INTERNET STIFTELSEN

Dnr: I2021/03264

Internetstiftelsens remissvar på it-driftsutredningens slutbetänkande Säker och kostnadseffektiv it-drift (SOU 2021:97)

Om Internetstiftelsen

Internetstiftelsen är en oberoende, affärsdriven och allmännyttig organisation. Vi verkar för ett internet som bidrar positivt till människan och samhället.

Vi är en stiftelse och vår urkund slår fast att vi ska säkerställa en stark och säker infrastruktur för internet som tillgodoser dagens och framtidens behov i Sverige samt främja forskning, utbildning och undervisning med inriktning på internet. Vi ansvarar för internets svenska toppdomän .se och sköter även drift och administration av toppdomänen .nu. Intäkterna från affärsverksamheten finansierar en rad satsningar i syfte att möjliggöra att människor kan nyttja internet på bästa sätt och att ge kunskap om internetanvändningen i Sverige samt digitaliseringens påverkan på samhället. Vi tillhandahåller evenemang och utbildningsinsatser som gör det enklare att förstå och använda internets tjänster och som bidrar till ökad kompetens och fler möten som främjar internetinnovation. Vi stöttar även olika fristående uppdrags- och forskningsprojekt som på olika sätt gynnar internets utveckling och ger förutsättningar för internetentreprenörer och utvecklare att ta steget från idéstadie till färdig produkt eller tjänst. Med våra identitetsfederationer förenklar vi inloggning och höjer säkerheten i identitets- och kontohantering för både användare och leverantörer av olika tjänster inom skola, hälso- och sjukvård.

Internetstiftelsen har blivit tillfrågade att lämna remissvar på Säker och kostnadseffektiv it-drift (SOU 2021:97).

Internetstiftelsen har tidigare lämnat synpunkter på utredningens delbetänkande: https://internetstiftelsen.se/app/uploads/2021/04/remissvar-sou-2021-1-samordnad-kostnadseffektiv-it-drift-delb.pdf

Övergripande synpunkter

Tidigare utredningar och revisioner om statlig it-drift har visat att myndigheternas it-driftslösningar varken är tillräckligt säkra eller kostnadseffektiva. Internetstiftelsen ställer sig bakom analysen att it-driften för statliga myndigheter behöver samordnas för att den ska vara säker, robust och kostnadseffektiv, men vill lägga till att det sker med förutsättning att hänsyn tas till totalförsvarets behov, att totalförsvaret inte blir lidande av kravet på kostnadseffektivitet.

Enligt utredningen är ett centralt syfte med en samordnad statlig it-drift att bidra till ökad informationssäkerhet i den statliga förvaltningen. **Enligt Internetstiftelsen** är det

sannolikt att ju fler myndigheter som ansluts till den samordnade it-driften, desto mer kostnadseffektiv blir den, eftersom kraven på säkerhet och robusthet är kostnadsdrivande i sig.

En viktig faktor i sammanhanget är förslaget till ett omarbetat NIS-direktiv, NIS2. I Artikel 18 av direktivet ställs krav på riskhanteringsåtgärder för cybersäkerhet, och där medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för att tillhandahålla sina tjänster. Med beaktande av den senaste tekniska utvecklingen ska dessa åtgärder säkerställa en säkerhetsnivå i nätverks- och informationssystem som är lämplig i förhållande till den föreliggande risken. De åtgärder som avses i det omarbetade NIS-direktivet ska åtminstone inbegripa:

a. strategier för riskanalys och informationssystemens säkerhet,
b. incidenthantering (förebyggande, upptäckt och åtgärder till följd av incidenter
c. driftskontinuitet och krishantering,
d. säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess leverantörer eller tjänsteleverantörer, såsom leverantörer av datalagrings- och databehandlingstjänster eller hanterade säkerhetstjänster,
e. säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av och information om sårbarheter,
f. strategier och förfaranden (testning och revision) för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet,
g. användning av kryptografi och kryptering.

Faktum är att kraven på myndigheternas arbete med informationssäkerhet kommer att skärpas i takt med att nya EU-direktiv antas och omsätts i svensk lag. Informationssäkerhet i en samordnad statlig it-drift måste vara på en sådan nivå att den skapar stabila förutsättningar för viktiga samhällsfunktioner och motsvarar de krav som ställs i bland annat EU-direktiv. En hög nivå på informationssäkerheten är enligt Internetstiftelsen också en förutsättning för att medborgare och andra intressenter ska känna tillit till vitala samhällsfunktioner. Säkerhetsnivån måste även vara motståndskraftig för cyberattacker mot Sverige. Idag hanteras inte säkerhetsfrågorna med tillräcklig systematik.

Det har genom åren funnits olika initiativ att försöka få till stånd en samordnad statlig it-drift, alltifrån Statnät som utreddes av Statskontoret på 90-talet till Statens servicecenter som kom till år 2012 och det uppdrag som Statens servicecenter fick av regeringen 2016 att analysera och föreslå vilka myndighetsfunktioner som kan vara lämpliga att bedriva samordnat inom staten och utanför storstadsområden. Statens servicecenter

överlämnade delrapporten En gemensam statlig molntjänst för myndigheternas it-drift i april 2017.[1]

Grunden för en samordnad statlig it-drift är tillgång till en nationellt täckande fiberinfrastruktur över vilken staten äger rådighet, vare sig man äger den själv eller upphandlar den från marknadens aktörer. Detta aktualiserades av IT-kommissionen redan år 1999 [2] och är i stora delar den modell enligt vilken det svenska universitetsdatanätet Sunet organiserats. En väl fungerande digital infrastruktur är enligt Internetstiftelsen en förutsättning för att verksamheter inom både privat och offentlig sektor ska kunna konkurrera i en alltmer globaliserad värld. Dagens bristande samordning utgör en risk i sammanhanget.

Precis som utredningen själv konstaterat är it-drift ett begrepp som saknar fastlagd definition, vilket gör det svårt att överblicka vad utredningens förslag om samordnad it-drift egentligen omfattar, särskilt som utredningen inte ger några exempel på hur en ”tjänsteprofil” skulle kunna se ut.

Ett mycket bra sätt att beskriva infrastrukturen är **enligt Internetstiftelsen** att använda sig av den så kallade lasagnemodellen som lyftes fram i Kungl. Ingenjörsvetenskapsakademiens rapport *Digitalisering för ökad konkurrenskraft*.[3]

Marknadens aktörer har en viktig roll att spela även i en miljö med samordnad it-drift för statliga myndigheter. System och tjänster utvecklas ofta av privata företag vilket är att föredra framför att staten själv lägger resurser på utveckling, något som historiskt inte heller visat sig vara särskilt framgångsrikt. En viktig utgångspunkt är enligt Internetstiftelsen att den som upphandlar system och applikationer ställer krav på att leverantörer i första hand håller sig till standardiserade protokoll.

Internetstiftelsen konstaterar att det behövs ett övergripande ansvar för gemensamma standarder och plattformar på vilka för samhället grundläggande system, applikationer och infrastruktur byggs, och ett motsvarande övergripande ansvar för

---

[1] Framtidssäker IT-infrastruktur för Sverige, SOU 1999:134

[2] https://www.statenssc.se/download/18.20508645162fe25cee35cc7/1548869369973/En%20gemensam%20statlig%20molntj%C3%A4nst%20f%C3%B6r%20myndigheternas%20it-drift%20(2017-02-07).pdf

[3] https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf

cybersäkerhet, det vill säga för den statliga förvaltningens gemensamma informationssäkerhetsfrågor. **Internetstiftelsen ser** också en risk för ökad byråkratisering med vissa av utredningens förslag. Mer detaljerade synpunkter lämnas i det följande.

1. Författningsförslag

I §7 anges att den samordnande myndigheten, DIGG, ska samråda med Försvarsmakten i frågor rörande Sveriges säkerhet. **Internetstiftelsen är av uppfattningen** att detta ligger inom Säkerhetspolisens uppdrag som tillsynsansvarig myndighet enligt säkerhetsskyddslagen. Stiftelsen bedömer att risken för dubbelarbete är stor.

Internetstiftelsen föreslår att det i §8 lämnas en öppning för att utöka antalet leverantörsmyndigheter, alternativt att förordningen i stället för att ange vilka leverantörsmyndigheterna är, hänvisar till en föreskrift med en förteckning över aktuella leverantörsmyndigheter och som torde vara lättare att uppdatera än en förordning.

I avsnitt 1.3 Förslag till förordning om ändring i förordningen (2007:975) med instruktion för Integritetsskyddsmyndigheten finns ett skrivfel i den föreslagna lydelsen till 4 a §, där står samordnade i stället för samordnande myndigheten. Samma skrivfel återfinns i avsnitt 1.5, 11 c §, avsnitt 1.9, 10 a §, avsnitt 1.10, 8 a § samt avsnitt 1.12, 7 a §.

2. Utredningens uppdrag, utgångspunkter och arbete

En av utgångspunkterna i utredningens arbete är att kompetensbrist inom it-säkerhet och juridik är en riskfaktor för säker it-drift, och beställarkompetens lyfts fram som ett särskilt problem.

Internetstiftelsen betonar att individer med rätt kompetens krävs för att med hjälp av digitala verktyg utveckla produkter och tjänster som är vitala för myndigheterna inom statsförvaltningen. Lika viktigt är förmågan att förstå och på ett effektivt sätt använda digitala lösningar i olika verksamheter. Genom att samordna den statliga it-driften och samordna det statliga tjänsteutbudet finns det **enligt Internetstiftelsen** en möjlighet att optimera användningen av den kompetens som finns.

Enligt Internetstiftelsen kommer en samordning av it-driften få stora konsekvenser på dagens driftssituation. Enligt Staten Servicecenters utredning från 2017, *En gemensam statlig molntjänst för myndigheternas it-drift*, är slutsatsen att det kommer att behövas högst tio datacenter för att driva det man där kallar för statens molntjänst, och att merparten av dessa av säkerhetsskäl bör placeras i bergrum utanför storstadsområdena. När den samordnade it-driften byggs upp kan statens gemensamma resurser såsom befintliga bergrum, fibernät m.m. användas. Det kan vara effektivt i kostnads-, resurs- och säkerhetshänseende. It-driftsutredningen har i sitt betänkande inte särskilt berört frågan om säkra utrymmen, något som

Internetstiftelsen saknar, särskilt mot bakgrund av den diskussion om begreppet Säker som förs i betänkandet (se nedan).

I avsnitt 2.3 diskuteras centrala begrepp och i avsnitt 2.3.1 diskuteras begreppet Säker. Enligt utredningen avses med säker på samhällsnivå att it-driften i den offentliga förvaltningen som helhet är organiserad på ett sådant sätt att den kan stå emot olika störningar och hotnivåer i samhället. Begreppet robusthet anges av utredningen nära kopplat till säker, det vill säga en förmåga att stå emot störningar till följd av såväl yttre som inre påverkan. **Internetstiftelsen vill i det sammanhanget föra in** begreppet *operational resilience*, eller operativ motståndskraft, vilket innebär förmågan hos en organisation och dess medarbetare, system, telekommunikationsnät, aktiviteter och processer att hantera effekterna av en störning, ett avbrott eller informationsförlust och kunna fortsätta tillhandahålla en acceptabel servicenivå. Detta har bland annat betydelse för det resonemang om prioriteringar som görs av utredningen i avsnitt 11.5.2.

Utredningen anger också att en högre säkerhetsnivå har betydelse även ur ett totalförsvarsperspektiv. **Internetstiftelsen saknar** dock ett resonemang kring just totalförsvarsperspektivet i den del av betänkandet som innehåller utredningens förslag. Det hade varit tydligare om utredningen i den delen av betänkandet betonat totalförsvarets ställning i relation till kravet på kostnadseffektivitet.

3. Digitalisering och en förändrad hotbild

Internetstiftelsen delar utredningens beskrivning av den bredare och mer komplexa hotbild vi står inför idag, inte minst med hänsyn tagen till utvecklingen av kriget som Ryssland för mot Ukraina, där båda sidor befaras kunna ta till cyberangrepp som riskerar att spilla över på andra nationer som inte är direkt inblandade i kriget. Det faktum att internet är en global företeelse, där den tidigare robusta, decentraliserade modellen alltmer har övergått till en modell där det sker en stark centralisering till ett fåtal tjänster och leverantörer leder i hög grad till ökade risker för omfattande avbrott. Det råder ingen tvekan om att cyberhotet riskerar att få allvarliga konsekvenser för samhällsfunktioner. **Internetstiftelsen välkomnar** det stora intresset för just dessa frågor. Internetstiftelsen har under en längre tid påtalat de brister som finns inom den offentliga förvaltningen när det gäller informations- och cybersäkerhet. Från resultaten av den mätning som Internetstiftelsen regelbundet gör och som går under benämningen *Hälsoläget på internet i .se*, kan vi konstatera att statliga myndigheter brister i arbetet med informations- och cybersäkerhet (se avsnitt 5 nedan).

4. Samverkan, samordning och styrning i staten

I avsnittet går utredningen igenom förutsättningar för samverkan och samordning i staten. Det pågår redan en hel del aktiviteter inom området, och regeringen har lämnat flera uppdrag, bland annat ett uppdrag om att etablera en förvaltningsgemensam digital infrastruktur för informationsutbyte. **Internetstiftelsen konstaterar** att beskrivningen av

vad detta innebär är oprecist och att det är svårt att bedöma vilka krav det ställer på den underliggande infrastrukturen.

5. Myndigheternas behov av samordnad statlig it-drift

Som utredningen lyfter fram finns redan exempel på samordnad it-drift inom staten. **Internetstiftelsen instämmer** i den analys som utredningen gjort i sammanhanget och det verkar dessutom klarlagt att det finns ett brett intresse för samordnad statlig it-drift inom statsförvaltningen.

När det gäller figur 5.1, Tjänstekarta **ställer sig Internetstiftelsen frågan** om vad som ingår i blocket Infrastrukturtjänster, om till exempel domännamnssystem (DNS) är en av de tjänster som kommer att erbjudas, och IP-tjänst?

Många myndigheter använder idag DNS-tjänster med låg kvalitet och säkerhet. I vissa fall hanteras domännamnssystemet styvmoderligt, där krav på säkerhet och tillgänglighet inte står i paritet med myndighetens generella krav. DNS-tjänster, mejltjänster och webbtjänster hos statliga myndigheter uppfyller inte ens basala hygienkrav på säkerhetssidan, och har inte implementerat de standardlösningar som funnits i 5-10 år, ett faktum som är lätt att verifiera genom att genomföra test på hardenize.com.

Tjänster som “syns” externt, och som riktar sig till medborgare, företag och andra myndigheter inom den offentliga förvaltningen behöver **enligt Internetstiftelsen** hålla hög kvalitets- och säkerhetsnivå. Staten bör föregå med gott exempel. Sådana tjänster är exempelvis IP (framför allt IPv6), DNS (inkl säker DNS), webb och mejl. Samtliga dessa bör **enligt Internetstiftelsen** ingå i den tjänstekarta som beskriver it-driftstjänster i en samordnad statlig it-drift.

Ett sådant basutbud av tjänster behöver kompletteras med etableringen av en gemensam lägsta säkerhetsnivå, en nivå baserad på de säkerhetskrav som ställs på samtliga myndigheter, något som **enligt Internetstiftelsen** skulle leda till en väsentlig förbättring jämfört med nuläget.

6. Utvärdering av Försäkringskassans uppdrag om samordnad och säker statlig it-drift

Försäkringskassan har erfarenhet av att hantera it-drift åt andra myndigheter, inte minst sedan myndigheten 2017 fick det riktade uppdraget från regeringen att tillhandahålla detta. **Internetstiftelsen vill uppmärksamma** den vitbok som Försäkringskassan har publicerat om *Molntjänster i samhällsbärande verksamhet – risker, lämplighet och vägen framåt* där myndigheten redovisat sin syn på frågan om samordnad och säker statlig it-drift[4].

[4] https://www.forsakringskassan.se/wps/wcm/connect/30cc57bd-b5cd-4e04-94cd-1f7a02a9ae1a/vitbok.pdf

Utredningen konstaterar att Försäkringskassan klarat uppdraget väl, och att såväl kundmyndigheterna som Regeringskansliet anger att de är nöjda med hur myndigheten tagit sig an uppdraget. **Enligt Internetstiftelsen** är detta en god anledning att bygga vidare på befintliga initiativ.

7. Andra exempel på samordnad it-drift

I detta avsnitt beskriver utredningen andra exempel på samordnad it-drift som redan existerar. Här finns delvis den konkretion som Internetstiftelsen saknar i utredningens förslag. Exempelvis ger det tjänsteutbud som Sunet erbjuder en bild av vad som är tänkbara tjänster i en framtida tjänstekatalog. Sunet arbetar nästan uteslutande med system baserade på öppen källkod. Sunet har enligt utredningen identifierat en klar vinst med en sådan strategi och det är att de undviker säkerhetsproblem som i större utsträckning drabbar system som inte är baserade på öppen källkod. **Internetstiftelsen anser** att öppen källkod även kan användas i den framtida samordnade it-driften för statliga myndigheter.

Det finns ett frivilligt initiativ till samarbete, SITSSAM, som lutar sig mot 6 § myndighetsförordningen och 8 § förvaltningslagen, där det framgår att myndigheter ska ”verka för att genom samarbete med andra myndigheter ta tillvara de fördelar som kan vinnas för enskilda samt för staten som helhet”.

Bakgrunden till att det myndighetsövergripande programmet SITSSAM bildades är just behovet av att involvera fler myndigheter som kan erbjuda it-drift till andra myndigheter. **Enligt Internetstiftelsen** är det logiskt att man bygger vidare på det arbetet.

Program 2032 är ett initiativ till samverkan avseende säkra it-utrymmen som en del av Försäkringskassans regeringsuppdrag att erbjuda samordnad och säker statlig it-drift. Program 2032 syftar till att arbeta vidare med de förslag som PTS 2018 lämnade i sitt regeringsuppdrag *Förslag till en förvaltningsmodell för skyddade it-utrymmen.*

Enligt Internetstiftelsen är detta en sund utveckling, och Internetstiftelsen anser att man bör fortsätta bygga vidare på befintliga initiativ och modeller, och den frivilliga samverkan som redan existerar i SITSSAM och Program 2032, snarare än att konstruera en ny modell, som dessutom riskerar att skapa onödig byråkrati och en osund koncentration av ansvar och mandat till en myndighet, DIGG, och ett departement, Infrastrukturdepartementet. DIGG bör spela en viktig roll att spela som administrativ koordinator för samordningen, men där leverantörsmyndigheterna är involverade i processen mycket tidigare och i högre omfattning än vad utredningen föreslår.

8. Marknadsrättsliga förutsättningar för samordnad it-drift

Internetstiftelsen har inga synpunkter på den mycket detaljerade genomgång som utredningen gör, och inte heller någon invändning mot att man får anse att rättsläget måste anses klarlagt på ett nationellt plan, på så vis att köp mellan två statliga myndigheter inte omfattas av upphandlingsregleringen, vilket ju varit föremål för

diskussion vid tidpunkten då Försäkringskassan fick regeringens uppdrag att erbjuda it-drift till andra statliga myndigheter.

9. Rättsliga förutsättningar för informationshantering inom samordnad it-drift

Internetstiftelsen har inga synpunkter på utredningens beskrivning av de rättsliga förutsättningarna.

10. Utgångspunkter och principer för varaktiga former för samordnad statlig it-drift

Internetstiftelsen är positiv till utredningens förslag i 10.1 att regeringen ska inrätta varaktiga former för en samordnad statlig it-drift som ska bidra till att lösa gemensamma behov och problem.

Internetstiftelsen ställer sig också bakom utredningens förslag i 10.2, att den samordnade statliga it-driften ska organiseras utifrån befintliga verksamheter, och en samlad styrning genom samordnade uppdrag till flera myndigheter.

Internetstiftelsen anser även att förslaget i 10.3.3 är rimligt, att den samordnade statliga it-driften ska regleras genom en förordning om samordnad statlig it-drift, med förbehåll för de kommentarer som framförs ovan i avsnitt 1.

Enligt Internetstiftelsen är det också rimligt att tjänsteutbudet kan bestå av både tjänster som levereras av privata leverantörer och av ett samordnat statligt tjänsteutbud (som i sin tur också kan bestå av tjänster som levereras av privata leverantörer) så som föreslås i 10.4.1. **Internetstiftelsen vill dock betona** att de största innovationerna sker i de övre lagren i ”lasagnen” medan bottenplattan, den gemensamma grundläggande it-infrastrukturen med de viktigaste hörnstenarna för en bra funktion, bör ligga inom statens rådighet.

Internetstiftelsen ställer sig bakom förslaget i 10.4.2 att privata leverantörers tjänster ska upphandlas samordnat.

Internetstiftelsen förstår inte innebörden i förslaget i 10.4.3 om att de tjänster som ska ingå i det samordnade statliga tjänsteutbudet ska fastställas genom att matcha myndigheternas efterfrågan mot de tjänster som de myndigheter som ska tillhandahålla it-drift har förmåga att leverera. Det är svårt att överblicka den egentliga betydelsen av ett sådant förslag. **Internetstiftelsen vill här betona** vikten av standardiserade lösningar för att undvika att staten hamnar i ett leverantörsberoende med leverantörsspecifika lösningar.

Medan utredningen bedömer att det inte är lämpligt att i det här skedet avgränsa vilket tjänsteutbud som ska ingå i det samordnade statliga tjänsteutbudet, **anser Internetstiftelsen** att man bör börja med det som är minsta gemensamma nämnare, bland annat de infrastrukturtjänster som innefattar IP-kommunikation, DNS (inkl

DNSSEC), webb- och mejlhosting. På myndighetssidan finns ett starkt behov av en gemensam kravbild för dessa tjänster.

Internetstiftelsen tillstyrker utredningens förslag i 10.5 att bedömningen av vilka myndigheter som ska anslutas ska ske i dialog mellan de myndigheter som ska tillhandahålla it-drift och de myndigheter som anmäler intresse för att ansluta sig, att anslutningen ska vara frivillig och bygga på överenskommelser mellan de samverkande myndigheterna. Detta skapar sund dynamik där det samordnade statliga tjänsteutbudet måste vara konkurrenskraftigt för att attrahera en myndighet att ansluta sig.

Internetstiftelsen delar utredningens uppfattning att en samordnad statlig it-drift har central betydelse i ett stärkt civilt försvar. **Internetstiftelsen ser behov av** konkreta förslag inom området, och ett ställningstagande om att totalförsvarets behov är överordnat kraven på kostnadseffektivitet. Säkerhet medför en kostnad i syfte att skapa en bra och stabil grund för statliga myndigheters informationshantering och fortsatta digitalisering.

I avsnitt 10.6.2 lägger utredningen ett förslag som **enligt Internetstiftelsen** mer är att uppfatta som ett önskemål. Att en samordnad statlig it-drift ska bidra till att ge myndigheter bättre förutsättningar att göra medvetna val av säkra och kostnadseffektiva it-driftslösningar är snarare en målsättning än ett förslag. Det är emellertid **enligt Internetstiftelsen** troligt att en samordnad it-drift har den effekten, om man hanterar frågan på rätt sätt.

Utredningens bedömning i 10.6.3, att säkerhetskraven påverkar utformningen av en samordnad statlig it-drift är **enligt Internetstiftelsen** närmast en självklarhet. **Internetstiftelsen vill också understryka vikten** av att statliga aktörer måste ha rådighet över det samordnade statliga tjänsteutbudet. **Internetstiftelsen delar** också utredningens uppfattning att en sektorsindelning för anslutning av myndigheter är olämplig.

Likaså **ställer sig Internetstiftelsen bakom** förslaget att tjänster inom ett samordnat statligt tjänsteutbud ska levereras av flera myndigheter för att minimera riskerna med aggregerade informationsmängder. Man ska dock ha med det faktum att den redundans som krävs bland annat föreslås säkerställas genom spegling, vilket innebär att aggregerad information på någon nivå ändå kommer att förekomma. Där kommer kravet på informationsskydd genom kryptering att spela stor roll.

I avsnitt 10.6.6 föreslår utredningen en avgränsning av säkerhetskänslig verksamhet, och vilka myndigheter som ska undantas från förordningens tillämpningsområde. I avsnitt 10.6.7 bedömer utredningen att säkerhetsskyddsklassificerade uppgifter inte ska hanteras inom det samordnade statliga tjänsteutbudet. **Internetstiftelsen delar inte** denna bedömning, det vill säga kraven på högre säkerhet och många myndigheters oförmåga att bedriva ett systematiskt informationssäkerhetsarbete. Bedömningen att utestänga en stor del av de myndigheter som hanterar säkerhetskyddsklassificerade uppgifter i sin verksamhet från den samordnade statliga it-driften, och hänvisa dem till

drift i egen regi bör omprövas. **Internetstiftelsen anser** det närmast självklart att den föreslagna it-driften ska kunna omfatta även säkerhetsskyddsklassificerade uppgifter. Försvarsmakten har till och med framhållit att det inte finns något hinder att inkludera säkerhetsskyddsklassificerade uppgifter i ett samordnat statligt tjänsteutbud om gällande krav i säkerhetsskyddslagen uppfylls.

Internetstiftelsen har inget att erinra mot förslaget om att leveransen av tjänster ska finansieras genom avgifter. **Internetstiftelsen delar också uppfattningen** att de myndigheter som får uppdraget att leverera tjänster tilldelas anslag för att finansiera förberedelser som krävs. Enligt Internetstiftelsen är kostnadstäckning eftersträvansvärt.

11. Förslag till varaktiga former för samordnad statlig it-drift

11.1 Mål och syfte för en samordnad statlig it-drift

Internetstiftelsen tillstyrker förslaget, men anser att MSB är den myndighet som i samverkan med DIGG och leverantörsmyndigheterna bör få uppdrag att ta fram nolläge och nyckelindikatorer för uppföljning av bland annat säkerhet och kostnadseffektivitet.

11.2 Organisering av en samordnad statlig it-drift

Internetstiftelsen tillstyrker förslaget om en samordnad statlig it-drift som organiseras genom en samordnande myndighet och flera leverantörsmyndigheter. I likhet med utredningen **anser Internetstiftelsen** att det är viktigt att omhänderta de initiativ som pågår samt det intresse som finns hos flera myndigheter att bidra till en samordnad statlig it-drift. **Internetstiftelsen föreslår** att det bästa är att bygga vidare på och genomföra dels Säkra it-tjänster i statlig samverkan (SITSSAM), dels Program 2032.

Internetstiftelsen anser att utredningen på ett för kortfattat sätt har avfärdat idén om en it-driftsmyndighet, utan djupare analys av tänkbara effekter och konsekvenser.

Internetstiftelsen delar inte helt bilden som utredningen ger av att it-drift är ett smalt område och därmed inte ska hanteras som en del av den förvaltningsgemensamma digitala infrastrukturen. Det är viktigt att ha ett helhetstänkande i sammanhanget.

11.3 Aktörer: uppgifter, ansvar och roller

Internetstiftelsen ser en uppenbar risk med utredningens förslag att koncentrera allt till en samordnande myndighet med omfattande ansvar och mandat. I förslaget framstår det som att leverantörsmyndigheterna kommer in alltför sent i processen, när val redan har gjorts och enbart själva anslutningsprocessen kvarstår. **Enligt Internetstiftelsen** innebär det en risk för friktion och mindre väl underbyggda beslut än om leverantörsmyndigheterna är med tidigt i processen.

Utredningen föreslår att den samordnande myndigheten ska samråda med Försvarsmakten i frågor om Sveriges säkerhet kopplade till den samordnade statliga it-driften. **Internetstiftelsen ställer sig frågande till** om detta inte blir en dubblering av det som idag är Säkerhetspolisens ansvar.

Internetstiftelsen delar inte utredningens uppfattning om att det är den samordnande myndigheten som ska bevaka och delta i relevanta samarbeten och sammanhang både nationellt och internationellt. Det förefaller **enligt Internetstiftelsen** som att den kompetens som redan finns hos leverantörsmyndigheterna är bättre lämpad att ingå i sådant arbete, något som flera av dem också gör.

11.3.2 Leverantörsmyndigheter

Internetstiftelsen anser att leverantörsmyndigheterna ska involveras långt tidigare i processen än vad utredningen föreslår.

11.3.3 Stöd- och expertmyndigheter

Internetstiftelsen delar i stort utredningens förslag.

11.4 Forum för samverkan

Utredningens bedömning att det finns behov av samverkan i olika forum och på olika nivåer riskerar **enligt Internetstiftelsens uppfattning** att leda till onödig byråkrati. Den föreslagna samverkansmodellen behöver **enligt Internetstiftelsens uppfattning** renodlas, och utvecklas över tid. Att redan från början inrätta flera olika råd för olika frågor förefaller inte vara effektivt.

11.5 Anslutning av myndigheter

Internetstiftelsen upprepar sin ståndpunkt att det utvecklingsarbete som bedrivs inom SITSSAM inte bara bör tillvaratas utan är det som man bör bygga vidare på. I det sammanhanget får den samordnande myndigheten just ett samordnande ansvar, med mindre operativa frågor på sitt ansvar. Dessa operativa delar bör hanteras av leverantörsmyndigheterna för att skapa en obruten kedja i processen från initiering, planering och till genomförande.

Internetstiftelsen delar utredningens bedömning i 11.5.2 att leverantörsmyndigheternas säkerhetsnivå bör dimensioneras efter de högst ställda kraven på säkerhet från en anslutande myndighet.

11.6 Förutsättningar utifrån säkerhetsskydd

I enlighet med vad Internetstiftelsen anfört tidigare **anser Internetstiftelsen** det självklart att även myndigheter som hanterar säkerhetsskyddad information ska kunna ta del av den samordnade statliga it-driften. Att utestänga en stor del av de myndigheter som hanterar säkerhetskyddsklassificerade uppgifter i sin verksamhet från den samordnade statliga it-driften, och hänvisa dem till drift i egen regi riskerar att befästa den situation som många av dem befinner sig i idag, och som är ett av motiven till varför man vill ha en samordnad it-drift.

Internetstiftelsen vill också understryka vikten av det utredningen påtalar, att den samordnande myndigheten och leverantörsmyndigheten behöver verka för att motarbeta oönskade beroenden där ett övervägande antal eller samtliga myndigheter

använder en eller ett fåtal produkter, tjänster eller leverantörer inom det samordnade statliga tjänsteutbudet.

11.7 Reglering av villkoren för leverantörsmyndigheternas behandling av personuppgifter

Internetstiftelsen tillstyrker förslaget om att behandling av personuppgifter regleras i förordning samt att villkor som följer av artikel 28.3 i dataskyddsförordningen regleras i den skriftliga överenskommelsen mellan de aktuella parterna.

11.8 Samordnad upphandling av privata leverantörers tjänster

Internetstiftelsen förordar en modell där myndigheterna i samverkan har en gemensam funktion för upphandling av it-driftstjänster. **Internetstiftelsen anser** dock att behovsbedömningen ska göras i ett större sammanhang än enbart av den samordnande myndigheten. Den samordnande myndigheten kan koordinera men ansvaret för behovsinsamling och teknisk och rättslig kravställning bör ligga hos den upphandlande myndigheten, Kammarkollegiet, i samverkan med leverantörsmyndigheterna, då det är där beställarkompetensen kan förväntas finnas.

Internetstiftelsen har inga invändningar mot förslaget om ramavtal för it-drift för små myndigheter.

11.9 Konkurrensrättsliga överväganden

Internetstiftelsen har inga synpunkter på de bedömningar och förslag som lämnas i dessa frågor.

11.10 Aktörer som kan vara aktuella i en samordnad statlig it-drift

Utredningen föreslår i 11.10.1 att DIGG ska ges i uppgift att vara samordnande myndighet för den samordnade statliga it-driften. **Internetstiftelsen delar uppfattningen, men med förbehållet** att DIGG:s roll bör bli mindre operativ och mer av karaktären kanslifunktion och koordinator till stöd för leverantörsmyndigheterna. DIGG framhåller själva att det för att myndigheten ska kunna ta ett uppdrag som samordnande myndighet enligt den modell som föreslås av utredningen kommer att krävas finansiering och tid för att bygga upp nödvändig kompetens och förmåga avseende it-drift. **Internetstiftelsen anser** det vara mer kostnadseffektivt och ändamålsenligt att använda den befintliga kompetensen hos leverantörsmyndigheterna.

DIGG har ett uppdrag att tillhandahålla rättsligt stöd till den offentliga förvaltningen i förvaltningsgemensamma digitaliseringsfrågor, och har tolkat sitt uppdrag som att innefatta informationssäkerhet. **Internetstiftelsen är av uppfattningen** att det redan är tillräckligt många myndigheter som har som uppdrag att ge stöd i frågor som rör informations- och cybersäkerhet. Dessutom ska den så kallade ansvarsprincipen fortfarande råda, och det kan **enligt Internetstiftelsen** uppfattas som att respektive myndighet fråntas sitt ansvar om den samordnande myndigheten ger ett starkare uttryck för att frågorna hanteras där.

Internetstiftelsen har inga invändningar mot utredningens förslag om vilka myndigheter som ska ges i uppgift att vara leverantörsmyndigheter och erbjuda it-driftstjänster inom ramen för ett samordnat statligt tjänsteutbud; Försäkringskassan, Lantmäteriet, Skatteverket och Trafikverket. **Internetstiftelsen anser** däremot att förordningen inte bör begränsa sig till dessa, utan lämna öppning för att ytterligare leverantörsmyndigheter kan tillföras på ett enkelt sätt.

11.11 Införande av varaktiga former för samordnad statig it-drift

Internetstiftelsen delar utredningens uppfattning om att den samordnade statliga it-driften ska etableras genom ett stegvis förfarande, men att MSB snarare än ESV bör få i uppdrag att ta fram indikatorer för uppföljning. **Internetstiftelsen välkomnar** att Statskontoret får ett uppdrag att utvärdera effekten och konsekvenserna av sådan drift.

12. Konsekvensutredning

Utredningen lyfter som en konsekvens av förslagen att DIGG behöver bygga upp egen kompetens och förmåga inom säkerhet för att kunna bedöma, hantera och samordna säkerhetsfrågor inom den samordnade statliga it-driften. Med tanke på att man i utredningen också lyfter fram den stora brist som råder på sådan kompetens **anser Internetstiftelsen** att det är mer effektivt att utnyttja den befintliga kompetens som finns hos leverantörsmyndigheten samt hos MSB, IMY, PTS och andra myndigheter, som redan har uppdrag på det området.

Internetstiftelsen delar bedömningen att en samordnad statlig it-drift kommer att bidra till en ökad informationssäkerhet i statsförvaltningen, trots att det kan innebära en ökad koncentration av uppgiftssamlingar. Detta går att hantera med krav på tillräckligt god informationssäkerhet. Med tanke på att flera myndigheter idag har anslutit till tjänster som tillhandahålls av ett fåtal privata aktörer är sådan koncentration i vissa fall redan ett faktum.

Sammanfattning

Internetstiftelsen ställer sig till stora delar bakom utredningens förslag om en samordnad statlig it-drift som i sin utgångspunkt baseras på leveransförmågan hos privata aktörer. Ett förslag till modifiering är att den samordnande myndigheten får en mer begränsad roll som för att stödja leverantörsmyndigheterna, men att det mer operativa ansvaret ligger hos leverantörsmyndigheterna under hela processen.

Internetstiftelsen efterlyser en konkretisering av vad som avses med it-drift, och föreslår att även grundläggande tjänster som DNS, webbhosting och mejlhosting ska ingå.

Internetstiftelsen föreslår också en gemensam specifikation av grundskyddsnivå som ska utgöra en lägsta ribba för säkerhetsnivån hos anslutande myndigheter. Kraven på myndigheternas arbete med informationssäkerhet kommer att skärpas i takt med att nya EU-direktiv antas och omsätts i svensk lag.

Stockholm den 21 mars 2022

Carl Piva

Vd, Internetstiftelsen