

# Säkerhets- och resiliensbedömning

CivicBase - Distribuerad infrastruktur för samhällsskydd och beredskap

Dokumenttyp: Förslag till Myndigheten för civilt försvar  
(MCF)

Datum: Januari 2026  
Klassificering: Öppen

**Sammanfattning:** Detta dokument beskriver **CivicBase** – en teknisk arkitektur för lokal ekonomisk kontinuitet och social sammanhållning under systemstörningar. Förslaget adresserar kritiska sårbarheter i Sveriges digitala infrastruktur, exponerade av kabelkapningarna i Östersjön november 2024, och operationaliseras Myndigheten för civilt försvars (MCF) totalförsvarsdoktrin genom distribuerad, offline-kapabel samhällsinfrastruktur.

## 1. Hotbild och strategisk kontext

### 1.1 November 2024: Konkret bevis på sårbarhet

**Händelse:** Kabelkapningar i Östersjön (november 2024)

**Drabbade kablar:** C-Lion1 (Finland-Tyskland), BCS East-West Interlink (Sverige-Litauen)

**Konsekvens:** Exponerade Sveriges totala beroende av centraliserad internetinfrastruktur

**Systemsvar:** Befintliga kommunala IT-system hade kollapsat vid längre avbrott. Inga redundanssystem fanns.

Denna händelse demonstrerade tre kritiska sårbarheter som CivicBase adresserar:

- Infrastruktursårbarhet:** Enstaka kabelkapningar kan isolera hela regioner
- Molnberoende:** Kommuner är 100% beroende av amerikanska molntjänster (AWS, Azure, Google) som kräver kontinuerlig internetåtkomst
- Betalningssystem:** 95% av transaktioner via Swish/BankID – totalt beroende av centrala servrar och internetåtkomst

### 1.2 Myndigheten för civilt försvars totalförsvarsdoktrin (2024:1032)

MCF:s förnyade totalförsvarsdoktrin betonar tre kärnområden som CivicBase operationaliseras:

**MCF:s identifierade gap:**

- Psykologiskt försvar:** "Försvarsvilja" kräver stark social sammanhållning – saknas i urbana miljöer
- Ekonomisk resiliens:** Lokala samhällen måste kunna upprätthålla grundläggande ekonomisk aktivitet vid störning av centraliserade system

- **Kommunikationsredundans:** Kritiska samhällsfunktioner måste fungera utan beroende av centraliserad internetinfrastruktur

### 1.3 Lärdomar från Ukraina

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

Angreppsvektor	Ukrainska exempel	Svensk sårbarhet
<b>Digital infrastruktur</b>	NotPetya (2017), koordinerade DDoS mot banker (2022)	Swish/BankID single points of failure; centralbaserade banktjänster; molnberoende
<b>Social atomisering</b>	Desinformation, splittring av civilbefolkning	Låg grannskapskoherens i urbana områden; socialt kapital eroderande
<b>Försörjningskedjor</b>	Blockad av Svartahavet; matbrist som vapen	Hög importberoende (60% av livsmedel i Stockholm); ingen lokal buffertkapacitet

**Nyckellärdom:** Områden med starkt socialt kapital och lokal redundans var markant mer motståndskraftiga mot rysk destabilisering och ockupation.

### 1.4 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, totalt molnberoende

## 2. Teknisk lösning: CivicBase infrastruktur

Global Governance Frameworks (GGF) föreslår inte att ersätta befintliga system, utan att tillhandahålla **redundans** – en resilient infrastruktur som aktiveras vid störning av primära system. **CivicBase** är den distribuerade plattform som möjliggör detta.

### 2.1 Arkitekturval: Distribuerad P2P-design (libp2p)

Till skillnad från blockchain (kräver global konsensus) eller molnapplikationer (kräver centrala servrar) bygger CivicBase på etablerad P2P-teknologi (libp2p – samma som driver IPFS/Filecoin):

#### PARTITIONSTOLERANS

**Offline-first design:** Transaktioner registreras lokalt på användarens enhet. Systemet kan fungera via lokala nätverk (LAN/mesh) även om global internet

#### DATASUVERÄNITET

**Ingen central attackyta:** Ingen central databas att hacka eller DDOSa. Data distribueras över ett community-nätverk. För att förstöra systemet krävs fysisk

kapas. Data synkroniseras automatiskt när anslutning återställs. Vid november 2024:s kabelkapningar skulle CivicBase-system fortsatt fungera lokalt.

förstöring av varje enskild nod. All data stannar i Sverige – inget molnberoende.

#### BEPRÖVAD TEKNOLOGI

**libp2p foundation:** CivicBase bygger på libp2p – etablerat P2P-protokoll som driver IPFS, Filecoin och andra distribuerade system. Battle-tested i produktionsmiljöer globalt. Eliminerar "single point of failure".

#### KRYPTOGRAFISK SÄKERHET

**Agent-centrerad identitet:** Varje användare har unik kryptografisk identitet. Ingen central identitetsdatabas att kompromittera. End-to-end kryptering. GDPR-compliant by design.

## 2.2 Arkitekturval: Varför inte blockchain?

En vanlig fråga är varför CivicBase inte använder etablerade blockchain-protokoll (Ethereum, Solana) för Hearts-valutan. Svaret är resiliens:

Krav	Blockchain (Solana/Ethereum)	CivicBase (libp2p)
<b>Internetberoende</b>	Kräver anslutning till globala validators (oftast USA/EU)	Fungerar offline via lokal mesh-nätverk
<b>Vid kabelkapning</b>	Transaktioner stoppar helt (som november 2024)	Transaktioner fortsätter lokalt, synkroniseras när anslutning återställs
<b>Datasuveränitet</b>	Data lagras på global, permanent ledger	Data ägs av svensk agent, raderas på begäran (GDPR)
<b>Energiförbrukning</b>	Hög (proof-of-work/stake kräver kontinuerlig validering)	Låg (endast lokal kryptografisk signering)
<b>Finansialisering</b>	Hearts blir spekulativ tillgång (volatilitet)	Hearts är lokal trust-signal, ej handelbar valuta

**Sammanfattning:** Blockchain optimerar för global finansiell konsensus. CivicBase optimerar för lokal social resiliens. För totalförsvarstillämpningar är det senare kritiskt.

## 2.3 Referensimplementationer internationellt

- **Estland:** X-Road (decentraliserad datautbyte); e-residency (digital suveränitet) – fungerade under cyberattacker 2007
- **Schweiz:** WIR-systemet (komplementär valuta sedan 1934; använd under krisperioder inklusive WWII)
- **Japan:** Fureai kippu (omsorgsvaluta; demografisk resiliens)

- **Protocol Labs:** libp2p/IPFS används i kritisk infrastruktur globalt

CivicBase kombinerar dessa lärdomar med modern P2P-teknologi och offline-kapacitet specifikt designad för totalförsvarsbehov.

### 3. Operativa förmågor under kris

---

#### 3.1 Ekonomisk kontinuitet vid betalningssystemsavbrott

Vid störning av centraliseraade betalningssystem (Swish/BankID) 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
- **Synkronisering:** När internetåtkomst återställs synkroniseras offline-transaktioner automatiskt via P2P-nätverket



*Figur 1: Bunker Mode-gränssnitt vid internetavbrott. Hearts-transaktioner fortsätter via lokalt mesh-nätverk och synkroniseras automatiskt när internetanslutning återställs. Detta operationalisrar MCF:s krav på ekonomisk kontinuitet under systemstörningar.*

**Konkret scenario - November 2024:** Vid kabelkapningarna skulle Hearts-aktiverade samhällen fortsatt kunna handla med lokala producenter, betala för äldreomsorg, och upprätthålla grundläggande ekonomisk aktivitet via mesh-nätverk, synkroniserande när kablar reparerades. Befintliga system: total kollaps.

#### 3.2 Resurskartläggning och tillgångsallokering

CivicBase 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
- **Offline-kapabel:** Resurskartläggning fungerar via lokal mesh-nätverk även under internetavbrott

#### 3.3 Psykologiskt försvar genom social sammanhållning

MCF:s 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 samhället mer sårbara för auktoritär och destabilisering kraft. Rekommenderar "valorisering av obetalt omsorgsarbete" som motåtgärd.

Genom att "gamifiera" och belöna vardagligt omsorgsarbete (kolla på grannar, gemensam odling, språkundervisning) under fredstid bygger CivicBase 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
- **Offline-resiliens:** Social koordination fortsätter via mesh-nätverk även när centrala kommunikationssystem faller

## 4. Pilotlokalisering: Stockholms skärgård

### 4.1 Strategisk motivering

Stockholms skärgård valdes som pilotzon baserat på fyra kriterier:

Kriterium	Motivering
<b>Geografisk avgränsning</b>	Naturliga gränser (öar) underlättar kontrollerad testmiljö; begränsat antal access points
<b>Kritisk infrastruktur</b>	Sjöfartsvägar in till Stockholm; strategiskt viktigt område vid konflikt i Östersjön (som november 2024 demonstrerade)
<b>Demografi</b>	Blandning av permanent- och fritidsboende; åldrande befolkning (testar omsorgsresiliens)
<b>Befintlig motivation</b>	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, replikerar november 2024-scenario)
- Mät: Transaktionshastighet, datasynkronisering vid återanslutning, användarupplevelse
- Test: 72+ timmar offline operation via mesh-nätverk

**Fas 2 (6 månader):** Integration med lokalt civilförsvar

- Samverkan med Frivilliga Resursgruppen (FRG) och Hemvärnet
- Genomför "tabletop exercise" – simulerat hybridhot scenario (kabelkapning + cyberattack)
- Mät: Responstid, resursallokering, social koordination under stress
- Test: Ekonomisk kontinuitet vid simulerat betalningssystemsavbrott

## 5. Säkerhetsrevision och compliance

---

### 5.1 GDPR och integritetsskydd

- **Privacy by design:** Ingen central identitetsdatabas; användare kontrollerar egna data via agent-centrerad arkitektur
- **Dataminimering:** Endast nödvändig metadata lagras; krypterad end-to-end via libp2p
- **Rätt till radering:** Användare kan när som helst lämna nätverket och radera sin data
- **Datasuveränitet:** All data stannar i Sverige – inget molnberoende på amerikanska tjänster

### 5.2 Säkerhetsgranskningsbehov

Vi söker MCF:s 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 (libp2p-baserad)
3. **Denial-of-service motstånd:** Hur systemet hanterar flood attacks på mesh-nätverket
4. **Cybersäkerhet:** Penetrationstestning av P2P-arkitektur under simulerade attacker

## 6. Koppling till befintligt GGF-arbete

---

CivicBase är den gemensamma tekniska plattformen för pågående GGF-initiativ:

- **TAK-405 "Regionens Nervsystem":** Inlämnat till Region Stockholm (december 2024); fokus på psykologisk resiliens i kollektivtrafik; extern finansiering via MCF och EU
- **Vinnova-ansökan (januari 2026):** 2,5 MSEK över 12 månader för CivicBase plattformsutveckling; fokus på offline-resiliens och kommunal innovation
- **Denna MCF-ansökan:** Säkerhetsrevision och skärgårdspilot av CivicBase för totalförsvarstillämpningar

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

- **Civil tillämpning:** Vardaglig välfärdsinnovation (omsorgsvaluta, hälsofrämjande incitament, kommunal administration)
- **Försvarstillämpning:** Kritisk redundans vid systemstörning – demonstrerat nödvändig av november 2024:s kabelkapningar

## 7. Begäran om samarbete

---

CivicBase adresserar MCF:s uppdrag att "stärka samhällets förmåga att förebygga och hantera olyckor och kriser" genom att operationalisera totalförsvarsdoktrinen med konkret infrastruktur. Vi söker dialog kring:

1. **Forsknings- och innovationsfinansiering** för säkerhetsrevisionen och fältsimuleringar
2. **Expertis från MCF:s cyber- och sociala resiliensavdelningar** för teknisk granskning av CivicBase-arkitekturen
3. **Pilotsamordning** med befintliga totalförsvarövningar i Stockholmsregionen
4. **Cybersäkerhetsgranskning** av distribuerad P2P-arkitektur under simulerade hot

**Avslutande reflektion:** November 2024:s kabelkapningar i Östersjön var inte en överraskning – de var en varning. Ukraina har lärt oss att resiliens inte byggas när krisen kommer – den måste vara inbyggd i vardagen.

CivicBase operationaliseras MCF:s doktrin om lokal beredskap genom att ge lokalsamhällen verktyg för ekonomisk och social kontinuitet som fungerar *under* störningar, inte bara före eller efter.

**Frågan är inte om** Sverige kommer utsättas för hybridhot mot kritisk infrastruktur. November 2024 visade att vi redan blir det. **Frågan är om** våra lokalsamhällen kommer ha redundanskapacitet nästa gång det sker.



Global Governance Frameworks

Systemarkitektur för samhällsresiliens

Huvudarkitekt: Björn K. Holmström | +46 79 333 94 62

[\[email protected\]](mailto:[email protected]) | globalgove