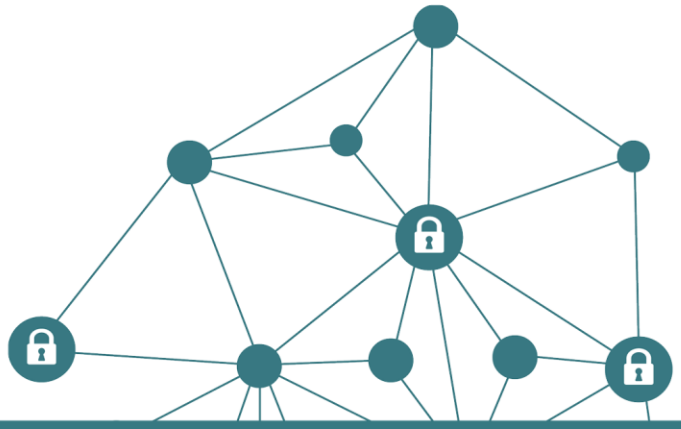
Interreg

Sverige – Norge

Medfinansieras av
EUROPEISKA UNIONEN



POLICY BRIEF

Stärk genomförandekapaciteten för digital resiliens genom pilotarenor

Cross Border Cyber Capacity (CBCC)

DIGITAL INNLANDET

compare

NTNU

INN Universitetet i Innlandet

VAAGER INNOVASJON

KARLSTADS KOMMUN

Policy brief: **Stärk genomförandekapaciteten för digital resiliens genom pilotarenor**

Huvudbudskap

Digital resiliens* byggs inte enbart genom strategier och regelverk. Den skapas genom operativa miljöer där man kan testa, öva, genomföra piloter och omsätta lösningar i praktiken.

Genom Interreg-projektet Cross Border Cyber Capacity har Innlandet och Värmland byggt upp ett gränsöverskridande ekosystem med just den här kapaciteten. Regionen framstår därför som en relevant operativ samverkansarena för fortsatt arbete med digital beredskap, robust digital infrastruktur och digital suveränitet – med tydlig nordisk relevans.

I denna policy brief uppmanas regionala och nationella myndigheter att ge pilotmiljöer såsom Innlandet–Värmland ett tydligt uppdrag, långsiktigt stöd och mandat. En pilotarena kan fungera som en praktisk test- och övningsmiljö där cybersäkerhet och digital beredskap utvecklas, verifieras och vidareutvecklas i verkliga sammanhang, och där offentlig sektor, näringsliv och akademi kan samverka för att testa och utveckla nya lösningar. När sådana miljöer används aktivt kan åtgärder snabbare gå från plan till genomförande – samtidigt som samordningen över gränserna stärks.

Gränsöverskridande samarbete är avgörande för att stärka digital resiliens i en allt mer sammanlänkad och osäker omvärld. I Norden är detta en del av vårt gemensamma tillitskapital – och ett sätt att stå starkare tillsammans i en tid då små länder vinner på att samordna sig och komplettera varandra. Innlandet–Värmland bör därför vidareutvecklas som en test- och övningsarena som kan skalas upp och fungera som modell för fler gränsöverskridande regioner.

**Digital resiliens är förmågan att stå emot, hantera och återhämta sig efter digitala incidenter – utan att samhällskritiska funktioner slås ut.*

Varför detta är viktigt nu

Digitaliseringen har gjort samhälle och näringsliv mer beroende av komplexa tekniska system – och därmed mer sårbara. Detta gäller särskilt förmågan att förebygga, hantera och återhämta sig efter digitala händelser. Sverige och Norge är högt digitaliserade samhällen med stor tillit, men också med beroenden som ställer ökade krav på faktisk genomförandeförmåga inom cybersäkerhet.

Samtidigt skärps kraven. Ett mer osäkert omvärldsläge, ökade digitala hot och EU-regelverk som NIS2, Cyber Resilience Act och AI Act driver behovet av tydligare prioriteringar och stärkt kapacitet.

Utmaningen är gemensam. Sverige och Norge delar sårbarheter och beroenden, och NATO-medlemskapet ökar kraven på samordning. I en nordisk kontext finns därför ett tydligt behov av stärkt samarbete kring digital beredskap, kritisk infrastruktur, kompetens och övning.

Det handlar inte bara om ökade risker, utan om bristande genomförandekapacitet. Det kräver mer operativa och gränsöverskridande arbetssätt – där pilot- och övningsarenor spelar en central roll och där även gränsregioner kan bidra till en mer robust och distribuerad struktur.

Policyutmaningen

Det största gapet i dag finns inte mellan ambition och förståelse, utan mellan ambition och genomförande.

Digital resiliens kräver operativa strukturer som kopplar samman behovsägare och användarmiljöer, till exempel:

- akademi och forskningsmiljöer,
- företag och aktörer i näringslivet,
- offentlig sektor och myndigheter,

i kombination med test-, tränings- och pilotarenor.

I dag saknas dock ofta tydligt mandat och ansvar för att samordna dessa aktörer och insatser. Samverkan sker i hög grad ad hoc och är beroende av enskilda initiativ, snarare än av etablerade och långsiktigt finansierade strukturer.

När sådana kopplingar saknas blir det svårt att omsätta beslutade strategier och krav i praktisk handling. När kopplingarna finns kan politiska mål föras över till övning, testning, kompetensuppbyggnad, pilotering och implementering i verkliga miljöer.

Behovet av operativa strukturer och fungerande kopplingar mellan aktörer är inte en perifer organisationsfråga. Det är en kärnfråga för samhällets förmåga att bygga digital motståndskraft i praktiken.

Den nordiska dimensionen

Samma utmaning gäller också för det nordiska samarbetet.

Om nordiska ambitioner om ökad digital robusthet och suveränitet ska bli mer än politiska signaler behöver de förankras i operativa regionala piloter och gränsöverskridande ekosystem. Det är sådana miljöer som kan samordna, testa och utveckla lösningar i praktiken.

Det finns ett särskilt behov av fördjupat nordiskt samarbete kring:

- cyberberedskap
- säkring av digitala värdekedjor
- test och övning
- utveckling av regionala pilotmiljöer med nordiskt överföringsvärde

Det nordiska samarbetet behöver operativa, regionala och gränsöverskridande byggstenar.

Varför Innlandet–Värmland är relevant

Innlandet och Värmland har under de senaste åren successivt byggt upp starka och kompletterande förmågor inom:

- digitalisering
- cyber- och samhällssäkerhet
- teknikutveckling
- kompetensuppbyggnad
- offentlig–privat samverkan

Genom Cross Border Cyber Capacity har dessa miljöer knutits samman i ett gränsöverskridande innovationsekosystem. Det har lett till:

- etablerade samarbetsstrukturer som kan vidareutvecklas operativt
- utvecklade och prövade samarbetsformer och modeller
- ökad kunskap om regionernas styrkor och behov

Innlandet–Värmland framstår därför som en relevant taktisk kopplingsarena mellan nationella ambitioner och praktiskt genomförande.

Regionen är inte bara ett samarbetsområde, utan kan också fungera som en operativ pilot för fortsatt nationell och nordisk operationalisering av samarbetet kring digital resiliens, beredskap och robust digital infrastruktur.

Erfarenheterna från Innlandet–Värmland visar hur en sådan modell kan fungera i praktiken. Den bygger på några enkla principer: att aktörer arbetar tillsammans i konkreta aktiviteter, att arbetet utgår från verkliga behov, att lösningar testas och övas i riktiga miljöer, och att det finns en tydlig koppling mellan strategi och genomförande. Dessa principer kan användas och anpassas i andra regioner.

Vad beslutsfattare bör uppmärksamma

Digitala hot hanteras inte enbart med politik och reglering, utan också genom miljöer som kan utveckla och genomföra nödvändiga beredskapsåtgärder.

Gränsöverskridande regionala ekosystem bör därför inte avfärdas som perifera nätverk eller tillfälliga projektsamarbeten. De bör i stället ses som en del av samhällets faktiska genomförandekapacitet för digital resiliens, beredskap och robust digital infrastruktur.

För regionala och nationella myndigheter innebär det här att:

- stärka genomförandekapacitet i hela kedjan – från strategisk inriktning till praktiskt genomförande
- använda mogna pilotregioner mer aktivt för operationalisering i praktiken
- göra samverkan mellan offentlig sektor, näringsliv och akademi handlingsinriktad
- förankra nordiskt samarbete i miljöer som redan kan leverera resultat i praktiken

Rekommendationer

1. Ge operativa regionala ekosystem en tydlig roll som genomförandekapacitet

Digital resiliens kräver miljöer som kan omsätta strategier i praktisk handling. Sådana strukturer bör ges en tydlig roll i regional och nationell politik. Regioner där samarbete redan är etablerat mellan kluster, offentlig sektor, akademi och näringsliv bör användas mer aktivt för att testa och genomföra åtgärder i praktiken.

2. Stärk operativ samverkan genom pilotarenor

Det behövs fler praktiknära arenor där lösningar kan prövas, utvärderas och tas vidare – inte minst som grund för bredare nordisk samordning.

Samarbete måste handla om gemensam utveckling, övning och implementering – inte stanna vid dialog. Innlandet–Värmland bör användas för att testa hur regionalt, nationellt och nordiskt samarbete om digital beredskap, övning, robust digital infrastruktur och offentlig–privat samverkan kan genomföras i praktiken. Erfarenheterna bör dokumenteras och ligga till grund för fortsatt nordisk överföring.

3. Integrera digital resiliens och genomförandekapacitet i regionala strategier och i totalförsvarsarbetet.

Digital resiliens bör förankras tydligare i regionala strategier för samhällssäkerhet, beredskap, näringsutveckling och innovation. Det kräver också investeringar i konkret genomförandekapacitet - inte bara strategisk inriktning. Regional genomförandekapacitet är en förutsättning för att kunna operationalisera nationella ambitioner och stärka totalförsvarets samlade digitala motståndskraft.

4. Stärk kompetensförsörjning och praktiknära utbildning inom digital resiliens

Tillgång till rätt kompetens är avgörande för att kunna genomföra arbetet i praktiken. Akademi, utbildning och forskning behöver kopplas nära behoven i offentlig sektor och näringsliv. Utbildning bör i större utsträckning kopplas till test-, övnings- och pilotmiljöer, så att kunskap omsätts i praktisk förmåga.

Från rekommendation till genomförande

För att skapa effekt behöver ansvar tydliggöras mellan nivåer:

- **Regional nivå** bör integrera digital resiliens i strategier, beredskapsarbete och näringsutveckling.
- **Nationell nivå** bör använda pilotregioner för att testa hur strategier och krav omsätts i praktiken.
- **Operativa ekosystem** (kluster och kunskapsmiljöer) bör ges mandat och resurser att mobilisera aktörer, genomföra piloter, testa och träna.
- **Nordisk nivå** bör använda erfarenheter från pilotregioner för skalning och gemensamt lärande.

Interreg, eller liknande verktyg, kan användas som en arena för att utveckla, testa och vidareutveckla gränsöverskridande arbetssätt, medan nationella och regionala strukturer säkerställer långsiktig förankring.

Innlandet–Värmland bör användas som en operativ pilot för att visa hur gränsöverskridande samarbete kan omsättas i praktiken och ligga till grund för vidare nordisk tillämpning.

Nästa steg är att ge ett tydligt uppdrag till en eller flera pilotregioner att testa hur nationella och nordiska ambitioner kan genomföras i praktiken, med Innlandet–Värmland som ett konkret exempel.

Avslutning

Om ambitionerna om digital resiliens, beredskap och digital suveränitet ska ge verklig effekt behöver de förankras i operativa miljöer som kan testa, öva, samordna och omsätta åtgärder i praktisk handling.

Regionala aktörer har här en särskild styrka genom sin närhet till företag och verksamheter, och god förståelse för deras behov, drivkrafter och förutsättningar.

Erfarenheterna från Innlandet–Värmland visar att gränsöverskridande ekosystem med den här kapaciteten går att bygga upp, och kan fungera som en länk mellan politiska mål och praktiskt genomförande.

Den här typen av miljöer bör därför ges en tydligare strategisk roll i det fortsatta arbetet med digital robusthet – regionalt, nationellt och nordiskt.