IVA | Svenska framtider

Resilient Digital Infrastruktur

Stärkt motståndskraft för framtidens samhälle och näringsliv

Innehåll

Förord

Sverige behöver vara ledande på resilient digital infrastruktur

Vår vardag, vår ekonomi och vår säkerhet vilar på en digital infrastruktur som vi tar för självklar, tills den prövas. Störningar, cyberhot, AI:s snabba utveckling och ett skarpare geopolitiskt läge gör att frågan om resiliens aldrig varit mer brännande. Denna infrastruktur är idag en absolut nödvändighet för samhällets funktion. Om den inte fungerar får det direkt negativa konsekvenser på funktioner långt utanför den digitala sektorn.

IVAs projekt Resilient Digital Infrastruktur har haft som mål att identifiera konkreta åtgärder för att stärka Sveriges digitala motståndskraft. Arbetet har utgått från realistiska störningsscenarier och analyserat både tekniska och organisatoriska sårbarheter, företeelser som blivit än mer aktuella under projektets gång.

Projektet visar tydligt hur avgörande en pålitlig och resilient digital infrastruktur är för industrin, näringslivet och samhället. För att möta framtiden måste Sverige ligga i nivå med de bästa länderna i världen.

Utöver konkreta förslag vill projektet bidra till en bredare och mer nyanserad diskussion om vikten av ett samordnat arbete mellan offentlig sektor och näringsliv för att stärka Sveriges digitala infrastruktur.

IVAs styrka som oberoende aktör är att engagera individer med djup kompetens och lång erfarenhet. Förutom styrgruppen har ett femtiotal personer medverkat i projektets arbetsgrupper. Rapportens analyser och förslag bygger till stor del på underlag från arbetsgrupperna, men styrgruppen ensam ansvarar för rapportens innehåll.

Som i alla IVA-projekt medverkar deltagarna i sin personliga kapacitet och inte som företrädare för organisationerna i vilka de är verksamma. Jag vill framföra ett varmt tack till deltagarna i styr- och arbetsgrupper för ert stora engagemang och bidrag till rapporten.

Stockholm i september 2025

Pia Sandvik, styrgruppsordförande

Styrgrupp

Pia Sandvik (ordf.), IVA-ledamot, Teknikföretagen
Daniel Akenine, IVA-ledamot, Microsoft
Björn Ekelund, IVA-ledamot, Ericsson
Anne-Marie Eklund Löwinder, IVA-ledamot, Amelsec

Patrik Fältström, IVA-ledamot, Netnod
Åke Holmgren, Myndigheten för samhällsskydd och beredskap (MSB)
Pontus Johnson, IVA-ledamot, Kungl. Tekniska högskolan (KTH)
Hans Lindberg, IVA-ledamot, Svenska Bankföreningen
Charlotte Lindgren, Försvarets radioanstalt (FRA)
Johan Malmliden, Omegapoint
Simin Nadjm-Tehrani, IVA-ledamot, Linköpings universitet
Anna Rathsman, IVA-ledamot, fd. gd Rymdstyrelsen

Projektledning

Per Hjertén, projektledare
Staffan Eriksson, delprojektledare
Linda Olsson, delprojektledare
Eva Lagerblad, projektkoordinator

Finansiärer

Combitech
Ericsson
Försvarets radioanstalt (FRA)

Internetstiftelsen

Microsoft

Myndigheten för samhällsskydd och beredskap (MSB)

Omegapoint

Svensk Dagligvaruhandel

Svenska Bankföreningen

Teknikföretagen

Vattenfall

Projektet är en del av visionsprojektet Svenska framtider.

Sammanfattning

Digital motståndskraft är grunden för innovation, tillväxt och trygghet

Den digitala infrastrukturen är grundläggande för samhällets funktion, ekonomi och säkerhet; något som ofta tas för givet. Med förändringar i det geopolitiska läget, återkommande cyberhot och en snabb teknologisk utveckling har digital motståndskraft blivit en än viktigare fråga.

Samhällets beroende av digitala system är så djupt att ett avbrott i centrala flöden – vare sig det gäller elförsörjning, logistik, sjukvård eller finansiella transaktioner – omedelbart kan lamslå vitala funktioner långt utanför den digitala sektorn. Funktioner i samhället som tidigare fungerade utan digitala system gör inte det längre. Konsekvenserna av ett sådant digitalt haveri kan vida överstiga effekterna av en traditionell kris. Att stärka Sveriges digitala resiliens är därför inte en framtidsfråga, utan en omedelbar nödvändighet för att säkra samhällets grundläggande funktioner.

För att bygga verklig motståndskraft krävs ett helhetsperspektiv där den digitala infrastrukturen ses som ett komplext ekosystem av ömsesidiga beroenden. Den svagaste länken kan finnas var som helst. Det räcker inte med att fiberkablarna är intakta och mobilnäten fungerar; ett samhälle kan ändå lamslås om digitala tjänster för identifiering eller betalningar slutar fungera, eller om kritisk information blir otillgänglig.

För att illustrera denna komplexitet används en modell där den digitala infrastrukturen är uppbyggd i lager och där varje lager är beroende av de underliggande. Hela denna struktur ramas in av ett övergripande skikt av lagar, regelverk och styrning. En störning i ett enda lager riskerar att få följdeffekter i hela systemet, vilket understryker behovet av samordnade insatser över alla nivåer och sektorsgränser.

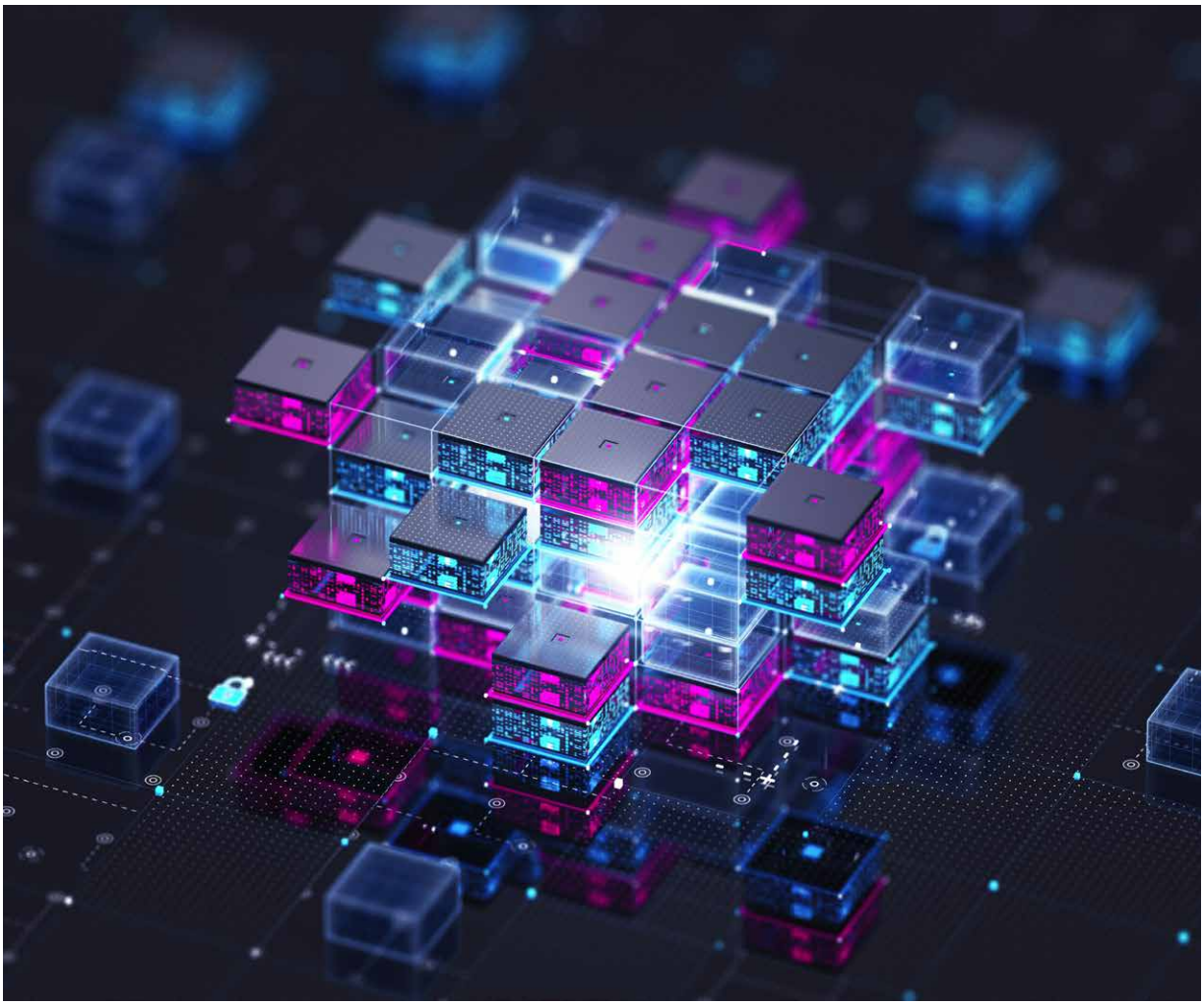
En robust digital infrastruktur är inte bara en förutsättning för att hantera kriser, utan även en motor för Sveriges innovation och konkurrenskraft. För att säkra både välfärd och tillväxt måste Sverige kunna dra nytta av avancerad teknik som 5G, AI, molntjänster och rymdbaserade system, utan att öka sårbarheten för tekniska eller geopolitiska störningar. Detta kräver en balansgång mellan möjligheter och risker, där innovation måste prioriteras lika högt som motståndskraft. En central utmaning är dagens regelverk, som ofta upplevs som fragmenterat, detaljerat och dåligt anpassat till den snabba teknikutvecklingen, något som skapar osäkerhet och en tung administrativ börda för många organisationer.

För att möta utmaningarna krävs ett långsiktigt och samordnat arbete med konkreta åtgärder som involverar både offent-

liga och privata aktörer och spänner över hela infrastrukturen. Därför föreslås ett antal åtgärder för att stärka resiliensen i den digitala infrastrukturen.

På en övergripande nivå föreslås en harmonisering av regelverk för att minska administrationen och undvika att företag och organisationer möts av motstridiga krav. Lagstiftaren bör fokusera mer på ansvarsutkrävande än regelefterlevnad, som exempelvis processer och tekniska krav, vilka snabbt blir föråldrade. För att stärka den praktiska förmågan vid kriser behövs ett utökat operativt privat–offentligt samarbete, där fler beredskapssektorer etablerar forum för samverkan. Denna samverkan måste kompletteras med tvärsektoriella tester och övningar för att hantera störningar som påverkar flera samhällsfunktioner samtidigt. Det konstateras att viss lagstiftning idag kan hämma innovation och utveckling och därför föreslås en översyn för att skapa bättre förutsättningar som kan möta framtida hot och störningar.

Vidare föreslås åtgärder med fokus på informations- och tjänsteresiliens. Det behövs ett tydligare ansvar för information, där Sverige implementerar principer för att undvika dubbellagring och säkerställa ansvaret för kvaliteten på grundläggande data.



Detta måste följas av ett lika tydligt ansvar för att informationen hålls tillgänglig och säker. För att stödja mindre aktörer i deras säkerhetsarbete föreslås en gemensam kravställning på digitala tjänster. För molntjänster betonas vikten av att både använda dem för att skapa resiliens och undvika inlåsningseffekter.

Slutligen adresseras den tekniska och fysiska delen av infrastrukturen. För att stärka den digitala infrastrukturens mot-

ståndskraft krävs att varje teknologi utnyttjas. Här föreslås bland annat stärkta åtgärder för skydd och övervakning av fiberinfrastruktur, en mer ändamålsenlig reglering av nationell roaming och prioritering i mobilnäten. Elförsörjning är vital för den digitala infrastrukturen och energigemenskaper föreslås som stärkande åtgärd. Rymden uppmärksammas som ett område där Sverige behöver stärka sitt engagemang. Även riktlinjer för hur AI bör hanteras i en resilient infrastruktur ingår i förslagen.

En resilient digital infrastruktur är en förutsättning för att samhället ska fungera. Med de föreslagna åtgärderna vill vi bidra till stärkt motståndskraft och innovationsförmåga. Vår förhoppning är att rapporten används som underlag för fortsatt gemensamt arbete mellan näringsliv, offentlig förvaltning och politik.

TABELL 1: Förslag på åtgärder med föreslagna aktörer för genomförande och önskade effekter.

Åtgärdsförslag	Aktörer för genomförande	Önskad effekt
Regelharmonisering	Privata aktörer, offentliga organisationer och myndigheter, regeringen, Förenklingsrådet	Minskad administrativ börda och ökad effektivitet
Operativt privat–offentligt samarbete vid incident-hantering och återställning	Regeringen, sektors-myndigheterna, NCSC	Snabbhet och effektivitet vid incidenter och återställning
Behov av tvärsektoriella tester och övningar	MSB, sektorsmyndigheterna, civil-områdena, NCSC, Cybercampus	Förbättrad beredskap och reaktionsförmåga, kompetens
Förutsättningar för utveckling av nya lösningar mot hot och störningar	Riksdagen, PTS	Ökad förmåga för företag att skapa resilient teknikutveckling
Tydligt ansvar för information	DIGG, de samordnade leverantörsmyndigheterna	Känt vilken information och tjänster som är viktiga
Tydligt ansvar för att information ska vara tillgänglig	MSB, sektorsmyndigheterna, de samordnade leverantörs-myndigheterna	Ökad tillgänglighet och skydd av information
Gemensam nationell krav-ställning på digitala tjänster	PTS, MSB, Upphandlings-myndigheten	Ökad säkerhet och kvalitet på digitala tjänster. Stöd till SME.
Molntjänster för resiliens och resiliens för molntjänster	Privata företag, Vinnova, Tillväxtverket, MSB, DIGG, de samordnade leverantörs-myndigheterna, privata och institutionella finansiärer	Minskad risk för leverantörs-beroenden samt stärkt resiliens-förmåga genom strategisk användning av molntjänster.
AI och resiliens	AI-kommissionens förslag för aktörer, alt. DIGG, PTS.	Säkring av AI:s del i resilient digital infrastruktur
Mobilnätens roll	Mobiloperatörer, Försvarsmakten, PTS	Ökad tillgång för olika användare och i olika nivåer av kris
Skydd och övervakning av fiberinfrastruktur	PTS, Försvarsmakten, Polismyndigheten, Kustbevakningen, fiberägare	Minskad sårbarhet och stärkt resiliens genom koordinerat och proaktivt arbete
Rymdbaserade tjänster och dess påverkan på övrig infrastruktur	Regeringen, PTS, RISE, Netnod, Försvarsmakten, MSB, Rymdstyrelsen, EU-samarbete	Ökat strategiskt engagemang för rymden och förbättrad redundans i viktiga funktioner
Mer robust elförsörjning genom kompletterande lösningar	Regeringen, riksdagen	Ökade möjligheter att generera och använda lokal el för infra-struktur vid avbrott eller angrepp

Motståndskraft i en tid av digitalt beroende

Den svagaste länken kan finnas var som helst

DEFINITIONER

Digital infrastruktur (inspirerad av Tech Sverige)

”Begreppet digital infrastruktur omfattar de komponenter som är avgörande för att stödja digitala tjänster och applikationer. Dessa kan vara både hårda (som kommunikationsnät och datacenter) och mjuka (som standarder, identitets- och betalningslösningar).”

Resilient (inspirerad av MSB)

”Relevant, tillförlitlig och motståndskraftig med förmåga till återhämtning och vidareutveckling.”

För att bygga verklig motståndskraft krävs ett helhetsperspektiv. Det räcker därför inte att säkra den fysiska infrastrukturen. Även om fiberkablarna ligger orörda och mobilnäten fungerar kan samhället lamslås om informationsflöden störs eller om digitala tjänster för betalningar, identifiering eller logistiksystem slutar fungera. Därför är det lika viktigt att säkra såväl informations- som tjänsteresiliens. Dessutom påverkas förmågan att skapa motståndskraft av lagar, regler och samverkansformer. En stabil och robust digital infrastruktur är också cen-

tral för näringslivets och Sveriges konkurrenskraft och innovationsförmåga.

Den snabba teknikutvecklingen, i kombination med ett ökat beroende av digitala produkter och tjänster från andra länder, skapar både möjligheter och osäkerhet. Tillgång till teknik som fiber, molntjänster, AI, 5G, rymdbaserade system och lösningar är avgörande för den digitala infrastrukturens resiliens. Sverige och EU måste kunna dra nytta av dessa tekniker utan att samtidigt öka sårbarheten för geopolitiska eller tekniska störningar.

Lager för lager – men hur stark är helheten?

För att visa hur de olika delarna av den digitala infrastrukturen hänger samman har IVA tidigare introducerat en beskrivande lagerstruktur, den så kallade Lasagnemodellen.[1] I detta projekt har modellen utökats med ett överliggande organisatoriskt lager som omfattar lagar, regelverk och styrning samt ett underliggande lager som innehåller elförsörjning.

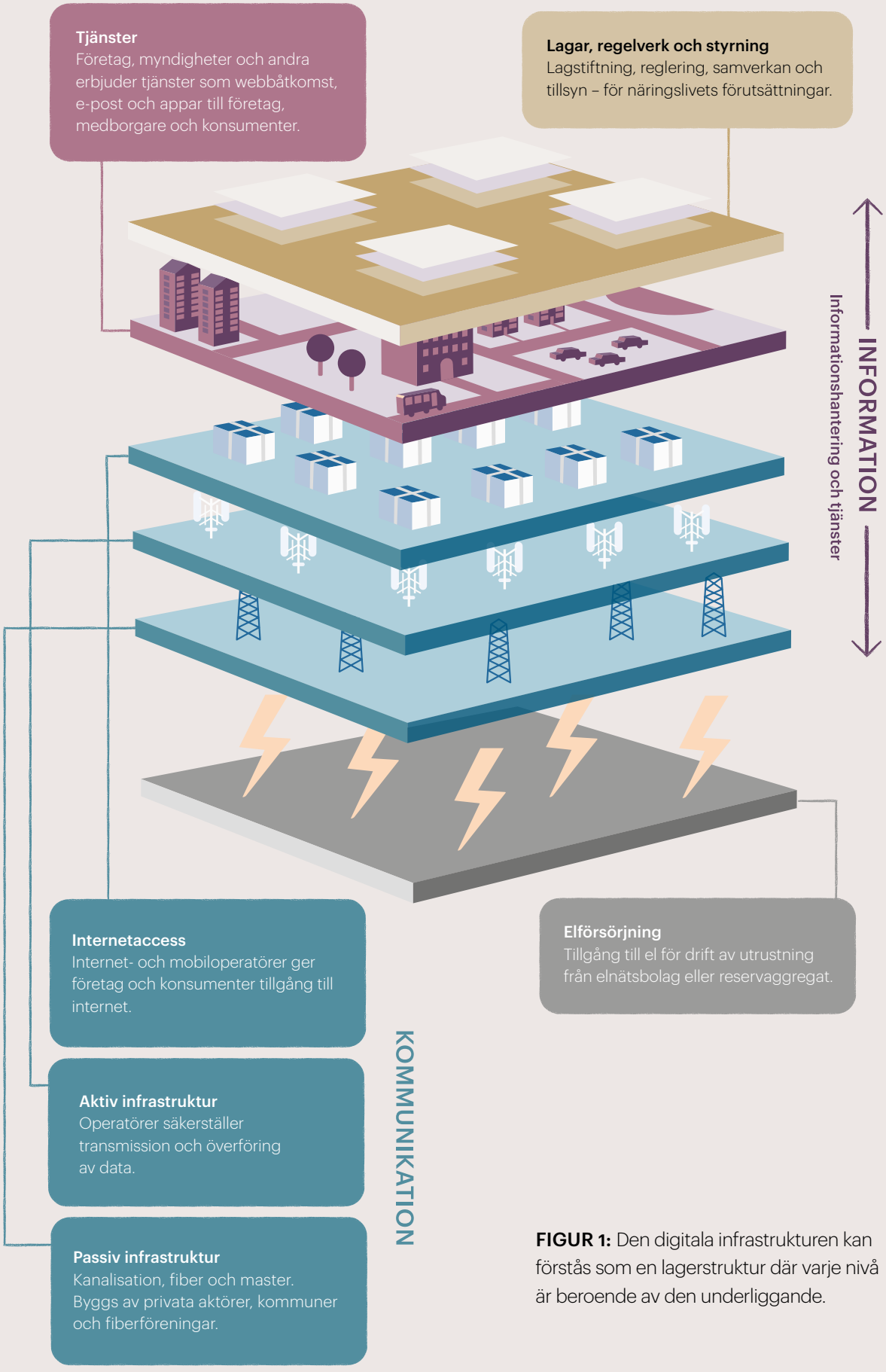
1 IVA, *Digitalisering för ökad konkurrenskraft*, projektrapport (2019), https://www.iva.se/publicerat/rapport-digitalisering-for-okad-konkurrenskraft/.

Modellen illustrerar komplexiteten i samverkan inom den digitala infrastrukturen där teknik, organisation och tillämpning är beroende av varandra.

Den digitala infrastrukturen kan förstås som en lagerstruktur där varje nivå är beroende av den underliggande, se Figur 1. Längst ned finns elförsörjningen, som möjliggör drift av all utrustning och därmed är en grundläggande förutsättning. Ovanpå detta vilar den passiva infrastrukturen i form av fiber, kanalisation och master, som tillsammans utgör nätens fysiska stomme. Den kompletteras av aktiv infrastruktur, där operatörer säkerställer överföring och transmission av data. Genom internetaccess kan företag och konsumenter koppla upp sig. På nästa nivå finns tjänster såsom webbåtkomst, e-post och appar som levereras av företag, myndigheter och organisationer. Överst finns lagar, regelverk och styrning, som sätter ramarna för en säker, robust och tillförlitlig digital miljö.

Modellen belyser också två genomgående perspektiv: kommunikation, som förbinder de undre lagren, och information, som beskriver flödet i de övre lagren där data hanteras och delas i tjänster för användare.

Aktörer som ansvarar för ett eller flera lager i modellen behöver



FIGUR 1: Den digitala infrastrukturen kan förstås som en lagerstruktur där varje nivå är beroende av den underliggande.

samordna sig och samarbeta för att upprätthålla och utveckla både funktionalitet och resiliens. I detta gemensamma arbete finns flera centrala begrepp och principer att förhålla sig till:

- **Redundans** i system och kommunikation, speciellt genom diversitet, säkerställer att funktioner kan upprätthållas även vid avbrott eller fel.
- **Isolering** och **segmentering** hindrar att störningar sprids.
- **Automatisering** och **kontinuerlig övervakning** möjliggör snabb respons och minskar sannolikheten för fel.
- **Verifiering** och **test** är centralt för att garantera att kritiska funktioner kan återupprättas snabbt och tillförlitligt.
- **Övning** utvecklar kompetens och avslöjar brister i lösningar och rutiner under säkra förhållanden och i en skyddad miljö.
- **Robusta säkerhetsåtgärder** som kryptering och åtkomstkontroll säkrar integritet och tillgänglighet.

För att digitala tjänster och system ska vara motståndskraftiga måste den underliggande fysiska infrastrukturen vara robust,

tillgänglig och skyddad mot både avsiktliga och oavsiktliga hot och störningar. Centralt är noggrant planerad arkitektur och diversifiering, det vill säga riskspridning genom att till exempel använda flera olika leverantörer.

I Sveriges nationella strategi för cybersäkerhet[2] adresseras den fysiska digitala infrastrukturen på flera sätt. Till exempel ska Försvarets Radioanstalt (FRA) och Myndigheten för samhällsskydd och beredskap (MSB), inom ramen för NCSC (Nationellt cybersäkerhetscenter), ta fram riktlinjer för att säkerställa tillgänglighet, integritet och konfidentialitet i den offentliga kärnan av det öppna internet, inklusive skydd av undervattenskablar. Myndigheterna ska också, inom ramen för NCSC, ta fram riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling.

Utöver detta ställer det förändrade hotläget och den snabba teknikutvecklingen inom både fast och trådlös kommunikation allt högre krav på säkerhet och tillförlitlighet. I många fall behö-

2 Försvarsdepartementet, *En ny era av cybersäkerhet – Nationell strategi för cybersäkerhet 2025–2029 Bilaga 1: Handlingsplan* (Regeringskansliet, 20 mars 2025), https://www.regeringen.se/informationsmaterial/2025/03/nationell-strategi-forcybersakerhet-2025-2029/.

ver lagar och regelverk anpassas för att möjliggöra forsknings- och utvecklingsinsatser för att ta fram efterfrågade tekniska lösningar.

För att uppnå god driftssäkerhet och upprätthålla viktiga samhällsfunktioner i krissituationer måste kommunikationsnät byggas med alternativa signalvägar och använda sig av den senaste teknologin som, rätt utnyttjad, kan ge högre tillförlitlighet, bättre prestanda i extremsituationer och ett bättre skydd mot avsiktliga störningar.

Innovation kräver kompetens och infrastruktur

Den digitala infrastrukturen är en viktig innovationsplattform

Digitalisering medför samhällsförändringar som gör att nya kunskaper och färdigheter behövs. Ett bortfall av digitala system skapar idag direkt negativa konsekvenser för sektorer som tidigare inte behövde sådana för sin funktion. Förutom behov av kompetensutveckling inom digitalisering krävs nu även kompetens tvärsektoriellt till följd av de nya beroenden som uppstått.

Innovation och konkurrenskraft kräver en robust och pålitlig infrastruktur att bygga på. Precis som elektrifieringen har format industrisamhället, utgör den digitala infrastrukturen grunden för dagens och morgondagens digitala ekonomi. Studier från bland annat FN[3] och World Economic Forum[4] visar att tillgång till digital infrastruktur inte bara accelererar ett lands digitala mognad utan också driver nyföretagande, innovation och konkurrenskraft.

3 "Sustainable development goals", Förenta Nationerna, åtkomstdatum 12 september 2025, https://www.un.org/sustainabledevelopment/infrastructure-industrialization/.

4 "Why digital public infrastructure is key to building a connected future", World Economic Forum, 17 april 2025, https://www.weforum.org/stories/2025/04/digital-public-infrastructure-building-connected-future/.

Inom OECD växer den digitala ekonomin dubbelt så snabbt som den totala ekonomin. Enligt analysföretaget Forrester[5] förväntas den motsvara 17 procent av världens BNP redan år 2028. Digital innovation är därför avgörande för Sveriges framtida konkurrenskraft och välfärd.

För att nå en ledande position inom digital innovation krävs en digital infrastruktur som bygger på den senaste tekniken. En modern 5G- och fiberinfrastruktur skapar betydligt större värden än äldre teknologiplattformar som 4G och kopparledningar – inte minst inom säkerhet och resiliens.

Länder som USA, Kina, Sydkorea och Japan har tagit fasta på detta och investerar offensivt i bland annat mobilnätsteknologi, väl medvetna om de potentiella nationalekonomiska vinsterna. Europa släpar däremot efter när det gäller 5G-utbyggnaden, vilket bland annat lyfts fram i Draghi-rapporten.[6]

5 Michael O'Grady, "The Global Digital Economy Will Reach $16.5 Trillion And Capture 17% Of Global GDP By 2028", Forrester, 23 juli 2024, https://www.forrester.com/blogs/the-global-digital-economy-will-reach-16-5-trillion-and-capture-17-of-global-gdp-by-2028/.

6 EU-kommissionen, *The Draghi report on EU competitiveness* (2024), https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

EU har uppmärksammat hur viktig den digitala infrastrukturen är för konkurrenskraften, och på EU-nivå görs bland annat stora satsningar på AI-kluster och datacenter. Något som dock ofta glöms bort är att det även krävs en infrastruktur för kommunikation av minst samma kaliber för att fullt ut realisera värdet av satsningarna.

Det är inte bara den digitala infrastrukturens prestanda som skapar värden utan också dess tillgänglighet och tillförlitlighet. Stabilitet, säkerhet, och tillförlitlighet kan också, precis som säker och billig energi, attrahera och driva investeringar och innovation.

I Sveriges nationella strategi för cybersäkerhet[7] finns ett antal åtgärder som adresserar innovation och kompetensförsörjning, till exempel *Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet*. Även *Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter* pekar på åtgärder inom AI och kvantkrypto. IVA anser dock att de inte täcker de

7 Försvarsdepartementet, *En ny era av cybersäkerhet – Nationell strategi för cybersäkerhet 2025–2029 Bilaga 1: Handlingsplan* (Regeringskansliet, 20 mars 2025), https://www.regeringen.se/informationsmaterial/2025/03/nationell-strategi-for-cybersakerhet-2025-2029/.

POSTKVANTKRYPTOGRAFI

Användning av kvantdatorer för kodknäckning är ett hot mot många av de kryptografiska lösningar som idag används för att skydda data. Postkvantkryptografi är samlingsnamnet för krypteringslösningar som förblir säkra även när kvantdatorer används. Detta är särskilt viktigt för att framtidssäkra branscher som till exempel banker, hälso- och sjukvård med flera som använder traditionell kryptering. Trots att kvantdatorer för kodknäckning fortfarande ligger några år bort finns redan i dag risker. Inget hindrar en antagonist från att lagra krypterad data för att senare dekryptera den när möjligheten finns. Det här är något som hanteras inom bland annat Försvarsmakten.

För att klara framtidens utmaningar behövs mer arbete för att skapa en infrastruktur som är redo för kvantdatorer. Flera andra länder bedriver redan sådana program, vilket är avgörande för att ligga steget före. Det finns goda exempel i till exempel USA och Nederländerna där Sverige kan hämta inspiration.

nya tvärsektoriella beroenden som skapas i och med samhällets digitalisering.

Lika viktigt som tekniken och infrastrukturen i sig är tillgång till kompetens på samma höga nivå. För Sverige förutsätter det

satsningar på digitala spetsteknologier som AI och cybersäkerhet, en stärkt STEM-utbildning och att livslångt lärande både bedrivs och premieras. Insatser behövs i hela utbildningskedjan, från skola och högre utbildning till fortbildning av yrkesverksamma. Även allmänhetens medvetenhet behöver stärkas genom breda folkbildningsinsatser, men snarare av skäl som handlar om allmän kunskap om it- och informationssäkerhet, och inte nödvändigtvis den digitala infrastrukturens resiliens.

Campus totalförsvar[8] är ett strategiskt samarbete mellan svenska lärosäten med målet att stärka Sveriges totalförsvarsförmåga genom utbildning och forskning. MSB och flera andra myndigheter har efter utredningen ”Plikten kallar!”[9] fått centrala roller i att utreda behovet av och förutsättningar för civilplikt för it-system och cybersäkerhet. Dessa och liknande pågående arbeten är viktiga sätt att praktiskt verka för ökad kompetensförsörjning.

8 Campus totalförsvar. (2025). https://campustotalforsvar.se/

9 SOU 2025:06 Plikten kallar! En modern personalförsörjning av det civila försvaret, Försvarsdepartementet, https://regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/01/sou-20256/.

Från direktiv till stärkt förmåga

Bra regelverk ökar förmågan och stärker den digitala resiliensen

Gemensamma spelregler och tydlig styrning leder till stärkt förmåga. Reglering på EU- och nationell nivå är delar i detta som syftar till att skapa förutsägbarhet. För att göra den digitala infrastrukturen mer robust, öka motståndskraften mot cyberhot och höja förmågan hos samhällsfunktioner som är beroende av digitala system genomför EU och Sverige omfattande regleringar och satsningar. NIS2[10] och Cyber Resilience Act[11] är två av de mest uppmärksammade regleringar som nu införs.

EU har stärkt cybersäkerhetslagstiftningen genom det uppdaterade direktivet om nät- och informationssäkerhet (NIS2), som antogs i november 2022. Direktivet syftar till att skapa en gemensam hög nivå av cybersäkerhet inom hela unionen och riktar sig specifikt mot medelstora och stora organisationer i samhällskritiska sektorer. Det innebär en tydlig ambitionshöjning jämfört med det ursprungliga NIS-direktivet från 2016.

NIS2 utvidgar tillämpningsområdet till fler sektorer och verk-

10 "NIS2 Directive: securing network and information systems", EU-kommissionen, åtkomstdatum 12 september 2025, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

11 "Cyber Resilience Act", EU-kommissionen, åtkomstdatum 12 september 2025, https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

samheter än tidigare, effektiviserar rapporteringsprocesser och pekar ut organisationers ledningar som ansvariga för arbetet med informationssäkerhet. NIS2 kommer att omsättas i en cybersäkerhetslag. Den nya lagen innehåller också regler om tillsyn och ingripandemöjligheter för verksamhetsutövare som inte följer lagens bestämmelser. Därutöver föreslås ändringar i andra lagar som rör elektronisk kommunikation, toppdomäner och sekretess. Den nya lagen och övriga lagändringar föreslås träda i kraft den 15 januari 2026.

Ett annat av EU:s nya regelverk är Cyber Resilience Act (CRA), som fastställer minimikrav för cybersäkerhet för alla produkter med digitala komponenter som säljs inom EU. Förordningen omfattar allt från konsumentelektronik till industriella styrsystem. CRA implementeras stegvis med olika delar som träder i kraft vid olika tidpunkter.

Förordningen kräver att tillverkare integrerar cybersäkerhet redan vid designen av en produkt, genomför regelbundna säkerhetstester och tydligt dokumenterar vilka hård- och mjukvarukomponenter som ingår i olika versioner av produkterna, inklusive öppen källkod.

CRA medför även att det införs motsvarande en CE-märkning för digitala och uppkopplade produkter. Märkningen, som traditionellt visat att produkter uppfyller EU:s grundläggande krav på hälsa, säkerhet och miljö, kommer framöver även att omfatta krav på cybersäkerhet. Produkter som saknar märkning kommer i allt väsentligt vara förhindrade från att säljas på EU:s inre marknad. Detta representerar ett tydligt skifte där cybersäkerhet går från att vara en "frivillig" fråga, styrd av marknadskrafter, till att bli en obligatorisk del av EU:s produktregler.

För att kostnadseffektivisera och snabba på utbyggnad av 5G- och fibernät med mycket hög kapacitet tillsatte regeringen en utredning[12] i augusti 2024. Syftet är att förenkla fiber- och 5G-utrullningen i Sverige. Utredningen ska föreslå kompletteringar och anpassningar för att möta kraven i EU:s förordning om gigabitinfrastruktur. Utredningen ska också föreslå hur tillträde till samhällsviktig infrastruktur, för installation av exempelvis basstationer, skulle kunna underlättas med bibehållen säkerhet.

12 ”Utredning för att snabba på utbyggnaden av 5G och fiber i Sverige”, Finansdepartementet, 29 augusti 2024, https://www.regeringen.se/pressmeddelanden/2024/08/utredning-for-att-snabba-pa-utbyggnaden-av-5g-och-fiber-i-sverige/.

Sveriges digitaliseringsstrategi 2025–2030[13] presenterades av regeringen i maj 2025. Ett av målen i strategin är att den digitala infrastrukturen ska vara motståndskraftig, säker och främja konkurrenskraft, innovation och hållbarhet. Strategin pekar på redan påbörjade arbeten hos ansvariga myndigheter och innehåller delmål inom områden som konnektivitet, robusthet, resiliens och redundans.

Enligt utredningen ”Samlade förmågor för ökad cybersäkerhet”[14] skulle en kraftsamling inom området informa-

13 Finansdepartementet, *Sveriges digitaliseringsstrategi 2025–2030* (2025), https://www.regeringen.se/rapporter/2025/05/sveriges-digitaliseringsstrategi-20252030/.

14 SOU 2025:79 *Samlade förmågor för ökad cybersäkerhet*, Försvarsdepartementet. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/07/sou-202579/

tions- och cybersäkerhet leda till synergier som stärker Sveriges strategiska och operativa förmåga. Utredningen pekar särskilt på att en gemensam struktur skulle möjliggöra en mer samlad och samordnad styrning av cybersäkerhetsarbetet i samhället. Detta skulle i sin tur underlätta ett effektivt ansvarsutkrävande – något som i dag ofta försvåras av otydliga gränsdragningar mellan myndigheter och sektorer.

Sverige har en av EU:s mest omfattande säkerhetsregleringar, men den saknar ofta den riskbaserade och proportionella inriktning som EU:s direktiv bygger på. Samtidigt uppstår konflikter mellan breda regelverk som NIS2 och sektorsspecifika förordningar som DORA,[15] vilket skapar en komplex och svårtolkad regelmiljö. NIS2 ställer dessutom krav utan att tydligt möjliggöra ansvarsutkrävande. Många företag upplever att kraven på digital säkerhet från olika myndigheter leder till mycket administration. Sammantaget leder detta till osäkerhet, dubbelarbete och ineffektivitet.

Trots lagar som säkerhetsskyddslagen och NIS-direktivet, samt

15 ”Om Dora”, Finansinspektionen, 12 februari 2024, https://www.fi.se/sv/forsakring/it-risker-dora/om-dora/.

befintliga strukturer för samhällsviktig verksamhet (exempelvis MSB:s sektorsindelning), är ansvarsfördelningen vid digitala störningar fortfarande oklar. Det är också otydligt hur väl samhället kan hantera digitala störningar. Regelverken är ofta så generellt formulerade att det blir svårt att översätta dem till konkret ansvar när något väl inträffar. Dessutom fokuserar lagstiftningen främst på vilka processer och rutiner som organisationer ska använda innan något inträffar, medan det ofta är oklart vilket ansvar som gäller efter att något har gått fel eller när en kritisk funktion inte fungerar, inklusive följdeffekter.

Vägen mot bättre informations-hantering

Grunden är att veta vilken information som är viktig, var den finns och vem som ansvarar för den

DEFINITIONER

Informationsresiliens innebär att kritisk information som är avgörande för att upprätthålla samhällsfunktioner och säkerställa kontinuitet i verksamheter är tillgänglig, korrekt och skyddad.

Tjänsteresiliens innebär att de digitala tjänster som används för att hantera och distribuera kritisk information är tillgängliga, robusta och pålitliga.

Den digitala infrastrukturen används för kommunikation, det vill säga hantering och utbyte av information, som i sin tur sker med hjälp av tjänster. Informations- och tjänsteresiliens är nödvändigt för att korrekt information ska finnas tillgänglig när den behövs, för den som behöver informationen och är behörig att ta del av den.

Dagens lagstiftning och föreskrifter pekar ut områden och principer, men lämnar ofta stort tolkningsutrymme om vem som bär ansvar i gränssnittet mellan myndigheter och privata aktörer, särskilt när de verkar i olika sektorer. Detta medför att ansvaret för *vad* som är viktigt, *vem* som faktiskt bär ansvaret och *hur* ansvar ska utkrävas, riskerar att falla mellan stolarna – sär-

skilt när information är spridd över flera system, sektorer och aktörer.

För att informations- och tjänsteresiliens i samhället ska uppnås behöver ett antal principer beaktas:

- **Identifiering** av vilken information som är viktig. Om en incident inträffar blir prioriteringen avgörande för att snabbt kunna skydda eller återställa just den informationen, men även i normalläge gäller det att veta vilken information som är mest kritisk (till exempel patientjournaler i vården).
- **Kunskap** om vilken information som finns var. Vid en allvarlig störning, som ett cyberangrepp, måste aktörer direkt kunna hitta rätt källa (till exempel var kopior av energibolagens styrdata finns) för att undvika längre avbrott.
- **Tydligt ansvar** för informationstillgänglighet. I normalläget kan ansvar ibland uppfattas som delat, men vid en incident måste det vara tydligt vem som ansvarar för att system och information hålls tillgängliga (till exempel att en myndighet inte förutsätter att en privat leverantör automatiskt tar det ansvaret).

Genom att följa dessa principer uppnås en ökad informations- och tjänsteresiliens som förbättrar förmågan att hantera framtida utmaningar och säkerställa kontinuitet i samhällsviktiga funktioner.

Åtgärdsförslag

Det finns mycket som näringslivet, akademin och myndigheterna kan göra redan idag

För att hantera de områden och övergripande utmaningar som beskrivits ovan föreslår vi ett antal konkreta åtgärder på olika nivåer i infrastrukturen. Det finns många regelverk, direktiv, utredningar, strategier och andra initiativ som tar frågorna på stort allvar och leder utvecklingen åt rätt håll. Utöver detta föreslår IVAs projekt ett antal åtgärder som presenteras här. Vi föreslår också lämpliga aktörer för genomförande. Förslagen har tagits fram i en iterativ process där ett stort antal experter och representanter från näringsliv, akademi, myndigheter och branschorganisationer medverkat.

Regelharmonisering

Nya lagar och förordningar ger olika myndigheter rätt att ställa krav och utöva tillsyn över företags resiliens- och cybersäkerhetsarbete. Om myndigheterna inte samordnar sig riskerar kraven att bli spretiga och motstridiga. Detta skapar osäkerhet kring hur reglerna ska följas. Inom finansbranschen kan en enskild incident som drabbar en bank kräva fler än fem olika incidentrapporter till olika myndigheter med olika definitioner, tröskelvärden och mallar. I dagligvaruhandeln kan större

livsmedelsföretag behöva förhålla sig till upp till tio olika myndigheter och andra aktörer med olika tolkning av lagar, regler och förordningar.

Det beror på att verksamheten är mångfacetterad och omfattar livsmedel, apoteksverksamhet, betalkort och korttransaktioner, personuppgiftshantering samt generell it- och informationshantering med krav på ackreditering, certifiering och revisioner. Lagstiftning och föreskrifter upplevs dessutom ofta som alltför tekniskt detaljerade och svåra att anpassa till den snabba teknikutvecklingen. Dessutom bygger de i för hög grad på regelefterlevnad snarare än ansvarsutkrävande.

Regelharmonisering skulle minska den administrativa bördan för företag och organisationer så att de kan fokusera på operativt riskhanterande säkerhetsarbete. Detta är i första hand en nationell angelägenhet men tillämpning av internationell standard och EU:s arbete med regelförenkling[16] leder i rätt riktning.

16 ”Ett djärvare, enklare och snabbare EU: kommissionens arbetsprogram 2025”, EU-kommissionen, 12 februari 2025, https://ec.europa.eu/commission/presscorner/detail/sv/ip_25_466.

Förslag

- Harmonisera föreskrifter för att undvika att olika tillsynsmyndigheter ställer olika eller otydliga krav på resiliens och cybersäkerhet. Föreskrifterna kan innehålla krav på olika skyddsnivåer som är gemensamma för alla sektorer inom områden som behörighetsstyrning, kryptering, utbildning, riskhantering, sårbarhetsuppdateringar och rutiner för ständiga förbättringar. Kraven kan med fördel hämtas från internationella standarder såsom ISO 27001 eller NIST Cybersecurity Framework. Vid behov kompletteras dessa med sektorsspecifika föreskrifter och krav.

- Svenska myndigheter bör använda etablerade internationella standarder för informations- och cybersäkerhet (exempelvis ISO 27001 eller NIST) och bör samverka om utformningen av föreskrifter snarare än att varje sektorsmyndighet skapar sina egna.

- Undvik detaljerade tekniska krav i lagstiftning och föreskrifter då tekniken som regel utvecklas snabbare än regleringen. Minimera sektorsspecifik och teknisk lagstiftning.

- Fokusera på ansvarsutkrävande snarare än strikt regelefterlevnad för att möjliggöra innovation över tid. Se EU-kommissionens rekommendation (EU) 2020/2245, recital 3.[17]

Flera aktörer behöver involveras i genomförandet av dessa åtgärder:

- Privata aktörer kan ansvara för att implementera gemensamma säkerhetskrav och använda etablerade internationella standarder.
- Offentliga organisationer och myndigheter kan stödja utvecklingen av gemensamma föreskrifter och tolkningar av dessa.
- Regeringen behöver tydligare inkludera förenkling och regelharmonisering i sitt strategiska arbete. Här kan till exempel Förenklingsrådet[18] spela en roll.

17 Kommissionens rekommendation (EU) 2020/2245, EU-kommissionen, 18 december 2020, https://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1757680986679&uri=CELEX%3A32020H2245.

18 Förenklingsrådet. (2025). https://forenklingsradet.se/

Operativt privat–offentligt samarbete vid incidenthantering och återställning

Vid större olyckor, tekniska fel eller angrepp krävs både resurser och snabb informationsdelning för att skyndsamt reparera skador och återställa funktionen i den digitala infrastrukturen. En enskild aktör har ofta kapacitet och kunskap för att återställa den egna utrustningen eller verksamheten, men när flera aktörer eller sektorer drabbas samtidigt saknas ofta konkret, operativ samordning.

Denna samordning behöver omfatta effektiv informationsdelning om hot och åtgärder före, under och efter incidenter. Många drabbade aktörer upplever idag att myndigheter inte delar information snabbt nog.

Det finns ett intresse för att skapa samordnande strukturer i olika sektorer. Två väl fungerande exempel är NTSG, Nationella Telesamverkansgruppen, för telekomsektorn och FSPOS, Finansiella sektorns privat-offentliga samverkan. Dessa övar och hanterar gemensam krishantering mellan myndigheter och företag. Några energiföretag har etablerat en samarbetsorgani-

sation, Energi-CERT Sverige[19] (Computer Emergency Response Team) med danska SektorCERT[20] som förebild. Liknande strukturer behövs inom alla beredskapssektorer och även över sektorsgränser. Skapande av fler sådana strukturer måste stöttas.

Sveriges nationella strategi för cybersäkerhet pekar på flera pågående och nya uppdrag inom incidenthantering. Några exempel är att FRA erbjuder tekniskt detekterings- och varningssystem (TDV) till de mest skyddsvärda verksamheterna. FRA ska även utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser. MSB/NCSC, Nationellt cybersäkerhetscenter, arbetar med att skapa en portal med smarta formulär för rapportering av incidenter, tillbud, sårbarheter och cyberhot. NCSC har dessutom sedan 2022 en etablerad samverkan med samhällsviktiga aktörer inom finansiell sektor, "Finansforum", för att stärka cybersäkerheten inom finanssektorn. Likaså har MSB/CERT-SE flera forum för informationsdelning,

19 Ann-Sofie Borglund, ”Energi-CERT ska hjälpa energiföretag med cybersäkerhet”, *Tidningen Energi*, 28 maj 2025, https://www.energi.se/artiklar/2025/maj-2025/energi-cert-ska-hjalpa-energiforetag-med-cybersakerhet/.

20 SektorCERT. (2025). https://sektorcert.dk/

som FIDI-Telekom (Forum för informationsdelning kring cybersäkerhet i telekomsektorn).

Det kan också noteras att Försvarsmakten har inrättat cyberförsvarsförband vars huvuduppgift är att försvara kritisk civil infrastruktur som Försvarsmakten är beroende av för att lösa sin huvuduppgift; försvaret av Sverige och våra allierade.

Den europiska cybersolidaritetsförordningen,[21] som trädde i kraft i februari 2025, reglerar bland annat ett europeiskt nätverk av så kallade cybernav. Dessa är under uppbyggnad och kan ses som nationella CERT:ar med utökad förmåga att upptäcka hot och incidenter för att kunna ge lägesbilder i realtid. Dessutom inrättas insatsgrupper, EU:s cyberreserv, bestående av företag som mot ersättning från EU:s cybersäkerhetsbyrå Enisa kan bistå vid hanteringen av storskaliga cybersäkerhetsincidenter.

Det som görs inom ramen för dessa strategier och initiativ är bra och bör fortsätta. Samtidigt ser vi behov av kompletterande åtgärder.

21 ”EU:s cybersolidaritetsakt”, EU-kommissionen, 9 juli 2025, https://digital-strategy.ec.europa.eu/sv/policies/cyber-solidarity.

En viktig princip är att säkerställa att incidentrapportering och informationsdelning är skiljt från tillsyn. Exempel på hur både tillsyn och stödjande aktiviteter kan förbättras finns i Riksrevisionens granskning[22] av Säkerhetspolisens verksamhet. Generellt finns dock ingen enkel lösning eftersom vissa incidentrapporteringskrav är regulatoriska och därmed förknippade med tillsyn, till exempel NIS2 och DORA. Tillsyn och revision bör också vara proaktiva och förebyggande snarare än reaktiva och straffande. En framgångsfaktor är att skapa goda incitament för inblandade aktörer att delta i samarbete, och att samarbete bygger på frivillighet och ömsesidigt förtroende.

Förslag

- Regeringen bör ge sektorsmyndigheterna i uppdrag att i samverkan med NCSC, etablera samverkansforum likt NTSG och FSPOS för sina respektive sektorer.

22 Riksrevisionen, RiR 2024:24 *Säkerhetspolisens verksamhet* (2024), https://www.riksrevisionen.se/download/18.73ed0f241939545744f9e97/1733952229669/RiR_2024_24_rapport.pdf.

Målet ska vara att dels förbättra informationsdelningen för snabb och effektiv återställning, dels att producera harmoniserade råd och rekommendationer såväl innan som efter incidenter. Detta innefattar samarbeten kring risk- och sårbarhetsanalys i syfte att höja robusthet, resiliens och redundans på samhällsnivå så att det operativa arbetet kan övergå till att vara proaktivt och inte bara reaktivt.

- Stärk det påbörjade arbetet som beskrivs i Sveriges nationella strategi för cybersäkerhet som ger det nationella cybersäkerhetscentret (NCSC) ansvar för att implementera och driva en portal för incidentrapportering och komplettera med operativ och snabb informationsdelning.
- Förtydliga skillnaden mellan myndigheternas tillsynsuppdrag och deras främjandeuppdrag, att arbeta för goda förutsättningar för samverkan.

Behov av tvärsektoriella tester och övningar

En god beredskap kräver förberedelser som inkluderar tester och övningar. Idag sker dessa ofta inom enskilda sektorer eller av enskilda aktörer. Det skapar beredskap för händelser och incidenter som drabbar en viss sektor eller aktör, men vid till exempel ett större elavbrott kan stora geografiska områden påverkas och därmed flera aktörer i olika sektorer drabbas.

Att genomföra tvärsektoriella tester och övningar är utmanande av flera skäl. Övningar är både tids- och resurskrävande att planera, genomföra och följa upp. Ofta är det oklart på vilken nivå aktiviteterna ska ske, vem som ansvarar för övningen och hur återkopplingen ska gå till. Ett annat hinder är att deltagande aktörer kan uppleva oro för att framstå i dålig dager eller för att bli föremål för tillsyn oavsett om några brister eller svagheter faktiskt avslöjas i tester och övningar.

Den nationella strategin för cybersäkerhet lyfter fram behovet av test och övning, medan Sveriges digitaliseringsstrategi 2025–2030 bara berör detta i begränsad omfattning. En övergripande förutsättning för effektiva tester och övningar är att frågan får större tyngd även på nationell strategisk nivå.

SÅ HÄR SKILJER VI PÅ TEST OCH ÖVNING

Test är en systematisk process för att utvärdera om ett system, en komponent eller en funktion fungerar som förväntat enligt kravspecifikation eller design. Syftet är att upptäcka fel, brister eller avvikelser innan systemet tas i bruk eller vidareutvecklas.

Övning är en förberedande och simulerad aktivitet där deltagare tränar på att identifiera, hantera och åtgärda fel eller störningar i ett system eller en process. Syftet är att förbättra beredskap, samarbete och reaktionsförmåga i en kontrollerad miljö. Övningar kan vara teoretiska (skrivbordsövningar) och praktiska (tekniska).

För att en övning ska ge effekt krävs ett tydligt syfte. Den ska utformas och genomföras i en lämplig miljö, och resultaten ska återföras och analyseras för att kunna användas för framtida förbättringar. Förbättringar såväl av det som övas som övningen i sig.

Aktuellt läge och förslag till genomförande

Vi bedömer att Sverige ännu inte är redo för större, sektorsöverskridande tekniska tester och övningar. Det beror bland

annat på att civilområdena, vilka är lämpliga huvudmän, fortfarande håller på att formeras och att strukturer för övningar generellt inte finns på plats.

Vi föreslår därför att genomförandet sker i ett antal steg:

Förslag: Steg 1

- Säkerställ tillgång till relevanta övningsmiljöer. Idag finns sådana till viss del i privat sektor samt hos RISE, FOI och genom CCDCOE[23] i Tallinn (CR14). Gör dessa miljöers kapacitet känd och se till att MSB, tillsammans med respektive sektorsansvarig myndighet, kan stödja aktörer som vill genomföra övningar att använda dem på bästa möjliga sätt.
- Genomför simulerade och realistiska övningar och skapa därmed möjlighet för operativa och tekniska återställningstester för fler sektorskombinationer än idag. Beredskapsmyndigheter och civilområden rekommenderas

23 CCDCOE. (2025). *The NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/

att genomföra tester med tydliga mål och avgränsningar, exempelvis för återställning av kritiska system eller inkoppling och användning av reservsystem. Fokus bör ligga på samverkan mellan samhällskritiska aktörer inom både privat och offentlig sektor.

- Genomför sektorsöverskridande skrivbordsövningar. Vid sådana övningar kan till exempel myndigheterna i den civila beredskapsstrukturen öva alla samhällskritiska funktioner vid kris eller krig. MSB bör bidra med metodstöd samt utbildningar i övningsdesign och ledning.

Förslag: Steg 2

- Genomför tvärsektoriella övningar av digitalt beroende samhällsfunktioner med komplexa och realistiska scenarier där flera infrastrukturer fallerar samtidigt. Övningarna bör även omfatta fördelning av ansvar och hantering av kaskadeffekter mellan organisationer i olika sektorer.

- Genomför praktisk utbildning för beslutsfattare om hur man hanterar avbrott och störningar i digital infrastruktur. Utbildningen bör innehålla:

- Övningar som simulerar systempåverkan i kritiska sektorer som el, telekom, finans och transport.
- Tydliga rutiner för eskalering och uthållighet samt kommunikation vid digitala avbrott.
- Fortsätt utveckla NCSC som sammanhållande av ett nationellt ramverk för övning och test, både tekniskt och organisatoriskt. Även Cybercampus kan bidra här.

Förutsättningar för utveckling av nya lösningar mot hot och störningar

Föråldrad lagstiftning, anpassad efter en tidigare verklighet och hotbild, begränsar möjligheterna inom områden som produktutveckling, etisk hackning och visselblåsning. Lagar, som bland andra lagen om elektronisk kommunikation (LEK),[24] utgör sådana hinder. Lagarna bör ses över, annars riskerar Sverige att

24 SFS 2022:482 Lag om elektronisk kommunikation. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/

gå miste om avgörande forskning, utveckling och innovation. Lagändringar och tydligare riktlinjer behövs bland annat för att göra det möjligt att bidra till samhällets cybersäkerhet och resiliens utan att riskera rättsliga påföljder.

Ett tydligt exempel på hur lagar och regler begränsar möjligheten att utveckla och testa ny teknik gäller förmågan att stå emot radiostörningar. Lagen om elektronisk kommunikation innehåller begränsningar i spektrumanvändning som inte uppfyller dagens behov. Syftet med lagen är att säkerställa att enskilda och myndigheter får tillgång till säker och effektiv elektronisk kommunikation. Trots dess goda intentioner är lagen i sin nuvarande form otydlig och utgör ett konkret hinder för svensk industri att effektivt utveckla och testa lösningar mot olika former av elektromagnetiska hot. Exempelvis är viss utrustning som är väsentlig för framtagandet av säkra och robusta system förbjuden eftersom den även kan användas för brottsliga ändamål. Vidare är lagens formuleringar kring tillståndsgivning för annan radioanvändning i harmoniserade frekvensområden oklara och svåra att tolka. Denna otydlighet leder i praktiken till att implementeringen och den praktiska tillämpningen av tillståndsprocessen blir både komplex och restriktiv, vilket hämmar innovation och teknikutveckling.

Ett annat exempel är etisk hackning som är ett effektivt sätt att upptäcka och åtgärda sårbarheter i digital infrastruktur för att dessa inte ska kunna utnyttjas av illvilliga aktörer. Men den som olovligen, det vill säga utan att ha inhämtat samtycke på förhand, bereder sig tillgång till ett it-system, eller påverkar det, kan dömas för dataintrång, oavsett syftet med intrånget. Svensk lagstiftning saknar idag ett uttryckligt ramverk som skyddar eller underlättar denna typ av säkerhetsforskning.

Förslag

- Se över lagstiftningen för att stärka möjligheterna att säkerställa resiliens. Exempelvis behöver lagen om elektronisk kommunikation (LEK) anpassas och förtydligas så att relevanta verksamheter, under kontrollerade former, får tillstånd att inneha och använda utrustning som kan klassas som störutrustning, det vill säga utrustning som avger elektromagnetiska signaler med risk för skadlig störning. Syftet är att möjliggöra forskning och utveckling av lösningar och produkter som kan lindra och motverka effekterna av sådana störningar.

- Det bör införas möjligheter för tillsynsmyndigheten att ge tillstånd att använda vissa spektrumområden och utrustning som kan vara skadlig genom att göra avvägningar mellan å ena sidan samhällets behov av att skydda sig mot brottslig verksamhet, å andra sidan att tillåta relevanta aktörer med adekvata kunskaper och resurser att bedriva forskning och utveckling.

Tydligt ansvar för information

En utmaning är att samhällskritisk information traditionellt har hanterats i olika system med minimalt eller obefintligt informationsutbyte. Regelverket har snarare förhindrat än främjat informationsdelning, särskilt mellan myndigheter. I detta avseende ligger Sverige långt efter andra länder, och det finns flera förklaringar till detta, bland annat:

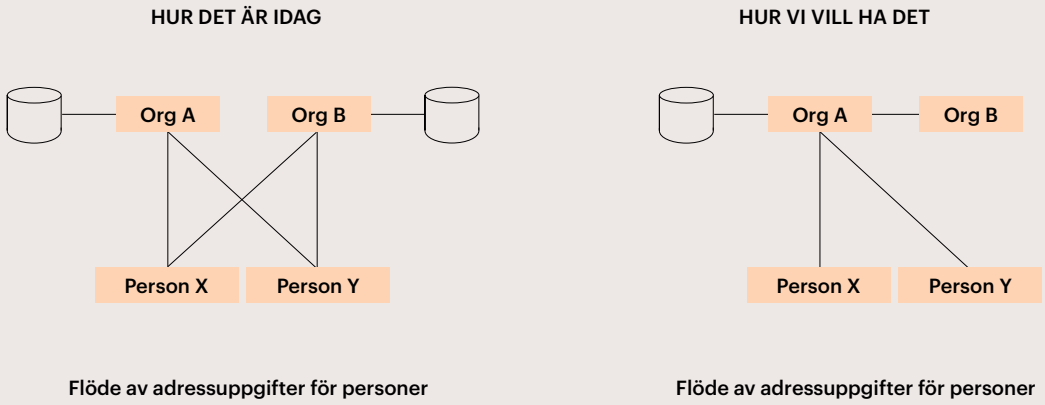
- Många system har traditionellt byggts isolerade, med all information lagrad internt.
- Tekniska hinder och behov av standardiserade protokoll och API:er och liknande krav försvårar utbyte.

- Lagar, förordningar och affärsintressen förhindrar delning av viss information. Regelverket har snarare förhindrat än främjat informationsdelning, särskilt mellan myndigheter.
- Vid utveckling av nya system är det ofta oklart var fullständig och korrekt information finns. Om informationen hämtas från en extern part kan kvaliteten vara oklar.
- Insamlad information kan vara värdefull, särskilt om det kostar att få tillgång till motsvarande information från tredje part. Möjligheten att sälja den insamlade informationen kan också minska incitamenten att dela den.

Informationsutbyte är på grund av detta fortfarande ett problem i Sverige, även om trenden går mot ökad delning. Till exempel har regeringen beslutat om en förordning[25] där ett antal myndigheter (Skatteverket, Trafikverket och Försäkringskassan) fått i uppdrag att samordna säker statlig it-drift. Även Sveriges digitaliseringsstrategi 2025–2030 innehåller åtgärder om data-

25 ”Regeringen stärker säkerheten och kostnadseffektiviteten genom statlig it-drift”, Finansdepartementet och Socialdepartementet, 7 november 2024, https://www.regeringen.se/pressmeddelanden/2024/11/regeringen-starker-sakerheten-och-kostnadseffektiviteten-genom-statlig-it-drift/.

FIGUR 2: Illustration av existerande och önskad hantering av viktig information där en ansvarig organisation lagrar till exempel adressuppgifter och andra får efterfråga dem.



delning och interoperabilitet. Detta är bra och leder i rätt riktning, men det räcker inte. Dessa pågående arbeten behöver stärkas, kompletteras och snabbas upp.

I samhället finns grundläggande information som är avgörande för många processer, till exempel adresser till personer och företag eller uppgifter i fastighets- och körkortsregister. Denna typ av data hanteras av utvalda organisationer med ett tydligt definierat ansvar för exempelvis tillgänglighet, säkerhet och redundans.

Trots detta samlar många andra aktörer in samma information lokalt. Ett bättre alternativ vore att dessa aktörer, i stället för att lagra informationen själva, hämtar den direkt från de organisationer som ansvarar för dess kvalitet och aktualitet, se Figur 2.

Om vi jämför med till exempel Estland ser vi i Sverige ett i stort sett obefintligt informationsutbyte medan man i Estland dels har arbetat sedan 2001 med strukturerad delning av information med hjälp av systemet X-Road,[26] dels har lagstiftning som sedan 2007 förbjuder skapande av parallella databaser med information.[27] I Estland har man även sedan 2014 förbjudit myndigheter att samla in information som redan finns tillgänglig för offentlig sektor;[28] detta som en del av deras implementation av *The once-only principle (TOOP)*.[29]

26 "X-road – Interoperability services", Enterprise Estonia, åtkomstdatum 12 september 2025, https://e-estonia.com/solutions/interoperability-services/x-road/.

27 "Public Information Act", Riigi Teataja, 14 november 2013, https://www.riigiteataja.ee/en/eli/514112013001/consolide.

28 "General Part of the Economic Activities Code Act", Riigi Teataja, 22 augusti 2014, https://www.riigiteataja.ee/en/eli/522082014004/consolide

29 "Once-only principle", Wikipedia, 7 augusti 2025, https://en.wikipedia.org/wiki/Once-only_principle

För att informations- och tjänsteresiliens i samhället ska uppnås behöver Sverige röra sig i samma riktning som bland annat Estland gjort.

Förslag

- Initiera arbete mot att implementera *The once-only principle* i Sverige och i övrigt följa den väg som Estland och andra länder i EU slagit in på.

Detta kan göras genom att ge ett utökat uppdrag till DIGG (Myndigheten för digital förvaltning) samt de leverantörsmyndigheter (Skatteverket, Trafikverket och Försäkringskassan) som ingår i samordningen enligt förordningen 2024:1005. Arbetet kan gärna inspireras av och dra lärdomar från den estniska lösningen X-Road.

Tydligt ansvar för att information ska vara tillgänglig

Information måste vara tillgänglig för behöriga användare och samtidigt skyddas mot obehörig åtkomst. Idag är det dock

oklart vem som ansvarar för att dessa krav uppfylls. Inom uppdraget om samordnad och säker it-drift pågår ett arbete med att centralisera viss informationshantering i offentlig sektor, men fortfarande hanteras stora mängder viktig information om exempelvis personer och organisationer på ett otydligt sätt. Även privata aktörer förvaltar samhällsviktig information som behöver hanteras med samma krav på tillgänglighet och säkerhet.

För att stärka tillgängligheten till samhällskritisk information kan geografisk spridning och samordnad lagring behöva testas, där samma data hålls uppdaterad på flera platser även om ansvaret ligger hos en tydligt utpekat aktör. Som en möjlig komplettering kan så kallade dataambassader prövas, där kritisk information speglas i länder med starkt dataskydd. En sådan lösning skulle kunna ge en sista försvarslinje vid extrema scenarier, men är främst relevant för långsiktig återställning snarare än snabb återstart.

Ett annat problem är att många mindre företag undantas från säkerhetsreglering, till exempel enligt lagen om elektronisk kommunikation och NIS. I stället borde reglerna baseras på hur kritisk verksamhet eller information man har, snarare än storlek på verksamheten.

Ett önskat läge är att det är känt vilken information och vilka tjänster som är samhällsviktiga (som upprätthåller samhällets grundläggande funktioner och behov) eller samhällskritiska (som, om de fallerar, ger allvarliga konsekvenser för samhällets säkerhet eller funktion). Delar av informationen kan omfattas av sekretess.

Förslag

- En inventering och klassificering av samhällsviktig och samhällskritisk information genomförs. Utifrån denna dras slutsatser om vilka tjänster som är samhällsviktiga eller samhällskritiska.
  Inventeringen kan till exempel genomföras av ansvarig sektorsmyndighet inom respektive beredskapssektor under överinseende av MSB i samverkan med de samordnade myndigheterna (Skatteverket, Trafikverket och Försäkringskassan) enligt förordningen 2024:1005.
- De tjänster som exponerar informationen måste vara robusta, pålitliga och tillgängliga i överenskomna it-miljöer. Ansvaret för att informationen är korrekt och tillgänglig bör ligga hos en tillsynsmyndighet.

Gemensam nationell kravställning på digitala tjänster

Den övervägande majoriteten av alla svenska företag har färre än 250 anställda. Samtidigt är de mindre företagen mer digitalt sårbara än större. Studier visar att knappt hälften[30] av alla startupföretag som råkar ut för ett allvarligt cyberangrepp överlever. Endast en liten del av de mindre företagen har kompetens att ställa rätt krav på digitala tjänsteleverantörer för att minimera risken för incidenter. Därför är de beroende av att tjänsternas kvalitet i grunden är god.

Även kommuner och många andra offentliga aktörer, exempelvis skolor, har liknande förutsättningar. De har begränsad upphandlingskompetens och köper därför digitala tjänster av mycket varierande kvalitet. Ytterligare ett problem är att tjänsteleverantörer inte alltid tar hänsyn till krav och önskemål från små aktörer.

30 Per Olof Lindsten, ”Småföretagen sämst rustade mot cyberattacker”, *Dagens industri*, 13 september 2021, https://www.di.se/nyheter/smaforetagen-samst-rustade-mot-cyberattacker/.

Mycket görs dock för att stödja minde företag och kommuner. Sveriges nationella strategi för cybersäkerhet innehåller exempel på stöd för mindre företag och kommuner. MSB vidareutvecklar Cybersäkerhetskollen för att även kunna bistå mindre företag. MSB förbereder även en nationell kartläggning av kommunernas tekniska cybersäkerhetsförmåga. Även kommande krav på och märkning av produkter enligt CRA bidrar till ökad kvalitet i upphandlingarna.

Stöldskyddsföreningen erbjuder en grundläggande nivå av cybersäkerhet för företag, kallad "Cybersäkerhet BAS", norm SSF 1101.[31] Denna norm ger riktlinjer för att skydda organisationers informationstillgångar från digitala hot och är ett kostnadseffektivt sätt för företag att stärka sitt skydd mot cyberhot.

Även i andra länder finns goda exempel, som ”Mittelstand Digital”,[32] ett program i Tyskland som stödjer små och medel-

31 Stöldskyddsföreningen, *SSF 1101 utg. 2 – SSF Cybersäkerhet Basnivå-Grundläggande IT-säkerhet*, 2:a uppl. (SFF, 2023), https://www.stoldskyddsforeningen.se/butik/foretag/ssf-normer/cybersakerhet/ssf-1101-utg-2-ssf-cybersakerhet-basniva-grundlaggande-it-sakerhet/.

32 Mittelstand Digital. (2025). https://www.mittelstand-digital.de/MD/Navigation/DE/Home/home.html

stora företag i digital transformation, inklusive cybersäkerhet. I Storbritannien finns ”Cyber Essentials”[33] – en certifieringsstandard för små och medelstora företag som ger vägledning och stöd kring it-säkerhet.

Förslag

- Upphandlingsmyndigheten bör se till att centralt förhandlade ramavtal för offentlig sektor omfattar en relevant och gemensam kravställning på digitala tjänster. Ett exempel på en existerande sådan kravställning är MSB:s Vägledning för fysisk informationssäkerhet i it-utrymmen.[34] I ett första steg kan exempelvis internetaccess och grundläggande IT-tjänster ingå. PTS bedöms bäst lämpad som ansvarig myndighet för internetförbindelse och MSB för grundläggande it-tjänster.

33 Cyber Essentials. (2025). https://www.ncsc.gov.uk/cyberessentials/overview

34 Myndigheten för samhällsskydd och beredskap, *Vägledning för fysisk informationssäkerhet i it-utrymmen* (2013), https://rib.msb.se/filer/pdf/27280.pdf.

Molntjänster för resiliens och resiliens för molntjänster

Molntjänster erbjuder unika möjligheter för att bygga resilienta digitala tjänster, särskilt i jämförelse med traditionella lokala datacenter. Den övergripande nyttan av dessa tjänster är att hålla information och funktionalitet tillgänglig, både vid normal användning och vid störning.

Några viktiga egenskaper hos molntjänster för ökad resiliens är:

- Inbyggd möjlighet till geografisk redundans genom replikering av data och tjänster mellan flera geografiska platser så att verksamheten kan fortsätta vid lokala incidenter som strömavbrott, bränder eller naturkatastrofer.
- Skalbarhet vid belastningstoppar som gör att det går att öka resurser automatiskt vid överbelastningsattacker (DDoS-attacker) eller plötsliga trafikökningar.
- Avancerade resilienstjänster som exempelvis möjlighet att hantera information inom valbara geografiska områden, vanligen kallade tillgänglighetszoner, vilket ofta önskas av juridiska skäl.

Särskilt värdefulla är möjligheterna att snabbt flytta data och applikationer samt att skapa geografisk redundans, något som är centralt för att skapa robusta digitala tjänster. För att fullt ut dra nytta av dessa möjligheter krävs planering och förberedelser för olika typer av händelser och scenarier.

Samtidigt kan naturligtvis även molntjänster drabbas av längre avbrott, exempelvis till följd av tekniska fel, politiska beslut, pandemier eller ekonomiska kriser. Därför behöver arbetet med tjänsteresiliens omfatta både hur molntjänster kan användas för att skapa resiliens, och hur man skapar resiliens för själva molntjänsten.

Molntjänster för resiliens

Erfarenheterna från Ukraina[35] har visat vikten av att snabbt kunna överföra tjänster från lokala datacenter till säkrare regioner vid krissituationer. Myndigheterna i Ukraina lyckades effektivt

35 Ryan White, "How the cloud saved Ukraine's data from Russian attacks", C4ISRNET, 22 juni 2022, https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks/.

evakuera data och applikationer till bland annat stora internationella molntjänster, belägna utanför de angripna områdena.[36]

Resiliens för molntjänster

Vissa funktioner i samhället kräver högre tillgänglighet än vad enstaka leverantörer kan leverera. Det finns också risker med att låsa fast sig vid en enstaka leverantör av juridiska eller tekniska skäl, särskilt om man använder funktioner som bara finns hos den leverantören. Då saknas ofta plattformsoberoende alternativ, vilket leder till inlåsningseffekter, avsaknad av redundans och otillräcklig beredskap.

Problemet delas i hög grad med övriga europeiska länder,[37] men Sverige kan vara särskilt sårbart eftersom svenska företag

36 Myndigheten för samhällsskydd och beredskap, *När kriget kom nära – Årsrapport it-incidentrapportering 2022*, (2022), https://rib.msb.se/filer/pdf/30339.pdf.

37 "Cloud computing – statistics on the use by enterprises", Eurostat, december 2023, https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights.

använder molntjänster i betydligt högre grad än EU-genomsnittet.

Sårbarhet och beroenden i leverantörskedjor lyfts även i Sveriges nationella strategi för cybersäkerhet. Där beskrivs hur FRA och MSB, inom ramen för NCSC, ska ta fram riktlinjer för cybersäkerhet i leveranskedjor för IKT-produkter och IKT-tjänster. MSB har dessutom fått i uppdrag att kartlägga digitala leveranskedjor och utveckla en modell för hur dessa kan följas upp. MSB representerar också Sverige på EU-nivå i samarbetsgruppen för NIS vars syfte är att stärka säkerheten i Europas digitala leveranskedjor.

Det är viktigt att organisationer kan fortsätta sin verksamhet även om en eller flera molntjänster, inklusive de tjänster de själva tillhandahåller, drabbas av störningar eller blir otillgängliga. För att minska riskerna och konsekvenserna av leverantörsberoende föreslås följande åtgärder:

Förslag

- Ansvariga för kritiska tjänster inom både privat och offentlig sektor bör planera för, och regelbundet öva på, att flytta

både data och applikationer med hjälp av molntjänster. Dessa kan vara implementerade av den egna eller en extern organisation. Övningarna ska inkludera administrativa, juridiska, tekniska och integritetsmässiga aspekter.

- Se till att applikationer är tekniskt anpassade för att snabbt och smidigt kunna flyttas i en krissituation. Applikationerna ska kunna flyttas till en molntjänst, från en molntjänst eller mellan molntjänster, egna eller andras.
- Tillämpa standarder som stödjer diversitet och minskar inlåsningseffekter genom att göra leverantörers tjänster utbytbara.[38]
- Skapa redundans både i *var* information lagras och *hur* den lagras, samt i val av tjänster för åtkomst och därmed diversitet. Detta kan inkludera standardiserad synkronisering av information mellan olika platser och utbytbara lokala och globala molntjänster.

38 Rahiel Nasir, "The Evolution of Digital Sovereignty: Moving Beyond Data and Cloud", IDC, 13 januari 2023, https://blog-idceurope.com/the-evolution-of-digital-sovereignty-moving-beyond-data-and-cloud/.

- Öka medvetenheten om riskerna med leverantörsberoende och hur dessa kan minimeras. Stöd omställningsarbete för att minska beroendet av enstaka leverantörer genom att etablera exit-strategier.

Flera aktörer behöver involveras i genomförandet av dessa åtgärder:

- Privata aktörer ansvarar för att implementera diversitet och redundans i sina molntjänstlösningar. Leverantörer har dessutom ansvar för att stödja och underlätta kundernas möjlighet till diversitet, till exempel genom att utveckla och anpassa sig till standarder.
- Offentliga organisationer – Vinnova, Tillväxtverket, MSB och DIGG – stödjer innovation, information och omställning.
- Myndigheter ansvarar för specifika åtgärder, såsom standardiserad synkronisering och utveckling av redundanta tjänster, inom ramen för den samordnade säkra statliga it-driften som Försäkringskassan, Trafikverket och Skatteverket ska tillhandahålla enligt förordningen (2024:1005).

- Privata och institutionella finansiärer har viktiga roller för att driva fram fler, och även nationella, alternativ.

AI och resiliens

AI påverkar den digitala infrastrukturens resiliens. Området är under snabb utveckling och svår att förutsäga. AI används både som fristående tjänster, såsom ChatGPT, och som integrerade funktioner i applikationer via mjukvarugränssnitt (API) för exempelvis analys, beslutsstöd eller språkförståelse. I dagsläget är konsekvenserna av driftstörningar ofta begränsade eftersom det finns flera generella språkmodeller tillgängliga och användningen sällan är tidskritisk.

AI-relaterade API:er används dock i allt fler applikationer och för alltmer autonoma funktioner. Självkörande fordon, smarta städer och mer automatiserat arbete kommer att vara beroende av ett fungerande AI-lager. AI-agenter väntas i ökande grad förändra dagens SaaS-applikationer *(Software as a service)*, vilket kan innebära att framtidens mjukvaruarkitektur kommer att

bestå av två huvudsakliga komponenter: AI-agenter och data.[39] Detta innebär i sin tur en förändring av delar av den digitala infrastrukturen och hur mjukvara skapas för den.

Denna utveckling kan innebära nya typer av driftstörningar. Om AI-modeller eller API:er slutar att fungera, eller fungerar på ett felaktigt sätt, kan det medföra betydande risker för hela städer, transportsystem och organisationer, särskilt om beslut och åtgärder är automatiserade eller AI-drivna.

För resiliens i den digitala infrastrukturen finns flera aspekter relaterade till AI att ta hänsyn till:

- **AI kan finnas på alla nivåer.** AI används inte bara i slutanvändarlagret utan kan bidra till resiliens i alla lager av lasagnemodellen. Exempelvis kan AI optimera elnät genom att förutse och hantera förbrukningstoppar. Vid nätverksoptimering i mobilnäten kan AI bidra till att förbättra signalstyrkan och minska störningar. AI spelar därmed en central och allt viktigare roll för den övergripande digitala resiliensen.

39 Bg2 Pod, ”Satya Nadella | BG2 w/ Bill Gurley & Brad Gerstner”, 12 december 2024, YouTube, https://youtu.be/9NtsnzRFJ_o?t=2800.

- **Beprövade metoder för hård- och mjukvarans resiliens gäller också för AI.** AI består av både dedikerad AI-hårdvara (GPU) och mjukvara. Regler som gäller för vanlig mjukvara gäller även för AI-mjukvara, inklusive klassiska åtgärder kring redundans för servrar, datacenter och systemkritiska felpunkter.

- **AI för AI:s resiliens.** AI-agenter kan övervaka andra AI-system i realtid för att upptäcka avvikelser från förväntat beteende eller andra problem. Dessa agenter kan initiera säkerhetsåtgärder, avstängningar eller reparationsprocesser. Genom att identifiera sårbarheter och riskfaktorer kan AI användas för att åtgärda dessa och därigenom stärka systemens resiliens och säkerhet.

- **Tillgång till hårdvara och beräkningskapacitet.** Geopolitiska konflikter kan begränsa tillgången på halvledare, GPU:er eller data. Att träna stora AI-modeller är kostsamt och kan kräva investeringar i miljardklass. Även driftskostnaderna för att använda AI-modeller växer, särskilt när det gäller större modeller och när användningen ökar. Dessa utmaningar kräver samarbete mellan aktörer,

exempelvis inom EU, för att säkerställa tillgången till hårdvara och beräkningskapacitet.

- **Resiliens i kedjor av AI-agenter.**
  Utvecklingen går mot AI-agenter som samverkar. I en fabrik kan AI-agenter exempelvis övervaka maskiner, förutse fel och optimera produktionen automatiskt. En utmaning är att även mindre fel som uppstår i början av denna kedja kan förstärkas och till slut ge oförutsägbara resultat.

För att möta både utmaningar och möjligheter krävs ökade investeringar inom nya områden, såsom AI-förklarbarhet och AI-funktioner kopplade till realtidsdata från fysiska system. Dessutom behöver Sveriges engagemang inom EU stärkas i dessa frågor.

Förslag

- Konkreta riktlinjer behövs för att hantera de utmaningar som uppstår i en digital infrastruktur där AI-tjänster används i realtid. Dessa riktlinjer måste bygga på verkliga behov och vara praktiskt tillämpbara.

Vi föreslår att ansvaret för att ta fram riktlinjer och rekommendationer antingen inkluderas i uppdraget för det institut som AI-kommissionen föreslagit,[40] placeras hos en befintlig myndighet som DIGG eller PTS, alternativt inom den struktur som etableras av det europeiska AI-kontoret.

- AI-kommissionen har presenterat flera förslag för att stärka tillgången till beräkningskraft för såväl träning som användning av AI-tjänster, samt för att göra mer data tillgänglig för träning. Vi stödjer dessa förslag och ser dem som viktiga för att bygga en AI-infrastruktur med ökad redundans.

Mobilnätens roll

Sveriges digitala infrastruktur byggs, ägs och drivs av ett stort antal olika aktörer med starkt varierande ambitioner inom de

40 SOU 2025:12 AI-kommissionens Färdplan för Sverige, Finansdepartementet, https://regeringen.se/rapporter/2024/11/ai-kommissionens-fardplan-for-sverige/.

två områden som är avgörande för dess resiliens: redundans och teknologi.

I Sverige finns idag väl utbyggda kärn- och spridningsnät baserat på fiber, som ser till att en effektiv och robust kommunikation är möjlig för såväl radio- (mobilnät) och fiberbaserad access. Utöver detta har vi både en fiber- och mobilbaserad accessinfrastruktur som båda når en stor del av landets hushåll och affärsverksamheter. Det fiberbaserade accessnätet saknar ofta redundans. Användarens router och fibermodem är dessutom normalt oövervakade och ansvaret faller därför på användaren att upptäcka och rapportera driftstörningar. Ur resiliensperspektiv är detta mindre bra. En enkel möjlighet att skapa accessredundans för fasta anslutningar är därför att förutom fiberaccess utnyttja mobilnätet.

Dessutom kan en väl fungerande mobil access bli än mer resilient genom åtgärder inom ett antal grundläggande funktioner.

Den första funktionen är beroendet av en enskild mobiloperatörs nät. Normalt är uppkopplade enheter knutna till ett enskilt mobilnät och kan enbart använda detta nät och dess resurser. För resor mellan länder har det dock sedan länge funnits så kallad ”internationell roaming” som möjliggör användning av

andra nät än det egna. Motsvarande lösning inom ett land, så kallad ”nationell roaming”, kan användas för att öka tillgängligheten av mobil infrastruktur vid driftsstörningar i radionät genom exempelvis fiberbrott eller elbortfall. I dessa fall fungerar operatörens kärnnät, men radionätet är utslaget. Av konkurrenslagstiftningsskäl är användningen av nationell roaming normalt starkt begränsad. I Sverige tillåter existerande regelverk aktivering först när landet är försatt i ”höjd beredskap”.

Denna restriktiva reglering av nationell roaming skapar problem och kan stå i strid med både samhällets och individers behov av tillgänglig och robust kommunikation vid incidenter eller i kris. Möjligheten att använda andra operatörers nät kan i vissa fall vara livsavgörande och vi ser därför behov av att aktivera nationell roaming även vid lägre hot- eller krisnivåer. Samhällsfunktioner som vård, polis och räddningstjänst måste alltid kunna kommunicera även om en enskild operatörs mobilnät är utslaget.

Ett mer flexibelt regelverk för nationell roaming kan skapa positiva incitament för investeringar i resiliens. En operatör med ett mer robust nät kommer, över tid, att förmedla mer trafik än den ”ger bort” till andra.

En annan funktion är prioritering. I ett hårt belastat nät – exempelvis vid en översvämning, men även vid mer positiva händelser som sportevenemang – måste både privatpersoner som ringer 112 och myndigheters kommunikation (exempelvis RAKEL G2/SWEN[41]) kunna garanteras. 5G har, till skillnad från tidigare teknikgenerationer, stöd för denna typ av prioritering.

Det måste dock finnas tydliga överenskommelser om vilka som ska prioriteras och hur dessa tjänster ska realiseras så att förväntningar på mobilnäten uppfylls – inklusive vilka myndigheter som ska kunna köpa MOCN-tjänster (Multi-Operator Core Network) av operatörer och hur övergripande prioritering sker, inte bara mellan operatörer, utan också mellan prioriterade tjänster. Idag baseras dessa prioriteringar på primärt marknadsekonomiska överenskommelser.

Utöver civilsamhällets behov av nationell roaming och prioritering finns även säkerhets- och försvarsrelaterade utmaningar.

41 ”Utveckling av nästa generations kommunikationssystem”, Myndigheten för samhällsskydd och beredskap, 8 augusti 2025, https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakra-kommunikationer/utveckling-av-nasta-generations-kommunikationssystem/.

Ett sådant exempel kan vara närvaro och stödjande av utländsk militär trupp på svensk mark. Skulle Sverige bli digitalt avskuret från truppens ursprungsland fungerar inte internationell roaming och därmed inte heller dess mobilt uppkopplade utrustning. Med Sveriges inträde i NATO är detta ett än mer realistiskt scenario.

Den tredje funktionen är slutna mobilnät. Mobilnät byggs och drivs idag företrädesvis som publika (av till exempel Telia, Net4Mobility eller Tre), men det finns också intresse av slutna nät, exempelvis inom tillverkningsindustrin. Om sådana slutna nät byggs som fysiskt separata nät i stället för som en isolerad del i ett publikt nät kan dess master inte tillgängliggöras för andra användare. I krissituationer blir de därmed heller ingen resiliensstärkande samhällsresurs, varken för roaming eller prioritering. Detta är av yttersta vikt då alla mobilnät tillsammans ger den förmåga som förväntas av samhället. Samtidigt måste marknadsekonomiska krafter fortsätta leda till innovation och investeringar.

Den sista funktionen bygger på behoven av att använda de senaste standarderna, till exempel 5G för mobilnät. Kommunikation via fiber är robust mot avsiktlig elektronisk störning medan

HUR BIDRAR 5G TILL ÖKAD RESILIENS?

Tillförlitlighet. 5G-nät ansluter inte en enskild plats utan täcker en geografisk yta. Slås en radiomast ut kan man normalt fortsätta kommunicera med andra.

Robusthet. En 5G-förbindelse är mycket svår att störa och kan inte klippas eller grävas av.

Uthållighet. 5G-nät har reservkraft och fungerar därför även vid strömavbrott.

Felsäkerhet. Utrustning kan automatiskt koppla över till 5G (eller till ett annat 5G-nät) när en förbindelse fallerar. Ett 5G-nät är ständigt övervakat, driftstörningar går aldrig oupptäckta.

Flexibilitet. En 5G-uppkoppling fungerar lika bra stationärt som rörligt. En temporär 5G-basstation kan anslutas via mikrovågslänk och installeras på någon timma.

Integritet. Ett 5G-nät kopplar bara upp identifierade, legitima användare eller enheter.

Snabbhet. 5G är snabbare än Wi-Fi-routern i ett genomsnittligt svenskt hem.

sådan som bygger på radiovågor är mer utsatt. I vidareutvecklingen av mobilstandarder kommer nya funktioner som ytterligare ökar tillförlitlighet, snabbhet och robusthet och närmar sig dessa för en fast anslutning. Redan 5G är långt mer robust än exempelvis 4G eller Wi-Fi.

Mobilnät, där 5G är fullt implementerat i både radionät och kärnnät (så kallad *stand-alone-5G*), erbjuder en högre nivå av resiliens och robusthet än tidigare generationers nät. För att stärka den digitala infrastrukturens motståndskraft krävs att varje teknologis styrkor utnyttjas, vare sig det gäller fiber, mobil eller kopparnät.

Eftersom mobilnät bygger på öppna standarder har teleoperatörer stor frihet i hur de bygger sina nät. I exempelvis USA, Kina och Indien har det funnits ett politiskt tryck och ekonomiska incitament att investera i så kallad *stand-alone-5G*. I Europa har situationen varit en annan. Detta ger visserligen europeiska mobilkunder många av 5G:s vinster som hastighet, kapacitet och låg fördröjning, men inte de resiliens- eller flexibilitetsfördelar en fullt implementerad 5G medför.

Att ha den senaste teknologin är inte bara gynnsamt ur ett resiliensperspektiv, det gynnar även innovations- och konkurrens-

kraft. En mer avancerad digital infrastruktur accelererar den digitala transformationen och driver innovation.

Förslag

För att adressera ovan nämnda utmaningar rekommenderar vi att:

- Sveriges mobiloperatörer accelererar sina implementationsplaner för nya 5G-funktioner i kärn- och accessnät.
- Försvarsmakten tillsammans med teleoperatörerna tar fram en lösning för internationell roaming vid förlust av digital kontakt med andra länder.
- PTS ser över och ändrar definitionerna av extrem- och krissituationer så att tillgängliggörandet och möjligheten att nyttja exempelvis nationell roaming förenklas och utökas.
- PTS ser över krav på aktörer som tilldelas spektrumlicens för mobilnät. Exempel på krav kan vara att aktören tillgängliggör nätet för särskilda användare (som MSB:s nät SWEN,

Försvarsmakten,[42] m.fl.) på ett förutsägbart sätt. Detta gäller både vilka som ska ges möjlighet till prioritet och koordinering av hur detta ska implementeras.

- PTS tillser att kraven ovan gäller alla som tilldelas spektrum, inklusive slutna mobilnät.

Skydd och övervakning av fiberinfrastruktur

Den fysiska infrastrukturen som bär upp digital kommunikation måste skyddas och övervakas på ett systematiskt och långsiktigt sätt. Särskilt sårbar är transportfiberinfrastrukturen, de geografiskt spridda förbindelser som kopplar samman regioner och större noder. Här är behoven av förbättrat skydd och ökad övervakning som störst. Denna del av infrastrukturen är kritisk för kommunikationsflöden på nationell nivå men är ofta svår att

42 Margareta Svensson, ”Försvaret ska testa ny 5G-teknik för att säkra uppkoppling”, *Sveriges radio*, 17 juni 2025, https://www.sverigesradio.se/artikel/forsvaret-ska-testa-ny-5g-teknik-for-att-sakra-uppkoppling.

överblicka och mer utsatt för både oavsiktliga skador och avsiktliga angrepp.

Fiberinfrastrukturen, både på land och till sjöss, utgör en kritisk del av Sveriges digitala ryggrad och är central för informationshantering, kommunikation och samhällsfunktioner. Den behövs oavsett om mobildata (till exempel 5G) eller fiber används för access. Trots denna avgörande betydelse är ansvarsfördelningen för övervakning och skydd av fiber fragmenterad. Idag är ansvaret uppdelat mellan flera myndigheter, ofta under olika departement inom Regeringskansliet, och dessutom ligger ett stort ansvar för spridningsnät hos kommuner och regioner. I vissa situationer råder oklara ansvarsområden, samtidigt som tillgången till fiberinfrastruktur kan vara begränsad eftersom endast transmission, och inte svartfiber, erbjuds. Detta skapar otydlighet, gränsdragningsproblem och risk för ineffektivitet i hanteringen av ett av Sveriges mest strategiska infrastruktursystem.

För att minska sårbarheten och stärka resiliensen i det svenska samhället krävs ett mer koordinerat och proaktivt angreppssätt. Det räcker inte med att veta var fiber finns förlagd, det krävs också en övergripande förståelse för hur användningen av

fiberinfrastrukturen[43] påverkar samhällets funktion. Avsaknad av tillgång till svartfiber, eller ett fiberbrott, särskilt i ett kritiskt segment, kan i värsta fall få samhällsövergripande konsekvenser.

Sveriges digitaliseringsstrategi beskriver åtgärder för att öka möjligheterna till kommunikation vid höjd beredskap. Vi menar dock att sådana möjligheter även behövs i mindre dramatiska lägen. PTS:s robusthetsarbete[44] adresserar många säkerhetsrelaterade aspekter men inte alla scenarier relaterat till tillgång till mobil kommunikation, exempelvis om en operatörs kärnnät eller radionät slås ut helt, eller om elförsörjningen i ett område försvinner under en längre tid.

Förslag

- PTS utses till ansvarig myndighet för samordning, tillsyn och övervakning av fiberinfrastrukturen inom Sveriges

43 "Optodas – The leading technology for distributed acoustic sensing", ASN, åtkomstdatum 12 september 2025, https://www.asn.com/fiber-sensing/.

44 "Robust kommunikation", Post- och telestyrelsen, 14 maj 2024, https://pts.se/internet-och-telefoni/robust-kommunikation/.

gränser, samt för de delar som korsar landsgränser. Detta inkluderar fiber till sjöss, i luften och i mark.

- PTS får mandat att samordna och samla in övervakningsdata från fiberägare och andra relevanta aktörer. Data från fiberövervakning ska integreras i nationella lägesbilder, vilket möjliggör snabbare och mer precis respons vid incidenter och kan bidra till att förebygga att incidenter inträffar.

- PTS ska samverka med:
  - Försvarsmakten, för att säkerställa att infrastrukturen skyddas ur ett nationellt säkerhetsperspektiv.
  - Polismyndigheten, för att möjliggöra effektiv brottsbekämpning kopplat till sabotage, intrång och andra hot mot digital infrastruktur.
  - Kustbevakningen, för att skydda fiberinfrastruktur till sjöss och i kustnära områden.
  - Fiberägare, för insamling av övervakningsdata, säkerställa operativ insyn, driftsäkerhet och riskhantering.

- PTS fortsätter och utökar sitt arbete med robusthetshöjande åtgärder gällande fiber, inkluderar användning för mobilaccess och ser över myndighetskrav på tillförlitlighet för aktörer som driver fiberaccessnät.

Rymdbaserade tjänster och dess påverkan på övrig infrastruktur

Satelliterna runt jorden utgör en viktig infrastruktur som levererar information och tjänster som används dagligen och är avgörande för samhället. Exempel är klimat- och väderinformation, positionering med tidsangivelse samt kommunikation. Rymdsystemen bidrar också till global transparens genom kontinuerlig jordobservation vilket gör det möjligt att upptäcka naturfenomen som bränder och översvämningar, men även var trupper eller flyktingar befinner sig. Inte minst kan rymden erbjuda ett alternativ till jordbaserad kommunikation via radio eller fiber.

I vissa situationer utgör rymdbaserade system det enda alternativet till markbaserad kommunikation. Utan rymdbaserade system skulle möjligheten att upprätthålla kommunikation kunna bli mer sårbar jämfört med om sådana system finns som komplement.

På grund av sin kritiska roll satsar många länder på rymden. Många av systemen är dessutom *”dual-use”* det vill säga att de kan användas både civilt och militärt. Den globala rymdmarknaden består både av offentligt finanseriade och kommersiella

aktörer och förväntas omsätta 944 miljarder dollar år 2033.[45] Sverige har en god kunskapsnivå inom satellitkonstruktion, sändning och mottagning av data.

Rymden är internationell till sin natur och förutom nationella initiativ lägger Sverige merparten av sin rymdbudget på ESA (European Space Agency). ESA kan jämföras med den amerikanska rymdstyrelsen NASA på så sätt att ESA, liksom NASA, har program inom en mängd olika rymdområden såsom jordobservation, navigation, teknikutveckling och bärraketer. ESA och EU har ett nära samarbete där utvecklingen sker inom ESA medan EU förvaltar och köper upp system och tjänster från ESA. Exempel på detta är Säker kommunikation (IRIS2), Galileo (GPS), jordobservation (Copernicus).

De flesta europeiska länder satsar mer på rymdområdet än vad Sverige gör, vilket i sin tur innebär att Sveriges inflytande är begränsat. Som följd av detta minskar även Sveriges inflytande och möjlighet till affärsmöjligheter inom EU. Detta får bland annat till följd att Sveriges rymdsektor halkar efter och att kompe-

45 Novaspace, *Space Economy report* (2025), https://nova.space/hub/product/space-economy-report/.

tensförsörjningen drabbas. Även om rymden ingår i Sveriges beredskapsstruktur har sektorn ingen tydlig plats i det teknikstrategiska innovationsarbetet. Rymden ingår inte bland de utvalda svenska strategiska teknikområdena, vilket skiljer sig från andra länder i Europa. Draghi-rapporten lyfter också rymden som viktig för Europas konkurrenskraft.

Vid kris och krig är positionering, navigering och tid, markobservation och kommunikation (framför allt reservkommunikation) kritiska för samhällets funktion och ekonomiska stabilitet. Dessa tjänster är sårbara för olika typer av hot, inklusive antisatellitmissiler och kärnvapendetonationer i rymden.

På samma sätt som rymdbaserade system kan vara alternativ till primära markbaserade system kan markbaserade system vara alternativ till primära rymdbaserade sådana. Inom tid- och frekvensdistribution ser vi utveckling av markbaserade system som dock fortfarande är beroende av viss rymdbaserad funktionalitet.[46] För att uppnå den förmåga som förväntas måste såväl mark som rymd användas i betydligt högre utsträckning, och detta på ett koordinerat sätt.

Ett annat allvarligt hot är att kollisioner eller användning av anti-satellitmissiler mot objekt i låg jordbana (Low Earth Orbit, LEO) kan ge kaskadeffekter som gör att mängden rymdskrot[47] ökar, ett så kallat "Kessler-syndrom".[48] Detta skulle kunna leda till att LEO-banorna blir så fulla med rymdskrot att vi inte längre kan använda den infrastruktur som finns där.

46 "PTS åtgärder för robust kommunikation", Post- och telestyrelsen, 14 maj 2024, https://pts.se/internet-och-telefoni/robust-kommunikation/robusthojande-atgarder/.

47 "Space debris", Wikipedia, 11 september 2025, https://en.wikipedia.org/wiki/Space_debris.

48 "Kessler syndrome", Wikipedia, 29 augusti 2025, https://en.wikipedia.org/wiki/Kessler_syndrome.

Förslag

- Säkerställ att det svenska forsknings- och innovationssystemet tydligt inkluderar rymden som ett för Sverige strategiskt område.
- Ge Rymdstyrelsen möjlighet att öka Sveriges engagemang inom relevanta ESA-program. Exempel på detta är Space Situation Awareness (SSA) och ESA Earth Online (ERS). Förutom att det ökar svensk innovations- och konkurrenskraft ger det även större inflytande inom EU:s rymdprogram.
- Fortsätt utveckla och implementera markbaserade alternativa navigationslösningar och redundanta system för tid, positionering och väder i samverkan med utveckling på rymdsidan. Ett samarbete inom EU[49] kan vara värdefullt för att bygga upp och finansiera sådana lösningar. Flera aktörer behövs för att realisera detta: Försvarsmakten, PTS, MSB, RISE och Netnod.

49 ”The European Commission unveils the 2023 European Radio Navigation Plan (ERNP)”, EU-kommissionen, 25 januari 2024, https://defence-industry-space.ec.europa.eu/european-commission-unveils-2023-european-radio-navigation-plan-ernp-2024-01-25_en.

Mer robust elförsörjning genom kompletterande lösningar

Digital infrastruktur är beroende av en stabil och tillförlitlig elförsörjning. Alla fysiska komponenter – från datacenter och knutpunkter till basstationer och förbindelselänkar – kräver tillgång till elektricitet för att fungera. Elförsörjningen kan ske via elnätet eller i form av lokalt hanterad reservkraft.

Vi har i Sverige god tillgång till el. Trots det inträffar avbrott som verksamheter ibland behöver hantera lokalt, delvis genom egen elproduktion och temporär lagring i batterier. Det finns fall då företags planerade (utökade) verksamhet har påverkats av elbrist. Behovet av att fortsätta bygga ut elnät i Sverige är fortsatt högt.[50]

Ett förslag för att förbättra situationen är så kallade energigemenskaper,[51] lokala sammanslutningar som ger möjlighet till lokal produktion, konsumtion, och lagring – men inte bara lokalt

50 IVA, *Elektrifieringen – så river vi barriärerna*, projektrapport (2025), https://www.iva.se/rapport-elektrifieringen.

51 Energimyndigheten, *Energigemenskaper*, ER 2024:20 (2024), https://energimyndigheten.a-w2m.se/System/TemplateView.aspx?p=Arkitektkopia&id=294bae20fa14458da8673d849234874b&q=2024%3A20&lstqty=1.

för en brukare, utan inom gemenskapen. Därmed kan en brukare, som har överskott i sin lokala produktion, dela med sig till en närliggande, som har överskott i lagring. Detta kan bidra till en tryggare elförsörjning genom möjligheter till olika grader av lokal så kallad ö-drift. Energigemenskaper skulle också kunna spela en viktig roll för att försörja kritisk infrastruktur vid ett omfattande elavbrott genom diversitet i form av alternativ till det lokala elnätsbolaget.

EU har tagit steg framåt gällande möjlighet att skapa sådana energigemenskaper (exempelvis Elmarknadsdirektivet[52] och REPowerEU-initiativet[53]). Några av förutsättningarna för energigemenskaper berörs även i promemorian ”Förbättrad utformning av EU:s elmarknad”.[54]

52 *Europarlamentets och Rådets direktiv (EU) 2019/944 om gemensamma regler för den inre marknaden för el*, Europeiska unionen, 5 juni 2019, https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019L0944.

53 *“REPowerEU Affordable, secure and sustainable energy for Europe”*, EU-kommissionen, 17 juni 2025, https://commission.europa.eu/topics/energy/repowereu_en.

54 Klimat- och näringslivsdepartementet, *Förbättrad utformning av EU:s elmarknad*, promemoria, februari 2025, https://www.regeringen.se/contentassets/58044ff46c1d44988751eee2fba1cfed/promemoria-forbattrad-utformning-av-eus-elmarknad.pdf.

Vi ser energigemenskaper som ett viktigt komplement till det centrala elnätet.

Förslag

- Utbyggnad av elnätet ska fortsätta för att minimera risk för elavbrott.
- Lagstiftaren[55] bör skapa förutsättningar att bilda energigemenskaper för att reducera beroenden av central eldistribution och öka resiliensen enligt den väg EU har valt. Här krävs initiativ från riksdag och regering.

55 SFS 2021:976 Förordning om ändring i förordningen (2007:215) om undantag från kravet på nätkoncession enligt ellagen (1997:857), https://svenskforfattningssamling.se/sites/default/files/sfs/2021-11/SFS2021-976.pdf.

Fortsatta steg mot en resilient digital infrastruktur

Gemensamma och effektfulla insatser behövs för en säkrare digital framtid

Vi har i denna rapport visat att utvecklingen av en resilient digital infrastruktur är ett långsiktigt arbete som kräver samverkan, uthållighet och förmåga att anpassa sig till förändrade förutsättningar. Det finns både starka drivkrafter och tydliga behov – men också en god grund att bygga vidare på.

De förslag som presenterats visar på vägar framåt. Nu krävs att berörda aktörer tar vid och omsätter insikterna i handling. IVA ser ett fortsatt behov av att följa upp och vidareutveckla de föreslagna åtgärderna samt främja sektorsöverskridande samverkan.

Teknikutvecklingen går snabbt, hotbilden förändras och nya möjligheter uppstår. Det innebär att frågorna om digital resiliens inte är statiska utan måste hållas levande. Resiliens handlar inte bara om teknik, utan också om struktur, samarbete och förtroende.

IVA kommer att verka för att dessa frågor fortsatt står högt på agendan. Rapporten är ett steg på vägen, men långt ifrån det sista. Genom gemensamma och målmedvetna insatser kan vi stärka Sveriges innovationskraft, säkerhet och konkurrenskraft.

Appendix

Referenser

ASN. “Optodas – The leading technology for distributed acoustic sensing”. Åtkomstdatum 12 september 2025. https://www.asn.com/fiber-sensing/.

Bg2 Pod. ”Satya Nadella | BG2 w/ Bill Gurley & Brad Gerstner”, 12 december 2024. YouTube, https://youtu.be/9NtsnzRFJ_o?t=2800.

Borglund, Ann-Sofie. ”Energi-CERT ska hjälpa energiföretag med cybersäkerhet”. Tidningen Energi, 28 maj 2025. https://www.energi.se/artiklar/2025/maj-2025/energi-cert-ska-hjalpa-energiforetag-med-cybersakerhet/.

Campus totalförsvar. (2025). https://campustotalforsvar.se/.

CCDCOE. (2025). The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/.

Cyber Essentials. (2025). https://www.ncsc.gov.uk/cyberessentials/overview.

Energimyndigheten, Energigemenskaper, ER 2024:20 (2024). https://energimyndigheten.a-w2m.se/System/TemplateView.as

px?p=Arkitektkopia&id=294bae20fa14458da8673d849234874b&q=2024%3A20&lstqty=1.

Enterprise Estonia. “X-road – Interoperability services”. Åtkomstdatum 12 september 2025. https://e-estonia.com/solutions/interoperability-services/x-road/.

EU-kommissionen. *The Draghi report on EU competitiveness* (2024). https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

EU-kommissionen. “NIS2 Directive: securing network and information systems”. Åtkomstdatum 12 september 2025. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

EU-kommissionen. “REPowerEU Affordable, secure and sustainable energy for Europe”, 17 juni 2025. https://commission.europa.eu/topics/energy/repowereu_en.

EU-kommissionen. ”Cyber Resilience Act”. Åtkomstdatum 12 september 2025. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

EU-kommissionen. ”Ett djärvare, enklare och snabbare EU: kommissionens arbetsprogram 2025”, 12 februari 2025.

https://ec.europa.eu/commission/presscorner/detail/sv/ip_25_466.

EU-kommissionen. ”EU:s cybersolidaritetsakt”, 9 juli 2025. https://digital-strategy.ec.europa.eu/sv/policies/cyber-solidarity.

EU-kommissionen. ”The European Commission unveils the 2023 European Radio Navigation Plan (ERNP)”, 25 januari 2024. https://defence-industry-space.ec.europa.eu/europe-an-commission-unveils-2023-european-radio-navigation-plan-ernp-2024-01-25_en.

EU-kommissionen. Kommissionens rekommendation (EU) 2020/2245, 18 december 2020. https://eur-lex.europa.eu/legal-content/SV/TXT/?qid=1757680986679&uri=CELEX%3A32020H2245.

Europeiska unionen. Europarlamentets och Rådets direktiv (EU) 2019/944 om gemensamma regler för den inre marknaden för el, 5 juni 2019. https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32019L0944.

Eurostat. “Cloud computing – statistics on the use by enterprises”, december 2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_

the_use_by_enterprises#Use_of_cloud_computing:_highlights.

Finansdepartementet, ”Utredning för att snabba på utbyggnaden av 5G och fiber i Sverige”, 29 augusti 2024. https://www.regeringen.se/pressmeddelanden/2024/08/utredning-for-att-snabba-pa-utbyggnaden-av-5g-och-fiber-i-sverige/.

Finansdepartementet. *Sveriges digitaliseringsstrategi 2025–2030* (2025). https://www.regeringen.se/rapporter/2025/05/sveriges-digitaliseringsstrategi-20252030/.

Finansinspektionen. ”Om Dora”, 12 februari 2024. https://www.fi.se/sv/forsakring/it-risker-dora/om-dora/.

Förenklingsrådet. (2025). https://forenklingsradet.se/.

Förenta Nationerna. ”Sustainable development goals”. Åtkomstdatum 12 september 2025. https://www.un.org/sustainabledevelopment/infrastructure-industrialization/.

Försvarsdepartementet. *En ny era av cybersäkerhet – Nationell strategi för cybersäkerhet 2025–2029 Bilaga 1: Handlingsplan* (Regeringskansliet, 20 mars 2025). https://www.regeringen.se/informationsmaterial/2025/03/nationell-strategi-for-cybersakerhet-2025-2029/.

IVA. *Digitalisering för ökad konkurrenskraft*, projektrapport (2019). https://www.iva.se/publicerat/rapport-digitalisering-for-okad-konkurrenskraft/.

IVA. *Elektrifieringen – så river vi barriärerna*, projektrapport (2025). https://www.iva.se/rapport-elektrifieringen

Klimat- och näringslivsdepartementet. *Förbättrad utformning av EU:s elmarknad*, promemoria, februari 2025. https://www.regeringen.se/contentassets/58044ff46c1d44988751eee2fba1cfed/promemoria-forbattrad-utformning-av-eus-elmarknad.pdf.

Lindsten, Per Olof, ”Småföretagen sämst rustade mot cyberattacker”. *Dagens industri*, 13 september 2021. https://www.di.se/nyheter/smaforetagen-samst-rustade-mot-cyberattacker/.

Mittelstand Digital. (2025). https://www.mittelstand-digital.de/MD/Navigation/DE/Home/home.html.

Myndigheten för samhällsskydd och beredskap. ”Utveckling av nästa generations kommunikationssystem”, 8 augusti 2025. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/sakra-kommunikationer/utveckling-av-nasta-generations-kommunikationssystem/.

Myndigheten för samhällsskydd och beredskap. *När kriget kom nära – Årsrapport it-incidentrapportering 2022*, (2022). https://rib.msb.se/filer/pdf/30339.pdf.

Myndigheten för samhällsskydd och beredskap. *Vägledning för fysisk informationssäkerhet i it-utrymmen* (2013). https://rib.msb.se/filer/pdf/27280.pdf.

Nasir, Rahiel. "The Evolution of Digital Sovereignty: Moving Beyond Data and Cloud". *IDC*, 13 januari 2023. https://blog-idceurope.com/the-evolution-of-digital-sovereignty-moving-beyond-data-and-cloud/.

Novaspace. *Space Economy report* (2025). https://nova.space/hub/product/space-economy-report/.

O'Grady, Michael. "The Global Digital Economy Will Reach $16.5 Trillion And Capture 17% Of Global GDP By 2028". *Forrester*, 23 juli 2024. https://www.forrester.com/blogs/the-global-digital-economy-will-reach-16-5-trillion-and-capture-17-of-global-gdp-by-2028/.

Post- och telestyrelsen. "PTS åtgärder för robust kommunikation", 14 maj 2024. https://pts.se/internet-och-telefoni/robust-kommunikation/robusthojande-atgarder/.

Post- och telestyrelsen. ”Robust kommunikation”, 14 maj 2024. https://pts.se/internet-och-telefoni/robust-kommunikation/.

Finansdepartementet och Socialdepartementet. ”Regeringen stärker säkerheten och kostnadseffektiviteten genom statlig it-drift”, 7 november 2024. https://www.regeringen.se/pressmeddelanden/2024/11/regeringen-starker-sakerheten-och-kostnadseffektiviteten-genom-statlig-it-drift/.

Riigi Teataja. “General Part of the Economic Activities Code Act”, 22 augusti 2014. https://www.riigiteataja.ee/en/eli/522082014004/consolide.

Riigi Teataja. “Public Information Act”, 14 november 2013. https://www.riigiteataja.ee/en/eli/514112013001/consolide.

Riksrevisionen. RiR 2024:24 *Säkerhetspolisens verksamhet* (2024). https://www.riksrevisionen.se/download/18.73ed0f241939545744f9e97/1733952229669/RiR_2024_24_rapport.pdf.

SektorCERT. (2025). https://sektorcert.dk/.

SFS 2021:976 *Förordning om ändring i förordningen (2007:215) om undantag från kravet på nätkoncession enligt ellagen*

(1997:857). https://svenskforfattningssamling.se/sites/default/files/sfs/2021-11/SFS2021-976.pdf.

SFS 2022:482 *Lag om elektronisk kommunikation*. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482/

SOU 2025:06 *Plikten kallar! En modern personalförsörjning av det civila försvaret*. Försvarsdepartementet. https://regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/01/sou-20256/.

SOU 2025:12 *AI-kommissionens Färdplan för Sverige*. Finansdepartementet. https://regeringen.se/rapporter/2024/11/ai-kommissionens-fardplan-for-sverige/.

SOU 2025:79 *Samlade förmågor för ökad cybersäkerhet*. Försvarsdepartementet. https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2025/07/sou-202579/.

Stöldskyddsföreningen. *SSF 1101 utg. 2 – SSF Cybersäkerhet Basnivå-Grundläggande IT-säkerhet*, 2:a uppl. (SFF, 2023). https://www.stoldskyddsforeningen.se/butik/foretag/ssf-nor-

mer/cybersakerhet/ssf-1101-utg-2-ssf-cybersakerhet-basniva-grundlaggande-it-sakerhet/.

Svensson, Margareta. ”Försvaret ska testa ny 5G-teknik för att säkra uppkoppling”. *Sveriges radio*, 17 juni 2025. https://www.sverigesradio.se/artikel/forsvaret-ska-testa-ny-5g-teknik-for-att-sakra-uppkoppling.

White, Ryan. “How the cloud saved Ukraine’s data from Russian attacks”. *C4ISRNET*, 22 juni 2022. https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks/.

Wikipedia. “Once-only principle”, 7 augusti 2025. https://en.wikipedia.org/wiki/Once-only_principle.

Wikipedia. “Space debris”, 11 september 2025. https://en.wikipedia.org/wiki/Space_debris.

Wikipedia. ”Kessler syndrome”, 29 augusti 2025. https://en.wikipedia.org/wiki/Kessler_syndrome.

World Economic Forum. “Why digital public infrastructure is key to building a connected future”, 17 april 2025. https://www.weforum.org/stories/2025/04/digital-public-infrastructure-building-connected-future/.

Ordlista

AI-agent, ett system som kan uppfatta sin omgivning, fatta beslut och utföra uppgifter självständigt, ofta med hjälp av artificiell intelligens.

AI-förklarbarhet, hur väl man kan förstå, följa och förklara hur ett AI-system fattar beslut eller kommer fram till sina resultat.

API, Application Program Interface, en uppsättning regler och verktyg som låter olika program eller system kommunicera och utbyta data med varandra.

CCDCOE, The NATO Cooperative Cyber Defence Centre of Excellence

CERT, Computer Emergency Response Team, en expertgrupp som hanterar och samordnar åtgärder vid it-incidenter och cyberattacker.

CRA, Cyber Resilience Act, EU-förordning som ställer krav på att digitala produkter och tjänster är säkra, motståndskraftiga mot cyberattacker och kan uppdateras vid säkerhetsbrister.

DDoS-attack, Distributed Denial-of-Service attack, en överbelastningsattack där många datorer samtidigt skickar stora mängder trafik mot en tjänst eller webbplats för att göra den otillgänglig.

Digital infrastruktur begrepp som omfattar de komponenter som är avgörande för att stödja digitala tjänster och applikationer. Dessa kan vara både hårda (som kommunikationsnät och datacenter) och mjuka (som standarder, identitets- och betalningslösningar). (Inspirerad av Tech Sverige.)

Diversitet, att använda olika typer av nätverk, servrar, programvaror eller leverantörer för att minska sårbarhet och öka motståndskraften.

DORA, Digital Operational Resilience ACT, EU-förordningen för digital operativ motståndskraft (Dora-förordningen).

FRA, Försvarets radioanstalt

Finansforum, etablerad samverkan inom NCSC med samhällsviktiga aktörer inom finansiell sektor.

FOI, Totalförsvarets forskningsinstitut

FSPOS, Finansiella sektorns privat-offentliga samverkan

GPU, Graphics Processing Unit, en processor som är specialiserad på att snabbt hantera grafik och parallella beräkningar, ofta använd för spel, 3D-rendering och artificiell intelligens.

Höjd beredskap, ett formellt tillstånd beslutat av regeringen där myndigheter och kommuner intensifierar förberedelser för att hantera allvarliga hot, kriser eller krig.

Informationsresiliens, innebär att kritisk information som är avgörande för att upprätthålla samhällsfunktioner och säkerställa kontinuitet i verksamheter är tillgänglig, korrekt och skyddad.

Internationell roaming, möjlighet för mobilanvändare att använda sin telefon i utlandet genom andra operatörers nätverk.

ISO 27001, internationell standard för informationssäkerhet.

LEK, Lagen om elektronisk kommunikation

MOCN-tjänster (Multi-Operator Core Network), Mobilnätslösningar där flera operatörer delar samma radiotillgångar (till exempel basstationer) men har separata kärnnät, vilket ger effektivare användning av nätverksinfrastruktur.

MSB, Myndigheten för samhällsskydd och beredskap. (Byter namn till MCF, Myndigheten för civilt försvar, den 1 januari 2026.)

NCSC, Nationellt cybersäkerhetscenter.

NIS2, direktivet om nät- och informationssäkerhet, EU-direktiv som ställer krav på företag och myndigheter att skydda sina nätverk och informationssystem, rapportera incidenter och öka cybersäkerheten.

NIST Cybersecurity Framework, Ett ramverk från NIST (National Institute of Standards and Technology, USA:s nationella standardiseringsinstitut) för att hantera och minska cyberrisker.

NTSG, Nationella Telesamverkansgruppen, en svensk myndighetsgrupp som samordnar tele- och kommunikationsfrågor vid kriser och höjd beredskap för att säkerställa fungerande kommunikation i samhället.

Nationell roaming, möjligheten för mobilanvändare att använda nätverk från andra operatörer inom samma land.

PTS, Post- och telestyrelsen.

Redundans, extra resurser eller reservlösningar som finns för att system ska fortsätta fungera om något går sönder, till exempel dubbla servrar eller nätförbindelser.

Resilient, relevant, tillförlitlig och motståndskraftig med förmåga till återhämtning och vidareutveckling. (Inspirerad av MSB.)

RISE, Research Institutes of Sweden, Sveriges forskningsinstitut och innovationspartner.

Roaming, se ”internationell roaming” respektive ”nationell roaming”.

Robusthet, systemets förmåga att fungera korrekt och motstå störningar eller fel, även under ovanliga eller påfrestande förhållanden.

STEM, förkortning för ämnesområdena Science, Technology, Engineering och Mathematics. Används för att beskriva utbildning och yrken inom naturvetenskap, teknik, ingenjörsvetenskap och matematik.

TOOP, the once-only principle, principen att medborgare och företag bara ska behöva lämna samma information till myndigheter en gång, eftersom myndigheter sedan delar uppgifterna sinsemellan på ett säkert sätt.

Test, en systematisk process för att utvärdera om ett system, en komponent eller en funktion fungerar som förväntat enligt

kravspecifikation eller design. Syftet är att upptäcka fel, brister eller avvikelser innan systemet tas i bruk eller vidareutvecklas.

Tjänsteresiliens, innebär att de digitala tjänster som används för att hantera och distribuera kritisk information är tillgängliga, robusta och pålitliga.

X-Road, en digital estnisk plattform som gör att myndigheter och företag i Estland säkert kan utbyta information och tjänster med varandra.

Övning, en förberedande och simulerad aktivitet där deltagare tränar på att identifiera, hantera och åtgärda fel eller störningar i ett system eller en process. Syftet är att förbättra beredskap, samarbete och reaktionsförmåga i en kontrollerad miljö. Övningar kan vara teoretiska (skrivbordsövningar) och/eller praktiska (tekniska).

Om projektet

IVAs projekt Resilient Digital Infrastruktur startade i juni 2024 och fortsätter fram till december 2025. Projektet leds av en styrgrupp som inledningsvis beslutade om den plan som beskriver projektets mål, syfte och arbetsprocess. Stora delar av

det operativa projektarbetet har bedrivits i tre arbetsgrupper. Dessa har under projektets gång rapporterat till, och fått återkoppling från, styrgruppen. Den politiska referensgruppen, som består av riksdagsledamöter från riksdagens åtta partier, har interagerat med projektet i arbetsmöten. Under projektet har kunskapsseminarier, workshoppar och möten hållits.

Styrgrupp

Pia Sandvik (ordförande), IVA-ledamot, Teknikföretagen
Daniel Akenine, IVA-ledamot, Microsoft
Björn Ekelund, IVA-ledamot, Ericsson
Anne-Marie Eklund Löwinder, IVA-ledamot, Amelsec
Patrik Fältström, IVA-ledamot, Netnod
Åke Holmgren, Myndigheten för samhällsskydd och beredskap (MSB)
Pontus Johnson, IVA-ledamot, Kungl. Tekniska högskolan (KTH)
Hans Lindberg, IVA-ledamot, Bankföreningen
Charlotte Lindgren, Försvarets radioanstalt (FRA)
Johan Malmliden, Omegapoint
Simin Nadjm-Tehrani, IVA-ledamot, Linköpings universitet
Anna Rathsman, IVA-ledamot, fd. gd Rymdstyrelsen

Arbetsgrupper

NÄRINGSLIVETS FÖRUTSÄTTNINGAR

Björn Ekelund (ordförande),
forskningsdirektör, Ericsson
Anna Björkegren, Manager Security R&D, Vattenfall
Erik Elmroth, professor, Umeå universitet
och Elastisys
Åsa Fast-Berglund, Development Portfolio Manager,
Stena Recycling
Katia Gallo, professor, NQCIS,
Kungl. Tekniska högskolan (KTH)
Magnus Jacobson, senior rådgivare, Svenska Bankföreningen
Nicklas Keijser, analytiker, Truesec
Thomas Lezama, Head of Architecture, Volvo Construction
Equipment
Daniel Persson, Head of Amyna, Ideon Science Park
Elin Ryrfeldt, CISO, Axfood, reprsenterar även Svensk
Dagligvaruhandel (SvDH)
Mattias Wallén, CISO, Swedish Space Corporation
Tomas Wallin, Försvarsmakten

STYRNING, SAMORDNING OCH SAMVERKAN

Simin Nadjm-Tehrani (ordförande), professor, Linköpings universitet
Anna Blix, beredskapsplanerare, Trafikverket
Sandra Elvin, National Security Officer, Microsoft
Mathias Ekstedt, professor, Kungl. Tekniska högskolan (KTH) och Google
Anders Fristedt, sr konsult, Informations- och Cybersäkerhet, Omegapoint
Robert Heiliger, Head of Technology & Innovation, E.ON Energidistribution
Anders Herrström, cyberstrateg, Försvarets radioanstalt (FRA)
Pernilla Jonsson, Head of Ericsson Consumer and Industry lab
Christoffer Karsberg, Senior Expert, Omegapoint
Eva Listi, Näringslivsrådets representant IVA, L.EVA/EAG
Ulf Pettersson, projektledare, Teracom
Patrik Sandgren, näringspolitisk expert inom digitalisering, Teknikföretagen

TEKNIK OCH SYSTEM

Patrik Fältström (ordförande), Säkerhetschef/CSO, Netnod
Daniel Akenine, teknikchef, Microsoft
Mehran Ghasemi, produktledare, Försvarets materielverk (FMV)
Johan Grufman, IT-säkerhetschef, Teracom
Johan Gunnarsson, CTO, Combitech
Cem Göcgören, enhetschef IT/cyber, Svenska Kraftnät
Annika Järvebro, Avancerad digitalisering
Göran Klang, Head of Research Project Office, Ericsson
Anton Lindström, produktägare, SVT
Per Nihlen, enhetschef Nättjänster, Vetenskapsrådet
Carl Piva, vd, Internetstiftelsen
Carolina Vendil Pallin, forskningsledare, Totalförsvarets forskningsinstitut (FOI)
Michael Westlund, partner och senior cybersäkerhetsstrateg, Omegapoint

Politisk referensgrupp

Lili André (KD)

Mats Berglund (MP)

Helena Gellerman (L)

Hanna Gunnarsson (V)

Niels Paarup-Petersen (C)

Jesper Skalberg Karlsson (M)

Markus Selin (S)

Johnny Svedin (SD)

Projektledning

Per Hjertén, huvudprojektledare, IVA

Staffan Eriksson, projektledare, IVA

Linda Olsson, projektledare, IVA

Eva Lagerblad, projektkoordinator, IVA

Marie Alpman, redaktör

Finansiärer

Combitech
Ericsson
Försvarets radioanstalt (FRA)
Internetstiftelsen
Microsoft
Myndigheten för samhällsskydd
och beredskap (MSB)
Omegapoint
Svensk Dagligvaruhandel
Svenska Bankföreningen
Teknikföretagen
Vattenfall.

Kungl. Ingenjörsvetenskapsakademien är en fristående akademi med uppgift att främja tekniska och ekonomiska vetenskaper samt näringslivets utveckling. I samarbete med näringsliv och högskola initierar och föreslår IVA åtgärder som stärker Sveriges konkurrenskraft.

Utgivare: Kungl. Ingenjörsvetenskapsakademien (IVA), 2025
Box 5073, SE-102 42 Stockholm
Telefon: 08-791 29 00

Inom ramen för IVAs verksamhet publiceras rapporter av olika slag. Alla rapporter sakgranskas av sakkunniga och godkänns därefter för publicering av IVAs vd.

IVA-M 560
ISSN: 1100-5645
ISBN: 978-91-89181-68-7

Projektledning: Per Hjertén, Staffan Eriksson,
Eva Lagerblad, Linda Olsson, IVA
Layout: Pelle Isaksson, IVA

Denna rapport finns att ladda ned på www.iva.se.

IVAs visionsprojekt **Svenska framtider** ska resultera i en väl förankrad och tydlig vision för Sverige som ledande teknik- och innovationsland år 2035 – med fokus på konkurrenskraft, hållbarhet och säkerhet.

Kungl. IngenjörsVetenskaps Akademien