Ett gemensamt språk för resilient digital infrastruktur

Kunskapsöversikt och rekommendationer om ansvar, rådighet och digitala beroenden i totalförsvaret

Daniel Dersén · Johan Magnusson · Jonny Holmström · Carl Piva · Carl Heath



FORUM Totalförsvar SCDI RI.SE digital förvaltning UTTC INTERNET STIFTELSEN

OM RAPPORTEN

Rapporten föreslår ett gemensamt språk för samtal om resilient digital infrastruktur. Den är skriven inom FORUM Totalförsvar, Swedish Center for Digital Innovations och RISE nationella initiativ för totalförsvarets omställning, och riktar sig till ledningar och experter i kommuner, regioner, myndigheter, näringsliv och civilsamhälle som delar ansvar för samhällsviktig verksamhet. Den bygger vidare på IVA:s rapport Resilient Digital Infrastruktur från 2025[1], som kartlägger den digitala infrastrukturens lager och föreslår konkreta åtgärder. Vår ambition är att utveckla och precisera IVA:s begrepp så att de kan bära samtal mellan aktörer.

Rapporten kan läsas på två sätt. Kapitel 1 är skrivet som en väckarklocka. Det beskriver varför frågan är brådskande och var samtalen oftast går fel. Kapitel 2 till 4 är skrivna för att slås upp i. De ger definitioner, forskningsstöd och en begreppstabell som kan användas som gemensam referens. Kapitel 6 omsätter språket i frågor som en ledning kan ställa till sin egen organisation. Bilagan innehåller en enkel bedömningsmall för workshoppar och ledningsgrupper.

Definitionerna är förslag grundade i såväl litteratur som praktik. De vilar på forskning och standarder, men de bör prövas i dialog med de aktörer som ska använda dem så att de kan ligga till grund för ett gemensamt språk.

INNEHÅLL

—	Sammanfattning	3
01	Varför ett gemensamt språk behövs	4
02	Två utgångspunkter: digital infrastruktur och rådighet	10
03	Vad vi menar med resiliens	18
04	Begreppsramen	20
05	Utblick: den finska modellen	29
06	Att använda språket	30
07	Avslutande kommentarer	33
B	Bilaga: Bedömningsmall	34
R	Referenser	36

FÖRFATTARE

Daniel Dersén, Johan Magnusson, Jonny Holmström, Carl Piva och Carl Heath

UTGIVARE

FORUM Totalförsvar

CITERA SOM

Dersén, D., Magnusson, J., Holmström, J., Piva, C. & Heath, C. (2026). *Ett gemensamt språk för resilient digital infrastruktur.* FORUM Totalförsvar.

UTGÅVA

November 2026

SAMMANFATTNING

Ansvaret ligger hos en aktör, kontrollen hos en annan

Sverige har på kort tid sett vad det innebär att samhällsviktig verksamhet vilar på digital infrastruktur som ingen enskild aktör överblickar.

När IT-leverantören Tietoevry angreps i januari 2024 slogs lönesystemet ut för omkring 120 myndigheter[2]. När IT-leverantören Miljödata angreps i augusti 2025 läckte personuppgifter för över 1,5 miljoner svenskar[3]. I båda fallen bar organisationerna ansvaret för verksamheten men saknade rådighet över den infrastruktur som bar den.

Vår huvudtes är att ett av de största hindren för digital resiliens är språkligt. Samma ord används för olika saker, och olika ord används för samma sak. Då faller ansvar mellan stolarna, regelefterlevnad förväxlas med förmåga och investeringar i redundans ger skenbar säkerhet. Vi föreslår därför en gemensam begreppsapparat. Den bygger vidare på IVA:s rapport Resilient Digital Infrastruktur[1] och vilar på två definitioner. Digital infrastruktur förstås som en samling möjliggörande, genomgripande och gränsöverskridande resurser. Rådighet förstås som förmågan att hålla samman kapacitet och mandat i handling, att veta, kunna, ha rätt och faktiskt få det gjort. Resilient digital infrastruktur definierar vi genom vad den klarar, att upprätthålla, återställa och vidareutveckla samhällsviktiga funktioner under störning och förändring. Vårt centrala anspråk är att den förmågan i hög grad avgörs av om de som bär ansvaret för funktionerna har rådighet. Digital suveränitet behandlar vi som en del av resiliensen, som rådighet över de villkor som digitala beroenden vilar på.

RAPPORTENS HUVUDPUNKTER

1. Den största sårbarheten ligger ofta i glappet mellan ansvar och rådighet.
2. Resiliens är en egenskap hos ett system av aktörer och teknik. Den byggs gemensamt och kan inte säkerställas enbart genom en enskild organisations upphandling.
3. Beroendet har flyttat neråt i infrastrukturen, till moln, plattformar och leverantörer som delas av många.
4. Redundans utan diversitet ger skenbar säkerhet mot gemensamma felorsaker.
5. Regelefterlevnad hos enskilda verksamheter behöver kompletteras med prövning av deras gemensamma beroenden.
6. Ett gemensamt språk är en förutsättning för en gemensam lägesbild och för gemensam handling.

01

Varför ett gemensamt språk behövs

Totalförsvaret bygger på att samhällsviktiga funktioner kan upprätthållas under svåra påfrestningar, i fred, kris och krig. Nästan alla sådana funktioner förutsätter i dag digital infrastruktur. Vård, omsorg, betalningar, livsmedelsförsörjning, transporter och kommunikation med invånare kräver att data, system och nät fungerar. Infrastrukturen ägs, drivs och styrs samtidigt av ett stort antal aktörer, många av dem privata och flera av dem utanför svensk jurisdiktion.

~120

myndigheters lönesystem slogs ut när Tietoevry angreps i januari 2024[2]

~160

kommuner drabbades när angreppet mot Miljödata upptäcktes i augusti 2025[4]

>1,5 milj

svenskars personuppgifter läckte i samma angrepp[3]

Det osynliga blir synligt när det fallerar

Infrastruktur blir synlig först när den fallerar[5]. Så länge den fungerar sjunker den undan och blir en förutsättning som ingen behöver tänka på. I vår kommande bok kallar vi denna process infrastrukturering, det vill säga hur något som en gång var ett eget objekt för styrning gradvis blir en osynlig förutsättning för något annat[6]. Ju mer verksamheten vilar på infrastrukturen, desto svårare blir den att se och att styra.

Två svenska händelser visar vad detta innebär i praktiken. Natten mot den 20 januari 2024 angreps ett av Tietoevrys svenska datacenter med utpressningsprogram. HR- och lönesystemet Primula slogs ut, och återställningen tog veckor[7]. Fyra regioner krävde i efterhand 12,5 miljoner kronor i ersättning, och bolaget beräknade sina ersättningskostnader till omkring 115 miljoner kronor[8]. Den 23 augusti 2025 upptäcktes ett angrepp mot Miljödata, som levere-

rar system till omkring 80 procent av landets kommuner. Angreppet drabbade system för läkarintyg, rehabilitering och arbetsskador hos omkring 160 kommuner och fyra regioner[4]. Kommuner som Lerum hanterade därefter rehabiliteringsplaner vid sidan av systemet enligt sina kontinuitetsplaner[9]. Det visar vad rådighet ser ut som när den finns. Rutinen fanns före angreppet och gick att använda utan systemet.

Ingen av händelserna var ett angrepp på kritisk infrastruktur i traditionell mening, utan angrepp på enskilda leverantörer. Ändå drabbades hundratals organisationer samtidigt, eftersom de delade ett beroende som få av dem hade med i sin egen riskbild. Desouza m.fl. kallar fenomenet ekosystemets transitivitet. Fel fortplantar sig genom kedjor av beroenden som är dolda för dem som vilar på dem, och få länder har en politik för den risken[10].

Samma mönster uppträder även utan faktiska angripare. Den 12 november 2026 fick Microsofts molntjänster ett avbrott som nådde användare i 74 länder[11]. Bolaget uppgav att det inte såg tecken på angrepp. När inloggningstjänsten slutade svara gick det inte heller att nå system som själva fungerade. Av 134 kommuner som 2025 besvarade Techtidningens fråga om sin e-post använde 126 samma leverantör[12]. Villkoren för en tjänst kan också ändras utan något fel. Internationella brottmålsdomstolens chefsåklagare förlorade enligt AP sin e-post 2025 sedan han belagts med amerikanska sanktioner[13], och domstolen har sedan dess arbetat med att byta kontorsplattform.

Fyra förskjutningar gör frågan brådskande

Den första förskjutningen rör koncentration. Internetmätningar visar att tjänster i allt högre grad samlas hos ett fåtal leverantörer av namnuppslagning, innehållsleverans och moln[14,15]. Ett enskilt fel slår då igenom på många ställen samtidigt.

Den andra rör att beroendet flyttar neråt i infrastrukturen. Värde och kontroll samlas i plattforms-, moln- och beräkningslagren. Med generativ AI blir infrastrukturen dessutom tjockare, eftersom den själv utför allt mer av det arbete som tidigare låg i verksamheten ovanför[6].

Den tredje rör det geopolitiska. Nav i globala nätverk kan användas som påtryckningsmedel[16], och den som kontrollerar infrastrukturens tekniska kontrollpunkter utövar makt över dem som

använder den[17]. En mätning av sex länders myndighetstjänster visar att uttalad policy om digital suveränitet och faktiska beroenden ofta går isär[18].

Den fjärde rör hotbilden. Säkerhetspolisen har under 2026 beskrivit försök till förstörande cyberangrepp mot Sverige och ett ökande sabotagehot[19,20]. En motståndare som vill störa många verksamheter samtidigt söker just de beroenden som många delar. Totalförsvaret behöver därför pröva sina digitala beroenden mot avsiktliga angrepp och mot höjd beredskap, och inte bara mot fel och brottslighet i fredstid.

Regelverken och de gemensamma beroendena

Cybersäkerhetslagen trädde i kraft den 15 januari 2026 och genomför NIS2-direktivet i svensk rätt[21]. Tillsammans med CER-direktivet och, för finanssektorn, DORA ställer den krav på riskhantering, incidentrapportering och ledningens ansvar. NIS2 omfattar bland annat kontinuitet och säkerhet i leveranskedjan. DORA, EU:s förordning 2022/2554 om digital operativ motståndskraft, omfattar även testning, koncentrationsrisker och tillsyn av kritiska IKT-leverantörer. IVA konstaterar att ansvarsfördelningen vid digitala störningar fortfarande är oklar, och att lagstiftningen främst reglerar processer före en händelse medan ansvaret efter att något gått fel ofta är otydligt[1]. Regelefterlevnad hos enskilda verksamheter visar inte i sig att deras gemensamma beroenden kan hanteras när många drabbas samtidigt. En kommun kan uppfylla lagen fullt ut och ändå stå utan system när en leverantör som delas med ett hundrasextiotal andra kommuner faller.

Sju vanliga förväxlingar

De flesta missförstånd i samtal om digital resiliens går att föra tillbaka till sju förväxlingar. Var och en leder till beslut som känns ansvarsfulla men som lämnar den verkliga sårbarheten orörd.

1

Ansvar förväxlas med rådighet

En kommun har ansvaret för sin verksamhet även när den körs i en leverantörs moln. När leverantören faller kvarstår ansvaret, medan kontrollen över systemet ligger hos någon annan. Rådigheten över funktionen finns då hos ingen av dem. Miljödatafallet visar detta mönster på nationell skala. Glappet mellan ansvar och rådighet är i sig en sårbarhet, och den syns inte i en riskanalys som bara frågar vem som är ansvarig.

2

Ägande förväxlas med rådighet

Att data lagras i Sverige eller att en anläggning ägs av en svensk aktör säger lite om vem som kan styra den. I vår kommande bok kallar vi detta suveränitetstvätt, när suveränitet hävdas i ett lager medan beroendet ligger kvar i ett annat[6]. Rådighet behöver därför bedömas lager för lager. Omvänt kan en organisation ha god rådighet över det den köper, om avtal, kompetens och arkitektur ger den rätt och förmåga att agera.

3

Redundans förväxlas med diversitet

Två datacenter hos samma leverantör, två regioner i samma moln eller två fiberförbindelser i samma kabelstråk ger redundans mot enskilda komponentfel men inget skydd mot gemensamma felorsaker, som ett fel i leverantörens plattform eller ett avbrott i kabelstråket. Frågan är alltid vilka felorsaker reserven delar med huvudlösningen. Det är därför IVA betonar redundans genom diversitet[1]. Digitaliseringsstrategin gör samma koppling och kräver att transportnät ska vara både redundanta och diversifierade[22].

4

Robusthet förväxlas med resiliens

En infrastruktur som står emot de hot den konstruerats för kan vara skör mot allt annat[23]. Resiliens kräver också förmågan att återhämta sig och anpassa sig när det oväntade inträffar.

5 Regelefterlevnad förväxlas med förmåga

Cybersäkerhetslagen, CER och DORA ställer viktiga krav, som också omfattar verksamheternas förmåga att hantera störningar. IVA konstaterar samtidigt att regelverken bygger mer på regelefterlevnad än på ansvarsutkrävande[1]. Holmström och Magnusson beskriver samma risk i svensk AI-politik som checklistesuveränitet. Det som går att bocka av blir synligt, medan de beroenden som ingen känner till lämnas obearbetade[24]. Samma glapp syns i stor skala. I 82 länder ökade den formella AI-styrningen med 20,3 poäng mellan 2020 och 2024, medan den mätta förmågan att tillämpa den ökade med 0,4 poäng[25]. Författaren påpekar själv att resultatet delvis beror på hur indexet har konstruerats. Detsamma gäller avtal. En avtalad rätt att få ut sina data eller byta leverantör visar inte att det går att göra inom den tid verksamheten tål. Det visar först ett prov. Förmågan att upprätthålla samhällsviktiga funktioner behöver därför också prövas över organisationsgränser.

6 Det egna förväxlas med det gemensamma

Varje organisation som väljer den mest kostnadseffektiva leverantören gör ett rationellt val. När hundratals organisationer gör samma val uppstår en koncentration som ingen av dem har beslutat om och ingen av dem äger. Resiliens på systemnivå är mer än summan av organisationernas resiliens, och den kräver någon som har mandat att se helheten.

7 Nätet förväxlas med infrastrukturen

Digital infrastruktur uppfattas ofta som kablar, nät och datacenter, med verksamhetssystemen som något som körs ovanpå. Tjänster och verksamhetssystem blir dock med tiden infrastruktur, eftersom allt mer av verksamheten vilar på dem. I de svenska händelserna var det verksamhetssystemen som slogs ut och som fick verksamheten att stanna. En resiliensanalys behöver därför omfatta hela stacken, från el till verksamhetssystem.

Språket är en del av sårbarheten

I samtal mellan kommuner, myndigheter, leverantörer och försvarsaktörer används ord som robusthet, resiliens, redundans, suveränitet och kritisk infrastruktur med skilda innebörder. För en

teknisk förvaltare betyder resiliens ofta återställningstid. För en beredskapssamordnare betyder det förmågan att upprätthålla en funktion. För en upphandlare betyder suveränitet att data lagras i Sverige. Även centrala officiella texter använder orden olika, vilket vi visar i avsnitt 3. Aktörerna tror sig vara överens, och frågan om det gemensamma får ingen ägare. Språket döljer därmed glappet mellan ansvar och rådighet, och det är glappet som är sårbarheten.

Svensk forskning har visat hur institutionell fragmentering försvårar resiliens i kritisk infrastruktur[26] och hur kommersialisering flyttar kontroll bort från dem som bär ansvaret för nationell säkerhet[27]. Ett gemensamt språk är en förutsättning för att fragmenteringen ska kunna hanteras. Avhandlingen *Rådighet i omställning* beskriver hur Helsingborgs stad i sitt arbete med digital resiliens behövde gemensamma arenor och ett delat språk för problem, risk och åtgärd mellan förvaltning, forskning och teknisk drift[28]. Det gör delade beroenden och glapp mellan ansvar och rådighet synliga, och ger stöd för en gemensam lägesbild och för beslut om vilka åtgärder som behövs. Forskningen ger byggstenarna, och IVA:s rapport[1] ger en gemensam karta över infrastrukturens lager och en rad konkreta åtgärdsförslag. IVA:s definitioner av digital infrastruktur och resiliens är inspirerade av Tech Sverige respektive MSB, och principerna presenteras som en lista snarare än som en sammanhållen begreppsram. Det är här denna rapport tar vid.

02

Två utgångspunkter: digital infrastruktur och rådighet

Begreppsapparaten vilar på två definitioner. Digital infrastruktur anger vilka resurser samhällsviktiga funktioner vilar på. Rådighet anger de ansvariga aktörernas kapacitet och mandat att agera på dessa resurser och beroenden. Tillsammans ligger de till grund för definitionen av resilient digital infrastruktur i avsnitt 2.3.

Utgångspunkten i IVA:s rapport

IVA:s rapport Resilient Digital Infrastruktur[1] är den mest genomarbetade svenska beskrivningen av området, framtagen med ett femtiotal experter från näringsliv, myndigheter och akademi. Vi behåller dess definitioner, modell och principer som utgångspunkt och preciserar dem där samtalen behöver mer stöd. Tabellen visar hur.

IVA:S UTGÅNGSPUNKT	DET VI BEHÅLLER	DET VI PRECISERAR
Digital infrastruktur: komponenter som stödjer digitala tjänster, både hårda (nät, datacenter) och mjuka (standarder, identitets- och betalningslösningar)	Bredden bortom kommunikationsnäten	Infrastrukturens relationella egenskaper, att den är möjliggörande, genomgripande och gränsöverskridande (avsnitt 2.1)
Resilient: relevant, tillförlitlig och motståndskraftig med förmåga till återhämtning och vidareutveckling	Hela definitionen, inklusive vidareutveckling	Skillnaden mellan vad resiliens är och hur den uppstår, med rådighet som vårt centrala anspråk (avsnitt 2.3)
Lasagnemodellen, med lager från elförsörjning till lagar, regelverk och styrning	Modellen som gemensam karta	Tjänstelagrets innehåll (moln, plattformar, AI, information) och styrningslagret som platsen för ansvar och rådighet (avsnitt 2.1)
Principer: redundans genom diversitet, isolering och segmentering, övervakning, test, övning och säkerhetsåtgärder	Principerna	En begreppsram i tre delar, struktur, handlingsförmåga och funktion, med villkorade samband (avsnitt 4)
Informations- och tjänsteresiliens, med kravet att veta vilken information som är viktig, var den finns och vem som ansvarar	Begreppen och principerna	Kopplingen till rådighetens fyra led (avsnitt 2.2 och 4.4)
Ansvarsutkrävande snarare än regelefterlevnad	Inriktningen	Skillnaden mellan ansvar, mandat och kapacitet (avsnitt 1 och 2.2)

2.1 Digital infrastruktur

I vår kommande bok *Digital infrastruktur: Att leda det som bär verksamheten*[6] utgår vi från Edith Penroses distinktion mellan resurser och tjänster. Resurser möjliggör värdeskapande, och värdet uppstår i de tjänster som resurserna ger upphov till. En infrastruktur är med detta synssätt en samling resurser som möjliggör en viss uppsättning tjänster, på samma sätt som vägnätet möjliggör transporter. I linje med Bowker m.fl.[29] definierar vi infrastruktur enligt följande.

DIGITAL INFRASTRUKTUR *är en samling möjliggörande, genomgripande och gränsöverskridande digitala resurser*[6].

- **Möjliggörande** betyder att infrastrukturen skapar förutsättningar för tjänster. På samma sätt som den möjliggör vissa tjänster motverkar den andra.
- **Genomgripande** betyder att den är insjunken i andra sociala arrangemang, rutiner och tekniker.
- **Gränsöverskridande** betyder att den sträcker sig över organisatoriska, sektoriella och nationella gränser.

Definitionen bygger vidare på IVA:s, som redan går bortom den äldre officiella bilden. Regeringens digitaliseringsstrategi från 2017[30] avgränsade delmålet för digital infrastruktur till infrastruktur för elektroniska kommunikationer, med en hård del (kablar, master, basstationer) och en mjuk del (lagar, standarder, begreppsanvändning och internetprotokoll). Begreppsanvändningen räknades alltså redan då till infrastrukturen, och ett gemensamt språk är i sig en del av den. IVA:s definition omfattar även datacenter, standarder och identitets- och betalningslösningar[1]. Den nya digitaliseringsstrategin för 2025–2030, som ersätter 2017 års strategi, vidgar på samma sätt begreppet till hård- och mjukvara för produktion av digitala tjänster, molntjänster och datacenter. Den slår fast att den digitala infrastrukturen ska vara motståndskraftig och säker, och att infrastrukturen för konnektivitet och digitalisering har blivit kritisk infrastruktur för både samhället och totalförsvaret[22]. Vi delar denna syn på behovet av ökad bredd. Identitet, data, plattformar, molntjänster, gemensamma komponenter och verksamhetssystem fungerar i dag infrastrukturellt, och det är ofta där de delade beroendena finns. Det vi lägger till är de tre egenskaperna ovan, som förklarar varför beroendena sprider sig och varför de är svåra att se.

Digital infrastruktur skiljer sig från fysisk på tre sätt som har betydelse för resiliens. Den är omprogrammerbar, så att funktionen kan ändras efter leverans. Den är reproducerbar, så att samma lösning kan spridas till nästan ingen kostnad. Den är generativ, så att användningen formas i användningen. En följd är att en tjänst kan bli en del av den infrastruktur den en gång bara använde. Identitetshantering, loggning och övervakning som byggs för en tjänst blir i det tysta något som allt annat förutsätter. Vi beskriver därför digital infrastruktur med bilden av ett mycel som växer och förgrenar sig, snarare än av räls som läggs en gång[6].

En tjänst kan bli infrastruktur på två sätt. Det första är medvetet. En tjänst som började som ett komplement blir så använd att den som driver den gör om den till en del av sitt infrastrukturerbjudande, som när molnleverantörer tar in den ena tjänsten efter den andra i sin plattform. Det andra sker utan att någon har beslutat det. Ett system för lön, ärendehantering, journalföring eller planering av hemtjänst upphandlas som en tjänst för en avgränsad verksamhet. Med tiden byggs rutiner, integrationer, data och andra system kring det, och det blir så svårt att byta att det sjunker ned i infrastrukturen. Då har systemet blivit infrastruktur, oavsett hur det en gång upphandlades eller var det redovisas[6].

Skillnaden har betydelse för rådigheten. I det första fallet finns en aktör som har valt att bära infrastrukturen, och frågan gäller vilka villkor den sätter för andra. I det andra har ingen tagit på sig den rollen, och ansvaret ligger kvar där systemet en gång upphandlades. Vi behandlar därför verksamhetssystemen som en del av den digitala infrastrukturen. Gränsen mellan ett systemlager och ett infrastrukturlager är en organisatorisk konvention, och den döljer de beroenden som avgör resiliensen. Både Tietoevry- och Miljödatahändelserna drabbade verksamhetssystem för lön, HR och rehabilitering, och det var där verksamheten stannade. Tjänstelagret är det lager där infrastrukturen växer snabbast, och det behöver bedömas med samma allvar som näten under det.

Som gemensam karta använder vi IVA:s lasagnemodell[1]. Den beskriver den digitala infrastrukturen som lager där varje nivå vilar på den underliggande, från elförsörjning till tjänster, inramade av lagar, regelverk och styrning. IVA skiljer också mellan ett kommunikationsperspektiv i de undre lagren och ett informationsperspektiv i de övre.

Lagerordningen säger också något om skyddsvärden. De övre lagren förutsätter att de undre levererar som det är tänkt, och en tjänst blir aldrig mer tillgänglig än det nät, den el och den drift den vilar på. Ett avbrott i ett undre lager slår därför igenom i alla lager ovanför. Skyddsvärdet hos en komponent i ett undre lager bestäms av summan av de funktioner som vilar på den, och den summan syns sällan för den som äger komponenten. I tabellen behåller vi lagren och preciserar två av dem.

LAGER I IVA:S MODELL	EXEMPEL	VÅR PRECISERING	TYPISKA DELADE BEROENDEN
Lagar, regelverk och styrning	Lagstiftning, reglering, samverkan, tillsyn	Platsen där ansvar och mandat fördelas, och där glappet mot rådighet uppstår	Avtal, delegationer, sektorsansvar
Tjänster	Webb, e-post, appar, e-tjänster, verksamhetssystem	Delas i plattformar och moln (inklusive AI och beräkningskapacitet), tillämpningar, där verksamhetssystemen ingår, och information	Få molnleverantörer, branschsystem som delas av många, data som bara kan läsas i leverantörens system
Internetaccess	Internet- och mobiloperatörer	Inklusive namnuppslagning (DNS) och utväxlingspunkter	Få DNS-operatörer och utväxlingspunkter
Aktiv infrastruktur	Transmission och överföring av data, mobilnätens radio- och kärnnät	Som i IVA:s modell	Operatörernas kärnnät
Passiv infrastruktur	Fiber, kanalisation, master och siter för mobilnät	Som i IVA:s modell	Kabelstråk, transportfiber, sjökablar
Elförsörjning	Elnät och reservkraft	Som i IVA:s modell	Lokala elnät, reservkraft

Internetinfrastrukturen i snäv mening finns i lagren aktiv infrastruktur och internetaccess. Rapporten omfattar ändå alla lager, eftersom beroenden rör sig vertikalt och sällan följer organisatoriska gränser. Uppdelningen av tjänstelagret följer av två iakttagelser i IVA:s rapport. Molntjänster och AI behandlas där som egna resiliensfrågor, och informationsresiliens hålls isär från tjänsteresiliens[1].

2.2 Rådighet

Begreppet rådighet hämtar vi från avhandlingen *Rådighet i omställning*[28]. Avhandlingen förenar två aspekter som organisationsforskningen ofta håller isär, nämligen kapacitet och mandat.

RÅDIGHET

är en organisations institutionaliserade förmåga att hålla samman kapacitet och mandat i ändamålsenligt handlande. Den kommer till uttryck när en organisation vet vad som behöver göras, kan göra det, har rätt att göra det och faktiskt får det gjort[28].

Kapacitet är att veta vad som behöver göras och att kunna göra det. Mandat är rätten att göra det. Att förmågan är institutionaliserad betyder att den sitter i rutiner, avtal, budget och övning, och att den byggs före störningen.

Det centrala i analysen är att kapacitet och mandat kan frikopplas i båda riktningar. En organisation kan ha förmågan men sakna rätten, eller ha rätten men sakna förmågan. Avhandlingen beskriver strategisk förlamning i kommunal omställning som en sådan frikoppling, buren av återkommande mekanismer. Den är ett strukturellt glapp snarare än en brist på kompetens eller auktoritet.

Ordet rådighet saknar en exakt motsvarighet på engelska. Det ligger nära digital suveränitet men har en mer operativ betydelse. Suveränitetslitteraturen handlar om kontroll i vid mening, ofta på statlig nivå[31,32]. En aktuell genomgång av EU-debatten visar hur spretigt begreppet används och identifierar fyra synsätt: suveränitet som anspråk, som kontroll över det digitala, som förmåga och som individens självbestämmande[33]. Rådighet avser varje aktör i styrkedjan och frågan om den kan handla. Den kan finnas hos en organisation eller organiseras gemensamt mellan flera aktörer. I rapporten behandlar vi digital suveränitet som en del av resiliensen. Den avser samhällets rådighet över de villkor som digitala beroenden vilar på, alltså möjligheten att genom ansvariga institutioner påverka villkoren och ha genomförbara alternativ när de förändras. En tjänst kan vara resilient mot tekniska fel och ändå sårbar för att villkoren ändras genom ett beslut i ett annat land, ett ägarbyte eller ett nytt avtal. Rådighet är också skild från ägande. En organisation kan ha god rådighet och ändå köpa mycket av det den använder, så länge den har insikt, avtal och flexibilitet nog att sitta i förarsätet[6].

Ordet rådighet används i dag på flera sätt i svensk förvaltning, och det är i sig ett exempel på rapportens tes. Regeringens molnpolicy beskriver digital suveränitet som rådighet över data och system, så att ingen utomstående part kan påverka, få tillgång till eller förneka tillgång till dem[34]. Teracom använder ordet om ägande och kontroll över den egna produktionskedjan[35]. Totalförsvarets forskningsinstitut påpekar att det inte räcker att äga en resurs på pappret om den inte går att förfoga över i kris och krig[36]. I avhandlingen nämnd ovan är rådighet en organisatorisk förmåga[28]. Betydelserna hänger ihop. De tre första gäller rådigheten över en resurs eller ett beroende, alltså vad den ansvariga själv kan se, ändra, flytta och stänga av inom den tid verksamheten tål. Den fjärde gäller organisationens förmåga att använda det förfogandet när det behövs. I rapporten bedöms rådigheten över varje kritiskt beroende, och det centrala anspråket avser organisationens rådighet.

Rådighetens fyra led blir ett analysverktyg när de används på digital infrastruktur. De ligger nära IVA:s principer för informations- och tjänsteresiliens, att veta vilken information som är viktig, var den finns och vem som ansvarar för att den är tillgänglig[1]. Rådighet lägger till de två led som principerna förutsätter men inte namnger, att kunna agera och att faktiskt få det gjort.

RÅDIGHETENS LED	FRÅGA FÖR DIGITAL INFRASTRUKTUR	TYPISK BRIST
Veta	Vet vi vilka beroenden våra funktioner har, i vilket lager och delat med vilka?	Ingen aktuell beroendekartläggning bortom första leverantören
Kunna	Kan vi byta leverantör, flytta data eller drifta själva inom acceptabel tid?	Inlåsning, kompetens som bara finns hos leverantören
Ha rätt	Har vi avtalsmässig, juridisk och jurisdiktionell rätt att agera?	Avtal utan rätt till data, loggar eller återställning
Få det gjort	Kan vi faktiskt genomföra åtgärden, ensamma eller tillsammans med andra?	Ingen ägare till frågan, åtgärden är aldrig övad, och ingen förberedd samverkan med andra som delar beroendet

Ansvar står utanför leden och fungerar som måttstock. Ansvar anger vem som svarar för funktionen. Mandat anger vem som får agera, och kapacitet vem som kan. Rådighet är föreningen av mandat och kapacitet, och den bedöms mot ansvaret. Sårbarheten uppstår där den som bär ansvaret saknar mandat, kapacitet eller båda.

Måttstocken har en motsvarighet i den svenska krisberedskapens ansvarsprincip. Den som ansvarar för en verksamhet under normala förhållanden har samma ansvar i kris och krig. Principen förutsätter att den ansvariga också kan handla. När driften av det verksamheten vilar på har lagts hos en leverantör ligger ansvaret kvar, medan förutsättningarna att handla har flyttat.

2.3 Resilient digital infrastruktur

IVA definierar resilient, med inspiration från MSB, som relevant, tillförlitlig och motståndskraftig med förmåga till återhämtning och vidareutveckling[1]. Vi behåller den innebörden och skiljer mellan vad resiliens är och hur den uppstår.

RESILIENT DIGITAL INFRASTRUKTUR

är digital infrastruktur som, tillsammans med de människor och organisationer som använder och förvaltar den, kan förutse och hantera störningar, upprätthålla samhällsviktiga funktioner på en acceptabel nivå samt återställa och vidareutveckla dem när förutsättningarna förändras.

Med störning avser vi tekniska fel, angrepp och förändrade villkor. Definitionen beskriver vad systemet klarar, men i bedömningen behöver två nivåer hållas isär. Den ena är vad de digitala tjänsterna klarar. Den andra är vad den samhällsviktiga funktionen klarar, inklusive manuella rutiner och andra alternativ. Funktionen kan beskrivas som processer som genomförs i system och stöds av människor. Resiliensen behöver bedömas i alla tre, eftersom en process kan ställas om till andra system eller till manuellt arbete när människorna vet hur och har övat det. En fungerande reservrutin kan hålla verksamheten igång innan den digitala infrastrukturen har återhämtat sig. Förklaringen till hur förmågan uppstår formulerar vi separat, som rapportens centrala anspråk.

CENTRALT ANSPRÅK

Förmågan att upprätthålla, återställa och vidareutveckla samhällsviktiga funktioner avgörs i hög grad av om de aktörer som bär ansvaret för funktionerna, var för sig och tillsammans, har rådighet över de resurser och beroenden som funktionerna vilar på.

Anspråket är ett påstående som bör prövas empiriskt. Tekniska egenskaper som redundans och diversitet skapar möjligheter till resiliens, och automatiska reservlösningar kan upprätthålla en tjänst utan nya beslut under störningen. Rådigheten avgör om möjligheterna kan förberedas och användas, och om ansvariga aktörer kan agera när en störning kräver nya prioriteringar, resurser eller samordnade insatser. Vad funktionen faktiskt klarar under störning visar om de användes. Sambanden är villkorade och behöver undersökas fall för fall, och begreppsramen i avsnitt 4 är byggd för att göra den prövningen möjlig.

03

Vad vi menar med resiliens

Forskningen rymmer minst fyra resiliensbegrepp, och valet mellan dem avgör vad som mäts och vad som styrs. Vi bygger på de två senare och använder de två första där de går att mäta. IVA:s definition rymmer delar av flera traditioner. Återhämtning hör hemma i ingenjörsresiliensen, och vidareutveckling i den socio-ekologiska traditionen och i resilience engineering.

TRADITION	KÄRNFRÅGA	NYCKELKÄLLOR	STYRKA OCH BEGRÄNSNING
Ingenjörsresiliens	Hur snabbt återgår systemet till normalläge, och hur stor är förlusten under tiden?	Bruneau m.fl.[37], Hosseini m.fl.[38]	Lätt att mäta, fångar dåligt styrning och samverkan
Socio-ekologisk resiliens	Hur stor störning tål systemet innan det byter tillstånd?	Walker m.fl.[39], Gunderson & Holling[40]	Inkluderar anpassning och omvandling, svår att operationalisera
Resilience engineering	Vad gör systemet när det oväntade inträffar?	Woods[41]	Ser resiliens som något ett system gör snarare än något det har
Digital resiliens i IS-forskningen	Hur formar informationssystem förmågan att hantera externa chocker?	Tim & Leidner[42], Kostis m.fl.[43]	Nära organisationen, ungt och splittrat fält

Bruneau m.fl.[37] gav den mest citerade ingenjörsformen: robusthet, redundans, resursrikedom och snabbhet. De skiljer redan där mellan resiliensens mål (robusthet och snabb återställning) och dess medel (redundans och resursrikedom). Woods[41] skiljer fyra betydelser: återhämtning, robusthet, förmågan att tänjas utan att brista (eng. graceful extensibility) och uthållig anpassning. Kostis m.fl.[43] beskriver digital resiliens som en process av relationellt resursskapande, det vill säga något som uppstår mellan aktörer.

För kommunikationsnät formulerar Sterbenz m.fl.[44] resiliensprinciper där redundans och diversitet ingår. NIST SP 800-160 vol. 2[45] anger fyra mål för cyberresiliens: att förutse, motstå, återhämta

och anpassa. NIST:s Cybersecurity Framework 2.0, som används brett av offentliga och privata organisationer, ordnar arbetet i sex funktioner: styra, identifiera, skydda, upptäcka, hantera och återställa[46]. Ramverket ger styrning och risker i leverantörskedjan en egen funktion och har en egen kategori för den tekniska infrastrukturens resiliens. Det ligger nära rådighetens led att ha rätten och att veta.

Två distinktioner är här särskilt viktiga för ett gemensamt språk. Den första gäller robusthet och resiliens. Robusthet är förmågan att stå emot en känd påfrestning. Resiliens inkluderar förmågan att hantera det okända. System som optimerats mot vissa störningar blir ofta robusta men sköra mot andra[23,47]. Den andra distinktionen gäller återhämtning och anpassning. Att återgå till utgångsläget kan vara fel mål, eftersom utgångsläget ibland var det som skapade sårbarheten[39,41].

Skillnaden syns även i de nationella policies. Digitaliseringsstrategin för 2025–2030 skiljer mellan robusthet, att motstå påfrestningar utan att funktionaliteten påverkas, resiliens, att återhämta sig och återgå till normal funktionalitet, och redundans och diversitet, att ha tillgång till alternativa lösningar, tekniker eller vägar[22]. Strategins resiliensbegrepp ligger nära ingenjörsresiliensen. IVA:s definition, med inspiration från MSB, rymmer också vidareutveckling[1]. Två centrala svenska texter använder alltså samma ord för olika saker. Det är ett konkret exempel på varför ett gemensamt språk behövs, och vi föreslår att resiliens används i IVA:s vidare mening.

Vår position följer av definitionen i avsnitt 2.3. Resiliens är en socio-teknisk förmåga som utövas av aktörer genom infrastrukturen. Infrastrukturens förmåga behöver bedömas tillsammans med den samhällsviktiga funktionens förmåga, inklusive fungerande alternativ till digitala tjänster. Ingenjörsmått som återställningstid och antal oberoende vägar används där de är meningsfulla, men de får aldrig ersätta frågan om vem som har rådighet.

04

Begreppsramen

Begreppsramen ordnar begreppen kring tre frågor. Hur är det byggt? Kan vi agera? Vad klarar funktionen? Den tekniska strukturen skapar möjligheter till resiliens, handlingsförmågan avgör om möjligheterna kan användas, och funktionen under störning visar om de användes. Handlingsförmågan är rådighet, uppdelad i de fyra led som beskrevs i avsnitt 2.2. Där IVA ger en definition utgår vi från den.

Ramen i ett exempel

KONSTRUERAT EXEMPEL

Exemplet är konstruerat men bygger på mönster från Tietoevry- och Miljödatahändelserna. En kommun planerar hemtjänsten i ett verksamhetssystem som en leverantör driver i sin molntjänst och som ett hundratal andra kommuner också använder. Med åren har scheman, rutiner och integrationer byggts kring systemet, och det har blivit infrastruktur för hemtjänsten. Funktionen är att varje brukare får sina insatser. Scenariot är att leverantören drabbas av ett utpressningsangrepp och att systemet ligger nere i två veckor. Minimikravet är att alla insatser kan genomföras från första dagen, med korrekt information om brukarnas behov.

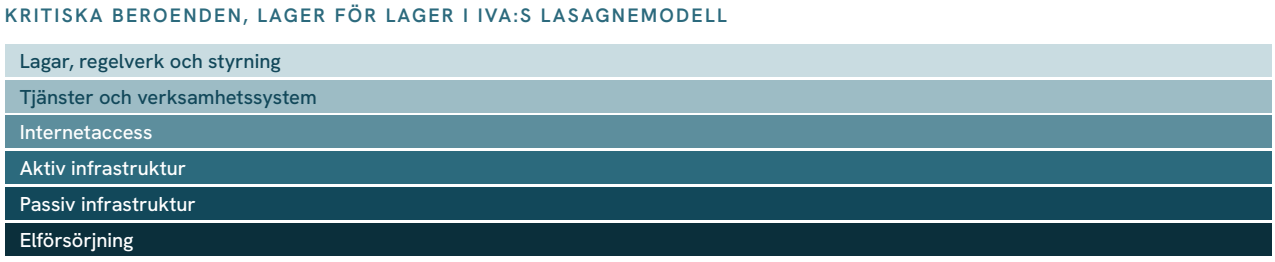
Hur är det byggt?	Leverantören har två driftplatser och säkerhetskopior. Det ger redundans mot ett fel på en av driftplatserna. Båda delar samma plattform, administration och inloggning, så angreppet slår ut båda. Diversitet saknas mot just den felorsaken.
Kan vi agera? Brist i alla fyra led	Kommunen känner till leverantören men inte att samma plattform bär hundra andra kommuners system (veta). Systemet saknar öppna gränssnitt och exportfunktion, och kommunen har ingen löpande uppdaterad egen kopia av planeringen (kunna). Avtalet ger ingen rätt till data eller till en viss återställningstid (ha rätt). Ingen i ledningen äger frågan, reservrutinen har aldrig övats, och det finns ingen förberedd samverkan med andra kommuner som drabbas samtidigt (få det gjort). Kommunen bär hela ansvaret för hemtjänsten men har mycket liten rådighet.
Vad klarar funktionen?	En övning med pappersrutiner, utifrån utskrifter som fanns före avbrottet, visar att insatserna kan genomföras i tre dagar innan informationen om brukarna blir för osäker. Hemtjänsten kan alltså upprätthållas på den angivna nivån i tre dagar trots att den digitala tjänsten är utslagen. Funktionens resiliens är begränsad, och den digitala infrastrukturens återhämtning beror helt på leverantören. Anpassning kan ske under störningen genom förändrade arbetssätt och efteråt genom ändrade avtal, arkitektur och samverkan. Förändringarnas effekt behöver verifieras.

Exemplet illustrerar varför de tre frågorna behöver ställas tillsammans. Den tekniska strukturen såg robust ut, men det var rådigheten som avgjorde vad kommunen kunde göra. Pappersrutinerna köpte tid, och lärdomarna kan därefter användas för att utveckla både infrastrukturen och rådigheten. Funktionen höll i tre dagar och störningen varade i fjorton. Skillnaden mellan hur länge funktionen håller och hur lång tid det tar att få ett fungerande alterna-

tiv på plats är det mått en ledning först behöver känna till. Bilagan innehåller en mall för att göra samma bedömning i den egna organisationen.

Figur 4.1 visar samma tre frågor som en ram, och tabellerna därefter definierar begreppen.





Figur 4.1 Begreppsramen. Strukturen skapar möjligheter till resiliens, rådigheten avgör om de kan förberedas och användas, och funktionen under störning visar om de användes. Bedömningen följer beroendena genom lagren i IVA:s lasagnemodell och mäter rådigheten mot ansvaret.

Tabell 1 beskriver de tio kärnbegreppen och vad vart och ett hjälper oss att upptäcka. Tabell 2 beskriver fem begrepp med andra roller. De behövs i bedömningen men ska inte vägas samman med kärnbegreppen.

Tabell 1 Kärnbegreppen

DEL	BEGREPP	DEFINITION	HJÄLPER OSS ATT UPPTÄCKA	FÖRHÅLLANDE TILL IVA	KÄLLOR
Struktur	**Diversitet**	Relevanta skillnader mellan tekniker, lösningar, leverantörer och vägar	Om samma fel kan drabba flera alternativ samtidigt	Följer IVA:s definition och principen om redundans genom diversitet	IVA[1], Sterbenz m.fl.[44], Li m.fl.[48]
Struktur	**Redundans**	Extra resurser eller alternativa lösningar som kan ta över en funktion	Om reserven har tillräcklig kapacitet och tillräckligt snabb övergång	Följer IVA:s definition	IVA[1], Bruneau m.fl.[37], Sterbenz m.fl.[44]
Struktur	**Decentralisering**	Hur funktioner, resurser och kontroll är fördelade	Om ett bortfall kan begränsas och vilka delar som fungerar självständigt. Teknisk fördelning och fördelning av beslut bedöms var för sig, liksom om gränssnitten gör att delar kan bytas eller tas över	Tillägg, nära IVA:s princip om isolering och segmentering	Park m.fl.[49], Kumar m.fl.[15]
Handling (veta)	**Beroendeförståelse**	Att identifiera och värdera egna och delade beroenden och upptäcka när de förändras	Dolda felpunkter, koncentrationsrisker och brister i förmågan att förutse störningar	Utvecklar IVA:s princip att veta vilken information som är viktig och var den finns	Holmström[50], Cohen & Levinthal[51]
Handling (kunna)	**Kompetens och handlingsfrihet**	Kompetens, resurser och tillträde, samt möjlighet att byta teknik, arkitektur eller leverantör till rimlig kostnad och inom rimlig tid	Inlåsning och kompetens som bara finns hos leverantören	Utvecklar IVA:s förslag om exit-strategier och utbytbara molntjänster	Arthur[52], Jansen m.fl.[18]
Handling (ha rätt)	**Mandat**	Rätten att agera på funktionen och dess infrastruktur, genom beslut, avtal och jurisdiktion	Avtal utan rätt till data, loggar eller återställning, och oklara beslutsvägar vid störning	Utvecklar IVA:s krav på tydligt ansvar	Heath[28], Bovens[53]
Handling (få det gjort)	**Genomförande och samordning**	Att kunna fatta och genomföra beslut i den egna organisationen och tillsammans med andra berörda aktörer	Om prioriteringar, informationsdelning och gemensamma insatser fungerar när flera drabbas samtidigt	Utvecklar IVA:s förslag om operativ privat-offentlig samverkan och tvärsektoriella övningar	Constantinides & Barrett[54], Ampratwum m.fl.[55]
Funktion	**Robusthet**	Att behålla acceptabel funktion under en angiven påfrestning	Vad som fortsätter fungera, för vilka och hur länge	Följer IVA:s definition, preciseras mot ett scenario	Carlson & Doyle[23], Woods[41]
Funktion	**Återhämtningsförmåga**	Att återställa nödvändig funktion efter försämring eller avbrott	Hur snabbt och säkert återställningen sker och vilken informationsförlust som uppstår	Ingår i IVA:s definition av resilient	Bruneau m.fl.[37], Tim & Leidner[42]
Funktion	**Anpassnings- och utvecklingsförmåga**	Att förändra teknik, beroenden och arbetssätt utifrån lärdomar och nya förutsättningar	Om identifierade brister leder till genomförda förbättringar	Motsvarar vidareutveckling i IVA:s definition av resilient	Walker m.fl.[39], Woods[41]

Tabell 2 Begrepp med andra roller

BEGREPP	ROLL	DEFINITION	FÖRHÅLLANDE TILL IVA	KÄLLOR
Ansvar	Måttstock	Vem som formellt svarar för en samhällsviktig funktion. Rådigheten bedöms mot ansvaret	Utvecklar IVA:s krav på tydligt ansvar och ansvarsutkrävande	Bovens[53], Cedergren m.fl.[26]
Informations- och tjänsteresiliens	Vad som bedöms	Att kritisk information är tillgänglig, korrekt och skyddad, och att tjänsterna som hanterar den är tillgängliga, robusta och pålitliga	Följer IVA:s definitioner	IVA[1]
Kollektiv resiliens	Nivå	Flera aktörers gemensamma förmåga att upprätthålla funktioner som ingen av dem kan bära ensam	Utvecklar IVA:s syn på privat–offentlig samverkan	Constantinides & Barrett[54], Ampratwum m.fl.[55]
Kritiska beroenden och koncentrationsrisk	Analysobjekt	Beroenden där ett och samma fel, angrepp eller beslut kan slå ut flera samhällsviktiga funktioner samtidigt	Utvecklar IVA:s iakttagelse att den svagaste länken kan finnas i vilket lager som helst	Rinaldi m.fl.[56], Farrell & Newman[16]
Uthållighetstid och ersättningstid	Mått	Hur länge funktionen kan upprätthållas på angiven nivå utan beroendet, och hur lång tid det tar att få ett fungerande alternativ på plats	Utvecklar IVA:s betoning av test och övning	ISO 22301[57]

4.1 Hur är det byggt?

Diversitet, redundans och decentralisering beskriver hur infrastrukturen är byggd och skapar möjligheter till resiliens. Diversitet är svaret på gemensamma felorsaker, där två identiska reservsystem faller av samma fel. Påtvingad diversitet minskar gemensamma fel bara under vissa villkor[58]. På organisationsnivå visar Li m.fl.[48] ett omvänt U-samband. Måttlig variation i IT-portföljen stärkte resiliensen under pandemin, medan stor variation gav samordningsproblem som åt upp vinsten. Mer är alltså inte alltid bättre.

Redundans är det mest etablerade begreppet, och IVA betonar redundans särskilt genom diversitet[1]. Litteraturen pekar på två fallgropar. Redundans utan diversitet skyddar mot enskilda komponentfel men ger skenbar säkerhet mot gemensamma felorsaker, eftersom huvudväg och reservväg kan bero på samma molnleverantör eller samma fiberstråk. Redundans kostar också i normalläge och är därför sårbar för besparingar.

Decentralisering är det begrepp där forskningen är mest oenig. Mätningar visar en tydlig rörelse mot centralisering hos få DNS-, CDN- och molnleverantörer[14,15]. Samtidigt visar Park m.fl.[49] att centraliserad IT-styrning hjälpte lärosäten att ställa om under pandemin. Begreppet behöver därför delas. Teknisk decentralise-

ring av felpunkter och styrningsmässig decentralisering av beslut kan verka i olika riktningar. Digitala infrastrukturer tenderar också att växa fram som kärna och periferi, där det som byggts tidigt blir allt svårare att ändra[59]. Den avsiktliga decentraliseringen dras ofta tillbaka mot centralisering i praktiken[60]. IVA:s princip om isolering och segmentering, som hindrar att störningar sprids[1], är ett sätt att få teknisk decentralisering utan att splittra styrningen. Decentralisering kan samtidigt begränsa lokala fel men lämna beroenden av gemensam el, programvara eller styrning orörda.

I tjänstelagret får decentraliseringen en konkret form genom komponerbar arkitektur. Funktionalitet byggs då av mindre, utbytbara delar som kopplas samman genom standardiserade gränssnitt[6]. Delarna kan bytas och återställas en i taget, och ett fel kan begränsas till den komponent där det uppstår. Arkitekturen präglades länge av en rörelse mot konsolidering i färre och större system, och den komponerbara arkitekturen är en rörelse tillbaka mot det mindre, nu sammanhållen av gemensamma gränssnitt[6]. En API-strategi bestämmer vilka gränssnitt organisationen själv äger och vilka den hyr, och vilken data och funktionalitet som går att nå utanför leverantörens system. Därmed kopplar den decentraliseringen till rådighetens led kunna och ha rätt i avsnitt 4.2. Med öppna gränssnitt och avtalad rätt att använda dem kan en organisation hämta ut sin information när ett system faller, eller låta en annan komponent ta över funktionen.

Komponerbarhet skapar samtidigt nya gemensamma punkter. Identitetstjänster, API- och integrationsplattformar blir den smala midja som allt annat passerar[6]. De behöver därför samma krav på diversitet, redundans och återställning som näten under dem. En komponerbar arkitektur stärker resiliensen när komponenterna verkligen går att byta och när "midjan" själv är robust.

4.2 Kan vi agera? Rådighetens fyra led

Veta: beroendeförståelse. Här finns minst forskning, och här finns sannolikt den största luckan. IVA:s princip att veta vilken information som är viktig och var den finns är en del av beroendeförståelsen[1]. Holmström[50] beskriver geografisk intelligens som förmågan att uppfatta och tolka var kritiska beroenden finns, hur koncentrerade de är och hur de styrs. Absorptionsförmåga[51], en organisations förmåga att ta till sig ny kunskap, påminner om att förmågan att förstå beroenden förutsätter tidigare kunskap. Forskning om ignorans i offentlig digital

transformation[61] och om strategisk okunskap[62] väcker en obekväm fråga, nämligen om bristande beroendeförståelse ibland är bekväm.

Kunna: kompetens och handlingsfrihet. Den egna förmågan är kompetens, resurser och tillträde. Handlingsfrihet handlar om reversibilitet. Freij m.fl. visar hur nordiska finansföretag möter staplade EU-regelverk genom att bygga IT-arkitekturer som går att backa[63]. Den ekonomiska grunden finns i teorin om inlåsning och byteskostnader[52,64]. Hur öppen en standard är avgör i praktiken hur fritt en myndighet kan byta lösning[65]. Jansen m.fl.[18] visar hur faktiska beroenden kan mätas med nätmätningar som traceroute, passiv DNS och geolokalisering. IVA föreslår att ansvariga för kritiska tjänster regelbundet övar på att flytta data och applikationer, tillämpar standarder som gör leverantörer utbytbara och etablerar exit-strategier[1]. Det är handlingsfrihet omsatt i praktik.

Ha rätt: mandat. Mandat är rätten att agera på funktionen och den infrastruktur den vilar på. Ansvaret är måttstocken som mandat och kapacitet bedöms mot. Bovens[53] hjälper att skilja formellt ansvar från möjligheten att utkräva det. I en upphandlad infrastruktur ligger mandatet ofta i avtalet, och avtalet ger sällan rätt till data, loggar eller återställning i den takt en kris kräver. IVA pekar på samma problem. Ansvaret riskerar att falla mellan stolarna i gränssnittet mellan myndigheter och privata aktörer, och lagstiftaren bör enligt IVA fokusera mer på ansvarsutkrävande än på regelefterlevnad[1]. Digitaliseringsstrategin lägger samtidigt ett tydligt ansvar på användarna. Verksamheter med större behov än operatörernas grundläggande krav förväntas själva identifiera dem och säkra dem genom avtal[22]. Ansvaret finns alltså, men rådigheten beror på vad avtalen faktiskt ger.

Få det gjort: genomförande och samordning. Ledet avser att åtgärden faktiskt blir gjord. I avhandlingen tidigare nämnd är det föreningen av kapacitet och mandat i handling[28]. Det börjar i den egna organisationen, med en utpekad ägare till frågan, beslut som går att fatta under en störning och reservrutiner som har övats. Därefter kommer samordningen med dem som delar beroendet.

Infrastruktur är en gemensam resurs[66], och utveckling av den är en form av kollektivt handlande[54]. Litteraturen om offentlig-privat samverkan för resiliens är omfattande men splittrad[55,67]. IVA föreslår sektorsvisa samverkansforum efter förebild av Nationella telesamverkansgruppen (NTSG) och Finansiella sektorns privat-offentliga samverkan (FSPOS), samt tvärsektoriella tester och

övningar[1]. Enligt digitaliseringsstrategin har samverkan i NTSG dessutom formaliserats i lag[22]. Ukrainska erfarenheter visar hur digitala förvaltningsförmågor kan hålla samhällsfunktioner igång under krig[68]. En lag som antogs en vecka före invasionen 2022 gjorde det möjligt att flytta statens data till molntjänster[69]. Det var rådighet som byggdes innan den behövdes. Samordningsförmågan är svårast att mäta, eftersom den uppstår mellan aktörer. Den är också det som tydligast kopplar ramen till totalförsvaret, där kollektiv resiliens är målet.

4.3 Vad klarar funktionen?

Kolumnen beskriver vad funktionen visar sig klara när den prövas, i en störning eller i en övning. Robusthet, återhämtning och vidareutveckling är alltså utfall som går att iaktta, medan leden i avsnitt 4.2 är förmågor som finns före störningen.

Robusthet behöver alltid anges i förhållande till ett hotscenario. En infrastruktur är robust mot något, och robusthet mot kända hot kan öka sårbarheten för okända[41]. Återhämtningsförmåga är kärnan i ingenjörsresiliensen. I kontinuitetsstandarden ISO 22301[57] operationaliseras den som maximal tolererbar avbrottstid och återställningstid. Förmågan behöver verifieras genom test och övas, vilket IVA betonar[1]. Rutiner fungerar här som stötdämpare[70], och resiliens i IT-organisationer byggs i hög grad genom människor och processer, som tjänstekvalitet och mogen IT-styrning[71]. Amiri m.fl. visar i en analys av 28 incidenter hur ett IT-avbrott sprider sig till brist på information och på verksamhetsförmåga, och hur självförstärkande tröghet i IT, information och verksamhet fördröjer återhämtningen[72].

Anpassnings- och utvecklingsförmåga finns redan i IVA:s definition av resilient, som förmåga till vidareutveckling[1]. Den finns också hos Walker m.fl.[39], Woods[41] och i NIST:s[45] fyra mål. Vi föreslår att den behandlas som en egen förmåga vid sidan av robusthet och återhämtning. Den är särskilt viktig för digital infrastruktur, eftersom omprogrammerbarheten gör att anpassning ofta är både möjlig och billig, förutsatt att rådigheten finns.

4.4 Vad bedöms, på vilken nivå och mot vilken måttstock?

Begreppen i tabell 2 anger vad bedömningen gäller, på vilken nivå den görs, vad den analyserar och vilken måttstock den använder. Informations- och tjänsteresiliens anger den del av bedömningen som gäller kritisk information och de digitala tjänster som hante-

rar den, i linje med IVA[1]. Tillgänglighet är då inte det enda kriteriet. Informationen måste också vara tillräckligt korrekt, åtkomsten behörig och skyddet godtagbart.

Kollektiv resiliens anger nivån. Flera aktörer upprätthåller tillsammans funktioner som ingen av dem kan bära ensam, och det är på den nivån totalförsvaret behöver resiliens. Den formas av samspelet mellan infrastrukturen och aktörernas rådighet, där samordningsförmågan i avsnitt 4.2 är central, och bedöms på systemnivå. Ansvaret är måttstocken, enligt avsnitt 2.2.

IVA understryker att den svagaste länken kan finnas i vilket lager som helst[1]. Rinaldi m.fl.[56] skiljer fysiska, digitala, geografiska och logiska beroenden. Keohane och Nye[73] bidrar med en distinktion som ett index annars lätt blandar ihop. Känslighet är hur snabbt en störning slår igenom. Sårbarhet är hur dyrt det är att ersätta beroendet. En ytterligare distinktion gäller tiden efter leveransen. Ett leveransberoende är något som måste komma fram. Ett fortsättningsberoende är något som måste fortsätta fungera, som en licens, ett konto, en uppdatering eller en molntjänst. Där behåller leverantören ett grepp om det som används, och rådigheten behöver hållas under hela användningstiden. Koncentrationsrisk har en teknisk sida, där ett fåtal tredjepartstjänster bär en stor del av webben[74], och en geopolitisk sida, där nav i nätverk kan användas som påtryckningsmedel[16]. Inom finanssektorn har DORA gjort koncentration till IKT-leverantörer till en regulatorisk kategori[75].

En praktisk konsekvens gäller mätning. Struktur, handling och funktion bör inte vägas samman som jämbördiga poster, flera dimensioner har sitt optimum i mitten, och decentralisering kan verka åt båda hållen. Resultatet av en bedömning bör därför redovisas som en resiliensprofil, där delarna och deras brister och osäkerheter syns var för sig. Ett index kan bli aktuellt först när det är prövat vad som går att mäta och jämföra på ett meningsfullt sätt.

05

Utblick: den finska modellen

Finland organiserar kollektiv resiliens i en form som saknar svensk motsvarighet. Modellen är väl dokumenterad i myndighetsmaterial men mer sällan i vetenskapliga tidskrifter. Tre drag är relevanta för ett svenskt språk om resilient digital infrastruktur.

- **Försörjningsberedskap som organiserad samverkan.** Företag deltar delvis frivilligt och delvis lagstadgat, och poolerna pekar själva ut vilka företag som är kritiska för försörjningsberedskapen[76]. Det är en institutionaliserad form av både beroendeförståelse och kollektiv resiliens.
- **Det digitala som egen sektor.** I slutet av 2025 beslutades om en ny sektor för det digitala samhället, med nya pooler som bygger på den tidigare Digitalpoolen[77]. Sektorn ska följa och bedöma läget för försörjningsberedskapen.
- **Offentliga medel där marknaden inte räcker.** Programmet Digital Security 2030 (ca €130M) stödjer projekt när den önskade nivån inte kan nås tillräckligt snabbt på marknadsmässiga villkor[78].

Modellen utgår från kritiska funktioner snarare än kritisk infrastruktur. Frågan är vad samhället måste kunna göra, och infrastrukturen bedöms utifrån det. Det ligger nära den definition av resilient digital infrastruktur som vi föreslår i avsnitt 2.3. Akademiska ingångar till det finska begreppet helhetssäkerhet finns hos Räisänen m.fl.[79] och Lehto och Limnéll[80]. IVA gör en motsvarande jämförelse med Estland, där strukturerad informationsdelning och principen att uppgifter bara ska lämnas en gång stärker informationsresiliensen[1]. De två jämförelserna kompletterar varandra.

06

Att använda språket

Ett gemensamt språk blir användbart när det går att ställa frågor med det. Frågorna nedan följer rådighetens fyra led och kan ställas av en ledningsgrupp till den egna organisationen, eller av flera organisationer till varandra.

6.1 Frågor för ledningen

VETA

- Vilka av våra samhällsviktiga funktioner delar beroende med andra organisationers, och i vilket lager?
- Var är vår reservlösning beroende av samma sak som vår huvudlösning?

KUNNA

- Hur lång tid och hur mycket skulle det kosta att byta leverantör för våra tre mest kritiska tjänster?
- Vilken kompetens som vår drift förutsätter finns bara hos leverantören?
- Hur många dagar håller våra tre mest kritiska funktioner om systemet de vilar på är borta, och när prövade vi det senast?

HA RÄTT

- Ger våra avtal oss rätt till data, loggar och återställning i den takt en kris kräver?
- För vilka kritiska beroenden saknar den som bär ansvaret också mandat att agera?

FÅ DET GJORT

- Vem i ledningen äger frågan, och när övade vi senast att klara funktionen utan systemet?

- Vilka andra organisationer behöver vi för att upprätthålla funktionen om en delad leverantör faller, och har vi övat med dem?
- Vem har i dag mandat att se och hantera de beroenden som vi delar med andra?

6.2 Rekommendationer

Rekommendationerna riktar sig till tre mottagare.

Till ledningen i en kommun, region, myndighet eller ett företag

L1 **Utse** en ägare till frågan i ledningsgruppen, med uppgift att redovisa organisationens kritiska delade beroenden för ledningen minst en gång om året.

L2 **Bedöm** en samhällsviktig funktion med mallen i bilagan, och ta reda på hur många dagar den håller utan sitt viktigaste system.

L3 **Öva** bortfall av en delad leverantör med ledningen i rummet, och gör det tillsammans med andra organisationer som delar leverantören.

Till regeringen och de myndigheter som ansvarar för beredskapen

S1 **Klargör** vem som har till uppgift att följa och bedöma de beroenden som många samhällsviktiga verksamheter delar i tjänstelagret, där moln, plattformar och verksamhetssystem finns.

Till FORUM Totalförsvar och dess parter

01 **Använd** IVA:s lasagnemodell som gemensam karta och begreppstabellen i avsnitt 4 som gemensam referens i FORUM Totalförsvars samtal, och pröva definitionerna i workshoppar med kommuner, regioner, myndigheter och leverantörer.

02 **Förankra** resiliens i IVA:s vidare mening, där förmågan till vidareutveckling ingår vid sidan av återhämtning, och behandla anpassnings- och utvecklingsförmåga som en egen förmåga i ramverket. Det gäller både i FORUM Totalförsvars eget arbete och i dialogen med de myndigheter som formulerar styrdokumenten.

03 **Kartlägg** delade beroenden lager för lager för ett fåtal samhällsviktiga funktioner, med början i nät- och namnlagret där data är öppna. Redovisa för varje kritiskt beroende om den som bär ansvaret också har kapacitet och mandat.

04 **Pröva** begreppsramen och bedömningsmallen på två eller tre samhällsviktiga funktioner tillsammans med FORUM Totalförsvars parter, där deltagarna bedömer samma fall och jämför sina tolkningar. Redovisa resultatet som resiliensprofiler och ta ställning till indikatorer och index först därefter.

05 **Jämför** systematiskt med den finska försörjningsberedskapens sektor för det digitala samhället.

06 **Stäm av** begreppen mot Internetstiftelsens begreppsanvändning och koppla dem till IVA:s åtgärdsförslag om tydligt ansvar för information, operativ privat–offentlig samverkan och tvärsektoriella övningar[1].

07

Avslutande kommentarer

Den digitala infrastrukturen har blivit totalförsvarets infrastruktur utan att någon fattade det beslutet. Den växte fram genom tusentals rimliga upphandlingar, var och en gjord för att lösa en verksamhets behov så effektivt som möjligt. Summan blev ett samhälle där hundratals organisationer delar samma beroenden, där ansvaret ligger hos en aktör och kontrollen hos en annan, och där ingen har mandat att se helheten.

Det går inte att upphandla sig till rådighet. Rådighet byggs genom att veta vad man är beroende av, genom att kunna byta och agera, genom att ha rätt att göra det och genom att ha förberett samverkan med dem som delar samma sårbarhet. Det kostar i normalläge, och därför kommer det alltid att finnas skäl att skjuta på det.

Ett gemensamt språk är det första steget. Det gör det möjligt att ställa samma frågor i en kommun, en myndighet och ett företag, och att förstå svaren på samma sätt. Nästa steg är en gemensam lägesbild. Steget därefter är gemensam handling. FORUM Totalförsvar avser bidra till alla tre.

Daniel Dersén, Johan Magnusson, Jonny Holmström, Carl Piva och Carl Heath
FORUM Totalförsvar, november 2026

B

Bedömningsmall

Mallen är ett stöd för att använda begreppsramen på en samhällsviktig funktion i den egna organisationen. Den är tänkt att fyllas i gemensamt av verksamheten, IT och de leverantörer som bär funktionen. Bedömningen görs i fyra steg.

1. **Funktion.** Bestäm vilken samhällsviktig funktion som bedöms och vem som bär ansvaret för den.
2. **Scenario.** Välj en eller flera störningar att pröva funktionen mot, till exempel ett långvarigt el- eller nätavbrott, ett utpressningsangrepp mot en leverantör eller ett beslut i ett annat land som begränsar en tjänst. Pröva minst ett scenario där störningen är avsiktlig och inträffar under höjd beredskap.
3. **Minimikrav.** Ange vad funktionen måste klara under scenariot, hur länge och för vilka. Ange också hur länge funktionen i dag bedöms hålla, och hur lång tid det skulle ta att ersätta det som fallit bort. Kravet gäller tillgänglighet men också att informationen är tillräckligt korrekt, att åtkomsten är behörig och att skyddet är godtagbart.
4. **Beroenden.** Följ funktionens beroenden genom lagren i IVA:s lasagnemodell, från tjänster och internetaccess ned till el och upp till lagar, regelverk och styrning. Notera var flera funktioner eller organisationer delar samma beroende.

Fyll därefter i tabellen för varje kärnbegrepp. Kolumnen Underlag anger vad bedömningen vilar på. Ett övat eller testat underlag väger tyngre än ett avtal eller en dokumentation, och ett uppgivet underlag väger lättast.

DEL	BEGREPP	VAD FINNS ELLER UPPGES FUNGERA	UNDERLAG (AVTAL, DOKUMENTATION, TEST, ÖVNING, INCIDENT)	BRIST ELLER OSÄKERHET	ÅTGÄRD, ANSVARIG, NÄR	UPPFÖLJNING
Struktur	Diversitet					
Struktur	Redundans					
Struktur	Decentralisering					
Handling	Veta: beroendeförståelse					
Handling	Kunna: kompetens och handlingsfrihet					
Handling	Ha rätt: mandat					
Handling	Få det gjort: genomförande och samordning					
Funktion	Robusthet					
Funktion	Återhämtningsförmåga					
Funktion	Anpassnings- och utvecklingsförmåga					

Resultatet är en resiliensprofil för funktionen under det valda scenariot. Profilen visar delarna var för sig, med brister och osäkerheter synliga, och vägs inte samman till ett tal. Jämför till sist rådigheten med ansvaret. Där ansvaret är stort och rådigheten liten finns den viktigaste åtgärden.

Referenser

1. Kungl. Ingenjörsvetenskapsakademien (IVA) (2025). *Resilient digital infrastruktur: Stärkt motståndskraft för framtidens samhälle och näringsliv*. IVA-M 560. ISBN 978-91-89181-68-7. iva.se. Lasagnemodellen introducerades i IVA (2019), *Digitalisering för ökad konkurrenskraft*.
2. TV4 (2024). Vd:n ber om ursäkt efter it-attacken. tv4.se
3. SVT (2025). Integritetsskyddsmyndigheten inleder granskning efter Miljödata-läckan. svt.se
4. Tech Insider (2026). Miljödata cyberattack 2026. Sammanställning av Integritetsskyddsmyndighetens uppgifter, minst 164 kommuner och 4 regioner. tech-insider.org/sv/miljodata-cyberattack-2026
5. Star, S. L. & Ruhleder, K. (1996). Steps toward an ecology of infrastructure. *Information Systems Research*, 7(1), 111–134.
6. Magnusson, J., Lindroth, T., Dersén, D. & Persson, P. (2027). *Digital infrastruktur: Att leda det som bär verksamheten*. Adda Förlag, Stockholm.
7. Läkartidningen (2025). Hackerattacken som skakade samhället. lakartidningen.se
8. SecurityWorldMarket (2024). Tietoevry krävs på miljoner av regioner efter cyberattacken. securityworldmarket.com
9. Lerums kommun (2025). Personuppgiftsincident i Adato. lerum.se
10. Desouza, K. C., Watson, R. T. & Xie, Y. (2026). Managing digital dependencies in a connected society: Policy options for ecosystem transitivity. *Journal of the Association for Information Systems*, 27(6), 1339–1356.
11. BBC News (2026). Microsoft says attempts to fix global outage not going "as expected". bbc.com
12. Nilsson, G. (2025). Unik genomgång: Så stor är Microsoft-dominansen ute bland kommunerna. *Techtidningen*. techtidningen.se
13. Quell, M. (2025). Trump's sanctions on ICC prosecutor have halted tribunal's work. *AP News*. apnews.com
14. Doan, T. V., van Rijswijk-Deij, R., Hohlfeld, O. & Bajpai, V. (2022). An empirical view on consolidation of the web. *ACM Transactions on Internet Technology*, 22(3), 1–30.
15. Kumar, R., Asif, S., Lee, E. & Bustamante, F. E. (2023). Each at its own pace: Third-party dependency and centralization around the world. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 7(1), 1–29.
16. Farrell, H. & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, 44(1), 42–79.
17. DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.
18. Jansen, B. m.fl. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4), 101862.
19. SVT (2026). Säpo: Ryssland mer riskbenäget än tidigare. svt.se
20. TV4 (2026). Säpochefen varnar för ryska sabotagehotet. tv4.se
21. Transportstyrelsen (2026). Nu träder cybersäkerhetslagen i kraft. transportstyrelsen.se. Se även cybersäkerhetslag (2025:1506), direktiv (EU) 2022/2555 (NIS2), direktiv (EU) 2022/2557 (CER) och förordning (EU) 2022/2554 (DORA).
22. Finansdepartementet (2025). *Sveriges digitaliseringsstrategi 2025–2030*. Regeringskansliet. Ersätter 2017 års digitaliseringsstrategi och bredbandsstrategin. regeringen.se
23. Carlson, J. M. & Doyle, J. (2002). Complexity and robustness. *PNAS*, 99(suppl. 1), 2538–2545.
24. Holmström, J. & Magnusson, J. (2026, under utgivning). Beyond checklist sovereignty: Known knowns, unknown unknowns, and the infrastructural politics of Swedish AI sovereignty. *Scandinavian Journal of Information Systems*.
25. Ben Brik, A. (2027). Form before capability? AI governance adoption, functional capability, and the limits of index-based evidence in the Global South. *Regulation & Governance*, 21(1), e70222.
26. Cedergren, A., Johansson, J. & Hassel, H. (2018). Challenges to critical infrastructure resilience in an institutionally fragmented setting. *Safety Science*, 110, 51–58.
27. Newlove-Eriksson, L., Giacomello, G. & Eriksson, J. (2018). The invisible hand? Critical information infrastructures, commercialisation and national security. *The International Spectator*, 53(2), 124–140.
28. Heath, C. (2026). *Rådighet i omställning*. Doktorsavhandling, Göteborgs universitet. Gothenburg Studies in Informatics 78. hdl.handle.net/2077/93411
29. Bowker, G. C., Baker, K., Millerand, F. & Ribes, D. (2010). Toward information infrastructure studies. I *International Handbook of Internet Research* (s. 97–117). Springer.
30. Näringsdepartementet (2017). *För ett hållbart digitaliserat Sverige – en digitaliseringsstrategi*. N2017/03643/D. Regeringskansliet. regeringen.se
31. Couture, S. & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10), 2305–2322.
32. Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4).
33. Macpherson, L. & Veit, D. J. (2027). Conceptualizations and boundaries of EU digital sovereignty. *Computers & Security*, 173, 105210.
34. Finansdepartementet (2026). *En molnpolicy för Sverige, för ökad säkerhet, effektivitet och innovation i den offentliga förvaltningen*. Fi2026/01233. Regeringskansliet. regeringen.se
35. Teracom (2026). *Års- och hållbarhetsredovisning 2025*. teracom.se
36. Ingemarsdotter, J. & Marklund, C. (2026). *Rådighet: Att sätta handling bakom ett av totalförsvarets viktigaste ord*. FOI Memo 9110. Totalförsvarets forskningsinstitut. foi.se/rapporter/rapportsammanfattning.html?reportNo=FOI%20Memo%209110
37. Bruneau, M. m.fl. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, 19(4), 733–752.
38. Hosseini, S., Barker, K. & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. *Reliability Engineering & System Safety*, 145, 47–61.
39. Walker, B., Holling, C. S., Carpenter, S. R. & Kinzig, A. P. (2004). Resilience, adaptability and transformability in social-ecological systems. *Ecology and Society*, 9(2), 5.

40. Gunderson, L. H. & Holling, C. S. (red.) (2002). *Panarchy: Understanding transformations in human and natural systems*. Island Press.

41. Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, 141, 5–9.

42. Tim, Y. & Leidner, D. E. (2023). Digital resilience: A conceptual framework for information systems research. *Journal of the Association for Information Systems*, 24(5), 1184–1198.

43. Kostis, A., Holmström, J. & Haefliger, S. (2026, under utgivning). Digital resilience as a process of relational resourcing. *MIS Quarterly*.

44. Sterbenz, J. P. G. m.fl. (2010). Resilience and survivability in communication networks. *Computer Networks*, 54(8), 1245–1265.

45. NIST (2021). SP 800-160 vol. 2 rev. 1. Developing cyber-resilient systems. National Institute of Standards and Technology.

46. NIST (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29. National Institute of Standards and Technology. doi.org/10.6028/NIST.CSWP.29

47. Munoz, A., Billsberry, J. & Ambrosini, V. (2022). Resilience, robustness, and antifragility. *International Journal of Management Reviews*, 24(2), 181–187.

48. Li, M., Hsieh, J. J. P.-A., Li, J., Wang, X. & Gu, B. (2025). Navigating the storm: Toward a theory of IT portfolio diversity, leadership power, and organizational resilience to major shocks. *Information Systems Research*.

49. Park, J., Son, Y. & Angst, C. (2023). The value of centralized IT in building resilience during crises: Evidence from U.S. higher education's transition to emergency remote teaching. *MIS Quarterly*, 47(1), 451–482.

50. Holmström, J. (2026). From digital sovereignty to geographic intelligence: Mapping the hidden geography of digital value and control with the SCALE framework. *Business Horizons*.

51. Cohen, W. M. & Levinthal, D. A. (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, 35(1), 128–152.

52. Arthur, W. B. (1989). Competing technologies, increasing returns, and lock-in by historical events. *The Economic Journal*, 99(394), 116–131.

53. Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal*, 13(4), 447–468.

54. Constantinides, P. & Barrett, M. (2015). Information infrastructure development and governance as collective action. *Information Systems Research*, 26(1), 40–56.

55. Ampratwum, G., Osei-Kyei, R. & Tam, V. W. Y. (2022). Exploring the concept of public-private partnership in building critical infrastructure resilience against unexpected events: A systematic review. *International Journal of Critical Infrastructure Protection*, 39, 100556.

56. Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, 21(6), 11–25.

57. ISO 22301:2019. Security and resilience. Business continuity management systems. Requirements.

58. Salako, K. & Strigini, L. (2014). When does "diversity" in development reduce common failures? *IEEE Transactions on Dependable and Secure Computing*, 11(2), 193–206.

59. Modol, J. R. & Eaton, B. (2021). Digital infrastructure evolution as generative entrenchment. *Journal of Information Technology*, 36(4), 342–364.

60. Magnusson, J. (2013). Intentional decentralization and instinctive centralization. *Information Resources Management Journal*, 26(4), 1–17.

61. Crusoe, J., Magnusson, J. & Eklund, J. (2024). Digital transformation decoupling: The impact of willful ignorance on public sector digital transformation. *Government Information Quarterly*, 41(3), 101958.

62. McGoey, L. (2012). The logic of strategic ignorance. *The British Journal of Sociology*, 63(3), 533–576.

63. Freij, Å., Buffart, M. & Wennberg, K. (2026, under utgivning). The recursive relationship between technology and regulations: Managing landscape frictions in the financial services industry. *Journal of Information Technology*.

64. Farrell, J. & Klemperer, P. (2007). Coordination and lock-in: Competition with switching costs and network effects. I *Handbook of Industrial Organization* (vol. 3, s. 1967–2072). Elsevier.

65. DeNardis, L. (2010). E-governance policies for interoperability and open standards. *Policy & Internet*, 2(3), 129–164.

66. Frischmann, B. M. (2012). *Infrastructure: The social value of shared resources*. Oxford University Press.

67. Petrenj, B., Lettieri, E. & Trucco, P. (2013). Information sharing and collaboration for critical infrastructure resilience: A comprehensive review on barriers and emerging capabilities. *International Journal of Critical Infrastructures*, 9(4), 304–329.

68. Mamediieva, G. & Moynihan, D. (2023). Digital resilience in wartime: The case of Ukraine. *Public Administration Review*, 83(6), 1512–1516.

69. Anderson, T. (2022). Ukraine leader describes emergency cloud migration. *The Register*. theregister.com

70. Berente, N., Lyytinen, K., Yoo, Y. & King, J. L. (2016). Routines as shock absorbers during organizational transformation. *Organization Science*, 27(3), 551–572.

71. Helou, W., Heath, M. & Henry, R. (2026). Resilient IT: Winning with people and process. *Information Systems Journal*, 36(5), 771–786.

72. Amiri, A. K., Cavusoglu, H., Benbasat, I. & Grover, V. (2026). A theory of strategic information technology unavailability. *Information Systems Research*, 37(3), 1571–1595.

73. Keohane, R. O. & Nye, J. S. (2012). *Power and interdependence* (4:e uppl.). Longman.

74. Kashaf, A., Sekar, V. & Agarwal, Y. (2020). Analyzing third party service dependencies in modern web services. *Proceedings of the ACM Internet Measurement Conference*, 634–647.

75. Parchimowicz, K. (2024). Do not get lost in the cloud: How EU financial institutions could avoid problems with cloud services arising under DORA. *Law, Innovation and Technology*, 16(2), 463–487.

76. Huoltovarmuuskeskus. Public-private partnership. huoltovarmuuskeskus.fi

77. Huoltovarmuuskeskus (2025). Security of supply of digital society strengthened: New sector added to the national emergency supply organisation. huoltovarmuuskeskus.fi

78. Huoltovarmuuskeskus. Digital Security 2030. huoltovarmuuskeskus.fi

79. Räisänen, H., Hakala, E., Eronen, J. T., Hukkinen, J. I. & Virtanen, M. J. (2021). Comprehensive security: The opportunities and challenges of incorporating environmental threats in security policy. *Politics and Governance*, 9(4), 91–101.

80. Lehto, M. & Limnéll, J. (2020). Strategic leadership in cyber security, case Finland. *Information Security Journal: A Global Perspective*, 30(3), 139–148.

FORUM TOTALFÖRSVAR

Samhällsviktig verksamhet vilar i dag på digital infrastruktur som ingen enskild aktör överblickar. Rapporten föreslår ett gemensamt språk för samtal om resilient digital infrastruktur, med rådighet som det centrala begreppet. Den bygger vidare på IVA:s rapport och ger begrepp, frågor och en bedömningsmall som ledningar kan använda direkt.

UTGIVEN AV FORUM TOTALFÖRSVAR I SAMARBETE MED

FORUM Totalförsvar · SCDI · RI SE · digital förvaltning · UTTC · INTERNET STIFTELSEN