Delat ansvar är ingens ansvar?

En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete

Mattias Svahn, Mathilde Jarlsbo,
Miranda Michélsen Forsgren, David Lindahl

FOI-R--5546--SE

Januari 2024

FOI

Mattias Svahn, Mathilde Jarlsbo,
Miranda Michélsen Forsgren, David Lindahl.

Delat ansvar är ingens ansvar?

En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete.

Titel	Delat ansvar är ingens ansvar? – En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete.
Title	From Everyone's Responsibility to No One's : An analysis of Swedish authorities' governance when protecting society against cyber threats
Rapportnr	FOI-R--5546--SE
Månad	Januari
Utgivningsår	2024
Antal sidor	70
ISSN	1650-1942
Uppdragsgivare	FOI
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr	A311021
Godkänd av	Emil Hjalmarsson
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover: FOI:s interna bild- och mediebank / Cyber Handshake

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Sverige, det svenska samhället och svensk förvaltning genomgår enligt många utredningar och analyser en digital transformation. Den påbörjades för ett trettiotal år sedan och accelererar fortfarande. Utvecklingen mot ett digitalt samhälle medför både innovationer och möjligheter likväl sårbarheter och risker. För att bemöta sårbarheterna och riskerna behöver det svenska samhället ett kontinuerligt pågående och väl styrt informations- och cybersäkerhetsarbete och då i synnerhet i statsförvaltningen.

Denna rapport utforskar fördelningen av ansvar för och styrning av svenska myndigheters informations- och cybersäkerhetsarbete i det digitala samhället, hur den fördelningen uppstått och om det finns någon problematik relaterat till den fördelning som finns.

Rapporten tar sin utgångspunkt i en litteraturgenomgång av forskningslitteratur, utredningar, regleringsbrev, lagtexter och andra offentligrättsliga dokument. Litteraturgenomgången kompletteras med intervjuer med fem centrala aktörer inom svensk cybersäkerhet.

Denna studie identifierar tre genomgående tendenser vilka samtliga speglar den svenska statsförvaltningens informations- och cybersäkerhetsarbete. Den första tendensen är otydlig ansvarsfördelning och styrning. Den andra tendensen är oklarheter i diskursens definitioner och den tredje tendensen är bristande återrapportering.

Rapportens resultat speglar aktuell samhällsvetenskaplig forskning i sin belysning av de problem kring ansvar för och styrning av cybersäkerhet i statsförvaltningen som studien uppmärksammar. Studien landar i att det finns en problematik med dagens styrning av cybersäkerhetsarbetet inom statsförvaltningen. Studien landar även i en försiktig optimism för kommande EU-harmonisering på området.

Rapporten avslutas med en lista med förslag på framtida forskning. Dessa förslag är förankrade i problembilden som denna rapport redogör för.

Nyckelord: digitalisering, informations- och cybersäkerhet, ansvar, delegering, styrning, lagstiftning

Summary

Sweden, Swedish society and Swedish administration are undergoing a digital transformation. It started some thirty years ago and is still accelerating. The development towards a digital society brings both innovations and opportunities as well as vulnerabilities and risks. In order to respond to these vulnerabilities and risks, Swedish society needs good cyber security work, especially in the authorities.

This report explores the distribution of responsibility for, and control of, Swedish public authorities' cyber security work in the digital society, how the distribution came to be, and what problems arise out of that distribution.

The report takes its starting point in a review of research literature, investigations and other public law documents. The literature review is supplemented by interviews with five central players in Swedish cyber security.

This study identifies three consistent themes, which influence the cyber security work of Swedish authorities. The first the unclear division of responsibilities and governance. The second theme is ambiguities in the definitions of the discourse and the third theme is a lack of feedback.

The study identifies that there are problems with the current governance of cyber security work within the state administration, but also finds a careful optimism regarding future EU harmonisation in the area.

The report's results reflect current social science research in its illumination of problems surrounding responsibility for, and governance of, cyber security in the state administration.

The report concludes with a list of suggestions for future research. These proposals emanate out of the problems this report describes.

Keywords: digitalization, cyber security, responsibilities and governance.

Innehållsförteckning

1 Inledning

I en rapport från Digitaliseringsmyndigheten från 2022 beskrivs hur en relativt stor del av den svenska befolkningen saknar grundläggande digital kompetens och att företag och myndigheter upplever stora svårigheter i att hitta och rekrytera den IT-kompetens som efterfrågas. Enligt rapporten är den offentliga förvaltningen ojämn i leveransen av offentlig digital service samtidigt som behovet av trygghet och säkerhet i det digitala samhället ökat.[1] Riksrevisionen menar i en rapport från 2023 att ansvaret för att hantera informations- och cybersäkerhetsarbetet i Sverige är splittrat, både inom Regeringskansliet och mellan myndigheterna.[2]

Båda rapporterna och även denna rapport handlar om det moderna samhället och vad det innebär att det i så stor utsträckning vilar på datorgenererade och datorburna tjänster, sådant som brukar betecknas med prefixet *cyber*. Prefixet cyber har ingen fastslagen definition i den undersökta litteraturen utan används allmänt med en vag innebörd. Prefixet används också i en specialiserad betydelse i kontexter där en ömsesidig förståelse råder om dess betydelse. I takt med digitaliseringens framfart i det svenska samhället, och västvärlden i stort, har användningen av prefixet cyber i varierande sammansättningar blivit allt mer frekvent. I diskursen om totalförsvar och det digitaliserade samhället används prefixet rikligt.

Ett annat centralt begrepp i denna studie är *delegering* av ansvar och uppdrag. Med det menas i rapporten en överföring av både beslutsrätt och åtaganden från en hierarkiskt överordnad part till en hierarkiskt underordnad part, där den mottagande parten åtar sig ansvar och uppgifter i den överordnades ställe. I den bästa av världar får den mottagande parten tillräckligt mandat och styrning för att kunna axla ansvaret. Delegering kan synas vara en enkel tanke men bär i praktiken en del komplexitet. Studier i bland annat systemteori visar att det i en komplex värld krävs ett decentraliserat och delegerat beslutfattande för att styrning ska kunna fungera.[3] Andra studier visar dock att även om en komplex omvärld kräver decentraliserat beslutfattande kan en omfattande decentralisering istället leda till mer komplexitet.[4] För att omfattande decentralisering av ansvar ska fungera framgångsrikt visar studier att delegeringen bör motsvaras av tydliga instruktioner till,

[1] Myndigheten för digital förvaltning. *Digitala Sverige 2022 En samlad analys av samhällets digitalisering.* Stockholm, 2023.
[2] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. RiR 2023:8. Stockholm, 2023.
[3] Alexander. F Siegenfeld & Yaneer Bar-Yam. *An introduction to complex systems science and its applications.* Complexity, 2020, s. 1-16.
[4] Shirin Ahlbäck Öberg, S. A., & & Helena Wockelberg, H. A*gency control or autonomy? Government steering of Swedish government agencies 2003–2017*. International Public Management Journal, 24(3), 330-349. 2021.

och tydligt specificerad kapacitet, hos mottagaren.[5] Det krävs med andra ord en god balans mellan delegering och styrning för att ta ansvar i ett komplext samhälle.

I Sverige utgår all makt från folket enligt 1 kap 1 § Regeringsformen och därefter delegerar folket makten och även det tillhörande ansvaret till riksdagen. Riksdagen i sin tur delegerar makt och ansvar till regeringen, som delegerar till statliga myndigheter. I fråga om myndigheter och ansvar är det värt att påminna om att svenska myndigheter ska följa regleringar från regeringen och även EU-regleringar, Europakonventionen och annan internationell rätt. Myndigheterna är dock självständiga i förhållande till svenska regeringen ifråga om enskilda beslut som fattas i utförandet av myndighetens uppgifter.

Statsförvaltningen är med dess myndigheter regeringens viktigaste instrument för att styra riket. Det är regeringens uppgift att ange mål för den statliga verksamheten och med olika medel styra sin förvaltning. Uttryckliga regler om hur denna styrning ska gå till saknas dock i Regeringsformen (RF). De styrmedel som regeringen har att tillgå kan i de flesta fall härledas från grundlagsreglerna om normgivningsmakt (8 kap. RF), finansmakt (9 kap. RF), utnämningsmakt (12 kap. RF) och kontrollmakt (13 kap. RF). Myndigheternas roll i det statliga förvaltningssystemet regleras i viss utsträckning i RF. Enligt 1 kap. 6 § RF är det regeringen som styr riket och enligt 12 kap. 1 § RF lyder de statliga förvaltningsmyndigheterna under regeringen. Dessa förvaltningsmyndigheters uppgift är att bland annat verkställa den politik som lagts fast. Det är regeringen som kollektivt utövar denna bestämmanderätt över myndigheterna (7 kap. 3 § RF), vilket utgör grunden till att Sverige sägs sakna så kallat ministerstyre. Sammanfattningsvis styr regeringen riket genom förvaltningen som därför har lydnadsplikt, men är självständig i de löpande myndighetsbeslut som ska fattas. Den enskilda beslutshandläggaren och ytterst myndigheternas högsta chef är de ansvariga parterna, snarare än den ämnesansvariga ministern.

Den konstituerande ramen för myndigheter och deras verksamheter anges i varje enskilt fall i myndighetsinstruktionen, regleringsbrev och andra föreskrifter samt särskilda regeringsbeslut. Utöver dessa finns även de tre svenska förvaltningsrättsliga grundprinciperna. Enligt ansvarsprincipen är det den som har ansvar för en verksamhet under normala förhållanden som ska ha det också under en krissituation. Likhetsprincipen fastslår att under en kris ska verksamheten fungera på i mesta möjliga mån liknande sätt som vid normala förhållanden. Enligt närhetsprincipen ska en kris hanteras där den inträffar och av dem som är närmast berörda och ansvariga. Dessa statsrättsliga och övergripande principer ska gälla i vardagen liksom vid alla former av kriser, inklusive en cybersäkerhetskris.[6] Myndigheterna

[5] Sjors Overman, S. *Great Expectations of* public service delegation*: A systematic review*. 2016 s. 1238-1262.

[6] Myndigheten för samhällsskydd och beredskap (MSB). *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. Stockholm, 2018, s. 24-26.

har befogenheter att självständigt och utan regeringens eller riksdagens ingripande hantera sitt vardagliga arbete.

1.1 Rapportens struktur

Föreliggande rapport har sex kapitel och två bilagor.

Det första kapitlet tar upp inledning, syfte, frågeställningar och metod. Det andra kapitlet redogör för en serie perspektiv och infallsvinklar som formar bakgrunden till rapportens arbetsområde. Det tredje kapitlet tar upp slutsatser och resultat ur litteraturgenomgången utifrån tre identifierade tendenser. I det fjärde kapitlet nyanseras de redovisade tendenserna utifrån det framtagna resultatet från intervjuerna. Det femte kapitlet redogör för samlade slutsatser från föregående kapitel. I det avslutande sjätte kapitlet ges förslag på framtida forskning.

Den första bilagan är en lista över centrala begrepp. En större litteraturgenomgång om svenska myndigheter och myndighetsorgans arbete med styrning av cybersäkerhet under åren 1990–2024 redogörs för i bilaga två. Den andra bilagan bör ses som en mer omfattande historisk redogörelse för hur arbetet med informations- och cybersäkerhetsarbete hamnat där det är idag.

1.2 Syfte och frågeställning

Rapporten syftar till att identifiera fördelningen av ansvar och styrning för den svenska statsförvaltningens informations- och cybersäkerhetsarbete i det digitala samhället. Vidare undersöker studien hur fördelningen uppstått och om det finns någon problematik relaterat till denna fördelning.

Forskningsfrågorna har formulerats enligt följande:

a) Hur ser fördelning av ansvar och styrning ut för informations- och cybersäkerhetsarbete i det svenska digitala samhället i den svenska statsförvaltningen?
b) Hur har denna fördelning uppstått?
c) Finns det någon problematik relaterat till hur fördelningen ser ut?

Denna rapport besvarar frågeställningarna genom att kombinera en litteraturgenomgång på området med en intervjustudie. Ett sådant tillvägagångssätt kombinerar resultaten från två olika datainsamlings- och analysmetoder.

Rapporten är ett internt initiativ inom FOI och den tilltänkta målgruppen är personer med ansvar för, delaktighet i och intresse för hur svensk informations- och cybersäkerhet är organiserad och hur den samverkar med totalförsvarsdomänen. Målgruppen inkluderar därmed spannet från politiker på riksnivå till enskilda beslutsfattare och projektledare på myndighets- och verksamhetsnivå. Avsikten är att det inte ska krävas någon djupare teknisk förståelse om IT-system, cybersäkerhet eller juridik för att läsa rapporten.

1.3 Metod

Studiens iakttagelser är baserade på två metoder för datainsamling med tillhörande analys: en litteratur- och dokumentstudie i kombination med djupintervjuer. Genom att använda två olika metoder för att undersöka samma frågeställning önskar denna studie skapa goda förutsättningar för en mer mångsidig belysning av studiens forskningsområde.[78]

Arbetet inleddes med en första litteraturgenomgång av forskningslitteratur och myndighetsrapporter på ämnet cybersäkerhetsarbete hos svenska myndigheter. Detta för att rama in och lägga grund för arbetsområdet. Därefter fortsatte litteraturstudien i en andra runda med att söka offentliga myndighetsdokument hämtade från Regeringskansliets samling av rättsliga dokument för digitaliseringspolitik. [9] Utifrån de där funna dokumenten initierades sedan ett så kallat snöbollsförfarande i en tredje runda, för att finna mer underlag som kunde befinnas relevant. Även dessa har lästs och analyserats så att underlaget metaforiskt uttryckt växer som en snöboll som rullas i snön.[10] Läsningen har fokuserat på frågor om ansvar, styrning och mandat. Dokument, forskningslitteratur och forskningsrapporter av teknologisk och företagsekonomisk karaktär har inte ingått i litteraturen.

Analysarbetet av litteraturen skedde genom kodning där relevanta delar kodades och grupperades. Ur detta observerades initiala tendenser, se kapitel 3. Dessa initiala tendenser togs sedan med in i djupintervjuerna som en del av underlaget för utformningen av intervjufrågor.

Djupintervjuer är en intervjumetod som tillåter fritt samtal mellan intervjuare och intervjuperson där diskussionstrådar som inte var underlag vid intervjuns inledning kan uppstå.[11] Djupintervjuer är en metod som är lämplig för att undersöka erfarenheter, upplevelser och attityder.[12] Denna metod valdes i syfte att täcka upp perspektiv som textläsningen inte gett, främst samspelet mellan skrivna perspektiv och praktiska livserfarenheter. Intervjuerna genomfördes under augusti till och med oktober 2023. Urvalet av intervjupersoner genomfördes i åtanke att finna representanter från olika ansvarsområden, från nationella (Regeringskansliet) till mer lokala (myndigheter) inom den svenska statsförvaltningen. Med hänsyn till att

[7] Amanda Barusch, Christina, Gringeri, & Molly George. *Rigor in Qualitative Social Work Research: A Review of Strategies Used in Published Articles*, Social Work Research, Volume 35, Issue 1. 2011, s. 11-19,

[8] Donna Adkins, Chauvin, Sheila. & Johnson, Jessica. L., *A review of the quality indicators of rigor in qualitative research*. American journal of pharmaceutical education. 2020, *84*(1).

[9] Regeringskansliet. Rättsliga dokument. December 2023.

[10] Changing Minds.com. *Snowball sampling*. 2023

[11] Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). *The Sage handbook of qualitative research*. Sage. Kap 15 & Kap 42

[12] Bryman. *Samhällsvetenskapliga metoder*, s. 213.

denna studie är avgränsad till att studera den svenska statsförvaltningen så är den privata sektorn inte inkluderad.

Djupintervjuerna genomfördes antingen på plats på deltagarnas arbetsplatser eller via Skype. Inledningsvis fick intervjupersonerna en muntlig presentation av studiens syfte och en förfrågan om att få spela in intervjun. Samtliga intervjupersoner accepterade inspelning. De inspelade intervjuerna transkriberades ordagrant med hjälp av ett externt. De transkriberade intervjuerna lästes och relevanta avsnitt markerades för att sedan kodas och grupperas utifrån de tendenser som identifierades i litteraturgenomgången. Läsning, kodning och gruppering skedde i flera omgångar i syfte att nå fram till kärnan i materialet.

Intervjupersonerna var:

- En representant för Myndigheten för Digital Förvaltning,
- En representant för Post- och telestyrelsen,
- Två representanter för Regeringskansliet, och
- En representant för Myndigheten för Samhällsskydd och Beredskap.

2 Bakgrund

2.1 Prefixet cyber

Det är väl känt i kommunikations- och diskursteori att båda sidor i en diskussion behöver ha samma uppfattning om ett nyckelbegrepps innebörd för att en diskussion ska kunna ske med klarhet.[13] Denna rapport presenterar därför här en kortare genomgång av prefixet *cyber*. Prefixet kan härledas till det grekiska ordet *kubernetes* som syftar till en pilot eller styrman och är nära besläktat med det också grekiska ordet *kubernesis* som betyder förmåga att styra och ledarskapets konst.[14] Det franska ordet *cybernétique* användes 1834 av fysikern André-Marie Ampère[15] som en beteckning för studiet av styr- och reglersystem. I slutet av 1940-talet myntade matematikern Norbert Wiener begreppet cybernetik.[16] År 1956 publicerade William Ashby Ross, ”A*n Introduction to Cybernetics”*[17] där cybernetik läggs fram som ett nytt ämne i relation till den tidens arbete inom informationsteori, kommunikationsteori, kontrollteori, spelteori och systemteori. Mellan 1982 och 1984 var den skönlitterära författaren William Gibson en av de första att skriva om cyberspace som beskrivs som en datorgenererad hallucination genom visualisering av data från det globala nätverket av all världens datorer.[18] I en FOI-rapport från 2023 analyseras förekomsten av cyberkrig i Ukraina och lägger fram att analytiker och forskare förlitar sig på begreppsmässigt olika uppfattningar av prefixet cyber när de klassificerar fientliga cyberaktiviteter, cyberkampanjer, cyberoperationer och cyberattacker.[19]

Det kan framstå som om prefixet cyber är ett sociologiskt överenskommet begrepp utan någon direkt definition och som därmed inte kan ge den ömsesidiga klarhet som beskrivs i kommunikations- och diskursteori. Föreliggande rapport definierar cyber som ett prefix som i sammansättningar står för *datorgenererad*.

[13] Zachary Sapienza. Aaron S. Veenstra, Kestas Kirtiklis & Steve S Giannino. *The transmission model of communication: Toward a multidisciplinary explication*. ETC: A Review of General Semantics, *73* (4). 2016 s. 321-341.

[14] Melissa Parsons. *The Humanity and Evolution of Cyber*. 2021

[15] Andre-Marie, Ampere. *Ampère et l'histoire de l'électricité.* 1865.

[16] Norbert Wiener. *Cybernetics, or control and communication in the animal and the machine* (2nd ed.). John Wiley & Sons, Inc.; Boston Review. 1961.

[17] William Ross Ashby, *An Introduction to Cybernetics*. London: Chapman & Hall. 1956. Ltd. ISBN 9781614277651.

[18] Jennifer Bussell. C*yberspace*. Encyclopedia Britannica: 2023.

[19] Per-Erik Nilsson. *Unraveling the Myth of Cyberwar - Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War 2014-2023*. FOI-R—5513–SE [i tryck]. 2023, s.13

2.2 Det digitala samhället

Det är i det nutida digitaliserade samhällets natur att vara uppkopplat och sammankopplat, såväl mellan svenska offentliga parter och privata företag som mot utlandet. Det digitala samhället för med sig effektivitet, bekvämlighet, välstånd och innovation men även nya sårbarheter, utmaningar och hot. Olika digitala tjänster i Sverige är i stor utsträckning sammankopplade och beroende av varandra.[20]

Så tidigt som 1998 skrev regeringen att utgångspunkten var att all information, som företag och individer behövde få från myndigheter, skulle vara tillgänglig elektroniskt.[21] Sedan dess har det funnits många uppmaningar att främja digitaliseringen i Sveriges myndigheter. I IT-propositionen (1999/00:86) ansågs Sverige vara en av de ledande IT-nationerna i världen och dåvarande regering införde målet att Sverige skulle bli det första landet som gjorde informationssamhället tillgängligt för alla.[22] Det digitaliserade samhället har drivits fram på grund av en önskan om effektivisering och ambitionen av att få ut mer ur tillgängliga resurser. IT-revolutionen från 1990-talet och framåt har till viss del erbjudit detta, inte minst inom offentlig förvaltning. Det har länge funnits en retorik där ordet digitalisering i praktiken fungerar som en synonym för det nya, moderna, smarta, effektiva och framtida.[23]

Ett exempel på hur det svenska samhället i mycket snabb takt digitaliserats och blivit mer uppkopplat är betalningsmarknaden. Tillsammans med sina grannländer i Norden är Sverige ett av de mest digitaliserade länderna i världen vad gäller betalning. Fysiska betalningssätt (sedlar och mynt) har minskat drastiskt till följd av förändrade konsumtionsmönster, konkurrensfrämjande regleringar och ny digital teknik. Idag har ett företag eller en enskild person flera olika leverantörer av betaltjänster som är sammankopplade med varandra och kan användas i olika betalningssituationer. Den digitala betalningsmarknaden har vuxit fram eftersom konsumenter, såväl företag som organisationer och privatpersoner, efterfrågar sömlösa, integrerade och snabba betalningar. Betalningar är en central del för ett fungerande samhälle och dess motståndskraft vid höjd beredskap (ytterst krig) eller fredstida krissituationer. Betalningsmarknadens beredskap är helt enkelt av stor betydelse för totalförsvaret där ett flertal funktioner, såsom utbetalning av löner, utbyte av varor och tjänster måste fungera. När dessa eller andra centrala

[20] Myndigheten för digital förvaltning. *Digitala Sverige 2022 En samlad analys av samhällets digitalisering.* Stockholm, 2023.
[21] Statskontoret. *Sammanhållen strategi för samhällets IT-säkerhet* 1998:18. Stockholm, 1998.
[22] Näringsdepartementet. *IT-propositionen (1999/00:86).- Ett informationssamhälle för alla*. Stockholm, 1999.
[23] Jenny Ingemarsdotter, Daniel Eidenskog & Vidar Hedtjärn Swaling. *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur.* Totalförsvarets forskningsinstitut 2020

digitala tjänster i en krissituation inte fungerar utgör de en sårbarhet och en grund för osäkerhet för den enskilde individen och totalförsvaret i stort.[24] [25]

Det digitala samhället med dess möjligheter och sårbarheter handlar inte bara om information utan även om funktion. Den industriella infrastruktur som samhällets kritiska tjänster är beroende av har systematiskt datoriserats under årtionden. Mindre omskrivet men minst lika viktiga är de digitala system som styr exempelvis järnvägsövergångar, trafikljus och reningsverk som också är en del av det digitala samhället. Tidigare rapporter från FOI har bland annat tagit upp hur automatisering och datorisering av vatten och avlopp (VA) och elkraft kan öppna upp för cyberattacker där redan korta avbrott i el och VA kan påverka samhällsfunktioner.[26] Vidare har FOI tagit upp att digitaliseringen av sjukvårdstekniska produkter kan öppna för cyberattacker som kan äventyra patientsäkerheten som en del av totalförsvaret,[27] och att framväxten av cyberfysiska system i svenska hamnar ökar risker för cyberattacker på transportlogistiken.[28] Under 2023 upptäckte myndigheter i Nederländerna vid ett test av nio olika typer av växelriktare[29] i solpaneler att alla de nio testade låg öppna för en antagonistisk part att använda för att skapa störningar i elnätet. Dessa nio modeller av växelriktare i solpaneler finns även i Sverige.[30]

Detta uppkopplade och sammankopplade samhälle kommer vidare att benämnas som det digitaliserade samhället. I det digitaliserade samhället är både det som kallas för cybersäkerhet och det som kallas för informationssäkerhet viktiga företeelser. Föreliggande rapport nöjer sig med att definiera informationssäkerhet och cybersäkerhet som två närbesläktade men olika begrepp. Informationssäkerhet fokuserar på informationen (oavsett hur den hanteras och lagras) medan cybersäkerhet fokuserar på skyddet av datorgenererade system och dess innehåll (se vidare redogörelse i avsnitt 3.2 samt rapportens definitioner i bilaga 1).

2.3 Totalförsvar

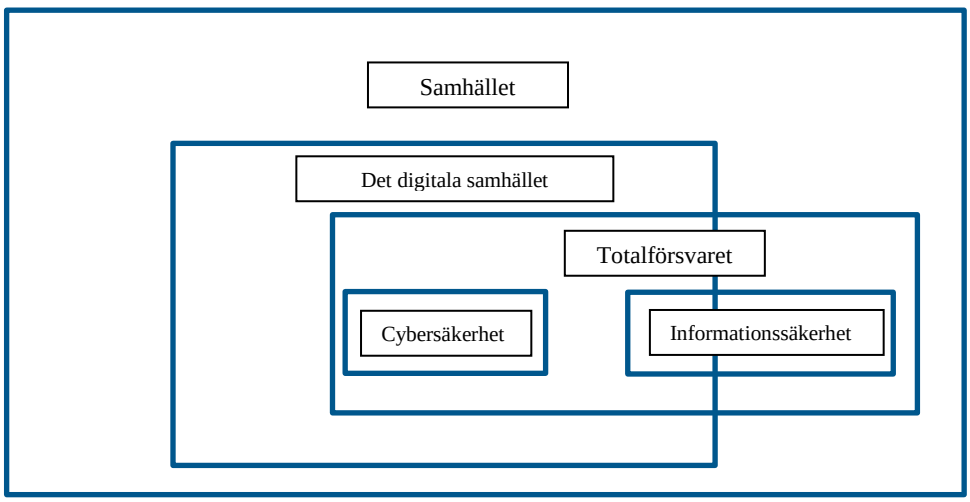
Idag utformas det svenska totalförsvaret på nytt med målsättningen att vara dimensionerat och utformat för att möta ett väpnat angrep mot Sverige. Genom krigsavhållande verksamheter ämnar totalförsvaret bygga upp ett uthålligt och beslutsamt

[24] Anna Kinberg Batra. *Staten och betalningarna*. SOU 2023:16. Stockholm 2023.
[25] Myndigheten för samhällsskydd och beredskap. *Betalningar och kontanter i kris.* 2023
[26] Annica Waleij, Louise Simonsson & Birgitta Liljedahl. *Konsekvenser av energibortfall på samhällets funktionalitet och civilbefolkningens hälsa.* Totalförsvarets forskningsinstitut 2019. FOI-R--4755--SE
[27] Eidenskog et. al. *Digitaliseringens risker i hälso- och sjukvård.* 2023.
[28] Mari Olsén, Christian Valassi & Ann-Sofie Stenérus Dover. *NCS3 – Ett skepp kommer lastat En kartläggning av informationsflöden, cyberfysiska system och aktörer inom svenska hamnar*. Totalförsvarets forskningsinstitut, 2023. FOI-R--5405--SE
[29] En växelriktare är en apparat som hanterar den el solpaneler levererar.
[30] Andreas Liljeheden. *Nederländerna varnar för solcellsanläggningar – risk även i Sverige*. Sveriges Radio. 2023.

motstånd. Inte minst gäller detta landets cybersäkerhetsförmåga som behöver stärkas genom att skapa förmågor till offensiva och defensiva operationer och systematiskt informations- och cybersäkerhetsarbete hos totalförsvarets aktörer.[31] Enligt lag (1992:1403) 1 § om totalförsvar och höjd beredskap definieras totalförsvar enligt följande:

> ”Totalförsvar är verksamhet som behövs för att förbereda Sverige för krig.”

Det är en kort och kärnfull definition där utgångspunkten är att totalförsvaret är all verksamhet (*civil eller militär*) som behövs för att förbereda och försvara Sverige i krig. Det övergripande målet för totalförsvaret är att försvara Sverige mot väpnat angrepp, värna om landets säkerhet, självständighet, frihet och handlingsfrihet.[32] Det innebär att det digitala samhällets styrkor såväl som sårbarheter blir av betydelse för totalförsvaret. I figur 1 framgår det hur cybersäkerhet, informationssäkerhet, totalförsvaret och det digitala samhället förhåller sig till varandra i samhället. Sedan 2022 finns förordning (2022:524) om statliga myndigheters beredskap i vilken det framgår vilka som valts ut som beredskapsmyndigheter. Dessa myndigheter anses ha ett särskilt ansvar inom en eller flera viktiga samhällsfunktioner. De bedöms även bedriva en verksamhet som har särskild betydelse för totalförsvarets och samhällets beredskap, inför och vid krig.



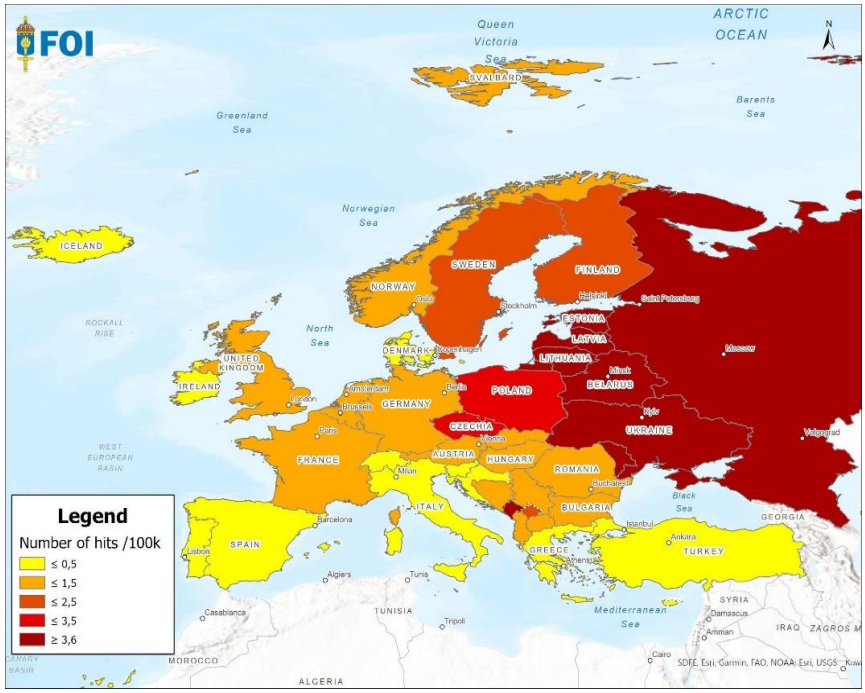
Figur 1, visar hur samhället består av bland annat det digitala samhället, vilket totalförsvaret bland annat ämnar försvara och där cybersäkerhet är en del av detta försvar. I bilden framgår det att totalförsvaret även önskar försvara andra delar än det digitala samhället, att cybersäkerhet är en del av det digitala samhället och att informationssäkerhet inte bara är en del av det digitala samhället utan även existerar utanför det digitala.

[31] Försvarsdepartementet. Prop. 2020/21:30 *Totalförsvaret 2021-2025 Sammanfattning av propositionen Totalförsvaret 2021–2025* Stockholm, 2020.
[32] Ibid. s. 86.

2.4 Hotbilden mot det digitala samhället

FRA konstaterar i en rapport från 2022 att Sverige är ett mål för andra länders underrättelseverksamhet och cyberangrepp.[33] I en separat rapport från Nationellt Cybersäkerhetscentrum (NCSC), utgiven av Försvarets radioanstalt (FRA), konstateras att Sverige utsätts för mångfacetterade cyberhot som kan kopplas till olika hotaktörer, i huvudsak statliga aktörer och kriminella.[34] Varje dag utsätts landet för säkerhetshotande aktioner i form av bland annat påverkansoperationer, underrättelseverksamhet och inte minst cyberangrepp. Hotet från främmande makt är fortsatt högt. Säkerhetspolisen (Säpo) skriver i sin årsrapport från 2022/2023 att de ser en förändrad hotbild där Sverige är en arena för en större konflikt,[35] inte minst i den digitala sfären med olika former av cyberattacker och hot mot informationssäkerheten i det digitaliserade samhället. Baserat på data från East Stratcom Taskforce har Svenonius och Serveta (2022) tagit fram figur 2 där det påvisas att Sverige och Finland är mer utsatta för desinformation från Ryssland i den internationella informationsmiljön än Danmark och Norge.[36]

[33] Försvarets radioanstalt. *Årsrapport 2022*. Stockholm, 2022.
[34] Försvarets radioanstalt. *Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden.* Stockholm, 2022.
[35] Säkerhetspolisen. *Årsrapport för 2022*. Stockholm, 2023 s. 28-40
[36] Ola Svenonius; & Marianna Serveta forskare på FOI *Privat Kommunikation 2023*.



Figur 2 visar på försök till desinformation från Ryssland i medier. Den visar att Sverige är mindre utsatt än Estland, Lettland och Litauen, på samma nivå som Finland, mer utsatt än Norge, och mycket mer än Danmark (Svenonius och Serveta 2022).

3 Ansvar för svensk cybersäkerhet (1990–2023)

I detta kapitel berörs tre tendenser som härrör ur litteraturgenomgången (se Bilaga 2). De identifierade tendenserna lade grunden för utformandet av djupintervjuerna och den diskussion som redovisas i kapitel 4.

3.1 Ansvarsfördelning och styrning

En av de tydligaste tendenserna som urskiljs i litteraturgenomgången är att inom myndigheter under regeringen har ansvarsfördelningen och styrningen av informations- och cybersäkerhetsarbete varit otydlig. Att informations- och cybersäkerhetsarbetet är en fråga av tvärsektoriell karaktär som kräver en sammanhållen styrning har påpekats sedan 1990-talet.[37] Idag är ansvaret fördelat utifrån ansvarsområden mellan olika departement och myndigheter där Justitiedepartementet och Försvarsdepartementet är mest centrala. Enligt Riksrevisionens granskning från 2023 saknas en bindande funktion mellan departementen som garanterar en holistisk styrning av området.[38] Det förekommer dock interdepartementala grupper på olika nivåer som diskuterar frågor kring informations- och cybersäkerhetsarbetet.[39] Vad gäller myndigheternas ansvar för informations- och cybersäkerhetsarbetet är de mest centrala myndigheterna Säkerhetspolisen (Säpo), Försvarsmakten, Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Försvarets materielverk (FMV), Myndigheten för samhällsskydd och beredskap (MSB) samt Polismyndigheten. Ingen av dessa har dock något övergripande ansvar. Myndigheterna styrs av tre olika departement vilka arbetar mot olika övergripande målsättningar inom sina olika politikområden. Det uppstår därmed en risk att myndigheternas och regeringens åtgärder inte är sammanhängande.[40] I detta avsnitt följer några utvalda exempel från bilaga 2 som illustrerar denna tendens i fråga om ansvarsfördelning för och styrning av det svenska informations- och cybersäkerhetsarbetet.

I strategin med tillhörande ansvarsprincip som regeringen presenterade i proposition 2001/02:158, *Samhällets säkerhet och beredskap* framgår det att ansvaret för informationssäkerheten i respektive verksamhet ska ligga hos alla de företag,

[37] Se exempelvis bet.1995/96:TU19, SOU 2001:41, SOU 2005:71 eller SOU 2015:23.
[38] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. RiR 2023:8. Stockholm, 2023.
[39] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. RiR 2023:8. Stockholm, 2023.
[40] Statskontoret Regeringens styrning i tvärsektoriella frågor - En studie om erfarenheter och utvecklingsmöjligheter, 2022, s. 11f.

myndigheter och organisationer som har det normala dagliga verksamhetsansvaret.

År 2003 grundandes *Samverkansgruppen för informationssäkerhet* (SAMFI) av dåvarande Krisberedskapsmyndigheten (KBM), på uppdrag av regeringen. Gruppen bestod av KBM/MSB, PTS, Polisen, FRA, SÄPO, FMV, Sveriges Certifieringsorgan för IT-säkerhet (CSEC) och Försvarsmakten. Under efterföljande år beslutade regeringen om en del uppgifter för samverkansgruppen som bland annat skulle skapa en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. Regeringen avsåg även att återkomma med fler framtida uppdrag, inte minst framtagandet av en nationell modell för systematiskt informationssäkerhetsarbete.[41] SAMFI presenterade handlingsplanen år 2019 men invänta de då fortfarande styrning från regeringen. Arbetet med den nationella handlingsmodellen kom inte längre än till principnivå i SAMFI-gruppen innan oenighet uppstod vad gällde syfte och tolkning då det inte fanns något tydligt uppdrag.[42] Det dröjde till 2021 innan det Nationella cybersäkerhetscentret (NCSC) tog sig an uppgiften och återupptog arbetet som SAMFI-gruppen påbörjat. Svårigheterna med styrning och oenighet fanns även hos NCSC men arbetet förenklades med hjälp av en något bättre styrstruktur där handlingsmodellen avgränsades till att fokusera på systematiskt cybersäkerhetsarbete.[43]

Redan 2007, och nu senast under 2023,[44] har Riksrevisionen (RRV) genomfört flera granskningar av regeringens och myndigheternas arbete med informations- och cybersäkerhet i Sverige. Att RRV funnit ett behov av återkommande granskningar av arbetet är talande i sig. RRV har i varje granskning rekommenderat att regeringen säkerställer en samlad styrning och former för samordning av de svenska informations- och cybersäkerhetsfrågorna. RRV har även sedan 2007 konstaterat brister i utformningen av regelverk som styr arbetet med informationssäkerheten där ansvar för att utöva tillsyn över informationssäkerheten i den civila statsförvaltningen inte varit tillräckligt.[45] Vidare har RRV bedömt att det behövts en starkare styrning från regeringen gentemot myndigheterna, så att nödvändiga säkerhetsåtgärder verkligen blir genomförda.[46] Att enbart ta fram ett övergripande regelverk har inte bedömts tillräckligt då RRV ansåg att regeringen även behövde styra genom att efterfråga information om myndigheternas informationssäkerhet.

[41] Justitiedepartementet. *Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022*. Ju2018/03737/SSK. Stockholm, 2018.
[42] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. RiR 2023:8. Stockholm, 2023.
[43] Försvarsdepartementet. Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter. Fö2019/01330. Stockholm 2020.
[44] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. RiR 2023:8.
[45] Ibid.
[46] Riksrevisionen. *Informationssäkerheten i den civila statsförvaltningen* RiR 2014:23 Stockholm 2014

Regeringen borde även framhålla vikten av god informationssäkerhet för att få myndigheternas ledningar att prioritera frågan.[47]

Riksrevisionen har genom åren framhållit att regeringen är ytterst ansvarig för myndigheternas verksamhet och därmed även deras informationshantering. Regeringen har dock valt att delegera majoriteten av detta ansvar för informationssäkerhetsarbetet till myndigheterna själva[48] samtidigt som regeringen inte har ett operativt ansvar för vilka åtgärder som vidtas eller ej.[49] Det är ledningen i respektive myndighet som bär det yttersta ansvaret för intern styrning och kontroll. Myndighetsledningarna har dock valt att delegera ansvaret för informationssäkerheten ut i organisationerna utan tillräckliga resurser och befogenheter.[50] Riksrevisionen anser att uppgifter och ansvar för informations- och cybersäkerhetsarbetet är delegerat från regeringen till myndigheterna där expertkunskapen ofta finns. Det finns dock inget hinder för regeringen att bedriva starkare styrning utifrån den svenska förvaltningsmodellen enligt Riksrevisionen.[51]

I föreliggande rapport framgår det att otydligheter i ansvarsfördelning och framförallt styrning har bestått över tid och försvårat det svenska informations- och cybersäkerhetsarbetet. Vidare ska svenska myndigheter följa den styrning som kommer från regleringar i EU, Europakonventionen och annan internationell rätt. Redan i IT-propositionen från 1999 (1999/00:86) ställs krav på att IT-system dels ska skydda individens identitet, dels samspela med internationellt erkända regleringar. I MSB:s kartläggning över EU-initiativ som påverkar Sveriges informations- och cybersäkerhetsarbete nämns åtta initiativ som förväntas få betydande påverkan på Sverige. Flera av initiativen syftar till att stärka motståndskraften och minska sårbarheter hos samhällsviktig verksamhet inom EU. Detta i sig innebär ett stärkt totalförsvar då såväl civilt försvar som militärt försvar är beroende av samhällsviktig verksamhet.[52]

I Riksrevisionens granskning från 2023 framgår det att regeringens arbete med informations- och cybersäkerhet på många sätt inte varit synkroniserat med samma arbete på EU-nivå.[53] Under de senaste åren har EU aviserat ett stort antal satsningar och regleringar med bäring på informations- och cybersäkerhetsområdet. Två exempel är de i Bilaga 2 nämnda EU-direktiven som allmänt kallas NIS och NIS2, där det första NIS-direktivet avsåg leverantörer av samhällsviktiga tjänster

[47] Riksrevisionen. RiR 2016:8. Informationssäkerhetsarbete på nio myndigheter. Stockholm, 2016.
[48] Riksrevisionen. *Granskning av regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*. Stockholm 2007.
[49] Riksrevisionen. RiR 2016:8. Informationssäkerhetsarbete på nio myndigheter. Stockholm, 2016.
[50] Riksrevisionen. *Granskning av regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*. Stockholm 2007.
[51] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. RiR 2023:8. Stockholm, 2023.
[52] Myndigheten för samhällsskydd och beredskap. *Policyöversikt Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*. Stockholm. 2023.
[53] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. Stockholm 2023, s.7 & 37.

och då endast inom sju särskilt utpekade sektorer. I NIS2 tillkommer 12 sektorer, däribland offentlig förvaltning samt nya starkare krav på cybersäkerhet med syftet att minska fragmenteringen av den inre marknaden genom att föreskriva minimiregler för ett samordnat regelverk.[54] En stor del av Regeringskansliets resurser går åt till att hantera initiativ från EU utan att Sverige driver någon sammanhållen linje i fråga om EU-initiativ på den nivån.[55]

3.2 Oklarheter i diskursens definitioner

En andra tydlig tendens som springer ur den samlade litteraturgenomgången är att informations- och cybersäkerhetens diskurs är bred med otydliga begrepp. En läsare av cybersäkerhetens diskurs bör vara medveten om det. De två svenska orden informationssäkerhet och cybersäkerhet representerar två viktiga och besläktade, men ändå olika, perspektiv i det moderna samhället. De två begreppen förekommer i litteraturen ibland omväxlande utan någon tydlig förankring (se även kap 2.1).

Cybersäkerhet kan sägas antyda skyddet av sammankopplade digitala system. Europeiska unionens cybersäkerhetsbyrå (Enisa) definierar cybersäkerhet som ”*all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot”*.[56] Det kan framstå som om Enisas definition i viss mån är självrefererande i och med att cybersäkerhet definieras som ett skydd mot cyberhot, och därmed inte informerar vad cybersäkerhet och cyberhot egentligen ses som. I FOI-rapporten ”Digitaliseringens risker i Hälso- och sjukvård” [57] finner författarna att *cybersäkerhet* helt enkelt saknar en väl etablerad definition. Den rapportens författare skriver att EU:s cybersäkerhetsbyrå Enisa inte finner något behov av en tydlig och enad definition då cybersäkerhetsområdet är för brett och därmed svårdefinierat. De skriver även att Enisa anger att det är mer relevant med en definition utifrån aktuell kontext i respektive fall, då olika organisationer lägger in olika aspekter i termen. Liksom tidigare nämnda rapport från FOI om förekomsten av cyberkrigföring i Ukraina,[58] konstaterar även denna rapport att det ligger utanför dess räckvidd att på djupet granska de grunder som andra kontexter använder.

[54] Försvarsdepartementet. *Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. Dir. 2023:30*. Stockholm, 2023.

[55] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. Stockholm 2023, s.7 & 37. S. 65

[56] Förordning 2019/881. *EU:s cybersäkerhetsakt – 'Cybersäkerhetsakten'*.

[57] Daniel Eidenskog, Ulrika Eckersand & Eva Mittermaier. *Digitaliseringens risker i hälso- och sjukvård*. Totalförsvarets forskningsinstitut 2023.

[58] Per-Erik Nilsson. *Unraveling the Myth of Cyberwar - Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War 2014-2023*. FOI-R—5513–SE [i tryck]. 2023.

*Informationssäkerhe*t kan sägas betyda skydd av information i sig. I en rapport från Krigsvetenskapsakademin [59] finns ett kapitel om svensk terminologi på området. Där återfinns att *informationssäkerhet* liksom i internationella sammanhang på engelska, omfattar skyddet av all information oavsett hur den förmedlas eller lagras. Det spelar alltså enligt Krigsvetenskapsakademin ingen roll för begreppet informationssäkerhet om informationen hanteras elektroniskt, på papper eller i ett samtal mellan två individer. Vidare antyder begreppet informationssäkerhet att informationen skyddas mot alla typer av hot, vilket inkluderar antagonistiska aktörer såväl som allmänna misstag, olyckor och naturhändelser. Vidare skriver samma rapport att en delmängd av informationssäkerheten är hur informationen ska skyddas när den behandlas i olika typer av IT-system.[60] Denna delmängd benämns ibland *IT-säkerhet.* I Försvarsmaktens nomenklatur finns följande definition för IT-säkerhet: ”*I IT-säkerhet inkluderas kommunikationssäkerhet. IT-säkerhet ingår som en del i informationssäkerheten”.*[61]

Redan 2004 uttrycktes ett behov av att enas kring definitioner på området för informations- och cybersäkerhet i “*Från IT-politik för samhället till politik för IT-samhället* (2004/05:175)”. Behovet uppstod då avsaknaden av gemensamma definitioner orsakade förvirring och missförstånd. [62] Tio år senare, år 2014, redogjorde Riksrevisionen vid sin granskning av informationssäkerheten i den civila statsförvaltningen att ingen myndighet valde att beskriva sin informationssäkerhet enligt rekommenderade definitioner från 2004 eller utifrån LIS-standarder[63] från 1999 trots krav på detta.[64] År 2015 fick den statliga utredningen SOU 2015:23 i uppdrag att klargöra definitioner på området för informations- och cybersäkerhet och vid behov föreslå förtydliganden, då det fortfarande saknades en konsensus för begreppen.[65] Ett ytterligare exempel framgår i Riksrevisionens granskning från 2023 där det redogörs för hur samverkansgruppen SAMFI år 2020 avbröt sitt arbete, bland annat på grund av oenighet mellan parterna om olika begrepps innebörd på informations- och cybersäkerhetsområdet. [66] I en FOI-rapport från 2023 redogörs för hur även den internationella diskursen på området

[59] Patrik Sternudd. *Cyberförsvar och cybersäkerhet: strukturer, ansvar och författningar 202*3 Kungliga krigsvetenskapsakademin.
[60] Ibid.
[61] Försvarsmakten. *Begrepp avseende cyberområdet, bil 1”.* Stockholm, 2016.
[62] Klimat- och näringslivsdepartementet. *Prop. 2004/05:175. Från IT-politik för samhället till politik för IT-samhället* Stockholm, 2004.
[63] LIS står för ledningssystem för informationssäkerhet och utgör ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter.
[64] Riksrevisionen. *Informationssäkerheten i den civila statsförvaltningen* RiR 2014:23 Stockholm 2014
[65]Regeringskansliet. SOU 2015:23. *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.*
[66] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig*. Stockholm 2023, s.7 & 37.

är mycket heterogen ifråga om användandet av prefixet cyber, dess betydelse och sammansättningar kring gråzoner och varianter av krig.[67]

3.3 Bristande återrapportering

En tredje tendens som synes springa fram ur litteraturgenomgången är att återrapportering av cybersäkerhetsincidenter ibland varit bristfällig. Redan i förordning (1995:1300) ställdes krav på myndigheter att upptäcka risker som skulle kunna innebära förluster eller skador för staten och att myndigheter ska vidta lämpliga åtgärder för att begränsa dessa eventuella risker.[68] Inga krav ställdes då på att återrapportera det som upptäckts, bara att upptäcka. Det dröjde drygt tio år innan krav på återrapportering infördes. Ur MSB:s föreskrifter om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2016:7) framgår det att de myndigheter som har ett särskilt ansvar för krisberedskap ska redovisa sina förmågor relaterat till vad som där kallas informationssäkerhetsfrågor utifrån ett antal punkter. Dessutom skulle de myndigheter som bedriver samhällsviktig verksamhet analysera sin förmåga till robusthet och redundans för myndighetens kommunikationssystem (radio, IT och tele).[69]

Enligt MSB:s föreskrifter från 2016 (MSB 2016:2) om statliga myndigheters rapportering av IT-incidenter ska en IT-incident rapporteras till MSB senast 24 timmar efter att den upptäckts. Bedömningen av om en inträffad IT-incident ska anses tillräckligt allvarlig att den behöver rapporteras görs dock lokalt hos myndigheten själv, vilket är värt att notera då det kan skapa medvetna eller omedvetna underrapporteringar. Det finns skriftligt stöd för bedömningen av incidenter och myndigheter kan även vända sig till Cert-SE för råd, men det är upp till varje enskild myndighet att välja om en IT-incident ska rapporteras eller inte.[70] I en FOI-rapport från 2020 (*IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering*) framgår att myndigheter upplever svårigheter i att bedöma vad som utgör en IT-incident och därmed vad som ska rapporteras. Vidare saknade de statliga myndigheterna enligt rapporten inarbetade rutiner för bedömning och hantering av incidenterna.[71] Detta trots att det finns styrning och riktning att följa

[67] Per-Erik Nilsson. *Unraveling the Myth of Cyberwar - Five Hypotheses on Cyberwarfare in the Russo-Ukrainian War 2014-2023*. FOI-R—5513–SE [i tryck]. 2023.
[68] Finansdepartementet. *Förordning (1995:1300) om statliga myndigheters riskhantering*. Stockholm, 1995.
[69] Myndigheten för samhällsskydd och beredskap. *Om statliga myndigheters risk- och sårbarhetsanalyser* . Stockholm, 2011
[70] Ibid.
[71] Stenerus, et. al. *IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering.* Totalförsvarets forskningsinstitut, Stockholm, 2020. & Myndigheten för samhällsskydd och beredskap. *MSBFS 2016:7 föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser.* Stockholm, 2016.

vad gäller en grundnivå på godtagbart säkerhetsarbete för bland annat återrapportering.[72].

MSB har i uppdrag att rapportera behov av åtgärder till regeringen vilka formuleras utifrån inkomna uppgifter från myndigheter. Trots att det finns förutsättningar och stöd för rapportering, som ligger på MSB i form av Cert-SE, finns det fortfarande utrymme för myndigheter att medvetet eller omedvetet undvika rapportering. Enligt föreskrifterna är det ledningen för respektive myndighet som ansvarar för att genomföra och följa upp arbetet med informationssäkerheten. När detta arbete inte genomförs får MSB svårt att utföra sitt arbete med att rapportera behov av åtgärder till regeringen.[73] Det är dock ur litteraturen svårt att urskilja om myndigheterna själva brustit i att vidta åtgärder eller om det varit avsaknaden av uppföljning och ledning från regeringen som resulterat i det ofullbordade arbetet med återrapportering i det större cybersäkerhetsarbetet.

Under 2024 ska EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2) införas i Sverige.[74] Detta direktiv medför ett antal viktiga förändringar inom cybersäkerhet. Exempelvis kommer det i hela EU att utfärdas sanktioner mot företag och organisationer som inte följer NIS2:s regler om cybersäkerhet, cyberrisker, penetrationstestning och incidenthantering. Det innebär att respektive myndighet ska redovisa en bedömning av om det finns tillräckligt god förmåga att upprätthålla informationstillgångarnas riktighet, tillgänglighet och konfidentialitet.[75]

[72] Myndigheten för samhällsskydd och beredskap. *MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter.* Stockholm, 2020.
[73] Riksrevisionen. *Informationssäkerhetsarbete på nio myndigheter.* Stockholm, 2016: s. 18.
[74] Europaparlamentet. *Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet).* Bryssel, 2023.
[75] Försvarsdepartementet. *Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. Kommittédirektiv Sverige. Dir. 2023.30*. Regeringen, 2023.

4 Analys och diskussion

I följande kapitel redovisas den analys och diskussion som genomförts med hjälp av intervjumaterialet och de ur litteraturgenomgången identifierade tendenserna.

4.1 Ansvarsfördelning och styrning

En av de tydligaste tendenserna i materialet är att det finns en omfattande och långtgående delegering av ansvar för arbetet med informations- och cybersäkerhet. Det framgår ur litteraturen att Riksrevisionen vid flera granskningar fastslagit att regeringen är och har varit ytterst ansvarig för att upprätthålla och styra arbetet med informations- och cybersäkerheten, trots att regeringen valt att delegera det ansvaret vidare till myndigheterna själva.[76] Delegeringen av ansvar och styrning framgår också ur intervjuerna och att denna delegering inte alltid följts av tydliga instruktioner, uppdrag eller mandat för det ansvar myndigheter fått delegerat till sig. Det resulterar i problematiken att myndigheterna inte alltid löst delegerade uppgifter. Inte heller förekommer det krav på uppföljning till regeringen vilket gör det svårt att identifiera vilket ansvar som tagits hos respektive myndighet. Intervjuerna visar på att myndigheterna arbetat med informations- och cybersäkerhet i olika konstellationer, antingen genom egeninitierade samverkansgrupper eller med viss styrning från regeringen. En intervjuperson belyser samverkan med andra myndigheter:

> ”Ja, vi har kontakter med IMY när det gäller personlig integritet och sådana frågor. Båda myndigheterna har roller som tangerar varandra, så med dem har vi en samverkan och träffar ofta. Digg likaså, har vi också med. Det kan hända att cybersäkerhet diskuteras där också.”

En annan intervjuperson menar att de egeninitierade grupperna styrs genom överenskommelser mellan myndigheterna:

> ”Det styrs genom överenskommelser mellan myndigheterna helt enkelt.”

En av regeringen initierad samverkansgrupp är SAMFI där all samverkan mellan myndigheterna var helt frivillig. Samverkansgruppen saknade mandat och styrning vilket ibland visade sig resultera i svårigheter att utföra de uppdrag de fick tilldelade.[77] Ett annat exempel på hur, av regeringen initierade, grupper har svårigheter att arbete tillsammans är det nuvarande Nationella cybersäkerhetscentret (NSCS).[78] Centret består av myndigheter med skilda synsätt och prioriteringar.

[76] Riksrevisionen. *Granskning av regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*. Stockholm 2007.
[77] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* s. 24 och not 59
[78] Nationellt cybersäkerhetscenter utvecklas efter ett uppdrag från regeringen till de myndigheter som tillsammans står bakom centret . Dessa myndigheter är FRA, Försvarsmakten, MSB och Säkerhetspolisen.

Exempelvis kan Säpo, FRA och MUST ses som underrättelsemyndigheter vars intresse i varje fall initialt inte är att offentliggöra information då de hanterar sekretess som inte får offentliggöras. Att inte kunna dela information med varandra försvårar möjligheten till samverkan.[79] Det framkommer i NCSC:s beskrivning att samverkan ska utvecklas stegvis under åren 2021–2023[80] men arbetet har ansetts vara alltför lågintensivt där uppdrag inte fullföljts.[81] Centrets arbete har förenklats jämfört med SAMFI-gruppen med hjälp av en bättre styrstruktur, men regeringen har inte följt upp eller uppmärksammat den passivitet som förekommit.[82] Att betrakta SAMFI och NCSC tillsammans med intervjuerna visar på ett mönster av svag medföljande styrning eller uppföljning från regeringen vilket försvårat deras arbete.

En del länder har valt att centralisera styrningen och koordineringen av myndigheters cybersäkerhetsarbete till en stark central part. Det kallas ibland för ”cyber security czar” eller liknande formuleringar.[83] [84] Det behöver inte i sig vara något negativt med den omfattande delegeringen som denna rapport identifierat. Det kanske mer handlar om instruktion och uppföljning än om delegering i sig. I relation till det svenska statsskicket kanske det till och med krävs en omfattande delegering. En intervjuperson hade synpunkter på detta.

> ”Rent personligen så tycker jag att cybersäkerheten inte är en disciplin som man behöver ha avsteg ifrån. Utan cybersäkerhet finns i varje sektor, den finns i varje verksamhetsområde – den finns inom tillsyn, inom reglering, inom främjande. Att separera ut just den disciplinen och skapa en annan beslutskanal, det … när upphör den att vara särskild? När ska den återföras till sektorsansvariga? Ska vi inte ha sektorsansvariga kvar – ja, men då blir det någonting helt annat.”

En annan intervjuperson föreslår att NCSC:s arbete skulle förbättras om det infördes en cybersäkerhetsmyndighet, men att regeringen inte ställer sig bakom det förslaget.

> ”Vill man ha max av ett centra då ska man bilda en cybersäkerhetsmyndighet,

Som beskrivits i rapportens inledning ska svenska myndigheter följa den styrning som kommer från regleringar i EU, Europakonventionen och annan internationell rätt. En intervjuperson berättar att implementeringen av ”NIS1” skapade viss förvirring:

---

[79] Ibid, s. 23 sid 20 och Not 40
[80] Försvarsdepartementet. *Fö2019/01330 Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscente.cybersäkerhetscenter.* Stockholm, 2020.
[81] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* s. 24 och not 59
[82] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* s. 28.
[82] John Kelly. *What does the U.S. cybersecurity czar do?*. 2023.
[84] Erik Chabrow, '*5 Duties of a Cybersecurity Czar*'. 2009

> ”Det är klart att vissa myndigheter i NIS1, de hade inte jobbat med cybersäkerhet tidigare. Men det föll sig så att vissa sektorer hamnade under … Inspektionen för vård och omsorg till exempel, de hade inte många anställda som höll på med cybersäkerhet. Ssomå att beroende på vilka som tilldelas tillsynsmandatet så blir utfallet olika. Har man inte alls någon kompetens så kanske man frågar sig ”Varför får vi det här mandatet?”

Ett annat citat belyser indikationer på fragmentering av ansvaret och styrningen för svensk cybersäkerhet för totalförsvaret. Intervjupersonen har samtidigt förhoppningar om att NIS2-direktivet och dess kommande implementering ska leda till ett mer samordnat och tydligare informations- och cybersäkerhetsarbete. Detta gäller inte minst genom högre krav på styrning från respektive ledning.

> ”En förhoppning är ju att det ska bli bättre ordning och tydligare… att det ska funka likartat och samordnat så mycket som möjligt… Så förhoppningsvis blir det lite tydligare och bättre ordning. Men att man ställer högre krav på ledningar – nu måste ledningen ta ansvar. Sedan är väl en förhoppning också nationellt, att vi kan få en bättre och starkare samordning.”

Det första NIS-direktivet avsåg leverantörer av samhällsviktiga tjänster endast inom 7 särskilt utpekade sektorer. NIS2, som intervjupersonen hänvisar till, ska införlivas i svensk lagstiftning under hösten 2024. I det nya direktivet tillkommer 12 sektorer utöver de 7 som ingick i det första direktivet. NIS2 innebär tydligare rapporteringskrav samt mer detaljerade bestämmelser om sanktioner jämfört med det första NIS-direktivet. NIS2 ses enligt intervjupersonerna till viss del som ett steg i rätt riktning för att bland annat förbättra den bristande incidentrapporteringen. Samtidigt tros NIS2 kunna skapa friktion och svårigheter vid implementeringen, på grund av att de regleringar som NIS2 kräver krockar med annan svensk lagstiftning och ställer nya och höga krav på verksamheterna.[85]

En intervjuperson menar att det kommer finnas svårigheter i samarbetet med EU och implementeringen av NIS2 när FRA ska vara huvudman för NCSC.

> ”Regeringen har ju angett att FRA ska vara huvudman för centret framöver. Med det signalerar man kanske att man vill att FRA i viss mån ska ha taktpinnen för hur vi jobbar med cybersäkerhetsfrågorna i Sverige. Men det är inte fullt ut förenligt med EU-rätten. eftersom cybersäkerhetsarbetet i Sverige i absoluta majoriteten av fallen, de regleras av NIS2-direktivet. Vars genomförande i stor utsträckning styrs av genomförandeakter som kommissionen reviderar.”

Denna intervjuperson leder fram till att huvudmannen för NCSC kan komma att få dubbla uppdragsgivare, både EU-kommissionen och regeringen, vilket kan vara problematiskt för en central underrättelsemyndighet som FRA.

[85] Myndigheten för samhällsskydd och beredskap. *Policyöversikt Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*. Stockholm. 2023. https://www.msb.se/contentassets/846ae8ad37e44b20b442f3c44eed0c9e/policyoversikt-eucyber_v1.1.pdf.

Vidare anser en av intervjupersonerna att Sverige i praktiken inte har någon nationell strategi för cybersäkerhetsarbetet, men att arbetet pågår med att skapa en ny i linje med de krav som ställs i NIS-2:

> ”…..Vi arbetar med en ny, för när det gäller NIS2-direktivet att varje land måste ha en cybersäkerhetsstrategi. Det arbetet har inletts …tanken då att presentera den sensommar/höst-24.”

Den svenska modellen för totalförsvarets uppbyggnad är till stor del baserad på frivillighet, fram till dess att krig brutit ut. NIS2 ger sanktionsmöjligheter till beredskapsmyndigheterna vilka förväntas använda sig av den mot de som inte sköter sig. Enligt en intervjuperson innebär införandet av NIS2 förändringar i den svenska modellen.

> ”Vi har i Sverige, i synnerhet i totalförsvarssammanhang, en förtroendebaserad modell som bygger mycket på frivilligt samarbete och så vidare, åtminstone innan höjd beredskap inträffar. Det är slut med den modellen nu, för att NIS2 är bara början av en serie regleringar som kommer på det här området på olika sätt. Som tar sin utgångspunkt i en mycket mer antagonistisk relation mellan staten och de privata utförarna. Bara för att ta ett exempel, den sanktionsmöjlighet som tillsynsmyndigheterna inte bara har, utan förväntas använda sig av ifall de upplever att objekten som verkligen inte sköter sig, det är att man kan gå in och avsätta de högsta cheferna temporärt.”

Likt andra EU-förhandlingar återfanns ett mycket högt tempo vad gällde NIS2 enligt intervjupersonerna. Det höga tempot resulterade i att berörda myndigheter inte hade speciellt stora möjligheter att vara med och påverka vad som beslutades. Intervjupersonerna menade att det inte fanns tid för referensgrupper och samråd. Denna brist på tid berodde delvis på en saknad dialog i Sverige gällande säkerhetsfrågor som rör EU, vilket leder till låg förståelse för besluten som tas i kombination med lite tid för återkoppling.

> ”De här förhandlingarna var så fruktansvärt forcerade redan från början…Ja, men jag tänker de fick ju också korta puckar, bara någon dag om de hade tur att återkoppla. Så ska vi försöka då analysera och förstå vad de menar. Tyvärr, det är så när man jobbar i förhandlingar, det finns inte den tiden.”

> ”Vi har ingen levande EU-debatt egentligen alls. I synnerhet inte när det gäller säkerhetsfrågorna. Det gör att det tas en massa initiativ på nationell nivå som inte riktigt är samordnade med arbetet som sker i EU… Man kan väl säga att förståelsen mellan myndigheterna, men också i synnerhet kanske på den politiska nivån, för att vi inte längre får bestämma hur vi ska lösa de här utmaningarna på egen hand, brister på en hel del håll.”

Med början av 2024 kommer NIS2-direktivet att implementeras i Sverige, vilket kommer att innebära en omstrukturering av den svenska cybersäkerheten.

4.2 Oklarheter i diskursens definitioner

Den terminologiskt mångfacetterade diskursen på området är en av nämnda tendenser som återkommer både i intervjuerna och litteraturgenomgången. En

intervjuperson menar att cybersäkerhet kan ses som den digitala delen av det civila försvaret och att det inte går att ha ett cyberförsvar om det inte finns god cybersäkerhet. Intervjupersonen tar därmed inte hänsyn till det militära försvaret (och därmed totalförsvaret) i sin definition vilket är en avgränsning som inte återfinns i tidigare nämnda definitioner. En annan intervjuperson resonerar kring cyber- och informationssäkerhet på följande sätt:

> ”Det är olika ord man använder och man betonar väl mer eller mindre hur mycket det handlar om riskhantering. Men på det stora hela så menar man väl att informationssäkerhet – det är uppgifter och data; och cybersäkerhet – det är då även systemen som hanterar och transporterar information.”

En annan intervjuperson resonerar kring begreppet cyberincidenter på följande sätt:

> ”För det första, innan jag säger det, här har vi också en terminologiskillnad som är viktig för att förstå var jag kommer ifrån versus vad andra säger, för mig är inte ett angrepp, eller rättare sagt ett försök till ett angrepp, en incident i sig. Det är inte att någon försöker hugga mig som är incidenten, det är att jag blöder som är incidenten.”

Denna intervjuperson menar då i hela sitt resonemang att ett ”angrepp” eller en ”incident” inte uppstår när det bara är ett försök till angrepp eller en potentiell incident. Det är när det uppstått en konsekvens (blöder) som det bedöms som en incident oavsett hur den uppstått. Samma person beskriver hur man kan sortera händelser:

> ”Därför att då kan jag börja sortera i de gånger jag blött för att någon högg mig, de gånger jag blött för att jag skar mig själv och så vidare. Det blir ett mycket bättre sätt att sortera i vad som händer, hitta de orsakskategorier som mest frekvent förekommer, och därmed lyckas lista ut vilka fenomen man bör lägga de gemensamma resurserna på att hantera först. Men det är en synsättsskillnad, de andra håller inte med om det alls. Men det är vår approach.”

En annan intervjuperson menar att de flesta IT-incidenter orsakas av misstag och inte av en antagonist trots att det från andra håll finns ett visst fokus på antagonistiska incidenter:

> ”Medans det på andra håll finns mycket, mycket större fokus på det antagonistiska. Vilket vi då från vår enhet har försökt hela tiden påminna om att det är inte där de flesta IT-incidenterna uppstår, utan det är andra – det är systemfel, handhavandefel och så vidare som står bakom de flesta.”

En intervjuperson anser att det råder terminologiskillnader beroende på vilken sfär och kontext en diskussion sker i. Exempelvis har prefixet cyber olika användning beroende på geografi och språk:

> ”… när man till exempel diskuterar med USA. Därför att för dem så begår man ett kategorimisstag om man talar om cybersäkerhet och pratar om naturhändelser till exempel. För det är inte det som ämnet handlar om, så som de ser det.”

Enligt denna intervjuperson antar en aktör i USA att en incident inom cybersäkerhet är antagonistisk. Bland intervjupersonerna finns inte den presumtionen som förförståelse i diskussionen på samma sätt.

4.3 Bristande återrapportering

I både litteraturen och intervjuerna framkommer ett mönster av bristande återrapportering. Bedömningen av om en inträffad IT-incident ska anses tillräckligt allvarlig för att behöva rapporteras görs av myndigheterna själva. Det är ledningen i respektive verksamhet som är ytterst ansvarig för att rapporteringen genomförs, vilket är något som beskrivs som problematiskt av intervjupersonerna. Den ”frågan” som nedanstående person åsyftar i en diskussion om återrapportering är återrapportering av incidenter.

> ”Infosäkkollen[86] visar att det är många myndigheters ledningar som inte tagit frågan på allvar, absolut.

Enligt en av intervjupersonerna tar inte statliga myndigheter och kommuner ett tillräckligt stort ansvar för att rapportera IT-incidenter, vilket kan bero på flera anledningar. Vidare framhålls att verksamheterna är oroliga för att myndighetens rykte ska skadas av att blotta sårbarheter.

> ”Fragmentering är väl just det här att det är oklart…har väl varit att man inte vet riktigt vad är det för regelverk man har att följa och att man inte alltid har följt det. Det finns väl olika teorier om varför man inte rapporterar till exempel incidenter. Att man är rädd för att det skulle kunna skada varumärket eller så där. Man vet kanske inte alltid heller exakt vad man ska göra.”

När både kommuner och statliga myndigheter brister i återrapportering får MSB svårt att utföra sitt arbete med att rapportera behov av åtgärder till regeringen.[87] Detta stöds av följande intervjucitat:

> ” … så var det en incident hos en stor leverantör av IT-tjänster som används inom den typen av verksamhet i kommunerna. Vi vet att strax över 150 kommuner har avtal med den här leverantören. Vi vet att de kommunerna, alla var för sig, omfattas av NIS-lagen i Sverige och därmed blir rapporteringsskyldiga när de har längre avbrott i en sådan tjänst som är central för deras utövande av hemtjänstservice till exempel. Men ändock så får vi kanske ett tjugotal rapporter.”

Detta citat stämmer väl överens med resultatet i den tidigare nämnda FOI-rapporten från 2020 om orsaker till utebliven rapportering av IT-incidenter på statliga myndigheter.[88] Det är ur både litteratur och intervjuerna svårt att urskilja

[86] Infosäkkollen är ett verktyg som stödjer uppföljning och förbättring av systematiskt informations- och cybersäkerhetsarbete i samhällsviktiga verksamheter som omfattas av NIS-regleringen.
[87] Riksrevisionen. *Informationssäkerhetsarbete på nio myndigheter.* RiR 2016:8. Stockholm, 2016.
[88] Ibid.

om verksamheterna själva brustit i att vidta åtgärder eller om det varit avsaknaden av uppföljning, information och ledning från regeringen eller departement som resulterat i den bristande återrapporteringen.

5 Slutsatser

Denna rapport har undersökt följande frågeställningar:

a) Hur ser fördelning av ansvar och styrning ut för informations- och cybersäkerhetsarbete i det svenska digitala samhället i den svenska statsförvaltningen?
b) Hur har denna fördelning uppstått?
c) Finns det någon problematik relaterat till hur fördelningen ser ut?

Rapporten har identifierat tre tendenser vilka samtliga påverkar det svenska informations- och cybersäkerhetsarbetet. Den första tendensen berör ansvarsfördelning och styrning. Den andra utgår från oklarheter i diskursens definitioner. Den tredje belyser bristande återrapportering av inträffade händelser.

Fördelningen av ansvar för och styrning av svenskt informations- och cybersäkerhetsarbete är idag fördelat mellan olika departement och myndigheter. De mest centrala aktörerna är Justitiedepartementet, Försvarsdepartementet Säkerhetspolisen (Säpo), Försvarsmakten, Post- och telestyrelsen (PTS) Försvarets radioanstalt (FRA), Försvarets materielverk (FMV), Myndighetens för samhällsskydd och beredskap (MSB) samt Polismyndigheten. Dock har inget departement eller någon myndighet något övergripande ansvar för styrning och koordineringen av cybersäkerhetsarbetet. Det finns en överhängande risk för åtgärder som inte blir koordinerande och sammanhängande, en risk som i viss mån redan realiserats. Regeringen är ytterst ansvarig för departements och myndigheters verksamheter och därmed även deras arbete med informations- och cybersäkerhet. Olika regeringar över tid har dock valt att delegera detta från regeringen till myndighetsledningar som i sin tur delegerat vidare ut i organisationerna. Denna modell är kanske ett måste enligt rådande svenskt statsskick och inte i sig problematisk. Modellen ställer dock krav på att informations- och cybersäkerhetsarbetet genomförs med rätt förutsättningar, mandat och inte minst styrning. Denna rapport redogör för att olika röster genom åren belyst att så inte är fallet.

Statsförvaltningen är med dess myndigheter regeringens viktigaste instrument för att styra riket. Det är regeringens uppgift att ange mål för den statliga verksamheten och med olika medel styra sin förvaltning. Uttryckliga regler om hur denna styrning ska gå till saknas dock i Regeringsformen (RF). Myndigheterna är självständiga i förhållande till regeringen ifråga om enskilda beslut som fattas i utförandet av myndighetens uppgifter. Det finns inget hinder för regeringen att bedriva starkare styrning av informations- och cybersäkerhetsarbetet utifrån den svenska förvaltningsmodellen.[89] Även om det inte är helt tydligt hur styrningen

[89] Riksrevisionen. Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig. RiR 2023:8. Stockholm, 2023.

ska gå till i praktiken är det tydligt att svenska myndigheter ska följa regleringar från regeringen och EU, Europakonventionen och annan internationell rätt.

Fördelningen av ansvar och styrning har vuxit fram under lång tid samtidigt som storskaliga satsningar på att digitalisera Sverige ägt rum. I IT-propositionen (1999/00:86) införde regeringen målet att Sverige skulle bli det första landet som gjorde informationssamhället tillgängligt för alla medborgare.[90] Det digitaliserade samhället har drivits fram och erbjudit nya, moderna, smarta, effektiva och framtida lösningar men även risker.[91] Ansvaret för informations- och cybersäkerhetsarbetet har genom åren, med hjälp av propositioner, lagändringar och regeringsuppdrag, delegerats från regeringen och ut i verksamheterna utan någon direkt sammanhållande styrning. De satsningar som regeringar dock genomfört för att öka säkerhetsarbetet har i största mån fokuserat på den offentliga sektorn. Det finns idag ingen tydlig styrning eller riktning att följa vad gäller grundnivån för vad som är godtagbart säkerhetsarbete.

I intervjumaterialet finns en försiktigt hoppfull inställning till det kommande NIS2-direktivet från EU. Trots befarade svårigheter med implementeringen av direktivet, inte minst utifrån den svenska totalförsvarsmodellen, tros direktivet med tillhörande sanktionsmöjligheter leda till ett mer samordnat och tydligare informations- och cybersäkerhetsarbete. Detta gäller inte minst genom att NIS2-direkt ställer högre krav på styrning från respektive ledning.

Fördelningen av ansvar och styrning för svenskt informations- och cybersäkerhetsarbete är allokerat över flera parter utan tydlig styrning, vilket kan minska effektiviteten i säkerhetsarbetet. I rapportens inledning beskrevs forskning som indikerade att en komplex värld kräver en decentraliserad styrning[92], men att en decentraliserad styrning istället kan leda till mer komplexitet.[93] För att decentraliserad styrning ska fungera framgångsrikt bör den motsvaras av tydliga instruktioner till mottagaren och tydligt specificerad kapacitet hos densamma.[94] Dessa förutsättningar har inte alltid funnits.

Det finns viss problematik relaterat till hur fördelningen av ansvar och styrning ser ut vilket flera röster genom åren belyst. Det har efterfrågats tvärsektoriella lösningar och samordning för att skapa ett skydd för det digitala samhället. Denna

---

[90] Näringsdepartementet. *IT-propositionen (1999/00:86).- Ett informationssamhälle för alla*. Stockholm, 1999.

[91] Jenny Ingemarsdotter, Daniel Eidenskog & Vidar Hedtjärn Swaling. *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*. Totalförsvarets forskningsinstitut 2020 FOI-R--4814--SE

[92] Alexander. F Siegenfeld & Yaneer Bar-Yam. *An introduction to complex systems science and its applications.* Complexity, 2020, s. 1-16.

[93] Shirin Ahlbäck Öberg, S. A., & & Helena Wockelberg, H. A*gency control or autonomy? Government steering of Swedish government agencies 2003–2017*. International Public Management Journal, 24(3), 330-349. 2021.

[94] Sjors Overman, S. *Great Expectations of* public service delegation*: A systematic review*. 2016 s. 1238-1262.

rapport belyser att en del av problematiken är en otydlig terminologi för informations- och cybersäkerhetsarbetet vilket är problematisk då det resulterar i begreppsförvirring och bristande konsensus.

Vidare återfinns en bristande återrapportering vad gäller incidenter. Det är ur både litteratur och intervjuerna svårt att urskilja om verksamheterna själva brustit i att vidta åtgärder eller om det berott på avsaknaden av uppföljning, information och styrning från regeringen, departement eller myndighetsledning. Oavsett orsak utgör den bristande rapporteringen ett problem för informations- och cybersäkerhetsarbetet då inträffade incidenter inte lyfts, vilket i sin tur minskar regeringens insikt i det aktuella cybersäkerhetsläget. Vidare visar resultatet i denna rapport att den bristande styrningen och spretiga terminologin kan utgöra bidragande anledningar till den bristande återrapporteringen.

Föreliggande rapport har fokuserat på studier av forskningslitteratur och offentliga dokument som speglar den digitaliseringspolitik som förts i Sverige, kompletterat med intervjuer. Urvalet till intervjuerna bör inte ses som representativa för alla perspektiv inom det svenska informations- och cybersäkerhetsarbetet utan utgör åsikter och insikter från några seniora företrädare. I nästa kapitel presenteras förslag på framtida studier där andra och fler perspektiv kan ges utrymme.

Det digitaliserade samhället har drivits fram i snabb takt utan ett tillräckligt konsekvenstänk där olika regeringsbildningar haft som ambition att Sverige ska ligga långt fram i utvecklingen. I takt med att samhället blivit mer digitaliserat ökar betydelsen av trygghet och säkerhet. De risker som medföljer det digitala samhället bör hanteras med god samordning och styrning vilket inte alltid varit fallet i den svenska statsförvaltningen.

6 Förslag på framtida forskning

Rapporten har övergripande studerat området svensk cybersäkerhet, inklusive dess styrning, dess regelverk och en del av dess problem. Det finns mycket forskning kvar att göra. Under arbetets gång har rapportens författare frågat intervjupersonerna, andra forskare inom FOI och nyckelpersoner inom svensk cybersäkerhetsarbete om vad de önskar för framtida forskning på området.

Här följer ett antal trådar som dessa anser är värda att ta upp i fortsatt arbete med nya projekt. Dessa här föreslagna projekt skulle till sin natur vara högst tvärvetenskapliga och sträcka sig över, bl.a. juridik, statskunskap, cybersäkerhet, analys och värdering av säkerhetsegenskaper i komplexa tekniska system, beteendevetenskap, psykologi, mediateori, medie- och krishantering, analys och forskning på metoder och processer för exempelvis säkrare systemutveckling, ekonomi, och ha en socioteknisk forskningsansats.

6.1 Jämförande decentralisering

- *En svensk cyber security czar*.
  En del länder har centraliserat ansvar för koordinering och styrning av cybersäkerhet till en central stark part. Denna kallas ibland cyber security czar. I ett internationellt perspektiv har Sverige ett relativt litet regeringskansli, och relativt starka och självständiga myndigheter. Kan en cyber security czar eller en cybersäkerhetsmyndighet fungera i Sverige, och vad skulle det innebära att ha en sådan?

- *Demokratiska perspektiv på självgående myndighetssamverkan*.
  Bland svenska myndigheter är det en dygd att samverka. Myndigheter ska självständigt förmå att lösa problem inom sin domän. I det arbetet uppstår ofta spontana samverkansgrupper myndigheter emellan. Ibland får en grupp av myndigheter ett samverkansuppdrag direkt från regeringen, men ibland sker det spontant. Denna studie skulle granska dessa samverkansformer för cybersäkerhetsarbete utifrån ett perspektiv av demokrati, transparens och styrning.

- *Smittskydd och cybersäkerhet.*
  En jämförelse på djupet mellan decentralisering i det svenska smittskyddet och decentralisering i cybersäkerheten. Denna jämförelse kan ta sin utgångspunkt från bland annat pandemirapporterna[95] samt denna här föreliggande rapport.

[95] Regeringskansliet. *SOU 2021 : 89. Sverige under Pandemin Vol 1 & 2 SOU 2021 : 89.* Stockholm, 2021.

- *Ansvar och implicita förväntningar.*
  Finns det i det svenska samhället en implicit förväntan att organisationer, privata eller offentliga, har ett större ansvar och mer utbyggd beredskap för cybersäkerhet än vad dessa enligt lag, annan reglering eller verksamhetens ekonomiska praktik är beredda att möta?

- *Dynamik mellan sektorer.*
  Hur kan cybersäkerhetsdynamiken mellan militära aktörer, kommersiella civila aktörer och offentliga sektorns civila aktörer beskrivas och analyseras? Vem har ansvar mot vem? Kan privata och offentliga företag förvänta sig hjälp från totalförsvaret i ett nödläge? Finns det en faktisk beredskap i sådana fall?[96]

- *Effektivisering, New Public Management och cybersäkerhet.*
  I Sverige har det sedan flera årtionden funnits en idéströmning ifråga om effektivisering och minskning av den offentliga sektorn. Detta kan läsas bland annat i en rapport från Riksrevisionen (2011)[97] och FOI-rapporten ”Vilse i Lasagnen”[98]. I vilken relation står den idéströmningen, ifråga om cybersäkerhet, till den nutida återuppbyggnaden av totalförsvarsberedskapen?

6.2 Jämförande implementering

- *NIS2 mellan länder.*
  Hur kommer implementeringen av EU-direktivet NIS2 att skilja sig mellan Sverige och övriga EU-medlemsstater? Varför kommer det skilja sig och vad innebär skillnaderna?

6.3 Konkurrens mellan normer och standarder

- *Normkonkurrens.*
  Hur kommer den institutionella interaktionen mellan Nato, Sverige och EU på området för cybersäkerhet att påverka riktningen och utvecklingen av cybersäkerhetsinitiativ och standarder? Detta särskilt

[96] Jfr. avsnitt 4.4 i Ju2022/01209/SSK.

[97] Riksrevisionen *IT inom statsförvaltningen - har myndigheterna på ett rimligt sätt prövat frågan om outsourcing bidrar till ökad effektivitet?* Stockholm, 2011 https://www.riksrevisionen.se/rapporter/granskningsrapporter/2011/it-inom-statsforvaltningen---har-myndigheterna-pa-ett-rimligt-satt-provat-fragan-om-outsourcing-bidrar-till-okad-effektivitet.html (hämtad december 2023).

[98] Jenny Ingemarsdotter, Daniel Eidenskog & Vidar S Hedtjärn. *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur.* FOI-R--4814—SE. Totalförsvarets forskningsinstitut. Stockholm, 2020.

med beaktande av att EU:s initiativ är tvingande och Natos initiativ frivilliga.

6.4 Cybersäkerhetens ekonomi

- *Priset för säkerhet.*
  Hur förhåller sig kostnaden för att upprätthålla kontinuerlig preventiv cybersäkerhet i relation till den reaktiva kostnaden för cybersäkerhetsincidenter? Denna studie genomför en jämförande analys av kostnaden för cybersäkerhet kontra kostnaden för en incident. I detta ingår till exempel att definiera vad som är en kostnad för cybersäkerhet såsom utbildning och löpande underhåll. Vad är den normala nivån på cybersäkerhet och vad är extraordinärt?

- *Myt och verklighet vid cyberincidenter*.
  Projektet jämför olika standarder och utbildningar inom cyberincidenthantering för att se om det råder enighet om vad som behövs för att en organisation ska ha vad som kan anses som god beredskap i cybersäkerhet. Föreställningarna om god cyberberedskap används som underlag för jämförelse med hur verkliga incidenter har hanterats. Detta i syfte att se om teori och praktik stämmer med varandra. Utfallet skulle kunna användas till att rekommendera de utbildningar och modeller som verkar stämma bäst med verklighetens krav.

6.5 Cyberangrepp och psykologiska effekter

- *Schrödingers cyberincident.*
  Hur samhällets cybersystem egentligen fungerar är ofta både okänt och svårbegripligt för en bredare allmänhet. En attack på ett cybersystem behöver inte ens ha ägt rum i verkligheten för att ändå utöva en betydande psykologisk påverkan, likt Schrödingers katt, som både kan vara levande och död samtidigt beroende på observerarens perspektiv. Denna forskning kommer att bidra till en djupare förståelse av dessa psykologiska aspekter och deras koppling till cybersäkerhet. Projektet tar sikte på tre huvudsakliga forskningsfrågor:
  a. Vad triggar psykologiska reaktioner vid en upplevd cyberincident? Detta inkluderar att undersöka de reaktioner och känslor som uppstår när individer och organisationer upplever att de utsätts för en cyberincident, oavsett om den är verklig eller endast upplevd.
  b. Vilken roll spelar kunskap om orsakerna till icke-funktion i vardagens digitala system? Detta skulle inkludera att analysera om det finns en

skillnad i de psykologiska reaktionerna beroende på om individer och organisationer känner till orsakerna till problemen i digitala system eller inte.

c. Hur skapas föreställningen om att en cyberincident har inträffat? Detta inkluderar att undersöka de mekanismer som leder till att individer och organisationer upplever att de har drabbats av en cyber-incident, oavsett om det är en verklig händelse eller en upplevd risk.

6.6 Cyberdomänen och rättsliga frågor

- *Storleken på det generella folkrättsliga handlingsutrymmet i cyberdomänen* Frågeställningen relaterar framför allt till de grundläggande folkrättsliga principerna som har betydelse för en stats säkerhet. Dessa kan vara statssuveränitet, icke-inblandning, våldsförbud och de förutsättningar under vilka en stats åtgärder i cyberdomänen utgör överträdelser av folkrätten. Ett agerande som därmed medför statsansvar och berättigar till sådana motåtgärder som annars skulle vara i strid med folkrätten.

- *Tolkning och tillämpning av den internationella humanitära rätten i cyberdomänen.* Frågeställningen inbegriper ett antal delfrågor som är specifika för cyberdomänen (jfr. kap 2) i väpnad konflikt, både i offensiva och defensiva operationer. Följande delfrågor är framför allt relevanta att besvara:
  - Kan åtgärder enbart i cyberdomänen göra att den internationella humanitära rätten blir tillämplig?
  - Ska digital egendom i cyberdomänen som både har militär och civil användning bedömas annorlunda vid offensiva cyberoperationer än fysisk egendom?
  - Hur ska risken för oavsiktliga skador på civila och civil egendom bedömas vid offensiva cyberoperationer? Häri ligger bland annat frågan huruvida data utgör egendom i den mening som avses i den internationella humanitära rätten, så att civil data måste beaktas i denna bedömning.
  - Vad har civila som deltar i cyberoperationer för folkrättslig status och skydd?
  - Var går gränsen mellan tillåten krigslist och otillåtet förrädiskt förfarande i cyberdomänen?
  - Vilka försiktighetsåtgärder måste enligt den internationella humanitära rätten vidtas i svenska cybersystem av olika slag för att undvika negativa effekter på civila och civil egendom om Sverige utsätts för angrepp i cyberdomänen?

- Vilka överträdelser av den internationella humanitära rätten som kan leda till individuellt straffrättsligt ansvar är särskilt relevanta för cyberdomänen?

- *Rättsutvecklingen för cyberdomänen*
  Frågeställningen omfattar framför allt bevakning och analys av folkrättsliga, EU-rättsliga och nationellrättsliga processer för rättsutveckling på området. Den omfattar också redovisning och analys av initiativ och positioner som framförs och intas i internationella forum av Sverige och av andra relevanta aktörer.

7 Referenser

Adkins, Donna., Chauvin, Sheila. & Johnson, Jessica. L., *A review of the quality indicators of rigor in qualitative research*. American journal of pharmaceutical education. 2020, 84(1).

Ahlbäck Ö, Shirin & Wockelberg, Helena. A*gency control or autonomy? Government steering of Swedish government agencies 2003–2017*. International Public Management Journal, 24(3), 330-349. 2021.

Ampere, André-Marie. *Essai sur la philosophie des sciences. ou Exposition analytique d'une classification naturelle de toutes les connaissances humaines*. 1834.

Ashby William Ross, *An Introduction to Cybernetics*. London: Chapman & Hall Ltd. 1956. ISBN 9781614277651

Barusch, Amanda, Gringeri Christina & George Molly. *Rigor in Qualitative Social Work Research: A Review of Strategies Used in Published Articles*, Social Work Research, Volume 35, Issue 1, March 2011, s. 11 19, https://doi.org/10.1093/swr/35.1.11

Bryman, Alan. *Samhällsvetenskapliga metoder*, Liber, Malmö. 2011, ss. 106;109

Bussell, Jennifer. *Cyberspace*. Encyclopedia Britannica, 15 okt. 2023, https://www.britannica.com/topic/cyberspace Hämtad 6 november 2023.

Norrby Catrin, *Samtalsanalys. Så gör vi när vi pratar med varandra.* Lund: Studentlitteratur AB. 2014, s. 33.

Chabrow Erik. *5 Duties of a Cybersecurity Czar*. 2009. Hämtad 2 november 2023. https://www.govinfosecurity.com/5-duties-cybersecurity-czar-a-1425

Corbin M, Juliet & Strauss, Anselm. *Grounded theory research: Procedures, canons, and evaluative criteria*. 1990. Qualitative sociology, 13(1), s. 3-21.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2011). *The Sage handbook of qualitative research*. Sage. Kap 15 & Kap 42

Eidenskog Daniel, Eckersand Ulrika & Mittermaier Eva. *Digitaliseringens risker i hälso- och sjukvård*. FOI-R--5367—SE. Totalförsvarets forskningsinstitut 2023.

Europaparlamentet. *Europaparlamentets och rådets 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*. 194 OJ L §. Bryssel, 2016. Hämtad 2 september 2023. http://data.europa.eu/eli/dir/2016/1148/oj/swe .

Europaparlamentet. *Förordning 2019/881 EU:s cybersäkerhetsakt – 'Cybersäkerhetsakten'.* Bryssel, 2019. Hämtad 2 september 2023. https://eur-lex.europa.eu/legal-content/SV/LSU/?uri=CELEX:32019R0881

Europaparlamentet. *GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET EU:s politik för cyberförsvar.* Bryssel, 2022. Hämtad 2 september 2023. https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX:52022JC0049

Europaparlamentet. *Direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen (NIS2-direktivet).* Bryssel, 2023. Hämtad 2 november 2023. *ht*tps://digital-strategy.ec.europa.eu/sv/policies/nis2-directive

Finansdepartementet. *Förordning (1995:1300) om statliga myndigheters riskhantering*. Stockholm, 1995. Hämtad 30 augusti 2023. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-19951300-om-statliga-myndigheters_sfs-1995-1300/

Finansdepartementet. *Prop. 2011/12:1 Budgetpropositionen för 2012 Utgiftsområde 22.* Stockholm, 2011.

Finansdepartementet. Prop. 2015/16:1. *Förslag till statens budget för 2016 Försvar och samhällets krisberedskap.* Stockholm 2015.

Finansdepartementet. *Prop. 2019/20:1 Budgetpropositionen för 2020.* Stockholm, 2019.

Finansdepartementet. *Förordning (2018:1486) Instruktion för Myndigheten för digital förvaltning.* Stockholm, 2018. Hämtad 30 augusti 2023. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20181486-med-instruktion-for_sfs-2018-1486/

Finansdepartementet. *Juridik som stöd för förvaltningens digitalisering*. SOU 2018:25. Stockholm 2018.

Försvarets materielverk. *Begrepp och förkortningar ISD 3.1*. bil 1. Stockholm, 2021.

Försvarets radioanstalt. Cybersäkerhet i Sverige 2022 Del 1: Hot, metoder, brister och beroenden. Stockholm, 2022. https://www.fra.se/download/18.48bef1f8184f6f888031cb/1673517570877/NCSC_Rapport_1_Cybersakerhet_i_Sverige_2022-hot_metoder_brister_och_beroenden.pdf

Försvarets radioanstalt. *Årsrapport 2022*. Stockholm, 2022. Hämtad 7 december 2023 https://www.fra.se/download/18.54ed4de8186313dc35672/1678969108444/FRA-arsrapport-2022-Uppslag.pdf

Försvarsdepartementet *Lag (1992:1403) om totalförsvar och höjd beredskap.* Stockholm, 1992. Hämtad 7 december 2023 https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-19921403-om-totalforsvar-och-hojd_sfs-1992-1403/

Försvarsdepartementet. *Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. Kommittédirektiv Sverige*. Dir. 2023.30. Regeringen, 2023

Försvarsdepartementet. *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter*. Fö2019/01330. Stockholm 2020.

Försvarsdepartementet. *Prop. 2001/02:10. Fortsatt förnyelse av totalförsvaret*. Stockholm, 2001. Hämtad 26 maj 2023.

Försvarsdepartementet. *Prop. 2001/02:158. Samhällets säkerhet och beredskap.* Stockholm, 2001. Hämtad 26 maj 2023.

Försvarsdepartementet. *Prop. 2005/06:133. Samverkan i kris – för ett säkrare samhälle*. Stockholm 2005.

Försvarsdepartementet. *Förordningen (2008:1002) Instruktion för Myndigheten för samhällsskydd och beredskap.* 11 a §. Stockholm, 2008. Hämtad 22 augusti 2023. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20081002-med-instruktion-for_sfs-2008-1002/

Försvarsdepartementet. *Prop. 2020/21:30. Totalförsvaret 2021-2025.* Stockholm, 2019.

Finansdepartementet. *Prop 2020/21:1. Budgetpropositionen för 2021.* Stockholm, 2020.

Försvarsdepartementet. *Förordning (2022:524) om statliga myndigheters beredskap.* Stockholm, 2022. Hämtad 22 augusti 2023. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-2022524-om-statliga-myndigheters_sfs-2022-524/

Försvarsdepartementet. *Uppdrag att lämna förslag på hur en ändamålsenlig och effektiv ledning, organisering och styrning av Nationellt cybersäkerhetscenter ska utformas (Fö2023/01606).* Stockholm 2023. Hämtad 30 augusti 2023. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/kommitteberattelse/uppdrag-att-lamna-forslag-pa-hur-en-andamalsenlig_hbb2f%C3%B6a/

Försvarsdepartementet. *Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. Kommittédirektiv Sverige*. Dir. 2023.30. Stockholm, 2023. Hämtad 7 december 2023 https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2023/03/dir.-202330

Försvarsmakten, ”Begrepp avseende cyberområdet, bil 1”. Stockholm, 2016.

Försvarsutskottet. Försvarsutskottets betänkande. *Samverkan vid kris - för ett säkrare samhälle,* 2005/06:FöU9. Stockholm, 2005.

Försvarsutskottet. Försvarsutskottets betänkande. *Samhällets säkerhet och beredskap, 2001/02:FÖU10.* Stockholm, 2001.

Ingemarsdotter Jenny, Eidenskog Daniel & Hedtjärn S Vidar. *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur.* FOI-R--4814—SE. Totalförsvarets forskningsinstitut. Stockholm, 2020.

Ivert Anna-Karin & Mellgren Caroline. *Student, forskning och etik.* I: Mellgren C, Tiby E, (Red) Kriminologi – En studiehandbok. Lund, 2021. Studentlitteratur, (s 89-110).

Johansson Morgan. *Nationell strategi för samhällets informations- och cybersäkerhet*. Skr. 2016/17:213. Stockholm 2016.

Justitiedepartementet. *Förordning 2015:1052 Om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.* Stockholm, 2015. Hämtad 7 december 2023

https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-20151052-om-krisberedskap-och_sfs-2015-1052/

Justitiedepartementet. *Ansvar, ledning och samordning inom civilt försvar Dir. 2018:79.* Stockholm, 2018. Hämtad 7 december 2023 https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2018/08/dir.-201879

Justitiedepartementet. *Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022.* Ju2018/03737/SSK. Stockholm, 2018.

Justitiedepartementet. *Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter (Fö2019/01330).* Hämtad 7 december 2023 https://www.regeringen.se/regeringsuppdrag/2020/12/uppdrag-om-fordjupad-samverkan-inom-cybersakerhetsomradet-genom-ett-nationellt-cybersakerhetscenter/

Justitiedepartementet. *Uppdrag till Myndigheten för samhällsskydd och beredskap att vidta förberedelser för att bli nationellt samordningscenter kopplat till det europeiska kompetenscentret för cybersäkerhet (Ju2021/03097).* Stockholm, 2021. Hämtad 7 december 2023. https://www.regeringen.se/contentassets/57ec4caeaa8341de86defee60b3aae85/uppdrag-till-msb-att-vidta-forberedelser-for-att-bli-nationellt-samordningscenter-kopplat-till-det-europeiska-kompetenscentret-for-cybersakerhet.pdf

Kelly John. *What does the U.S. cybersecurity czar do?* 2023. Hämtad 7 december 2023 https://computer.howstuffworks.com/cybersecurity-czar.htm

Kinberg B Anna. *Staten och betalningarna, SOU 2023:16.* Hämtad 7 december 2023 *https://www.regeringen.se/contentassets/c01377cf65424cf0b12addf64c04374a/staten-och-betalningarna-del-1-av-2-kapitel-1-18-sou-202316.pdf*

Klimat- och näringslivsdepartementet. *Prop. 2004/05:175. Från IT-politik för samhället till politik för IT-samhället* Stockholm, 2004.

Kristersson Ulf et. al. *FRA får ta över ansvaret för Sveriges cybersäkerhet*. DN.se, publicerad torsdag 27 april 2023. https://www.dn.se/debatt/fra-far-ta-over-ansvaret-for-sveriges-cybersakerhet/ (hämtad december 2023).

Landsbygds- och infrastrukturdepartementet. *Förordning om horisontella cybersäkerhetskrav för produkter med digitala inslag*. 2022/23:FPM6.

Liljeheden Andreas. *Nederländerna varnar för solcellsanläggningar – risk även i Sverige*. Sveriges Radio. Hämtad 25 oktober 2023. https://sverigesradio.se/artikel/nederlanderna-varnar-for-solpaneler-risk-aven-i-sverige

Myndigheten för digital förvaltning. *Digitala Sverige 2022 En samlad analys av samhällets digitalisering.* Stockholm, 2023. Digitala Sverige 2022 (digg.se)

Myndigheten för samhällsskydd och beredskap. *Om statliga myndigheters risk- och sårbarhetsanalyser*. MSBFS 2009:10. Stockholm 2009.

Myndigheten för samhällsskydd och beredskap. *Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av krisberedskapsförmåga*. s. 66-70. Stockholm 2012.

Myndigheten för samhällsskydd och beredskap. *Samlad bedömning av samhällets krisberedskapsförmåga 2013 – Komplettering av regeringsuppdrag nummer.* Dnr 2013-5294.*26*. s. 16. Stockholm 2013.

Myndigheten för samhällsskydd och beredskap. *MSBFS 2016:2 föreskrifter och allmänna råd om statliga myndigheters rapportering av IT-incidenter*. Stockholm, 2016.

Myndigheten för samhällsskydd och beredskap. *MSBFS 2016:7 föreskrifter och allmänna råd om statliga myndigheters risk- och sårbarhetsanalyser.* Stockholm, 2016.

Myndigheten för samhällsskydd och beredskap (MSB). *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. Utgåva 4. Advant Produktionsbyrå Tryck DanagårdLiTHO (s. 24-26). Stockholm, 2018.

Myndigheten för samhällsskydd och beredskap. *Samlad informations- och cybersäkerhetshandlingsplan 2019-2022.* S. 16, 17, 18. Stockholm 2018. Hämtad 7 december 2023 https://rib.msb.se/filer/pdf/29920.pdf

Myndigheten för samhällsskydd och beredskap. *MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter*. Stockholm, 2020. Hämtad 6 juni 2023.

https://www.msb.se/sv/regler/gallande-regler/krisberedskap-och-informationssakerhet/msbfs-20206/

Myndigheten för samhällsskydd och beredskap. *Betänkandet SOU 2021:25 - Struktur för ökad motståndskraft.* Stockholm 2021.

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

Myndigheten för samhällsskydd och beredskap. *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – redovisning 2021*. Stockholm 2021.

Myndigheten för samhällsskydd och beredskap. *Nationell risk- och sårbarhetsbedömning (NRSB) 2023 Enligt 2 § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap*. Stockholm 2023. Hämtad 6 september 2023. Https://www.msb.se/contentassets/e1e46c8ec261465984a510eb5275c0cc/nationell-risk-och-sarbarhetsbedomning-nrsb-2023.pdf

Myndigheten för samhällsskydd och beredskap. *NIS-direktivet*. Stockholm, 2021. Hämtad 2023-10-12. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/

Myndigheten för samhällsskydd och beredskap. *När kriget kom nära – Årsrapport it-incidentrapportering 2022.* Stockholm 2023. Hämtad 12 oktober 2023. https://www.msb.se/sv/publikationer/nar-kriget-kom-nara--arsrapport-it-incidentrapportering-2022/

Myndigheten för samhällsskydd och beredskap. *Policyöversikt Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*. Stockholm. 2023. Hämtad 12 oktober 2023. https://www.msb.se/contentassets/846ae8ad37e44b20b442f3c44eed0c9e/policyoversikt-eucyber_v1.1.pdf .

Myndigheten för samhällsskydd och beredskap. *Betalningar och kontanter i kris.* Hämtad 2 november 2023. https://www.msb.se/sv/rad-till-privatpersoner/forbered-dig-for-kris/hemberedskap---preppa-for-en-vecka/betalningar-och-kontanter/.

Nationalencyklopedin. *Delegering*. Hämtad 25 oktober 2023. Https://www.ne.se/uppslagsverk/encyklopedi/lång/delegering

Norrby Catrin. *Samtalsanalys. Så gör vi när vi pratar med varandra.* Lund: Studentlitteratur AB. 2014, s. 33.

Näringsdepartementet. *IT-propositionen (1999/00:86).- Ett informationssamhälle för alla*. Stockholm, 1999. Hämtad 26 maj 2023. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/ett-informationssamhalle-for-alla_gn0386/

Olsén Mari, Valassi Christian & Stenérus Ann-Sofie Dover. *NCS3 – Ett skepp kommer lastat En kartläggning av informationsflöden, cyberfysiska system och aktörer inom svenska hamnar*. FOI-R--5405—SE. Totalförsvarets forskningsinstitut. Stockholm, 2023.

Overman Sjors. *Great Expectations of Public Service Delegation: A systematic review, Public Management Review*. 2016, s. 1238-1262. DOI: 10.1080/14719037.2015.1103891

Parsons Melissa. *The Humanity and Evolution of Cyber.* 2021. Hämtad 11 November 2023. https://www.tripwire.com/state-of-security/humanity-and-evolution-of-cyber

Post och Telestyrelsen. *Förutsättningar för att inrätta en särskild funktion för IT-incidentrapportering,* Dnr 99-194489. Stockholm, 2000.

Regeringen. *Inrättande av Myndigheten för totalförsvarsanalys.* Kommittédirektiv Dir. 2022:119. Stockholm, 2022.

Regeringen. *Riksrevisionens rapport om digitala tjänster till privatpersoner*. Regeringens skrivelse 2023/24:7. Stockholm 2023. Https://www.regeringen.se/contentassets/f6e51fc704b842ec86c47efdb07bbfba/riksrevisionens-rapport-om-digitala-tjanster-till-privatpersoner-skr.-2023247.pdf

Regeringskansliet. Rättsliga dokument. Hämtad 25 oktober 2023. Https://www.regeringen.se/rattsliga-dokument/#1238

Regeringskansliet. *SOU 2015:23. Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.* Stockholm 2015. Hämtad 2023-06-02 Https://www.regeringen.se/contentassets/8ae8ef6d5d3f45058c981cbab4e297de/informations--och-cybersakerhet-i-sverige.-strategi-och-atgarder-for-saker-information-i-staten-sou-201523

Regeringskansliet. *SOU 2001:41. Strategi för ökad IT-säkerhet och skydd mot informationsoperationer.* Stockholm 2001.

Regeringskansliet. *SOU 2021:103. Totalförsvarsanalys – en oberoende myndighet för uppföljning och utvärdering. Betänkande av*

Utredningen om totalförsvarsanalys. Stockholm 2021. Hämtad 2023-10-24

Regeringskansliet. *SOU 2021:25 Struktur för ökad motståndskraft*. Stockholm 2021. Hämtad 2023-06-02

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

Regeringskansliet. *Inrättande av Myndigheten för totalförsvarsanalys.* Kommittédirektiv. 2022:119. Stockholm, 2022. Hämtad 7 september 2023. Https://www.riksdagen.se/sv/dokument-och-lagar/dokument/kommittedirektiv/inrattande-av-myndigheten-for-totalforsvarsanalys_HAB1119/

Regeringskansliet. *Nationell strategi för samhällets informations- och cybersäkerhet*. Hämtad 2023-09-02. www.regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet/

Regeringskansliet. *Rättsliga dokument*. Hämtad 25 oktober 2023. www.regeringen.se/rattsliga-dokument/#1238

Riksrevisionen. *RiR 2007:10. Granskning av regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*. Stockholm 2007. Hämtad 2023-05-24. https://www.riksrevisionen.se/download/18.78ae827d1605526e94b2e595/1518435488911/RiR_2007_10.pdf

Riksrevisionen. *RiR 2014:23. Informationssäkerheten i den civila statsförvaltningen.* Stockholm 2014. Hämtad 2023-05-23 https://www.riksrevisionen.se/rapporter/granskningsrapporter/2014/informationssakerheten-i-den-civila-statsforvaltningen.html

Riksrevisionen. *Uppföljning Riksdagens behandling av regeringens skrivelse.* Stockholm, 2018. Hämtad 2023-05-23 https://www.riksrevisionen.se/rapporter/granskningsrapporter/2014/overenskommelser-mellan-regeringen-och-skl-inom-halso--och-sjukvarden---frivilligt-att-delta-men-svart-att-tacka-nej/uppfoljning.html

Riksrevisionen. *RiR 2023:6. Digitala tjänster till privatpersoner – stora utvecklingsmöjligheter för statliga myndigheter.* Stockholm, 2023. Hämtad 2023-05-23. https://www.riksrevisionen.se/rapporter/granskningsrapporter/2023/digitala-tjanster-till-privatpersoner---stora-utvecklingsmojligheter-for-statliga-myndigheter.html

Riksrevisionen. *RiR 2023:8. Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* Stockholm, 2023. Hämtad 2023-05-23. https://www.riksrevisionen.se/rapporter/granskningsrapporter/2023/regeringens-styrning-av-samhallets-informations--och-cybersakerhet---bade-bradskande-och-viktig.html

Sapienza Zachary. Veenstra S Aaron., Kirtiklis Kestas & Giannino S Steve. *The transmission model of communication: Toward a multidisciplinary explication. ETC: A Review of General Semantics*, *73* (4), 321-341. 2016.

Siegenfeld Alexander. F, & Bar-Yam Yaneer. *An introduction to complex systems science and its applications*. Complexity, 2020, s. 1-16.

Statskontoret. *Sammanhållen strategi för samhällets IT-säkerhet* (1998:18). Stockholm, 1998.

Statsrådsberedningen. *Förordning (1996:1515) med instruktion för Regeringskansliet*. Stockholm, 1996. Hämtad 3 september 2023. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-19961515-med-instruktion-for_sfs-1996-1515/

Stenerus Ann-Sofie, Bengtsson Johan & Olsson Matilda. *IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering*. Totalförsvarets forskningsinstitut. Stockholm, 2020. FOI-R--4815—SE

Sternudd, Patrik. *Cyberförsvar och cybersäkerhet: strukturer, ansvar och författningar 202*3. Kungliga krigsvetenskapsakademin. Stockholm, 2023. Hämtad 12 september 2023. https://kkrva.se/cyberforsvar-och-cybersakerhet-strukturer-ansvar-och-forfattningar/

Säkerhetspolisen. Årsrapport för 2022. Stockholm, 2023. https://sakerhetspolisen.se/download/18.36cda2851868025da5b2b/1677241538918/SP_A%CC%8Arsbok_2022__Anpassad.pdf

Utbildningsdepartementet. *Prop. 2008/09:96. Behandling av personuppgifter inom studiestödsområdet.* Stockholm 2008.

Waleij Annica, Simonsson Louise & Liljedahl Birgitta. *Konsekvenser av energibortfall på samhällets funktionalitet och civilbefolkningens*

hälsa. FOI-R--4755—SE. Totalförsvarets forskningsinstitut. Stockholm, 2019.

Wiener Norbert. *Cybernetics, or control and communication in the animal and the machine* (2nd ed.). John Wiley & Sons, Inc.; Boston Review. 1961. Hämtad 12 september 2023 https://doi.org/10.1037/13140-000

Wilson Mark. *Information technology security training requirements: A role- and performance-based model*. 1998. Hämtad 12 september 2023. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Bilaga 1 – Centrala begrepp och koncept

I detta avsnitt beskrivs centrala begrepp som används i rapporten.

- **Cyber**
  Cyber är ett samlingsbegrepp och framför allt ett prefix.[99]

- **Cyberförsvar**
  Definieras som en nations eller annan aktörs samlade förmågor och åtgärder i digitala system, såväl offensiva som defensiva, till skydd för dess kritiska samhällsfunktioner i den digitala domänen samt förmågan att försvara sig mot kvalificerade angrepp.[100]

- **Cybersäkerhet**
  Cybersäkerhet är den samling av säkerhetsåtgärder, tekniker och riskhanteringsmetoder som kan användas i syfte att bevara konfidentialitet, spårbarhet, tillgänglighet och riktighet i cyberrymden. Cybersäkerhet är en delmängd av informationssäkerhet. Informationssäkerhet omfattar även åtgärder utanför cyberrymden.[101]

- **Informationssäkerhet**
  Informationssäkerhet innebär bevarande av konfidentialitet, riktighet och tillgänglighet hos information” med tillägget att det även kan ”inkludera egenskaper som autenticitet, ansvarsskyldighet, oavvislighet och tillförlitlighet”.[102]

- IT-**säkerhet**
  I IT-säkerhet inkluderas kommunikationssäkerhet. IT-säkerhet ingår som en del i informationssäkerheten.[103]

- **Totalförsvar**
  Enligt lag (1992:1403) om totalförsvar och höjd beredskap definieras totalförsvar enligt följande: *”Totalförsvar är verksamhet som behövs för att förbereda Sverige för krig.*[104]

[99] Försvarsmakten. *Begrepp avseende cyberområdet, bil 1*. 2016.
[100] Ibid.
[101] Försvarsmakten. *Begrepp avseende cyberområdet, bil 1*. 2016.
[102] Svensk Standard (2017). SS-EN 27000
[103] Försvarsmakten. *Begrepp avseende cyberområdet, bil 1”.* Stockholm, 2016.
[104] 1§ Lag (1992:1403) *om totalförsvar och höjd beredskap*.

Bilaga 2 – Litteraturgenomgång 1990–2023

I denna bilaga beskrivs en litteraturstudie av explorativ karaktär. Med hjälp av olika dokument, exempelvis lagrum och andra regleringar, bidrar bilagan med en historisk tillbakablick.

1995–1996

Ett av de första försöken att organisera ansvaret för informations- och cybersäkerhet är den brittiska standard som skapades 1995 i syfte att på ett systematiskt sätt styra en verksamhets informationssäkerhet. Den blev 1999 en internationell standard vid namn ISO/IEC 17799. I Sverige går den från 1999 under benämningen *Ledningssystem för informationssäkerhet (LIS)* eller *ISO 27000* och kan tillämpas på alla typer av verksamheter med syftet att förbättra den interna kontrollen av informationssäkerheten.[105]

Svenska regeringar har under flera decennier gett förslag på hur hanteringen och användningen av internet i Sverige bör se ut och hur internets påverkan på informationssäkerheten bör regleras. Under 1995 beslutades förordning (1995:1300) *Om statliga myndigheters riskhantering* i vilken det ställdes krav på att myndigheter ska identifiera risker som skulle kunna innebära förluster eller skador i myndighetens verksamhet. I förordningen framgår det även att myndigheter ska vidta lämpliga åtgärder för att begränsa dessa eventuella risker.[106] Så tidigt som 1996 framgick det i förordningen (1996:1515) med instruktion för Regeringskansliet att ansvaret för förvaltnings- och lagstiftningsärenden om informationssäkerhet låg på Justitiedepartementet.[107] Proposition (1995/96:125) *Om åtgärder för att bredda och utveckla användningen av informationsteknik* lämnades in av regeringen 1996. Riksdagen besvarade propositionen med att det fanns behov av ett mer samordnat ansvar för det som då kallades "IT-säkerhetsfrågorna" och beslutade att regeringen skulle inkomma med en mer utvecklad strategi på området. I uppdraget var regeringen tydlig med utgångspunkten att all information som företag och individer behövde få från myndigheter skulle vara tillgänglig elektroniskt. [108] I den nya strategin skulle statens ansvar preciseras och IT-säkerhetsarbetet skulle organiseras.[109]

1997–2001

[105] Riksrevisionen. *Informationssäkerhetsarbete på nio myndigheter*. RiR 2016:8. Stockholm, 2016.
[106] Finansdepartementet. *Förordning (1995:1300) om statliga myndigheters riskhantering*. Stockholm, 1995.
[107] Statsrådsberedningen. *Förordning (1996:1515) med* instruktion för Regeringskansliet. Stockholm, 1996.
[108] Statskontoret. *Sammanhållen strategi för samhällets IT-säkerhet (1998:18)*. Stockholm, 1998.
[109] Regeringskansliet. *Strategi för ökad IT-säkerhet och skydd mot informationsoperationer. SOU 2001:41*. Stockholm 2001.

En första nationell strategi för det som då kallades ”samhällets IT-säkerhet” togs fram av Statskontoret 1998 och innehöll förslag på bland annat att alla myndigheter med samhällsviktig information borde göra risk- och sårbarhetsanalyser. I strategin ingick även förslag på ändringar i lagstiftningen för att harmonisera med det som då kallades ”det nya IT-samhället”.[110] År 1998 tillsattes en arbetsgrupp av regeringen som utredde skydd mot informationskrigföring vid namn Sårbarhets- och säkerhetsutredningen. Denna arbetsgrupp gav förslag på liknande åtgärder som framgick i den nationella strategin som Statskontoret tagit fram.[111]

I IT-propositionen (1999/00:86) *Ett informationssamhälle för alla* konkretiserades den nationella strategin som Statskontoret tagit fram. I propositionen framgick det att informationssäkerhetsfrågor skulle ingå i det prioriterade området “tilliten till IT” där ambitionen var att IT-system och regler skulle vara säkra, teknikneutrala och förutsägbara. Vidare var ambitionen att IT-systemen skulle skydda individens identitet och vara internationellt erkända. I propositionen skrev regeringen att IT-politiken inte är ett tekniskt projekt utan ett demokratiskt sådant och som handlar om att ge alla människor tillgång till den nya teknikens möjligheter. Sverige ansågs då vara en av de ledande IT-nationerna i världen. Regeringen införde samma år målet att Sverige skulle bli det första landet som gör informationssamhället tillgängligt för alla.[112]

I propositionen *Fortsatt förnyelse av totalförsvaret* (2001/02:10) skrev regeringen att det var angeläget att ett nationellt harmoniserat regelverk upprättas för att säkerställa överblick och samordning av olika regler och för att skapa sammanhållna och entydiga bestämmelser avseende informationssäkerhet.[113] Samma år presenterade regeringen en strategi med tillhörande ansvarsprincip i proposition 2001/02:158, *Samhällets säkerhet och beredskap*. Det framgick där att ansvaret för informationssäkerhet skulle ligga hos de företag, myndigheter och organisationer som hade det normala verksamhetsansvaret. Med utgångspunkt från tidigare förslag från Sårbarhets- och säkerhetsutredningen och Statskontorets nationella strategi presenterade regeringen i proposition 2001/02:158 även fyra verksamhets- och ansvarsområden för fyra olika myndigheter. Det första ansvarsområdet var att skapa en sammanhållande funktion som skulle ansvara för omvärldsanalys och denna funktion lades på dåvarande Krisberedskapsmyndigheten (KBM).[114] Det andra området ansvarade FMV för och gick ut på att evaluera och certifiera IT-säkerhetsprodukter. FRA fick det tredje ansvarsområdet teknikkompetens. I det fjärde ansvarsområdet skulle PTS ansvara för en IT-incidenthanteringsfunktion

[110] Statskontoret. *Sammanhållen strategi för samhällets IT-säkerhet.* Stockholm 1998.
[111] Regeringskansliet. *Strategi för ökad IT-säkerhet och skydd mot informationsoperationer. SOU 2001:41*. Stockholm 2001.
[112] Näringsdepartementet. *IT-propositionen (1999/00:86).- Ett informationssamhälle för alla*. Stockholm, 1999.
[113] Regeringskansliet. *Prop. 2001/02:10. Fortsatt förnyelse av totalförsvaret*. Stockholm, 2001.
[114] Krisberedskapsmyndigheten grundades 2002, och ersattes 2009 av Myndigheten för Samhällsskydd och Beredskap.

och inrättade därmed Sitic.[115] Sitic som funktion hade redan föreslagits av Sårbarhets- och säkerhetsutredningen 1998.[116]

I sitt betänkande av båda propositionerna som presenterats 2001 underströk försvarsutskottet vikten av tvärsektoriella lösningar och samordning för att skapa ett skydd för hela samhället mot informationsoperationer. I betänkandet framgick det även att de förslag som regeringen lagt fram borde ses som delar i en utvecklingsprocess samt att uppföljning och översyn av arbetet skulle genomföras under de kommande åren. Detta uppföljningsarbete skulle sedan redovisas för riksdagen enligt försvarsutskottets betänkande.[117]

2002–2007

För att underlätta samarbetet mellan de ansvariga myndigheterna KBM, PTS, FMV och FRA kring strategin som föreslagits i proposition *Samhällets säkerhet och beredskap* (prop. 2001/02:158) skapades samverkansgruppen för informationssäkerhet (SAMFI) 2003. Vid skapandet av gruppen anslöt även MUST, Säpo och Rikskriminalpolisen.[118]

År 2005 presenterade regeringen några preciseringar gällande begrepp för säkrare användning av internet i propositionen *Från IT-politik för samhället till politik för IT-samhället* (2004/05:175). Samma år påpekade regeringen i en ny proposition (2005/06:133, *Samverkan i kris – för ett säkrare samhälle*) att den framtagna nationella strategin för IT-säkerhet (*Sammanhållen strategi för samhällets IT-säkerhet* av Statskontoret (1998:18)) nu var gammal och behövde utvecklas. De förberedande och förebyggande åtgärderna ansågs nu behöva bli en del av varje myndighets sektorsansvar.[119] I en annan proposition (2005/06:133)[120] från samma år ansåg regeringen vidare att skyddet av personlig integritet skulle förbättras i syfte att upptäcka, agera och ingripa i samband med störningar. Det ansågs också att det behövdes insatser från rättsvårdande myndigheter och att dessa skulle ha förmåga att hantera och förhindra allvarliga störningar i samhällsviktig verksamhet. Regeringen gav dåvarande KBM i uppdrag att ta fram en handlingsplan och mål för informationssäkerheten för att på bästa sätt kunna genomföra strategin. Grunden för det fortsatta arbetet skulle utgöras av målen, krav på tillämpning av standarder, kompletterande åtgärder för informationssäkerhet samt krav på prestationsförmåga eller säkerhet för samhällsviktig verksamhet.[121]

---

[115] Regeringskansliet. *Prop. 2001/02:158. Samhällets säkerhet och beredskap.* Stockholm, 2001.
[116] Post och Telestyrelsen. *Förutsättningar för att inrätta en särskild funktion för IT-incidentrapportering.* Stockholm, 2000.
[117] Försvarsutskottet. *Försvarsutskottets betänkande. Samhällets säkerhet och beredskap, 2001/02:FÖU10*. Stockholm, 2001.
[118] Regeringskansliet. *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.* SOU 2015:23. Stockholm 2015.
[119] Försvarsdepartementet. *Prop. 2005/06:133. Samver*kan i kris – för ett säkrare samhälle. Stockholm 2005.
[120] Ibid.
[121] Ibid.

Försvarsutskottet gjorde flera anmärkningar i sitt betänkande rörande propositionen (2005/06:133). Dessa anmärkningar presenterades tillsammans med tre motioner. Regeringen fick bland annat kritik för sin hantering av informationssäkerhetsfrågorna där försvarsutskottet ställde krav på bättre och tydligare utvärdering av incidenthantering och skapandet av en generell säkerhetspolicy.[122] Denna kritik visades återkommande under åren som följde. Försvarsutskottet ansåg inte att regeringen presenterat åtgärder som avsåg myndigheternas ansvar för kontroll och intern styrning av informationssäkerhet. Inga krav ställdes heller på en sådan rapportering eller återkoppling som efterfrågades av försvarsutskottet redan 2001.[123]

Åren 2005–2007 genomförde Riksrevisionen en granskning av elva myndigheters[124] arbete med informationssäkerhet och regeringens styrning av myndigheternas informationssäkerhetsarbete. Under denna tidsperiod var ansvaret för ledning och styrning av statsförvaltningens informationssäkerhetsarbete fördelat mellan regeringen, riksdagen och de sju av regeringen utsedda tillsyns- och stödmyndigheterna[125] samt övriga myndigheters ledning. I Riksrevisionens resultat framkom det bland annat brister i säkerhetsarbetet på de sju myndigheterna men även i regeringens uppföljning och styrning av arbetet. Vidare ansågs inte regeringen ha vidtagit tillräckliga initiativ för att effektivisera arbetet med informationssäkerheten i myndigheterna. Riksrevisionen ansåg att regeringen inte gett tillräcklig styrning och mandat för de utvalda expertmyndigheterna där kraven på de enskilda myndigheterna borde anpassas utifrån myndigheternas förmågor.[126]

2008–2013

År 2008 utfärdade Verket för Förvaltningsutveckling (Verva) föreskrifter med krav på att myndigheter under regeringen skulle tillämpa tidigare nämnda ledningssystem för informationssäkerhet (LIS).[127] Under åren 2008 och 2009 skrev regeringen att teknisk infrastruktur för den kommunikation som offentlig förvaltning ger medborgarna borde bygga på internetstandarder. Vidare skrev regeringen att det i internetbaserade tekniker fanns en stor utvecklingspotential som skulle bidra till att öka förvaltningens öppenhet. Regeringens ambitioner för IT-stöd i den

[122] Försvarsutskottet. *Försvarsutskottets betänkande. Samverkan vid kris - för ett säkrare samhälle*, 2005/06:FöU9. Stockholm, 2005
[123] Ibid
[124] Endast myndigheter som tillhörde statsförvaltningens största myndigheter och har omfattande skyddsvärda informationstillgångar granskades.
[125] Krisberedskapsmyndigheten (KBM), Säkerhetspolisen (SÄPO), Post- och telestyrelsen (PTS), Försvarets radioanstalt (FRA), Försvarets Materielverk (FMV), Datainspektionen (DI) samt Verket för Förvaltningsutveckling (Verva).
[126] Riksrevisionen. *Granskning av regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*. Stockholm 2007.
[127] Riksrevisionen. *Informationssäkerheten i den civila statsförvaltningen.* RiR 2014:23. Stockholm *2014.S. 67.*

statliga förvaltningen var mycket höga och beroendet av uppkoppling och IT blev allt större i samhället i stort.[128]

I samband med att MSB skapades 2009 tog de över huvudansvaret för tidigare nämnda SAMFI-gruppens arbete.[129] Ur MSB:s föreskrifter om *statliga myndigheters risk- och sårbarhetsanalyser* (MSBFS 2009:10) framgår det att de myndigheter som har ett särskilt ansvar för krisberedskap ska redovisa sina förmågor relaterat till informationssäkerhetsfrågor på ett antal punkter. Respektive myndighet som då hade ett särskilt ansvar för krisberedskap skulle redovisa en bedömning av om det fanns tillräckligt god förmåga hos myndigheten att upprätthålla informationstillgångarnas riktighet, tillgänglighet och konfidentialitet. Dessutom skulle de myndigheter som bedriver samhällsnyttig verksamhet bedöma sin förmåga till robusthet och redundans för myndighetens kommunikationssystem (radio, IT och tele).[130] Med stora delar av Vervas föreskrifter som förlaga trädde MSB:s verkställighetsföreskrifter om ledningssystem för informationssäkerhet i kraft 2010. I stort sett alla myndigheter under regeringen skulle därmed bedriva sina arbeten enligt svensk standard (LIS) och tillämpa föreskrifternas paragrafer. Vidare framgick det i föreskrifterna att det var ledningen för respektive myndighet som ansvarade för att minst en gång om året följa upp och utvärdera arbetet med informationssäkerhet. MSB hade under denna tid ett särskilt uppdrag och särskild funktion inom området samhällets informationssäkerhet med att stödja och samordna arbetet, bedöma och analysera omvärldsutvecklingen samt lämna stöd och råd i fråga om förebyggande insatser till behövande myndigheter. MSB skulle även rapportera till regeringen om förhållanden på området som skulle kunna leda till behov av åtgärd.[131] En viktig poäng som påverkade MSB:s arbete var att myndigheterna inte hade någon skyldighet att rapportera varken sina uppföljningar, utvärderingar på arbetet eller IT-incidenter till MSB. Dessa uteblivna skyldigheter resulterade i att MSB var beroende av att såväl privata aktörer som myndigheter lämnade in uppgifterna frivilligt. Det försvårade MSB:s rapporteringsuppdrag gentemot regeringen.[132]

I sitt regleringsbrev från år 2012 fick MSB i uppdrag av regeringen att genomföra ett arbete med en nationell bedömning avseende sårbarheter, risker och förmågor i Sverige. Syftet med uppdraget var att skapa en gemensam förståelse för allvarliga risker i landet. Som resultat publicerade MSB 2012 rapporten *Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive*

[128] *Klimat- och näringslivsdepartementet. Prop. 2004/05:175. Från IT-politik för samhället till politik för IT-samhället Stockholm, 2004.s. 64.*
[129] *Regeringskansliet. Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. SOU 2015:23. Stockholm 2015.*
[130] *Myndigheten för samhällsskydd och beredskap. Om statliga myndigheters risk- och sårbarhetsanalyser. MSBFS 2009:10. Stockholm 2009.*
[131] *Regeringskansliet. Förordningen (2008:1002) Instruktion för Myndigheten för samhällsskydd och beredskap. 11 a §.*
[132] *Riksrevisionen. Informationssäkerheten i den civila statsförvaltningen. RiR 2014:23. Stockholm 2014.S. 67.*

bedömning av krisberedskapsförmåga vilken ämnade ge stöd till det gemensamma uppdraget att utveckla beredskapen och samhällsskyddet på regional och lokal nivå. Utifrån ett antal indikatorer undersökte MSB krisberedskapsförmågan där även informationssäkerhet var inkluderad. I korthet visade undersökningen att informationssäkerhetsarbetet tycktes variera mellan de olika aktörerna samt att informationssäkerhetsförmågorna förutspåddes förändras i takt med den snabba pågående utvecklingen på området. Det medförde enligt MSB nya möjligheter men även risker beroende på hur myndigheterna valde att hantera säkerhetsarbetet med den snabba tekniska utvecklingen.[133]

Under 2013 gick MSB, på uppdrag av Riksrevisionen, igenom 23 myndigheters hantering av informationssäkerhet utifrån deras risk- och sårbarhetsanalyser. Ur resultatet framgick att varken informationssäkerhetsarbetet eller cybersäkerhetsarbetet behandlades i någon av myndigheternas analyser trots uttryckta krav i föreskrifter från MSB (exempelvis MSBFS 2009:10). De gånger informationssäkerhetsområdet omnämndes i någon av de 23 myndigheternas analyser bedömde MSB att det var till följd av att den aktuella myndigheten ansåg att det vid tillfället förelåg ett (prioriterat) hot på området. Granskningen visade att ingen av de 23 myndigheterna valde att beskriva sin informationssäkerhet enligt rekommenderade LIS-standarder från 1999 trots kravet som utfärdades av Verva 2008 och MSB:s verkställighetsföreskrifter om ledningssystem för informationssäkerhet från 2010.[134]

2014–2019

År 2014 publicerade MSB ett PM (MSB: PM 2014-04-24 *Samlad bedömning av samhällets krisberedskapsförmåga 2013 – Komplettering av regeringsuppdrag nummer 26*) som kompletterade tidigare regeringsuppdrag och där det framgick att myndigheters behov att samverka med andra aktörer inom området för informationssäkerhet enbart delvis var identifierat och tillgodosett. Enligt MSB kunde det bero på att det var svårt för myndigheterna att identifiera vilken informationshantering som ansågs vara samhällsviktig i Sverige samt vilka verksamheter som hade ett direkt samverkansbehov vid en störning.[135]

I syfte att utreda den civila statsförvaltningens arbete med informationssäkerhet publicerade Riksrevisionen år 2014 en ny revision. Utredningen var inspirerad av MSB-rapporten som släpptes 2012 (*Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av*

[133] Myndigheten för samhällsskydd och beredskap. *Risker och förmågor 2012 – Redovisning av regeringsuppdrag om nationell riskbedömning respektive bedömning av krisberedskapsförmåga*. s. 66-70. Stockholm 2012.

[134] Riksrevisionen. *Informationssäkerheten i den civila statsförvaltningen. RiR 2014:23.* Stockholm 2014. s. 47

[135] Myndigheten *för samhällsskydd och beredskap. Samlad bedömning av samhällets krisberedskapsförmåga 2013 – Komplettering av regeringsuppdrag nummer.* Dnr 2013-5294.26Stockholm 2013. s. 16.

krisberedskapsförmåga) och utredningen granskade huruvida regeringens styrning av informationssäkerhet ansågs vara tillräckligt effektiv. Regeringens stöd- och tillsynsmyndigheter granskades även utifrån om de vidtagit tillräckliga åtgärder för att informera sig och regeringen om vilka hot som fanns mot den civila statsförvaltningen, i vilken omfattning åtgärderna realiserats samt vilka skyddsåtgärder som vidtagits. Likt den granskning som publicerades 2007 ansåg Riksrevisionen 2014 att arbetet med informationssäkerheten inte var tillräckligt ändamålsenligt då regeringen saknade en samlad lägesbild för förmågan att hantera en allvarlig incident. Regeringens styrning av informationssäkerheten ansågs av Riksrevisionen inte vara effektiv i den civila statsförvaltningen samtidigt som de utsedda stöd- och tillsynsmyndigheterna inte vidtagit tillräckliga åtgärder för att förbättra arbetet. Riksrevisionens granskning 2014 utgick till viss del från de hot och risker som det allt mer digitaliserade samhället inneburit och från hur allt fler samhällsfunktioner blivit beroende av IT för att kunna verka i sina roller. I underlaget för Riksrevisionens granskning 2014 ingick även information om den sårbarhet som det inneburit att allt fler tekniska system blivit sammankopplade och beroende av varandra. Slutligen framkom det i granskningen att regelsystemet för informationssäkerhet inte förändrats i speciellt stor utsträckning och att de brister som påpekades vid revisionen 2007 i majoritet kvarstod 2014.[136]

Regeringen inkom med en skrivelse till riksdagen där de svarade på Riksrevisionens iakttagelser. I huvudsak instämde regeringen med det som framkommit i granskningen men påpekade att justeringar skett sedan det att 2014 års granskning påbörjades och genomfördes. Vidare lade regeringen fram förslag på justeringar i frågorna om allmän ordning, krisberedskap och säkerhet samt styrning av MSB, Polismyndigheten och Säpo. På så vis skulle det skapas bättre förutsättningar för bättre styrning av informationssäkerhetsarbetet. Vidare hade respektive myndighet med särskilt ansvar för höjd beredskap och krisberedskap fått i uppdrag att redovisa sitt arbete med informationssäkerhet. Som enskild myndighet skulle även MSB ansvara för att undersöka hur respektive kommun vid tidpunkten arbetade med informationssäkerhet. Gällande rapporteringen av IT-incidenter till MSB fattade regeringen 2015 beslut om obligatorisk inrapportering för alla statliga myndigheter.[137] Samma år publicerade Justitiedepartementet en statlig utredning *Strategi och åtgärder för säker information i staten* (SOU 2015:23) i vilken det föreslogs en strategi med tillhörande sex mål för informations- och cybersäkerhet i staten.[138] År 2015 skapades även en arbetsgrupp (Nationell Samverkan mot allvarliga IT-hot (NSIT)) bestående av FRA, SÄPO och MUST. Arbetsgruppen arbetade med bedömning av sårbarheter och hot relaterat till kvalificerade eller allvarliga IT-angrepp mot det svenska samhällets mest skyddsvärda nationella

[136] Riksrevisionen. *Informationssäkerheten i den civila statsförvaltningen. RiR 2014:23.* Stockholm 2014. s. 53.
[137] Riksrevisionen. *Uppföljning Riksdagens behandling av regeringens skrivelse.* Stockholm, 2018.
[138] Regeringskansliet. *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.* SOU 2015:23. Stockholm 2015.

intressen.[139] I förordning (2015:1052) om krisberedskap och höjd beredskap framkommer det att statliga myndigheter ska se till så att informationshanteringen uppfyller de säkerhetskrav som fastställts. Myndigheterna ska även rapportera in IT-incidenter och införa ledningssystem för informationssäkerhet.[140] Förordningen har använts flitigt av MSB som styrkande argument för att, i linje med sitt uppdrag, få in redogörelser av risk- och sårbarhetsanalyser.[141]

Riksrevisionen genomförde 2016 en uppföljning av sin tidigare granskning från 2007 och undersökte då åter de utvalda myndigheternas[142] arbete med informationssäkerhet. Vid uppföljningen ingick även regeringen med dess kansli samt Ekonomistyrningsverket. I 2016 års granskning framkom det att samtliga myndigheter fortfarande hade allvarliga brister i sina informationssäkerhetsarbeten. Ingen godtagbar nivå på arbetena uppmättes och regeringen ansågs inte ha skapat tillräckliga förutsättningar för myndigheterna att utföra det arbete som ansågs krävas. Regeringen hade tidigare beslutat att ledningen för respektive myndighet skulle intyga att den interna kontrollen och styrningen var tillräcklig, vilket den enligt Riksrevisionen 2016 alltså inte var. Myndigheterna levde helt enkelt inte upp till de kravställningar som framgick i MSB:s föreskrifter.[143] Enligt MSB:s föreskrifter från samma år (MSB 2016:2) om statliga myndigheters rapportering av IT-incidenter specificerades rapporteringskravet där en IT-incident ska rapporteras till MSB senast 24 timmar efter att den upptäcktes. Om en inträffad IT-incident ska anses behöva rapporteras avgör myndigheten själv. Myndigheterna erbjuds skriftligt stöd i bedömningen av om incidenten ska rapporteras eller ej. Myndigheterna kan även vända sig till Cert-SE för råd.[144] Cert-SE ligger under MSB och är Sveriges nationella Computer Emergency Response Team med uppgift att stötta samhället i arbetet med att hantera och förebygga IT-incidenter.

En bidragande anledning till att arbetet var fortsatt otillräckligt enligt Riksrevisionens granskning från 2016 var enligt granskningen att förståelsen för vikten av informationssäkerhet var för liten hos de granskade myndigheterna. Den begränsade förståelsen resulterade i sin tur i att informationssäkerhetsarbetet blivit nedprioriterat i förhållande till andra mer påtagliga risker. Enligt 2016 års revision hade en del av arbetet med informations- och cybersäkerhet avstannat då myndigheternas ledning visat lågt engagemang och delegerat vidare ansvaret utan att skapa rätt förutsättningar hos mottagaren, eller på något sätt följa upp arbetet lokalt hos respektive myndighet. Kunskapen om de framtagna dokumenten på

[139] Riksrevisionen. *Uppföljning Riksdagens behandling av regeringens skrivelse.* Stockholm, 2018.
[140] Regeringskansliet. *Förordning 2015:1052 Om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap.* Stockholm, 2015.
[141] Riksrevisionen. *Uppföljning Riksdagens behandling av regeringens skrivelse.* Stockholm, 2018.
[142] Affärsverket svenska kraftnät, Arbetsförmedlingen, Bolagsverket, Försäkringskassan, Lantmäteriet, Migrationsverket, Post- och telestyrelsen, Sjöfartsverket samt Statens tjänstepensionsverk.
[143] Riksrevisionen. *Informationssäkerhetsarbete på nio myndigheter.* RiR 2016:8. Stockholm, 2016.
[144] Myndigheten för samhällsskydd och beredskap. *MSBFS 2016:2 föreskrifter och allmänna råd om statliga myndigheters rapportering av it-incidenter.* Stockholm, 2016.

informations- och cybersäkerhetsområdet har enligt 2016 års revision varit genomgående låg hos såväl chefer som medarbetare bland Sveriges myndigheter. Riksrevisionen ansåg 2016 att myndigheterna hade prioriterat bort informationssäkerhetsarbetet på grund av avsaknad av direkt styrning och efterfrågan av information från regeringen. Vidare har informationssäkerhet och IT-säkerhet setts som ett hinder för myndigheternas kärnverksamhet vilket resulterat i att kravet på funktionalitet och effektivitet gått före kravet på informations- och IT-säkerhet. Nyttan av moderna IT-tjänster i vardagsverksamheten var synbar, men det var inte nyttan av säkerhetsarbete vilket gjorde det svårare att se behovet av informations-, IT- och cybersäkerhetsarbete. Det fanns inte heller ett tydligt incitament för lärande vilket hade resulterat i fokus på statistisk presentation snarare än proaktivt arbete där man beskrev dagsläget och försökte förbättra. Detta skedde inte minst gällande aspekten av förebyggande incidenthantering.[145] I den statliga utredningen SOU 2015:23 fick Justitiedepartementet i uppdrag att föreslå mål för informationssäkerhetsarbetet i samhället och hur det svenska samhället skulle upprätthålla personlig integritet och säkerhet i samhällsviktig IT-infrastruktur. Utredningen skulle även vid behov föreslå förtydligande definitioner på området. Vidare skulle ansvarsfördelningen på området presenteras för respektive statlig myndighet. Författarna till utredningen ansåg att hoten mot cyber- och informationssäkerheten inte kan hanteras med endast en nationell strategi. Istället skulle det krävas flera olika strategier, men där en första nationell strategi skulle åtgärda de mest angelägna bristerna i statsförvaltningens säkerhetsarbete på området.[146] I budgetpropositionen för 2016 skrev regeringen, bland annat mot bakgrund av Riksrevisionens granskning samma år, att det krävs ett fortsatt arbete för att stärka arbetet med informationssäkerhet.[147] Liknande formuleringar förekom senare i 2017 års budgetproposition med specificeringen att MSB skulle få ytterligare medel för att stärka informationssäkerhetsarbetet på svenska myndigheter.[148] År 2016 uppdaterades även föreskriften om statliga myndigheters risk- och sårbarhetsanalyser (MSBFS 2016:7, tidigare MSBFS 2010:7 och MSBFS 2015:3). Den nya föreskriften har revideringar för att bättre likna redan nämnda förordning (2015:1052) om krisberedskap och höjd beredskap. Den nya föreskriften syftade till att förtydliga krav på, och former för, redovisning av risk- och sårbarhetsanalyserna för de myndigheter som var ålagda att göra detta.[149]

---

[145] Riksrevisionen. *Informationssäkerhetsarbete på nio myndigheter*. RiR 2016:8. Stockholm, 2016.

[146] Regeringskansliet. *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.* SOU 2015:23. Stockholm 2015.

[147] Finansdepartementet. PROP. 2015/16:1. *Förslag till statens budget för 2016 Försvar och samhällets krisberedskap.* Stockholm 2015. utgiftsomrade-6-forsvar-och-samhallets-krisberedskap.pdf (regeringen.se) PROP. 2015/16:1. *Förslag till statens budget för 2016 Försvar och samhällets krisberedskap.* Stockholm 2015.

[148] Ibid.

[149] Myndigheten för samhällsskydd och beredskap. *MSBFS 2016:7 föreskrifter och allmänna råd om statliga myndigheters risk- och* sårbarhetsanalyser. Stockholm, 2016.

Regeringen presenterade 2016 den nya nationella strategin (Nationell strategi för samhällets informations- och cybersäkerhet Skr. 2016/17:213) för samhällets informations- och cybersäkerhet, vilken inkluderade ett antal framtagna nationella intressen som skulle utgöra vägledning tillsammans med konkreta åtgärder och ett antal målsättningar. Exempel på målsättningar var ändamålsenlig tillsyn samt ökad tydlighet i myndighetsstyrningen, vilket skulle resultera i ett systematiskt informationssäkerhetsarbete. MSB och andra bevakningsansvariga myndigheter fick diverse uppdrag för att nå målsättningarna i den nationella strategin.[150] Först två år senare vid 2018 års budgetproposition uttryckte regeringen att arbetet med cyber- och informationssäkerhet hade förbättrats, men också att det fanns stort behov av ett fortsatt arbete, inte minst utifrån att totalförsvaret behövde förstärkas. Detta var något som även visade sig i ett markant ökat budgetanslag för totalförsvaret. År 2018 infördes även det första NIS-direktivet.[151] NIS-direktivet i sig antogs av Europaparlamentet och rådet i juli 2016 och fastställde åtgärder för att uppnå en hög gemensam nivå av säkerhet i informationssystem och nätverk inom EU. Syftet var att förbättra funktionen av den inre marknaden.[152] Till följd av NIS-direktivet uppdaterade regeringen cyber- och informationssäkerhetsstrategin från 2016 som fram tills dess saknat skrivningar om styrnings- och ledningsstruktur.[153]

År 2018 grundades Myndigheten för digital förvaltning med uppgift att stödja, samordna och följa upp digitalisering inom svensk offentlig förvaltning.[154] Samma år beslutade regeringen om att ge SAMFI -myndigheterna uppdrag att skapa en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022. I beslutet framkom det även att regeringen avsåg att återkomma med fler framtida uppdrag, inte minst framtagandet av en nationell modell för systematiskt informationssäkerhetsarbete som skulle komplettera den nationella strategin från 2016.[155] År 2019 presenterade SAMFI -gruppen sin första handlingsplan i vilken det fanns 77 åtgärder som föll inom någon av de sex strategiska prioriteringarna från den nationella strategin från 2016. Handlingsplanen innehöll till stor del förslag på samordning och samverkan mellan myndigheter i syfte att ge regeringen ett bättre analysunderlag. I redovisningen framkom det vilken myndighet som var ansvarig för vilken åtgärd samt att åtgärderna sedan skulle rapporteras årligen till regeringen. Avslutningsvis skulle en slutredovisning genomföras år 2023.[156] Trots att regeringen redan 2018 antydde att det borde skapas en nationell modell för att styra

[150] Morgan Johansson. Nationell strategi för samhällets informationsoch cybersäkerhet. Skr. 2016/17:213. Stockholm 2016.
[151] Riksrevisionen. *Uppföljning Riksdagens behandling av regeringens skrivelse.* Stockholm, 2018.
[152] Myndigheten för samhällsskydd och beredskap. *NIS-direktivet.* Stockholm, 2021.
[153] Regeringskansliet. *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten.* SOU 2015:23. Stockholm 2015.
[154] Finansdepartementet. *Förordning (2018:1486) Instruktion för Myndigheten för digital förvaltning.* Stockholm, 2018
[155] Justitiedepartementet. *Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022.* Ju2018/03737/SSK. Stockholm, 2018.
[156] Försvarets radioanstalt. Samlad informations- och cybersäkerhetshandlingsplan 2019-2022.Stockholm 2018, S. 16, 17, 18.

informationssäkerhetsarbetet saknades det ett regeringsuppdrag för detta arbete. SAMFI-gruppen valde därmed 2019 att skapa en egen förstudie till en nationell modell för arbetet med informations- och cybersäkerhet, men den förstudien slutfördes aldrig.[157]

2020–2023

Med uppgift att starta sitt arbete under 2020 upprättade regeringen Nationellt Cybersäkerhetscentrum (NCSC) som bestod av FRA, Försvarsmakten, MSB och Säpo. NCSC fick i uppgift att förmedla stöd och råd avseende risker, hot och sårbarheter, koordinera arbete för att förebygga, hantera och upptäcka IT-incidenter samt verka som en nationell plattform för informationsutbyte och samverkan inom cybersäkerhetsområdet. Vidare skulle PTS, Polismyndigheten och FMV höras för inhämtning av information och synpunkter.[158] Vad gällde arbetet med den tidigare nationella handlingsmodellen kom det inte längre än till principnivå i SAMFI-gruppen innan oenighet uppstod vad gällde syfte och tolkning.[159] Det dröjde ytterligare 3 år efter det att arbetet avbröts innan NCSC tog sig an uppgiften och återupptog arbetet med förstudien som SAMFI-gruppen påbörjat. Svårigheterna och oenigheten var inte helt försvunna, men arbetet förenklades med hjälp av en god styrstruktur inom NCSC som avgränsade handlingsmodellen till att fokusera på systematiskt cybersäkerhetsarbete. Efter att förstudien slutförts har arbetet med själva modellen inte återupptagits.[160] Det dröjde fram till 2022 innan regeringen uppmärksammade passiviteten i arbetet. Först då hade ansvariga statsråd samtal med företrädare för berörda myndigheter.[161] Även om det framkommer i regeringsuppdraget som ligger till grund för NCSC:s arbete att samverkan ska utvecklas stegvis under åren 2021–2023 anses arbetet för lågintensivt på flera områden, inte minst rörande arbetet med den nationella modellen.[162]

I en FOI-rapport från 2020 framgår det att svenska myndigheter upplever svårigheter i att bedöma vad som utgör en IT-incident som ska rapporteras. Vidare saknades inarbetade rutiner för bedömning och hantering av incidenterna.[163] År 2021 framhöll regeringen vikten av sin egen styrning av statsförvaltningen. Enligt regeringen själva ska deras arbete vara helhetsinriktat, verksamhetsanpassat,

---

[157] Ibid.

[158] Försvarsdepartementet. Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter. Fö2019/01330. Stockholm 2020.

[159] Riksrevisionen. Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig. RiR 2023:8. Stockholm, 2023.

[160] Försvarsdepartementet. Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter. Fö2019/01330. Stockholm 2020.

[161] Riksrevisionen. Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig. RiR 2023:8. Stockholm, 2023.

[162] Försvarsdepartementet. Uppdrag om fördjupad samverkan inom cybersäkerhetsområdet genom ett nationellt cybersäkerhetscenter. Fö2019/01330. Stockholm 2020.

[163] Ann-Sofie Stenerus, Johan Bengtsson & Matilda Olsson. *IT-incidenter på statliga myndigheter. Orsaker till utebliven rapportering.* Totalförsvarets forskningsinstitut. Stockholm, 2020. FOI-R--4815—SE

långsiktigt, strategiskt och tillitsbaserat. Regeringen bör visa förmåga och handlingskraft när myndigheter inte genomför arbetet på ett fullständigt sätt.[164] Regeringens satsningar har i största mån fokuserat på informationssäkerhetsarbetet inom den offentliga sektorn. Trots fokus på den offentliga sektorn uttryckte regeringen redan 2019 att ökad cyber- och informationssäkerhet i samhället är beroende av att aktörer i både privat och offentlig sektor prioriterar och avsätter resurser till säkerhetsarbetet på området.[165] Det finns dock ingen tydlig styrning eller riktning att följa vad gäller grundnivån för godtagbart säkerhetsarbete. Det närmaste alternativet är MSB:s föreskrifter om systematiskt informationssäkerhetsarbete.[166] Det som finns att tillgå för privata aktörer, och mer specifikt privata leverantörer, är de krav på att vidta säkerhetsåtgärder för att öka säkerheten i sina informationssystem som ställs i det första NIS-direktivet.[167] Samtidigt menar några av NCSC:s myndigheter att näringslivet ställer för höga förväntningar på det faktiska arbetet med informationssäkerhet.[168] Exempelvis finns det en uppfattning om att så fort information från regeringen och riksdag görs tillgänglig ska den gå att förvalta inom den privata sektorn för att bedriva ett bättre säkerhetsarbete. Detta snabba informationsdelningssätt är svårt enligt användarna då det bland annat saknas standardiserade metoder för hur informationen ska delas på säkraste och bästa sätt. Avsaknaden av snabb informationsdelning resulterar i försvårade processer för informationsutbytet mellan såväl statliga verksamheter som privata.[169]

I redovisningen av den nationella handlingsplanen från 5 mars 2019 och från myndigheternas åtgärdsarbete framkommer det att SAMFI-gruppens arbete behövt förhålla sig till inrättandet av NCSC som på sikt skulle kunna komma att ta över en del åtgärder, vilket senare också skedde.[170] Dessutom präglades myndigheternas arbete av covid-19-pandemins påverkan vilket försvårade arbetet med framtagna åtgärder i handlingsplanen. Bland annat då personal under året behövt arbeta med att hantera pandemins konsekvenser i kombination med att samverkanstillfällen var tvungna att ställas in.[171] År 2021 kom en statlig utredare fram till att det nationella informations- och cybersäkerhetsarbetet var uppdelat i delvis överlappande ansvarsområden och att ansvaret var fördelat på flera olika nivåers

[164] Finansdepartementet. *Prop 2020/21:1 Budgetpropositionen för 2021.* Stockholm, 2020.
[165] Finansdepartementet. *Prop. 2019/20:1 Budgetpropositionen för 2020.* Stockholm, 2019.
[166] Myndigheten för samhällsskydd och beredskap. *MSBFS 2020:6 föreskrifter om informationssäkerhet för statliga myndigheter.* Stockholm, 2020.
[167] Ibid.
[168] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* RiR 2023:8. Stockholm, 2023
[169] Ibid.
[170] Myndigheten för samhällsskydd och beredskap. *Samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022 – redovisning 2021*. Stockholm 2021
[171] Ibid. S. 14.

samt att det uppstod utmaningar i verksamheterna främst orsakat av bristande samordning och styrning. Denna brist borde enligt utredaren utredas separat.[172]

I fråga om totalförsvaret har försvarsbeslutet för perioden 2021–2025 konkretiserat och intensifierat planeringen av totalförsvaret. Regeringen och riksdagen har under en förhållandevis kort tid beslutat om ett antal åtgärder, däribland resurstillskott och lagstiftning, för att öka Sveriges beredskap. I försvarsbeslutet framgår det att Försvarsmakten ansvarar för den offensiva försvarsförmågan med stöd från delar av totalförsvaret. Där framhålls också att Sveriges säkerhet och ekonomiska välstånd vilar allt mer på digitala grunder och att digitaliseringen i Sverige och omvärlden påverkar både militär och civil verksamhet inom och utom totalförsvaret. Det skapas ständigt nya stora möjligheter i takt med den teknologiska utvecklingen, utbredningen av digitala lösningar och ökade datavolymer, men också risker och sårbarheter för myndigheter och för samhället i stort. Sårbarheterna som följer vid den ökade digitaliseringen återfinns i alltifrån elektroniska kommunikationer, sjö- och luftfart, till elnät, industriella styrsystem och det finansiella systemet.[173]

I syfte att bedriva internationellt arbete inom ramen för NIS-direktiven (1 och 2) fick MSB år 2021 i uppdrag att skapa förutsättningar för att bli samordningscenter nationellt för cybersäkerhet inom forskning, teknik och näringsliv.[174] I sin årsrapport från 2022 påpekade MSB att det behövdes en generell satsning på att stärka arbetet med informationssäkerhet i den offentliga förvaltningen då stora delar inte arbetade systematiskt och i linje med framtagna föreskrifter.[175] Under 2022 kom Europeiska kommissionen med ett gemensamt meddelande till Europaparlamentet och Europeiska unionens råd om förslag till en cyberförsvarspolicy för EU. Meddelandet syftade till att stärka unionens cyberförsvarsförmågor, inklusive medlemsstaternas förmåga att genomföra gemensamma cyberoperationer. Cyberförsvarspolicyn syftar till att bidra till att minska strategiska beroenden av kritisk cyberteknik och samtidigt stärka den europeiska försvarsteknologiska industribasen på området med en mer effektiv cyberkrishantering inom EU. Vidare skulle koordinering, informationsdelning och samverkan mellan cybersäkerhet och cyberförsvar, det vill säga mellan de civila och militära cybergemenskaperna, stärkas. Policyn skulle leda till mer effektiv cyberkrishantering inom EU.[176] Under 2022 kom Europeiska kommissionen med ett förslag till förordning om horisontella cybersäkerhetskrav för produkter med digitala inslag

[172] Regeringskansliet. *SOU 2021:63. Sveriges säkerhet: behov av starkare skydd för nätverks- och informationssystem*. Stockholm 2021.
[173] Försvarsdepartementet. *Prop. 2020/21:30. Totalförsvaret 2021-2025.* Stockholm, 2019.
[174] Justitiedepartementet. *Uppdrag till Myndigheten för samhällsskydd och beredskap att vidta förberedelser för att bli nationellt samordningscenter kopplat till det europeiska kompetenscentret för cybersäkerhet (Ju2021/03097).* Stockholm, 2021.
[175] Myndigheten för samhällsskydd och beredskap. *När kriget kom nära – Årsrapport it-incidentrapportering 2022. Stockholm 2023*
[176] Europaparlamentet. *GEMENSAMT MEDDELANDE TILL EUROPAPARLAMENTET OCH RÅDET EU:s politik för cyberförsvar. Bryssel, 2022.*

och ändring av förordning 2019/1020 (Cyberresiliensakten). Syftet med förslaget var att skapa förutsättningar för utveckling av säkra produkter med digitala inslag genom att försäkra att hård- och mjukvara placeras på marknaden med färre sårbarheter och att tillverkare tar större ansvar för produkters cybersäkerhet genom deras livscykler. Förslaget syftade även till att konsumenter skulle få tillräcklig information om cybersäkerheten för de produkter med digitala inslag som de köper och använder. Akten önskar att tillverkarna till hårdvaru- och programvaruprodukter tar säkerheten på allvar.[177] I takt med den ökade digitaliseringen får avbrott och fel i digitala leveranskedjor allt större påverkan. Detta ställer krav på förebyggande systematiskt arbete och utveckla förmågor för incidenthantering.[178] Ansvaret för lagstiftnings- och förvaltningsärenden om cyber- och informationssäkerhet ligger idag på Försvarsdepartementet, dessförinnan under Justitiedepartementet. Begreppet cybersäkerhet fördes in i förordningar hösten 2022. Varje departement ansvarar för cyber- och informationssäkerhetsfrågor inom sitt ansvarsområde utan att det anges i förordningen. Ansvaret för förvaltnings- och lagstiftningsärenden är spritt på flera olika departement.[179] I underlaget till utredningen som ligger till grund för förordningen (2022:524) om statliga myndigheters beredskap framkom det ett förslag på att informations- och cybersäkerhetsfrågorna skulle hanteras i ett tvärsektoriellt led. Något som inte implementerades.[180]

Förordningen om statliga myndigheters beredskap (2022:524) fastslår att statliga myndigheter under regeringen, genom sin verksamhet, ska minska sårbarheten i samhället. I 6 § specificeras vad som i lagrummet avses med ”fredstida krissituationer”, nämligen sådana situationer som ”avviker från det normala; drabbar många människor, stora delar av samhället eller hotar grundläggande värden; innebär en allvarlig störning eller en överhängande risk för en allvarlig störning av viktiga samhällsfunktioner; och kräver samordnade och skyndsamma åtgärder från flera aktörer”. Under 2022 beslutade regeringen att en särskild utredare skulle förbereda och genomföra bildandet av en ny myndighet för uppföljning och utvärdering av totalförsvaret. Denna nya myndighet fick namnet Myndigheten för totalförsvarsanalys. Den nya myndigheten ska ha ett systemperspektiv, följa upp, analysera och utvärdera verksamheten inom totalförsvaret, med fokus på det samlade funktionssättet och det övergripande målet för totalförsvaret respektive målen för det militära respektive civila försvaret.[181]

---

[177] Landsbygds- och infrastrukturdepartementet. *Förordning om horisontella cybersäkerhetskrav för produkter med digitala inslag.* 2022/23:FPM6. Stockholm, 2022.

[178] Myndigheten för samhällsskydd och beredskap. *Nationell risk- och sårbarhetsbedömning (NRSB) 2023 Enligt 2 § förordningen (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap.* Stockholm 2023.

[179] Statsrådsberedningen. *Förordning (1996:1515) med instruktion för Regeringskansliet.* Stockholm, 1996.

[180] SOU 2021:25.

[181] Regeringen. *Inrättande av Myndigheten för totalförsvarsanalys. Kommittédirektiv Dir. 2022:119*. Stockholm, 2022.

Sedan 2022 finns förordning (2022:524) om statliga myndigheters beredskap i vilken det framgår vilka myndigheter som valts ut som beredskapsmyndigheter. Dessa myndigheter anses ha ett särskilt ansvar inom en eller flera viktiga samhällsfunktioner. De bedöms även bedriva en verksamhet som har särskild betydelse för totalförsvarets och samhällets krisberedskap, inför och vid fredstida krissituationer samt höjd beredskap. Det rör sig om 60 myndigheter vilka ansvarar för 10 olika beredskapssektorer. För respektive sektor finns en sektorsansvarig myndighet som bland annat ska leda, stödja och samordna arbetet i sektorn. I respektive beredskapsmyndighets ansvar ingår att lämna en risk- och sårbarhetsbedömning baserad på identifiering och analys av samhällsviktig verksamhet inom myndighetens ansvarsområde. Bedömningen ska även innehålla en uppskattning av vilka åtgärder som bör vidtas och hur dessa ska prioriteras samt vilka åtgärder som vidtagits. Vidare ansvarar myndigheterna för sin, och delvis andras, kontinuitet genom att upprätthålla sin samhällsviktiga verksamhet och verka för att andra aktörer (övriga statliga myndighet, regioner, kommuner och berörda näringsidkare) inom ansvarsområdet också genomför sina verksamheter och utvecklar sin förmåga. Det framgår även i förordningen (2022:524) att beredskapsmyndigheterna ska ha god förmåga att förebygga sårbarheter, motstå risker och hot, genomföra sina uppgifter vid höjd beredskap och hantera fredstida krissituationer. Särskilt ansvar ligger på beredskapsmyndigheterna där de bland annat ska samverka med varandra, samverka med Försvarsmakten avseende behovet av stöd till det militära försvaret, samverka med övriga myndigheter, regioner och kommuner samt de näringsidkare och sammanslutningar som är berörda. Särskilt ansvar åläggs även de geografiskt områdesansvariga beredskapsmyndigheterna att samverka med berörda länsstyrelser.[182]

Beredskapsmyndigheterna har även ett särskilt ansvar att beakta internationella samarbeten som rör totalförsvar och krisberedskap, beakta behovet av erfarenhetsöverföring, utvecklings- och forskningsinsatser, samverka kring övningsverksamhet, genomföra omvärldsbevakning samt de förberedelser, planeringar och utbildningsinsatser som krävs för att klara sina uppgifter vid höjd beredskap och fredstida krissituationer. Efter beslut av regeringen ska beredskapsmyndigheterna även kunna påskynda nödvändiga åtgärder inför höjd beredskap. De 60 myndigheterna har även rapporteringsskyldighet och annan informationsskyldighet där de ska hålla regeringen, MSB och sin respektive sektorsansvariga myndighet informerad (när myndigheten ingår i en sektor). Även länsstyrelserna ska ges underlag för att de ska kunna fullgöra sina uppgifter.[183] *Utredningen för civilt försvar* som publicerades i februari 2021 hade i uppgift att analysera och föreslå en struktur för ansvar, ledning och samordning inom civilt försvar på central, regional och lokal

[182] Försvarsdepartementet. *Förordning (2022:524) om statliga myndigheters beredskap*. Stockholm, 2023.
[183] Försvarsdepartementet. *Förordning (2022:524) om statliga myndigheters beredskap.* Stockholm, 2022.

nivå.[184] I utredningen framkommer det ett förslag på att de tio beredskapssektorerna skulle kompletteras med fyra så kallade särskilda beredskapsområden. De fyra särskilda beredskapsområdena bedömdes bedriva samhällsviktiga verksamheter och funktioner som var av särskild betydelse att upprätthålla i kris, höjd beredskap och ytterst krig. Cybersäkerhet utgjorde ett av de fyra särskilda beredskapsområdena och skulle bedrivas i samarbete mellan Säpo, MSB, Försvarsmakten och FRA. Utgångspunkten skulle vara uppdrag i instruktioner, beslut av regeringen eller annan reglering.[185] Detta var ett förslag som tillstyrktes av bland annat MSB[186] men som inte inrättades i förordning (2022:524) om statliga myndigheters beredskap. Vidare omnämns inte cybersäkerhet utan endast informationssäkerhet i förordningen.[187]

Redan 2021 och i propositionen (2020/21:30) underströk regeringen betydelsen av att de ekonomiska tillskotten till totalförsvaret efterföljs och att det sker en oberoende uppföljning och utvärdering av totalförsvaret. Därför tillsattes en utredning i april 2021 [188] och 1 januari 2023 inrättades Myndigheten för totalförsvarsanalys med intentionen att den skulle byggas upp successivt under 2023.[189]

Under 2023 publicerades två nya granskningar från Riksrevisionen (*Digitala tjänster till privatpersoner – stora utvecklingsmöjligheter för statliga myndigheter RiR 2023:6* & *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig RiR 2023:8)* vilka båda två anses relevanta för denna studie. I RiR 2023:6 framkom det att statens insatser för att utveckla myndigheternas digitala tjänster inte har varit tillräckligt effektiva. Det fanns även brister i myndigheternas sätt att arbeta med att utveckla användbara och tillgängliga digitala tjänster. Vidare fanns de största hindren för den fortsatta utvecklingen av digitala tjänster till privatpersoner på systemnivå, vilket kräver åtgärder från regeringen. Den svenska digitaliseringspolitiken har högt uppsatta mål vilka hindras från att uppnås på grund av existerande regelverk, något som har framgått i flera olika statliga utredningar.[190] Det rör sig bland annat om juridiska begränsningar för myndigheter att utbyta information, vilket är ett av flera välkända hinder som inte regeringen gjort tillräckligt för att hantera, enligt Riksrevisionen. Vidare framgår det i granskningen att regeringens styrning av Myndigheten för digital förvaltning bör bli mer långsiktig där myndigheten under

[184] Justitiedepartementet. *Ansvar, ledning och samordning inom civilt försvar Dir. 2018:79.* Stockholm, 2018.
[185] Regeringskansliet. *SOU 2021:25. Struktur för ökad motståndskraft*. Stockholm 2021.
[186] Myndigheten för samhällsskydd och beredskap. *Betänkandet SOU 2021:25 - Struktur för ökad motståndskraft.* Stockholm 2021.
[187] Försvarsdepartementet. *Förordning (2022:524) om statliga myndigheters beredskap.* Stockholm, 2022.
[188] Regeringskansliet. *SOU 2021:103. Totalförsvarsanalys – en oberoende myndighet för uppföljning och utvärdering. Betänkande av Utredningen om totalförsvarsanalys. Stockholm 2021.*
[189] Regeringen. *Inrättande av Myndigheten för totalförsvarsanalys. Kommittédirektiv Dir. 2022:119.* Stockholm, 2022.
[190] Finansdepartementet. *Juridik som stöd för förvaltningens digitalisering. SOU 2018:25.* Stockholm 2018.

sin första tid fått ett stort antal uppdrag i regeringsbeslut och i sitt regleringsbrev. Uppdragen i sig skiljer sig åt och regeringens styrning av myndigheten upplevs som inkonsekvent, vilket resulterar i otydligheter för myndighetens roll och ansvar. Riksrevisionen rekommenderade regeringen att styra främst med instruktioner snarare än regeringsuppdrag.[191] Regeringen svarade i en skrivelse att Riksrevisionens granskning utgör ett viktigt bidrag i det kontinuerliga förbättringsarbetet av myndigheternas digitala tjänster i linje med målet att Sverige ska vara bäst i världen på att utnyttja digitaliseringens möjligheter.[192] Vidare instämmer regeringen delvis i de rekommendationer som revisionen redovisat.[193]

I den andra granskningen som Riksrevisionen publicerade i mars 2023 ”*Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig RiR 2023:8”* framgår det att ansvaret för att hantera informations- och cybersäkerhetsarbetet är splittrat, både inom Regeringskansliet och mellan myndigheterna. Rapporten konstaterar bland annat att det fortfarande finns problem inom samtliga områden i fråga om regeringens tidigare nämnda informations- och cybersäkerhetsstrategi. Det kan ses i kombination med att strategin saknar vision och uppföljningsbara målsättningar samt uttalat ansvar med tillhörande resurssättning. Riksrevisionens övergripande slutsats i *RiR 2023:8* är att regeringens cyber- och informationssäkerhetsarbete inte varit tillräckligt effektivt där det saknas prioriteringar och avvägningar. Arbetet brister på flera punkter, inte minst i hur Sverige arbetar med cyber- och informationssäkerhetsfrågorna i relation till EU. Riksrevisionen menar att regeringen på olika sätt försökt skapa alternativa lösningar på säkerhetsarbetet, bland annat genom att inrätta tidigare nämnda NCSC. Revisionen bedömer dock att skapandet av det nationella centret inte resulterat i effektivare arbete eller styrning, och inte heller någon ökad förmåga att prioritera insatser utifrån Sveriges samlade behov på informations- och cybersäkerhetsområdet.[194]

Regeringen besvarade Riksrevisionen med en skrivelse som publicerades i oktober 2023. Regeringen instämmer huvudsakligen med vad som framkommer i granskningen där cyber- och informationssäkerhetsområdet behöver vara mer strategiskt sammanhållet. Regeringen utlovar åtgärder i form av arbete med att ta fram en ny informations- och cybersäkerhetsstrategi, i linje med Europaparlamentets och rådets direktiv (EU) 2022/2555. Detta arbete kommer att inkludera näringsliv och statliga myndigheter.[195] Som en konsekvens av RiR 2023:8 tillsatte regeringen i oktober 2023 en utredning som ska lämna förslag på former för en ändamålsenlig

[191] Riksrevisionen. Digitala tjänster till privatpersoner – stora utvecklingsmöjligheter för statliga myndigheter. RiR 2023:6. Stockholm, 2023.
[192] Finansdepartementet. Prop. 2011/12:1 Budgetpropositionen för 2012 Utgiftsområde 22. Stockholm, 2011.
[193] Ulf Kristersson. Riksrevisionens rapport om digitala tjänster till privatpersoner. Regeringens skrivelse 2023/24:7. Stockholm 2023.
[194] RiR 2023:8
[195] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* RiR 2023:8. Stockholm, 2023

och effektiv ledning, organisering och styrning av NCSC. Utredaren ska också lämna förslag på hur samarbetet mellan de sju statliga myndigheterna inom centret kan organiserats och styras framöver, efter att FRA fått huvudmannaskapet.[196]

För att kunna samordna insatser och arbeta mot samma målsättningar krävs goda förutsättningar för informationsutbyte, vilket det enligt revisionens granskning *RiR 2023:8* inte finns i dagsläget. Utbytet av information är (likt resultatet av föregående revision) förenat med utmaningar vad gäller både teknologi och regleringar. I granskningen rekommenderas regeringen att skapa en inriktning för arbetet som omfattar en analys av de utmaningarna som finns, där arbetets intressenter bör vara involverade. Vidare bör NCSC ses över vad gäller de hinder som existerar för informationsutbyte och styrningen av arbetet generellt vad gäller ansvarsfördelning, kompetenskrav och samordning.[197] Redan innan Riksrevisionens rapport publicerades skrev statsminister Ulf Kristersson och andra regeringsrepresentanter i en debattartikel att FRA skulle få ett huvudansvar för NCSC. Motiveringen var att det delade ansvaret mellan flera olika myndigheter i NCSC lett till svårigheter med såväl styrning som uppföljning och ansvarsutkrävande.[198]

Som tidigare nämnts var NIS-direktivet från 2016 EU:s första rättsakt om cybersäkerhet som gällde för alla medlemsstater.[199] På svenska heter direktivet ”Åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen”.[200] Direktivet genomfördes i Sverige genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174). Under 2020 utvärderades NIS-direktivet och ett förslag till nytt direktiv presenterades för att ersätta och uppdatera NIS-direktivet.[201] I och med detta förhandlades NIS2-direktivet fram, som syftar till en högre gemensam cybersäkerhetsnivå i hela unionen.[202] NIS2 kommer att införlivas i svensk lagstiftning under hösten 2024.[203] Den största skillnaden mellan NIS och NIS2 är att fler sektorer än tidigare kommer att omfattas samt att kraven på cybersäkerhet stärks ytterligare. Regeringens kommittédirektiv understryker även att ”syftet med det nya direktivet är att minska fragmenteringen av den inre marknaden genom att föreskriva minimiregler för ett

[196] Försvarsdepartementet. *Uppdrag att lämna förslag på hur en ändamålsenlig och effektiv ledning, organisering och styrning av Nationellt cybersäkerhetscenter ska utformas (Fö2023/01606).* Stockholm, 2023.
[197] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* RiR 2023:8. Stockholm, 2023
[198] Kristersson Ulf et. al. *FRA får ta över ansvaret för Sveriges cybersäkerhet*. DN.se, publicerad torsdag 27 april 2023.
[199] Europaparla uropaparlamentet. *Europaparlamentets och rådets 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*. 194 OJ L §, 2016.
[200] Ibid.
[201] Ibid.
[202] Ibid.
[203] Morgan Johansson. Nationell strategi för samhällets informations och cybersäkerhet. Skr. 2016/17:213. Stockholm 2016.

samordnat regelverk."[204] NIS-direktivet avsåg leverantörer av samhällsviktiga tjänster och då endast inom sju särskilt utpekade sektorer. I NIS2 tillkommer 12 sektorer, däribland offentlig förvaltning.

Regeringen har tillsatt en särskild utredare som ska arbeta med att ta fram förslag på anpassningar av svensk rätt för att NIS2-direktivet ska kunna genomföras i Sverige.[205] Uppdraget ska redovisas i februari 2024.

Under de senaste åren har EU aviserat ett stort antal satsningar och regleringar med bäring på informations- och cybersäkerhetsområdet.[206] 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.[207] I MSB:s kartläggning över initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete nämns NIS2 tillsammans med sju andra initiativ som förväntas att få betydande påverkan på Sverige. Vidare nämns Critical Entities Resilience Directive (CER-direktivet) vilket syftar till att stärka den fysiska motståndskraften och minska sårbarheter hos samhällsviktig verksamhet inom EU för att säkerställa ett oavbrutet tillhandahållande av tjänster. Detta i sig innebär ett stärkt totalförsvar då såväl civilt försvar som militärt försvar är beroende av samhällsviktig verksamhet. Direktivet kan liknas vid det ursprungliga NIS-direktivet fast för fysisk samhällsviktig verksamhet istället för nätverk och informationssystem. Ett annat initiativ i EU som syftar till att skapa förutsättningar för utvecklingen av säkra produkter med digitala element är redan nämnda Cyber Resilience ACT (Cyberresiliensakten).[208]

DORA-förordningen, redan nämnda EU:s cyberförsvarspolicy, Cybersolidaritetsakten och cyberdiplomatiska verktygslådan är ytterligare fyra initiativ där det första (DORA) syftar till att bidra med att öka den digitala operativa motståndskraften inom EU:s finanssektor och dess kritiska informations- och kommunikationsrelaterade tjänster. Förslaget till Cybersolidaritetsakten presenterades av EU-kommissionen i april 2023 och syftar till att stärka medlemsstaternas solidaritet och samordnande insatskapacitet kring gränsöverskridande cyberincidenter och hot. Akten ämnar lösgöra resurser för att stärka resiliens och situationsmedvetenhet inför cyberhot, samtidigt som den befintliga samarbetsramen stärks. Avslutningsvis är syftet med den cyberdiplomatiska verktygslådan, som antogs

[204] Försvarsdepartementet. Genomförande av EU:s direktiv om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen och EU:s direktiv om kritiska entiteters motståndskraft. Kommittédirektiv Sverige. Dir. 2023.30. Regeringen, 2023

[205] Ibid.

[206] Myndigheten för samhällsskydd och beredskap. *Policyöversikt Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*. Stockholm. 2023.

[207] Riksrevisionen. *Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig.* RiR 2023:8. Stockholm, 2023

[208] Myndigheten för samhällsskydd och beredskap. *Policyöversikt Initiativ på EU-nivå som påverkar Sveriges informations- och cybersäkerhetsarbete*. Stockholm. 2023.

redan 2017, att bidra till att begränsa hot mot cybersäkerhet, förebygga konflikter, öka stabiliteten i internationella relationer och försöka påverka beteenden hos potentiella hotaktörer.[209]

[209] Ibid.

ISSN 1650-1942

www.foi.se