Säkerhets- och resiliensbedömning

Distribuerad infrastruktur för samhällsskydd och beredskap

Dokumenttyp: Förslag till Myndigheten för civilt försvar
Datum: Januari 2025
Klassificering: Öppen

Sammanfattning: Detta dokument beskriver en teknisk arkitektur för lokal ekonomisk kontinuitet och social sammanhållning under systemstörningar. Förslaget adresserar kritiska sårbarheter i Sveriges digitala betalningsinfrastruktur och sociala resiliens, identifierade i Myndigheten för civilt försvars totalförsvarsdoktrin och förstärkta av lärdomar från Ukraina-konflikten.

1. Hotbild och sårbarhetsanalys

1.1 Aktuell säkerhetskontext

Sveriges säkerhetssituation har förändrats fundamentalt sedan 2022:

- **NATO-medlemskap (2024):** Sverige är nu explicit mål för hybridhot från antagonistiska aktörer
- **Ukraina-konflikten:** Demonstrerar effektivitet av kombinerade digitala attacker och social destabilisering
- **Östersjön som konfliktzon:** Kritisk infrastruktur (kablar, pipelines) dokumenterat utsatt
- **Myndigheten för civilt försvars (tidigare MSB) bedömning:** Totalförsvar 2024:1032 kräver ökad lokal resiliens och psykologiskt försvar

Identifierad kritisk sårbarhet: Sveriges betalningsinfrastruktur är extremt centraliserad. **95% av transaktioner** går via Swish/BankID som är beroende av kontinuerlig internetanslutning och centrala API:er. En målinriktad störning av ISP-backbone eller bankens API-tjänster skulle göra lokala samhällen ekonomiskt paralyserade inom **6-12 timmar**.

1.2 Lärdomar från Ukraina

Rysslands hybridkrigsföring i Ukraina 2022-2025 demonstrerar tre kritiska angreppsvektorer:

Angreppsvektor	Ukrainska exempel	Svensk sårbarhet
Digital infrastruktur	NotPetya (2017), koordinerade DDoS mot banker (2022)	Swish/BankID single points of failure; centralbaserade banktjänster
Social atomisering	Desinformation, splittring av civilbefolkning	Låg grannskapskoherens i urbana områden; socialt kapital eroderande

Försörjningskedjor	Blockad av Svartahavet; matbrist som vapen	Hög importberoende (60% av livsmedel i Stockholm); ingen lokal buffertkapacitet

1.3 Jämförelse med nordiska grannar

- **Finland:** Omfattande beredskapslager på hushållsnivå; stark "sisu"-kultur av självförsörjning
- **Norge:** Oljefondens buffert; lägre digitalisering av kontanta transaktioner
- **Sverige:** Högst digitaliseringsgrad, lägst kontantanvändning, minst decentraliserad resiliens

2. Teknisk lösning: Redundant ekonomisk arkitektur

Global Governance Frameworks (GGF) föreslår inte att *ersätta* befintliga system, utan att tillhandahålla **redundans** – en "backup-ekonomi" som aktiveras vid störning av primära system.

2.1 Arkitekturval: Agent-centrerad design (Holochain)

Till skillnad från blockchain (kräver global konsensus) eller molnapplikationer (kräver centrala servrar) bygger denna arkitektur på:

PARTITIONSTOLERANS

Offline-first design: Transaktioner registreras lokalt på användarens enhet. Systemet kan fungera via lokala nätverk (LAN/mesh) även om global internet kapas. Data synkroniseras automatiskt när anslutning återställs.

DATASUVERÄNITET

Ingen central attackyta: Ingen central databas att hacka eller DDOSa. Data distribueras över ett community-nätverk (DHT). För att förstöra systemet krävs fysisk förstöring av varje enskild nod.

2.2 Referensimplementationer internationellt

- **Estland:** X-Road (decentraliserad datautbyte); e-residency (digital suveränitet)
- **Schweiz:** WIR-systemet (komplementär valuta sedan 1934; använd under krisperioder)
- **Japan:** Fureai kippu (omsorgsvaluta; demografisk resiliens)

GGF:s arkitektur kombinerar dessa lärdomar med modern kryptografisk säkerhet och offline-kapacitet.

3. Operativa förmågor under kris

3.1 Ekonomisk kontinuitet vid betalningssystemsavbrott

Vid störning av centraliserade betalningssystem aktiveras **Hearts-protokollet** som lokal bytesmekanism:

- **Funktion:** Möjliggör fortsatt handel av nödvändiga tjänster (äldreomsorg, matdistribution, manuellt arbete) utan kontantlikviditet eller internetåtkomst

- **Verifiering:** Transaktioner kryptografiskt signerade av båda parter på enheten; skapar oföränderlig skuld/kredit-redovisning som persisterar offline
- **Säkerhet:** Ingen "double-spend" möjlig; varje agent har unik kryptografisk identitet; manipulation kräver fysisk åtkomst till enheten

3.2 Resurskartläggning och tillgångsallokering

Systemet skapar en integritetsskyddande inventering av lokal resiliens:

- **Kompetenskartläggning:** Vem har medicinsk utbildning? Vem kan svetsa? Vem talar språk?
- **Materiella tillgångar:** Vem har generator? Vem har överskott av rotfrukter?
- **Säkerhetsarkitektur:** Kartan lagras *inte* centralt (där motståndare kan targetera den) utan distribuerad bland betrodda peers med kryptering

3.3 Psykologiskt försvar genom social sammanhållning

Myndigheten för civilt försvars (tidigare MSB) doktrin (2024:1032) betonar **försvarsvilja** som kritisk komponent. Resiliens är i grund och botten social.

> **G20 Global Inequality Report (November 2025):** Dokumenterar att höga nivåer av ojämlikhet underminerar social sammanhållning och demokrati, vilket gör samhällen mer sårbara för auktoritära och destabiliserande krafter. Rekommenderar *"valorisering av obetalt omsorgsarbete"* som motåtgärd.

Genom att "gamifiera" och belöna vardagligt omsorgsarbete (kolla på grannar, gemensam odling, språkundervisning) under fredstid bygger plattformen högtillitsnätverk:

- **Resultat:** Vid krishändelse är det "sociala nätverket" redan aktivt. Grannar är inte främlingar; de är lagkamrater. Detta stärker "Försvarviljan" mot destabilisering.
- **Kontrast:** I Ukraina visade sig områden med starkt socialt kapital vara mer motståndskraftiga mot rysk desinformation och ockupation

4. Pilotlokalisering: Stockholms skärgård

4.1 Strategisk motivering

Stockholms skärgård valdes som pilotzon baserat på fyra kriterier:

Kriterium	Motivering
Geografisk avgränsning	Naturliga gränser (öar) underlättar kontrollerad testmiljö; begränsat antal access points
Kritisk infrastruktur	Sjöfartsvägar in till Stockholm; strategiskt viktigt område vid konflikt i Östersjön

Demografi	Blandning av permanent- och fritidsboende; åldrande befolkning (testar omsorgsresiliens)
Befintlig motivation	Redan aktiva lokala Hemvärnsgrupper och Frivilliga Resursgrupper; receptivitet för beredskapsinitiativ

4.2 Pilotfaser

Fas 1 (3 månader): Stresstestning av offline-funktionalitet

- 50 lokala noder (hushåll) deltar
- Simulerad internetavbrott (kontrollerad miljö)
- Mät: Transaktionshastighet, datasynkronisering vid återanslutning, användarupplevelse

Fas 2 (6 månader): Integration med lokalt civilförsvar

- Samverkan med Frivilliga Resursgruppen (FRG)
- Genomför "tabletop exercise" – simulerat hybridhot scenario
- Mät: Responstid, resursallokering, social koordination

5. Säkerhetsrevision och compliance

5.1 GDPR och integritetsskydd

- **Privacy by design:** Ingen central identitetsdatabas; användare kontrollerar egna data
- **Dataminimering:** Endast nödvändig metadata lagras; krypterad end-to-end
- **Rätt till radering:** Användare kan när som helst lämna nätverket och radera sin data

5.2 Säkerhetsgranskningsbehov

Vi söker Myndigheten för civilt försvars expertis för granskning av:

1. **Offline reconciliation-protokoll:** Säkerställa att ingen manipulation kan ske under internet-disconnection
2. **Kryptografisk implementation:** Peer review av signeringsprotokoll och nyckelhantering
3. **Denial-of-service motstånd:** Hur systemet hanterar flood attacks på mesh-nätverket

6. Koppling till befintligt GGF-arbete

Detta förslag kompletterar pågående GGF-initiativ:

- **TAK-405 "Regionens Nervsystem":** Inlämnat till Region Stockholm (december 2024); fokus på psykologisk resiliens i kollektivtrafik; extern finansiering via Myndigheten för civilt försvar och EU

- **Vinnova-ansökan:** Teknisk plattformsutveckling för kommunal innovation; samverkar med denna säkerhetsapplikation

Den tekniska arkitektur som utvecklas har därmed **dual-use** karaktär:

- **Civil tillämpning:** Vardaglig välfärdsinnovation (omsorgsvaluta, hälsofrämjande incitament)
- **Försvarstillämpning:** Kritisk redundans vid systemstörning

7. Begäran om samarbete

Denna infrastruktur adresserar Myndigheten för civilt försvars uppdrag att *"stärka samhällets förmåga att förebygga och hantera olyckor och kriser"*. Vi söker dialog kring:

1. **Forsknings- och innovationsfinansiering** för säkerhetsrevisionen och fältsimuleringar
2. **Expertis från Myndigheten för civilt försvars cyber- och sociala resiliensavdelningar** för teknisk granskning
3. **Pilotsamordning** med befintliga totalförsvarövningar i Stockholmsregionen

> **Avslutande reflektion:** Ukraina har lärt oss att resiliens inte byggas när krisen kommer – den måste vara inbyggd i vardagen. Denna infrastruktur operationaliserar Myndigheten för civilt försvars doktrin om lokal beredskap genom att ge lokalsamhällen verktyg för ekonomisk och social kontinuitet.
>
> **Frågan är inte om** Sverige kommer utsättas för hybridhot mot kritisk infrastruktur. **Frågan är om** våra lokalsamhällen kommer ha redundanskapacitet när det sker.

Global Governance Frameworks
Systemarkitektur för samhällsresiliens
Huvudarkitekt: Björn K. Holmström | +46 79 333 94 62
bjorn.holmstrom@globalgovernanceframeworks.org