redan utförs då föreslagna aktiviteter och åtgärder ska rymmas inom respektive myndighets givna ekonomiska ramar.[232] Enligt Riksrevisionen är detta uppdrag ett exempel på att Regeringskansliet inte samordnat de strategiska prioriteringarna i den nationella informations- och cyberssäkerhetsstrategin med myndighetsstyrningen och därmed inte förmått identifiera lämpliga uppdrag som bidrar till att genomföra strategin. Som nämnts i kapitel 3 har myndigheterna visserligen även fått andra uppdrag inom informations- och cybersäkerhet, men ett sammanhållet genomförande där helheten står i fokus kan Riksrevisionen inte se.

Regeringskansliet har framfört att Sverige har ett gott renommé internationellt avseende cyberfrågor, men att Sverige behöver bli bättre på att utforma proaktiva vägval utifrån nationella intressen, behov och resurser.[233] För detta saknas adekvata underlag. Exempelvis kan en svensk representant på ett internationellt möte ha underlag bestående av flera hotlägesbilder från olika aktörer som inte är bearbetade

230 Intervju MSB 1; regeringsbeslut Fö2019/01330.

231 Regeringskansliet har i faktagranskningen framfört att NCSC-uppdraget inte är tillfälligt och de ekonomiska medel som föreslagits i budgetpropositionen är en finansiering som ligger på lång sikt. Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023.

232 Regeringsbeslut Ju2018/03737/SSK; MSB, *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – redovisning mars 2022*; intervju MSB 1.

233 Minnesanteckningar från arbetsmaterial inför möte i statssekreterargruppen för digitalisering och cybersäkerhetsfrågor 2020-09-30 och 22-05-19:2; intervju Regeringskansliet 11.

och sammanfogade eller som inte ser till Sveriges sammantagna intressen.[234] Andra exempel där en gemensam svensk handlingslinje har saknats inom cyberområdet är vid framtagandet av underlag till Cyberresiliensakten[235] och rådsarbetsgruppen HWP Cyber samt till EU:s datastrategi.[236] Riksrevisionen bedömer att svensk representation internationellt skapar möjligheter för Sverige att vara drivande på olika internationella arenor. Ett sändebud som kan representera hela Sverige i cyberfrågor internationellt, motsvarande UD:s samordnare för cyberfrågor som håller samman de diplomatiska kontakterna, kommer dock att utses först 2023.[237] Riksrevisionen bedömer att Sverige kan bli mer proaktivt i dessa frågor. Sverige skulle exempelvis kunna förhandla för att i största möjliga mån tillgodose de nationella intressena i stället för att endast säga ja eller nej till EU-förslag.[238] Bristande intern samordning på Regeringskansliet har även lett till uteblivet svenskt deltagande på internationella möten där beslut som påverkar Sverige tagit form.[239] Myndighetsrepresentanter har beskrivit hur de bistått Regeringskansliet med omfattande underlag inför förhandlingar i EU, men inte fått information om vad som tagits med till förhandlingsbordet eller utfallet.[240]

---

234 Intervju Regeringskansliet 10.

235 Cyberresiliensakten syftar till att skapa förutsättningar för utvecklingen av säkra produkter med digitala element genom att säkerställa att hårdvaru- och programvaruprodukter har färre sårbarheter när de släpps ut på marknaden och att tillverkarna tar säkerheten på allvar under produktens hela livscykel, och att skapa förutsättningar för att användarna ska kunna ta hänsyn till cybersäkerheten när de väljer och använder produkter med digitala element (CE märkning av digitala produkter). För ekonomiska aktörer som vill placera produkter med it-funktionalitet på den inre marknaden innebär detta att de måste säkerställa att produkterna är säkra ur ett cybersäkerhetsperspektiv samt ta ansvar för potentiella sårbarheter. För myndigheter innebär det att ett väldigt stort antal produkter och aktörers efterlevnad behöver säkerställas. Cyberresiliensakten ställer omfattande krav på berörda aktörer, i synnerhet om de tillhandahåller, producerar, distribuerar eller nyttjar högriskprodukter med it-funktionalitet, standardisering, CE-märkning. Förslag till EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020 (Cyberresiliensakten); MSB, *Promemoria Initiativ på EU-nivå av relevans för säkerhet i Sverige och EU – fokus informations- och cybersäkerhet*, 2023-03-20. Att certifiera enskilda produkter innebär en stor mängd arbete. Ett mer effektivt alternativ till att certifiera produkter hade varit att certifiera kvalitetsprocesserna vid de företag som framställer produkterna. Om Regeringskansliet hade involverat rätt kompetens vid berörda myndigheter i framtagandet av underlag till förhandlingarna gällande Cyberresiliensakten så hade Sverige kunnat agera annorlunda i förhandlingarna.

236 Minnesanteckningar från arbetsmaterial inför möte i statssekreterargruppen för digitalisering och cybersäkerhetsfrågor 2020-09-30.

237 Av Utrikesdeklarationen 2023 framgår att regeringen avser att tillsätta ett särskilt sändebud för internationella frågor. Regeringens deklaration vid 2023 års utrikespolitiska debatt i riksdagen onsdagen den 15 februari 2023.

238 Intervju MSB 1.

239 Intervju Regeringskansliet 10.

240 Intervju MSB 3.

Riksrevisionen bedömer att ett utökat informationsutbyte mellan Regeringskansliet och myndigheterna i utformandet av svenska ståndpunkter skulle öka Sveriges inflytande internationellt. Riksrevisionens slutsats är att Regeringskansliets förmåga att hantera internationella initiativ och vara proaktiva på den internationella arenan inte har varit tillräcklig.

Alla aktörer som är engagerade i informations- och cybersäkerhetsfrågor lyfter vikten av ökad kompetens inom området[241] och diskussioner har förts om att ge tjänstemannagruppen som var knuten till statssekreterargruppen för digitalisering och cyberfrågor i uppdrag att kartlägga kompetens inom stat och näringsliv för att se hur dessa bäst kan komma till nytta.[242] Regeringskansliet genomförde dock inte kartläggningen eftersom det interdepartementala arbetet avseende digitalisering- och cyberfrågor avslutades under hösten 2022.[243] Det har framförts att Regeringskansliet behöver kunskap på strategisk, taktisk och operativ nivå i organisationen för att kunna värdera cyberdomänen och ha en holistisk syn, men att den strategiska kompetensen inte alltid finns där.[244] Det blir ofta fokus på den organisatoriska ansvarsuppdelningen mellan departementen i stället.[245] Helhetsperspektivet på informations- och cybersäkerhetsfrågorna, där olika intressen balanseras mot varandra, är tänkt att diskuteras i de interdepartementala grupperna. Av skriftliga underlag som Riksrevisionen tagit del av framgår att det interdepartementala arbetet behöver bli mer effektivt och bemannas på ett sådant sätt att den har förmågan att adressera cyberfrågorna på djupet.[246] Andra underlag från Regeringskansliet visar att de vill höja kompetensen internt genom rekrytering och utbildning för att bland annat kunna vara mer proaktiva i formuleringen av positioner och policy.[247]

---

241 Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen med ansvar för digitalisering- och cyberfrågor 2022-05-19:1.

242 Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen med ansvar för digitalisering- och cyberfrågor 2022-03-31.

243 Regeringskansliet uppger i faktagranskningen att en sådan kartläggning aldrig genomfördes eftersom gruppens arbete de facto avlutades under hösten 2022. Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet,* 2023.

244 Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2020-06-12; Intervju Regeringskansliet 7.

245 Intervju Regeringskansliet 6; intervju MSB 1 och 2.

246 Minnesanteckningar från arbetsmaterial inför och anteckningar från mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2022-03-18.

247 Minnesanteckningar från arbetsmaterial inför och anteckningar från mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet– förslag till gemensamma åtgärder att driva. *PM om strategiska frågor* 2021-09-03.

5 Slutsatser och rekommendationer

Riksrevisionens övergripande slutsats är att regeringens arbete för att stärka Sveriges informations- och cybersäkerhet inte har varit effektivt. Regeringens strategi och implementeringen av den når inte upp till vad som anses vara internationell bästa praxis. Den centrala bristen är avsaknad av en strategisk avvägning och prioritering som riktar in arbetet. Det har också funnits svårigheter i att säkerställa en effektiv samordning och i att involvera relevanta intressenter. Bristerna har lett till en svag styrning från regeringens sida. Till del beror detta på att Regeringskansliets arbetsmetoder, organisering och resursanvändning inte har möjliggjort ett effektivt arbete med informations- och cybersäkerhetsfrågorna.

Sex år efter att informations- och cybersäkerhetsstrategin antogs kvarstår utmaningar inom strategins alla områden. Framsteg har gjorts hos en del aktörer, men det verkar inte ha skett någon generell förbättring av säkerheten. Trots lagändringar på området kvarstår problem med att utreda it-relaterade brott och att stötta vid incidenter. Bristen på kompetens i samhället kopplat till informations- och cybersäkerhet är fortsatt kritisk. En stor del av Regeringskansliets resurser går åt till att hantera initiativ från EU utan att Sverige driver någon sammanhållen linje på den nivån. Alla som ska inkluderas känner sig heller inte beaktade. Näringslivet upplever sig exempelvis sakna stöd från statens sida.

5.1 Det saknas en styrande strategisk inriktning

Enligt strategin skulle den utgöra en plattform för Sveriges fortsatta arbete, stötta aktörer i deras informations- och cybersäkerhetsarbete och skapa ett mer samlat agerande på området. Så som strategin är utformad fyller den enligt Riksrevisionen inte den funktionen. Granskningen visar att det inte är ett dokument som upplevs som centralt för myndigheterna som bedriver arbete på området. Den har heller inte styrt eller fyllt någon särskild funktion i regeringens styrning av myndigheterna. En strategi som inte pekar ut ansvar eller resurser innebär låg eller ingen styreffekt. Till skillnad från det tätt sammanlänkade digitaliseringsområdet där det finns en digitaliseringspolitik, saknas något sådant för informations- och cybersäkerhetsfrågorna. Departementen och myndigheterna som arbetar med frågorna har sina prioriteringar och mål, men det saknas en tydlig samlad sakpolitik för informations- och cybersäkerhet.

Regeringens styrning består därmed i mångt och mycket av minsta gemensamma nämnare bland de perspektiv som departementen lyfter fram. Samtidigt saknas en funktion och arbetsmetod på Regeringskansliet som kan värdera och rangordna

olika preferenser utifrån vad som gynnar Sverige som helhet och upptäcka viktiga frågor, områden eller aspekter som inte lyfts av departementen. Detta har försvårat en långsiktig, strategisk, holistisk och sammanhållen styrning.

Denna avsaknad gör det svårt att säkerställa att de insatser som görs är rätt insatser för Sveriges samlade informations- och cybersäkerhet, liksom att insatserna görs på rätt sätt. Det riskerar att leda till att de åtgärder som vidtas inte får effekt, men också till ett ineffektivt resursutnyttjande.

En förklaring till bristerna i strategin och dess implementering är Regeringskansliets organisation och arbetsmetoder. Regeringskansliet har förmåga att bereda ärenden. Baserat på Riksrevisionens iakttagelser rörande den departementsövergripande samordningen av strategiska informations- och cybersäkerhetsfrågor bedömer Riksrevisionen dock att en förklaring till bristerna är att det saknas tillräcklig operativ och taktisk kunskap om hur cybersäkerhetsarbetet bedrivs på myndigheterna och inom den privata sektorn såväl som specifik domänkunskap såsom internets funktionalitet, kryptokunskap, tekniska säkerhetslösningar och andra centrala komponenter inom cybersäkerhetsområdet. Utan egen kunskap i dessa frågor är risken stor att bedömningar kring vad som behöver ske avseende styrning och förmågehöjning blir felaktiga.

Bristen på kompetens och resurser, både inom det offentliga och det privata, har framförts i intervjuer och i skriftliga underlag. Med begränsade resurser borde det vara än viktigare att arbeta gemensamt för att nyttja resurserna väl.

5.2 Stuprör och otydligt ansvar hindrar arbetet

Både Regeringskansliet och myndigheterna arbetar till stor del i stuprör med sina respektive sakfrågor utan överblick över området i stort. Försök har gjorts att bygga hängrännor mellan stuprören både på Regeringskansliet och på myndighetsnivå. I Regeringskansliet har det funnits interdepartementala grupper på olika nivåer. Regeringskansliet uppger att det har ökat förståelsen mellan departementen och underlättat den gemensamma beredningen. Riksrevisionens bedömning är dock att det inte har lett till en ökad förmåga att prioritera insatser utifrån Sveriges samlade behov av informations- och cybersäkerhet eller till en långsiktig, strategisk, holistisk och sammanhållen styrning av informations- och cybersäkerhetsområdet.

De mer centrala myndigheterna har haft olika samarbeten under lång tid, främst inom Samfi, NSIT och numera NCSC. Trots att samarbete inte var nytt för myndigheterna som ingår i NCSC, har det tagit lång tid att bygga upp centret, och

mycket tid i den processen har gått till att lösa formella frågor kring formerna för samverkan. Erfarenheterna både inom Regeringskansliet och mellan myndigheterna visar enligt Riksrevisionens bedömning på svårigheterna med att nå en effektiv samverkan. Även samverkan med näringslivet har varit svår att få till. Samverkan med privata aktörer har funnits tidigare, men dessa har involverats i begränsad omfattning både i framtagandet av strategin och i uppbyggnaden av NCSC.

Till viss del har ansvaret för olika uppgifter varit otydligt. Det har framför allt gällt frågor som kräver insatser från flera olika aktörer eller frågor som inte tillhör någon aktörs huvudprioriteringar. Granskningen visar att detta exempelvis omfattat uppbyggnaden av NCSC. Vissa av centrets uppgifter har myndigheterna haft svårt att förstå, eller så har de tolkat dem olika. Otydligheten har lett till att uppgifterna tagit lång tid att genomföra eller prioriterats bort helt och hållet. Även koordineringen av internationella frågor är ett exempel där det inte alltid har funnits en huvudansvarig och resultaten har varit svaga. Samtidigt har styrningen av enskilda myndigheter i huvudsak vara tydlig. Strategin har inte pekat ut ansvar för att genomföra åtgärder inom de prioriterade områdena eller tilldelat resurser för arbetet. Finansiella resurser har tilldelats i vissa fall, men de flesta åtgärderna ska genomföras inom befintliga anslag. Cirka hälften av områdena i Enisas bästa praxis för att implementera en strategi har inte tilldelats några öronmärkta medel alls.

5.3 Regeringen har varit passiv i viktiga frågor

Enligt Riksrevisionen har regeringen inte agerat tillräckligt i flera centrala frågor. Den långsamma utvecklingen av NCSC visar exempelvis på en passivitet från regeringens sida. Inom Regeringskansliet identifierade man att arbetet med att inrätta NCSC inte var tillfredsställande och att det borde ha kommit längre. Det var först under första halvåret 2022 som ansvariga statsråd hade samtal med företrädare för berörda myndigheter gällande problematiken med utvecklingstakten. Denna passivitet har också funnits på andra områden. Exempelvis i förhållande till att ta fram en gemensam nationell modell för informations- och cybersäkerhet. Regeringen lyfte detta som en viktig fråga i den nationella informations- och cybersäkerhetsstrategin. Relevanta myndigheter har arbetat med frågan både inom ramen för Samfi och inom ramen för NCSC. När de inte har nått samsyn har regeringen inte gått in och vidtagit åtgärder för att föra arbetet framåt. Granskningen visar att vissa av de olika intressen som funnits hos myndigheterna också funnits på departementen. De har också värnat intressen inom sitt sakområde, vilket i vissa fall har hindrat progress på informations- och

cyberssäkerhetsområdet. Detta förklarar delvis regeringens passivitet även i frågor som har sagts vara prioriterade och viktiga. Riksrevisionens bedömning är att svagheten i styrningen har lett till att regeringens ambitioner inte har infriats.

5.4 Informationsutbytet har inte fungerat väl

Informationsutbyte är viktigt för att kunna samordna insatser så att alla arbetar mot samma mål och har en gemensam bild av läget, behov, mål och åtgärder som behövs för att komma dit. Både myndigheter, tjänstemän inom Regeringskansliet och företrädare för näringslivet har lyft att det till exempel saknas en gemensam lägesbild. Myndigheterna tar i dagsläget fram flera olika lägesbilder. Det ger en fragmenterad bild av området som inte tillgodoser behovet av överblick. Det försvårar enligt Riksrevisionen möjligheten att väga olika åtgärder mot varandra. Utbyte av information är behäftat med vissa legala, tekniska och kulturella utmaningar. Det är därför viktigt att myndigheterna och Regeringskansliet identifierar vilka utmaningar som finns och hittar strukturer för att hantera dem. Däremot bedöms inte begränsningarna i informationsdelning enbart ha med dessa utmaningar att göra. Vilja att värna sina egna sakfrågor och prioriteringar har sannolikt också påverkat. Ett sådant agerande riskerar att förstärka stuprören, men också att än mer försvåra möjligheterna att se till Sveriges behov som helhet. Granskningen visar att detta beteende har funnits både inom Regeringskansliet och mellan myndigheterna.

Informationsutbytet mellan det offentliga och näringslivet har inte heller fungerat fullt ut. Det handlar om att näringslivet inte upplever sig få tillräcklig information från det offentliga, men också om att företag uppfattar det som att myndigheterna inte är intresserade av att ta emot information från dem. Det riskerar att leda till att Regeringskansliet och myndigheterna inte får en bra lägesbild av de viktigaste riskerna och hoten mot Sverige i cybermiljön, en god förståelse för näringslivets behov eller vad företagen kan bidra med.

5.5 Rekommendationer

Riksrevisionen lämnar följande rekommendationer till regeringen:

- Skapa en strategisk, holistisk och långsiktig inriktning för arbetet med informations- och cybersäkerhet. Inriktningen bör omfatta en analys av de nationella strategiska utmaningarna, avvägningar och prioriteringar samt resurstilldelning och handlingsplan för genomförandet. Arbetet bör involvera berörda intressenter.

- Säkerställ en samlad styrning med tydlig ansvarsfördelning, tillräcklig kompetens och effektiva former för samordning av informations- och cybersäkerhetsfrågorna i Regeringskansliet.
- Identifiera hinder för informationsutbyte och se till att det finns strukturer som medger det informationsutbyte som är nödvändigt mellan myndigheter såväl som mellan det offentliga och det privata för att arbetet med samhällets informations- och cybersäkerhet ska fungera effektivt.
- Se över det nationella informations- och cybersäkerhetscentrets uppdrag, mandat och organisatoriska hemvist för att säkerställa dess bidrag till hela samhällets informationssäkerhet såväl som cybersäkerhet.

Referenslista

Litteratur, rapporter med mera

4c Strategies, ”Kompetensbristen inom cybersäkerhet – en nationell utmaning” https://www.4cstrategies.com/nordic/kompetensbristen-inom-cybersakerhet/, hämtad 2022-05-23.

Almega, *Tjänsteföretagen och Stärkt cybersäkerhet i Sverige*, 2022.

Bilaga till protokoll vid regeringssammanträde 2018-07-12 I:11.

Central Intelligence Agency (CIA), ”Producing Timely Tailored Finished Intelligence: Writing for the Consumer”, https://irp.fas.org/offdocs/dcid17m.htm, hämtad 2023-01-30.

Computer Sweden, ”Kritik mot regeringens utredning om it-säkerhet: För mycket myndighetsfokus”, https://computersweden.idg.se/2.33337/1.615935/kritik-mot-regeringens-utredning-om-it-sakerhet--for-mycket-myndighetsfokus, hämtad 2023-02-07, 2015.

Direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

Enisa, *An Evaluation Framework for National Cyber Security Strategies*, 2014. https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies.

Enisa, *NCSS Good Practice Guide. Designing and Implementing National Cyber Security Strategies*, 2016. https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

Europaparlamentet, ”Cybersäkerhet: vikten av att minska kostnaderna för cyberattacker”, https://www.europarl.europa.eu/news/sv/headlines/society/20211008STO14521/varfor-ar-cybersakerhet-viktigt-for-eu, hämtad 2022-06-08, 2021.

Franke, U, *Cybersäkerhet för en uppkopplad ekonomi*, Entreprenörskapsforum, 2020.

Försvarets radioanstalt, *Årsrapport 2022*, 2023.

Försvarets radioanstalt, *Årsrapport 2020*, 2021.

Försvarsmakten/Must, *Årsöversikt 2022,* 2023.

Försvarsmakten Försvarsmaktens faktagranskning av Riksrevisionens rapportutkast, 2023.

Gemensam beredning 2018-05-07 av regeringsbeslut om: Uppdrag att ta fram och genomföra en gemensam informations- och cybersäkerhetshandlingsplan för åren 2019–2022.

Handling från FRA till Fö/SUND daterad 2018-05-07.

Information Sharing and Analysis Organization Standards Organization, https://www.isao.org/.

Justitiedepartementet, Information till PM om vissa it-incidenter, PM från L4, riktad till chefsleden uppåt i Ju.

Klimburg, Alexander (red.), *National cyber security framework manual*, NATO Cooperative Cyber Defence Centre of Excellence, 2012.

Kungörelse (1974:152) om beslutad ny regeringsform.

Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Länsstyrelserna, ”Uppdrag till länsstyrelserna att redovisa regionala lägesbilder till Regeringskansliet” https://www.lansstyrelsen.se/stockholm/om-oss/pressrum/nyheter/nyheter---stockholm/2022-03-11-uppdrag-till-lansstyrelserna-att-redovisa-regionala-lagesbilder-till-regeringskansliet.html, hämtad 2023-02-07, 2022.

Motion till riksdagen 2021/22:3245 av Niels Paarup-Petersen m.fl. (C), Cybersäkerhet och cyberförsvar, Motion 2021/22:3639 av Pål Jonson m.fl. (M).

Myndigheten för samhällsskydd och beredskap, ”Aktuella EU-regleringar för informations- och cybersäkerhetsområdet”, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/eus-cyberregleringar/, hämtad 2023-04-09.

Myndigheten för samhällsskydd och beredskap, *Det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen*, publicerad i juni 2022.

Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6).

Myndigheten för samhällsskydd och beredskaps föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter (MSBFS 2020:7).

Myndigheten för samhällsskydd och beredskaps föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8).

Myndigheten för samhällsskydd och beredskap, ”Infosäkkollen”, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/systematiskt-informationssakerhetsarbete/infosakkollen, hämtad 2023-03-09.

Myndigheten för samhällsskydd och beredskap, ”It-incidentrapportering för statliga myndigheter”, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering-for-statliga-myndigheter, hämtad 2023-02-08.

Myndigheten för samhällsskydd och beredskap, ”Metodstöd för systematiskt informationssäkerhetsarbete”, https://www.informationssakerhet.se/siteassets/metodstod-for-lis/1.-om-metodstodet/vagledning-utforma-klassningsmodell_kommentarsperiod.pdf, hämtad 2023-03-29.

Myndigheten för samhällsskydd och beredskap, *MSB:s roll och ansvar inom NIS*, 2021.

Myndigheten för samhällsskydd och beredskap, *Nationell strategi för systematisk övningsverksamhet. För krisberedskap och civilt försvar*, 2020.

Myndigheten för samhällsskydd och beredskap, *När kriget kom nära: årsrapport it-incidentrapportering 2022*, 2023.

Myndigheten för samhällsskydd och beredskap, *Promemoria Initiativ på EU-nivå av relevans för säkerhet i Sverige och EU – fokus informations- och cybersäkerhet*, 2023-03-20.

Myndigheten för samhällsskydd och beredskap m.fl., *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*, redovisning mars 2022, 2022.

Oltsik, J, *The Life and Times of Cybersecurity Professionals 2020*, ESG, ISSA, 2020.

Post- och telestyrelsens föreskrifter och allmänna råd om säkerhetsåtgärder för samhällsviktiga tjänster inom sektorn digital infrastruktur (PTSFS 2021:3).

PwC, *Nordic Cyber Crime Survey 2020*, 2020.

Regeringsförklaringen 21 januari 2019.

Regeringskansliet, *Arbetsgrupper och andra osjälvständiga organ inom Regeringskansliet* SB PM 2021:02.

Regeringskansliet, *Promemoria 20230323 Svar på frågan från Riksrevisionen om faktagranskning av utkastet till granskningsrapporten Regeringens styrning av samhällets informations- och cybersäkerhet*, 2023.

Regeringskansliet Näringsdepartementet, *Statens ägarpolicy och principer för bolag med statligt ägande 2020*, 2020.

Regeringskansliet, Beredning av ärendet, https://www.regeringen.se/sa-styrs-sverige/sa-arbetar-regeringen-och-regeringskansliet/regeringsarende/beredning-av-arendet/, hämtad 2023-02-08.

Regeringskansliet, *Två nya departement startar upp*, https://www.regeringen.se/artiklar/2023/01/tva-nya-departement-startar-upp/, hämtad 2023-02-08, 2023.

Riksrevisionen, *Informationssäkerheten i den civila statsförvaltningen,* RiR 2014:23.

Riksrevisionen, *Internetrelaterade sexuella övergrepp mot barn – stora utmaningar för polis och åklagare,* RiR 2021:25.

Riksrevisionen, *It-relaterad brottslighet – polis och åklagare kan bli effektivare,* RiR 2015:21.

Riksrevisionen, *Livsmedels- och läkemedelsförsörjning: samhällets säkerhet och viktiga samhällsfunktioner,* RiR 2018:6.

Rumelt, Richard P., *Good strategy, bad strategy: the difference and why it matters*, Profile Books, 2011.

Rådslutsatser om EU:s samordnade insatser vid storskaliga cyberincidenter antogs juni 2018 (10086/18 Cyber 139).

Schwarz, Å, ”Kompetensbristen inom cybersäkerhet skenar”, https://blogg.knowit.se/cybersakerhet-och-juridik/kompetensbristen-inom-cybers%C3%A4kerhet-skenar, hämtad 2022-05-23, 2020.

SOFF, *Näringslivets syn på Sveriges kommande nationella cybersäkerhetscenter*, skrivelse till Regeringskansliet 20-04-23.

Statskontoret, *Regeringens styrning i tvärsektoriella frågor: en studie om erfarenheter och utvecklingsmöjligheter*, OOS 44, 2022.

Sundström, G, *Att tala med en röst: en studie av hur EU-medlemskapet påverkar samordningen inom regeringskansliet*, Stockholms centrum för forskning om offentlig sektor, Stockholms universitet, 1999.

Svenskt Näringsliv, *Företagen och it-säkerheten – hotbilder, motåtgärder och behov*, 2021.

Sveriges Riksbank, *Finansiell stabilitetsrapport 2021:2*, 2021.

Säkerhetspolisen, *Årsbok 2022,* 2023.

Wiktorin, Johan (red), *Cyberförsvaret – en introduktion*, Kungl. Krigsvetenskapsakademien, Stockholm, 2022.

Utredningar

Ds 2017:66 *Motståndskraft Inriktningen av totalförsvaret och utformningen av det civila försvaret 2021–2025.*

SOU 2005:71 *Informationssäkerhetspolitik: organisatoriska konsekvenser: slutbetänkande.*

SOU 2015:23 *Informations- och cybersäkerhet i Sverige – Strategi och åtgärder för säker information i staten.*

SOU 2016:57 *Säkerhet i ny tid: betänkande av utredningen om Sveriges försvars- och säkerhetspolitiska samarbeten.*

SOU 2017:75 *Datalagring - brottsbekämpning och personlig integritet.*

SOU 2017:89 *Hemlig dataavläsning - ett viktigt verktyg i kampen mot allvarlig brottslighet.*

SOU 2017:100 *Beslag och husrannsakan - ett regelverk för dagens behov.*

SOU 2021:63 *Sveriges säkerhet: behov av starkare skydd för nätverks- och informationssystem.*

Regeringsbeslut och regleringsbrev

Regeringens deklaration vid 2023 års utrikespolitiska debatt i riksdagen onsdagen den 15 februari 2023.

Regeringsbeslut Fi2017/03084/DF Uppdrag att föreslå en förvaltningsmodell för skyddade it-utrymmen

Regeringsbeslut Fi2017/03257/DF, *Uppdrag att erbjuda samordnad och säker statlig IT-drift.*

Regeringsbeslut Fi2022/01168, *Uppdrag att lämna förslag till ytterligare åtgärder som bedöms ändamålsenliga för att stärka den digitala motståndskraften i den finansiella sektorn.*

Regeringsbeslut Fö2019/01330, *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter.*

Regeringsbeslut I2019/01963/D, *Uppdrag att samverka kring kompetensförsörjningen av digital spetskompetens.*

Regeringsbeslut I2019/0414/D, *Uppdrag att ta fram ett förslag till riskanalys avseende nationell 5Ginfrastruktur i enlighet med Europeiska kommissionens rekommendation IT-säkerhet i 5G-nät.*

Regeringsbeslut I2020/01087/D, *Uppdrag att kartlägga hot och risker för elektroniska kommunikationsnät samt föreslå lämpliga åtgärder för att reducera riskerna.*

Regeringsbeslut Ju2016/05127, *Uppdrag till Myndigheten för samhällsskydd och beredskap och Polismyndigheten att fördjupa samverkan gällande inrapporterade och polisanmälda it-incidenter.*

Regeringsbeslut Ju2017/05786/L4, *Uppdrag att förbereda genomförandet av direktivet 2016/1148/EU om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.*

Regeringsbeslut Ju2017/05787/SSK, *Uppdrag till samtliga bevakningsansvariga myndigheter att analysera och bedöma informationssäkerheten i den egna verksamheten.*

Regeringsbeslut Ju2017/05788/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att bidra till ökad kunskap om informationssäkerheten hosbevakningsansvariga myndigheter.*

Regeringsbeslut Ju2017/05789/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att bidra till ökad kunskap och samverkan på informationssäkerhetsområdet.*

Regeringsbeslut Ju2018/01866/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att stärka allmänhetens samt små och medelstora företags motståndskraft mot it-incidenter.*

Regeringsbeslut Ju2018/02265/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att förbättra kommunernas informationssäkerhet i samarbete med länsstyrelserna.*

Regeringsbeslut Ju2018/03737/SSK, *Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022.*

Regeringsbeslut Ju2018/05292 (delvis), Ju2021/02005, *Uppdrag till Försvarsmakten och Säkerhetspolisen om kompetensförsörjningen inom säkerhetsskyddsområdet.*

Regeringsbeslut Ju2019/03057/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att genomföra riktade utbildningsinsatser på informationssäkerhetsområdet till offentlig sektor.*

Regeringsbeslut Ju2019/03058/SSK, Ju2019/02421/SSK, *Uppdrag till Myndigheten för samhällsskydd och beredskap att ta fram en struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen.*

Regeringsbeslut Ju2020/00378/PO, *Uppdrag till Polismyndigheten att vidta åtgärder rörande kompetensförsörjning och kompetensutveckling avseende bekämpning av it-relaterad brottslighet.*

Regeringsbeslut Ju2021/01245 *Uppdrag till Försvarsmakten och Säkerhetspolisen att vidta åtgärder inför etableringen av ett nytt tillsynssystem inom säkerhetsskyddsområdet.*

Regeringsbeslut Ju2021/03097, *Uppdrag till Myndigheten för samhällsskydd och beredskap att vidta förberedelser för att bli nationellt samordningscenter kopplat till det europeiska kompetenscentret för cybersäkerhet.*

Regeringsbeslut Ju2022/01292, *Uppdrag till MSB att genomföra en informationskampanj till allmänhet och företag om informations- och cybersäkerhet.*

Regeringsbeslut Ju2022/02042 *Uppdrag att föreslå utbildningar inom säkerhetsskyddsområdet*.

Regeringsbeslut Ju2022/02143, *Uppdrag till bevakningsansvariga myndigheter att lämna en sammanfattande redovisning av risk- och sårbarhetsanalyser*.

Regeringsbeslut Ju2022/02219, *Uppdrag till Myndigheten för samhällsskydd och beredskap att stärka funktionen CERT-SE samt utveckla och förenkla det stöd som lämnas inom informations- och cybersäkerhetsområdet*.

Regleringsbrev för Försvarets materielverk 2017–2022.

Regleringsbrev för Försvarets radioanstalt 2017–2022.

Regleringsbrev för Försvarshögskolan 2018 och 2019.

Regleringsbrev för Försvarsmakten 2017–2022.

Regleringsbrev för Myndigheten för samhällsskydd och beredskap 2017–2022.

Regleringsbrev för Polismyndigheten 2017–2022.

Regleringsbrev för Post- och telestyrelsen 2017–2022.

Regleringsbrev för Säkerhetspolisen 2017–2022.

Regleringsbrev för Upphandlingsmyndigheten 2018.

Regleringsbrev för Vetenskapsrådet 2021 och 2022.

Författningar med mera

Bet.1995/96:TU19, *Informationsteknikens användning*.

Bet. 2014/15:FöU11, *Försvarspolitisk inriktning – Sveriges försvar 2016–2020*, rskr. 2014/15:251.

Bet. 2017/18:FÖU4, *Nationell strategi för samhällets informations- och cybersäkerhet*.

Bet.2020/21:FiU1, *Statens budget för 2021*, rskr.2020/21:63.

Bet. 2020/21:FöU4, *Totalförsvaret 2021–2025*.

Förordning (1996:1515) med instruktion för Regeringskansliet.

Förordning (2007:854) med instruktion för Försvaret materielverk.

Förordning om ändring i förordningen (2007:937) med instruktion för Försvarets radioanstalt, SFS 2022:776.

Förordning (2007:951) med instruktion för Post- och telestyrelsen.

Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.

Förordning (2014:1103) med instruktion för Säkerhetspolisen.

Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Förordning (2022:524) om statliga myndigheters beredskap.

Prop. 2001/02:158 *Samhällets säkerhet och beredskap*.

Prop. 2014/15:109, *Försvarspolitisk inriktning: Sveriges försvar 2016–2020*.

Prop. 2016/17:1 *Budgetpropositionen för 2017*.

Prop. 2017/18:1 *Budgetpropositionen för 2018*.

Prop. 2018/19:1 *Budgetpropositionen för 2019*.

Prop. 2018/19:96 *Polisens tillgång till underrättelser från Försvarets radioanstalt*.

Prop 2019/20:1 *Budgetpropositionen för 2020*.

Prop 2020/21:1 *Budgetpropositionen för 2021*.

Prop 2021/22:1 *Budgetpropositionen för 2022*.

Skr. 2009/10:124 *Samhällets krisberedskap: stärkt samverkan för ökad säkerhet*.

Skr. 2016/17:213 *Nationell strategi för samhällets informations- och cybersäkerhet,* 2017.

Skr. 2016/17:213 *Uppdatering om genomförandet av Nationell strategi för samhällets informations- och cybersäkerhet Bilaga till Nationell strategi för samhällets informations- och cybersäkerhet, skr. 2016/17:213*, 2018.

Minnesanteckningar

Minnesanteckningar från möte i ida-gruppen för informationssäkerhetsfrågor 2018-01-26.

Minnesanteckningar från arbetsmaterial från statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet, *PPT Cyber/Digitalisering – Förslag, process arbetssätt* 2020-06-12.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2020-06-12.

Minnesanteckningar från arbetsmaterial inför möte i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2020-09-30.

Minnesanteckningar från arbetsmaterial inför och anteckningar från mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2020-11-03.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2020-12-18.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-02-18.

Minnesanteckningar från arbetsmaterial från möte i ida-gruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-04-23.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-05-25: 1 och 2.

Minnesanteckningar från arbetsmaterial inför och anteckningar från mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet– förslag till gemensamma åtgärder att driva *PM om strategiska frågor* 2021-09-03.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2021-09-15.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen med ansvar för digitalisering- och cyberfrågor 2022-03-31.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2022-03-18.

Minnesanteckningar från arbetsmaterial inför möte i statssekreterargruppen för digitalisering och cybersäkerhetsfrågor 2022-05-19:1 och 2.

Minnesanteckningar från arbetsmaterial inför mötet i statssekreterargruppen för strategiska frågor om digitalisering och cybersäkerhet 2022-08-26:1 och 2.

Minnesanteckningar från Regeringskansliets arbetsmaterial 1.

Minnesanteckningar från Regeringskansliets arbetsmaterial 2.

Minnesanteckningar från Regeringskansliets arbetsmaterial 3.

Intervjuer, e-post m.m.

E-post Regeringskansliet 1.

E-post Regeringskansliet 2.

E-post Regeringskansliet 3.

E-post Regeringskansliet 4.

Intervju Regeringskansliet 5.

Intervju Regeringskansliet 6.

Intervju Regeringskansliet 7.

Intervju Regeringskansliet 8.

Intervju Regeringskansliet 9.

Intervju Regeringskansliet 10.

Intervju Regeringskansliet 11.

Intervju C NCSC 1.

Intervju Försvarets radioanstalt 1.

Intervju Försvarets radioanstalt 2.

Intervju Försvarsmakten 1.

Intervju Försvarsmakten 2.

Intervju Försvarsmakten 3.

Intervju Försvarsmakten 4.

Intervju Försvarsmakten 5.

Intervju Försvarsmakten 6.

Intervju MSB 1.

Intervju MSB 2.

Intervju MSB 3.

Intervju MSB 4.

Intervju MSB 5.

Intervju Polismyndigheten 1.

Intervju Säkerhetspolisen 1.

Intervju Säkerhetspolisen 2.

Möte Försvarets radioanstalt 1.

Möte Regeringskansliet 1.

Möte Regeringskansliet 2.

Möte Säkerhetspolisen 1.

Möte Säkerhetspolisen 2.

Riksrevisionen har granskat om regeringens arbete för att stärka Sveriges informations- och cybersäkerhet har varit effektivt. Riksrevisionens övergripande slutsats är att regeringens arbete inom området inte har varit det. Den centrala bristen är avsaknad av strategiska avvägningar och prioriteringar som inriktar informations- och cybersäkerhetsarbetet.

Regeringen har inte heller tagit fram eller implementerat den nationella strategin för samhällets informations- och cybersäkerhet enligt internationell bästa praxis. Enligt Riksrevisionen saknar strategin en tydlig vision, uppföljningsbara målsättningar, ansvariga för att genomföra åtgärder och tilldelade resurser för arbetet. I avsaknad av en tydlig politik på området arbetar departementen och myndigheterna utifrån sina respektive mål och prioriteringar. Det gör det svårt att säkerställa att de insatser som görs är rätt insatser för Sveriges samlade informations- och cybersäkerhet, liksom att insatserna genomförs på ett effektivt sätt. Det riskerar att leda till att de åtgärder som vidtas inte får effekt, men också till ett ineffektivt resursutnyttjande.

Informationsutbyte är viktigt för att kunna arbeta mot samma mål och samordna insatser. Riksrevisionens bedömning är att utbyte av information, både inom det offentliga och mellan det offentliga och det privata, i nuläget inte fungerar effektivt.

Riksrevisionen

S:t Eriksgatan 117
Box 6181, 102 33 Stockholm
08-5171 40 00
www.riksrevisionen.se