



Policy avseende det öppna internets offentliga kärna

Nulägesbeskrivning och analys sammanställdes i november 2025. Dessa kommer att uppdateras till slutversionen av policyn.

Definitioner

Begreppet 'den offentliga kärnan av det öppna internet' definieras inte närmare i NIS2-direktivet. I den engelska språkversionen av NIS2-direktivet är den motsvarande formuleringen 'the public core of the open internet', vilket är ett begrepp som syftar på internets fysiska infrastruktur inklusive centrala protokoll.¹ Direktivets svenska lydelse bör tolkas i enlighet med detta (se närmare avgränsning nedan under Introduktion).

Introduktion

Internet är byggt för robusthet och motståndskraft. Den decentraliserade infrastrukturen, i kombination med standardiserade protokoll, gör det möjligt för internet att fortsätta fungera även om delar av nätverket fallerar.

Det kan samtidigt konstateras att internet inte är felsäkert. Allvarliga avbrott i den offentliga kärnan kan till följd av systemfel, misstag, sabotage eller cyberangrepp, få omfattande konsekvenser för samhället och nationell säkerhet. Det öppna internets offentliga kärna utgör således en viktig samhällsfunktion.

Internet utgörs av en global infrastruktur som saknar ett enhetligt ägarskap. Det utvecklas, drivs och underhålls av ett stort antal oberoende aktörer, från internationella standardiseringsorgan och internetoperatörer, till privata företag och ideella organisationer. Dess offentliga kärna omfattar de gemensamma och gränsöverskridande infrastrukturer, protokoll och system som möjliggör ett öppet, sammanhängande och tillgängligt internet för alla användare i Sverige.

Den offentliga kärnan utgörs av:

- Kabelbunden och trådlös nätinфраstruktur
- Internetknutpunkter, gränsroutrar och switchar

¹ Se t.ex. *The Public Core of the Internet – An international agenda for Internet governance*, Dennis Broeders, och den nederländska *International Cyber Strategy 2023-2028 – Decisive Diplomacy in the Digital Domain*.

- DNS, tidstjänster och routingprotokoll

Privata nätverk och enheter som ansluter till det öppna internet, men ägs eller förvaltas av privatpersoner och organisationer, utgör inte en del av den offentliga kärnan.

Nulägesbild

I Sverige hanteras den offentliga kärnan av internet av ett antal aktörer, både privata och offentliga. Nulägesbilden presenterar den offentliga kärnans beståndsdelar, aktörerna som upprätthåller dem och samverkansformer.

Följande lagstiftning och förarbeten aktualiseras i policyn:

- Lag (2022:482) om elektronisk kommunikation
- Lag (2006:24) om nationella toppdomäner för Sverige på internet
- Prop. 2025/26:28 – Ett starkt skydd för nätverks- och informationssystem – en ny cybersäkerhetslag

Ansvarsprincipen gäller i Sverige, vilket innebär att den som ansvarar för en verksamhet under normala förhållanden också gör det i händelse av kris, höjd beredskap och krig. På nationell nivå ansvarar Nationella telesamverkansgruppen (NTSG) för koordinering vid allvarliga samhällsstörningar. Det är ett samarbete mellan myndigheter och centrala aktörer i telekom- och nätinфраstrukturen och deras huvudsakliga uppgift är att stödja återställandet av bland annat digital nätinфраstruktur. Ytterligare fora för samverkan och koordinering i både freds- och kristider finns även på verksamhetsnivå (se nedan).

Trådlösa nät (5G och 4G)

5G- och 4G-näten i Sverige når upp till 99,9% av den svenska befolkningen och frekvensbanden hos de största operatörerna täcker 90% av Sveriges geografiska yta.² Operatörer som äger och driver 5G- och 4G-nät idag är Telia, Tre och Net4Mobility (ett samarbete mellan Tele2 och Telenor). PTS rapporterade under 2025 att andelen 5G-abonnemang, samt mängden datatrafik i 5G-näten, hade ökat i snabb takt under 2024. I jämförelse med äldre generationers nät klarar 5G-nätet betydligt fler uppkopplade enheter per basstation utan att bli överbelastat. Det finns 10 000-tals³ basstationer som är anslutna till operatörernas övriga nät (och den offentliga kärnan) via antingen fiberoptiska kablar eller radiolänk.

Fram till slutet av 2025 kommer 2G- och 3G-näten att fasas ut i Sverige och ersättas med 4G och 5G (Telia fasar ut sitt 2G-nät fram till 2027)⁴.

² Telia och Net4Mobility anger samma siffror för täckning på sina respektive hemsidor.

³ Uppgifter från Tele2:s hemsida.

⁴ Se Telias pressmeddelanden från den 30 maj 2024, <https://press.telia.se/pressreleases/telia-skjuter-upp-nedstaengningen-av-2g-naetet-till-2027-3325928>

Fiberoptiska kabelnät

Sverige har ett geografiskt välutbyggt fibernät som når ut till närmare 98% av hela den svenska befolkningen (räknat på glesbygden är den siffran något lägre, ca 90%).⁵ I Sverige har vi ett system med så kallade stadsnät, det vill säga fibernät som ägs och driftas på lokal/regional nivå. Det finns totalt cirka 170 stadsnät varav den övervägande majoriteten är kommunalt ägda (genom kommunala bolag eller kommunal förvaltning). Tillsammans utgör stadsnäten ungefär hälften av Sveriges bredbandsinfrastruktur. OECD har framhållit den svenska stadsnätsmodellen som en avgörande faktor för den goda tillgängligheten på fiberuppkoppling i Sverige.⁶ Resterande nät ägs i huvudsak av de stora telekomföretagen (Telia, Tele2, Telenor och Tre) och en mindre procentandel utgörs av glesbygdsnät.⁷

Samverkansforum och gemensamma initiativ:

- **Stadsnästens infrastruktursamverkansgrupp (SISG)** har en samordnande funktion mellan stadsnät och andra aktörer vid kris och allvarliga händelser. SISG är en del av PTS samverkansstruktur och har via Stadsnätsföreningen en kontaktyta till NTSG (se ovan).
- **Stadsnätsföreningen** är en bransch- och intresseorganisation vars medlemmar (företag och kommuner) utgör huvuddelen av alla aktörer i Sverige som utvecklar och investerar i bredbandsinfrastruktur. Stadsnätsföreningen har sedan 2022 ett beredskapsuppdrag från PTS som syftar till att stärka förmågan att upprätthålla den digitala infrastrukturen vid kris, höjd beredskap och krig. Uppdraget ger stadsnäten tillgång till beredskapsmateriel, utbildning och fördjupad samverkan.
- **Robust fiber** är ett svenskt branschgemensamt initiativ som har tagit fram anvisningar med stöd och minimikrav till den som vill beställa eller anlägga driftsäkra fibernät. Robust fiber erbjuder även certifieringsmöjligheter och utbildning till företag i branschen. Representanter i Robust fibers förvaltningsråd är PTS, Stadsnätsföreningen, SKR, Bredbandsforum, m.fl.

Internetknutpunkter (IXP)

Internetknutpunkter möjliggör fiberoptiska kabelnät tillhörande olika internetleverantörer och CDN:er⁸ att kommunicera med varandra genom att dirigera trafik mellan dem. Internetknutpunkter kan utgöras av en eller flera ethernet-switchar lokaliserade på en eller flera platser. Netnod är den största tillhandahållaren av internetknutpunkter i Sverige (och Norden) och ägs av den oberoende TU-stiftelsen⁹. Det finns även några mindre aktörer på området som är verksamma mer regionalt.

⁵ Se PTS rapport *Mobiltäcknings- och bredbandskartläggningen 2024 – Geografisk översikt av tillgången till bredband och mobiltelefoni i Sverige*.

⁶ Se OECD:s rapport *Development of High-Speed Networks and the Role of Municipal Networks*.

⁷ Stadsnätsföreningens siffror från hemsidan.

⁸ Engelskans "Content Delivery Network", på svenska "innehållsleveransnätverk".

⁹ Stiftelsen för telematikens utveckling.

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

Satellitkommunikation

Sverige har ingen egen allmänt tillgänglig konstellation av satelliter för digital kommunikation, som skulle kunna anses vara en del av internets öppna kärna. Det finns en svensk kommersiell satellit i geostationär bana som täcker en tredjedel av planetens yta. Vi är annars beroende av utländska kommersiella tjänster såsom Starlink, Eutelsat och SkyDSL, som primärt riktar sig till civila konsumenter. Därtill saknar Sverige statligt ägda markstationer för kommunikation med satelliter och vi är därmed beroende av markstationer i utlandet.

På EU-nivå pågår projektet för satellitkommunikation *Infrastructure for Resilience, Interconnectivity and Security by Satellite* (IRIS²). IRIS² ska tillhandahålla kommunikationstjänster till EU och dess medlemsstater, privata företag och organisationer, samt EU-medborgare. Det kommer vara anpassat för militära och statliga ändamål (t.ex. säker kommunikation mellan ambassader) och kunna nyttjas vid krishantering och territoriell övervakning. IRIS² implementerar EuroQCI och kommer således nyttja avancerad krypteringsteknologi, inklusive kvantkryptografi, samt ha en secure-by-design-arkitektur för att säkerställa konfidentialiteten i dataöverföringen. IRIS² planeras vara i drift 2030.¹⁰

Den senaste tiden har allt fler leverantörer börjat erbjuda D2D (Direct-to-Device), vilket gör det möjligt för enskilda enheter att direkt ansluta sig till satelliter utan anpassad utrustning. Många stora satellitoperatörer skjuter idag upp ett stort antal satelliter i låg omloppsbana för D2D-tjänster, men dessa har begränsningar vid högre latituder.

Undervattenskablar

Undervattenskablar utgör stommen i det globala internet och transporterar åtminstone 95% av världens datatrafik.¹¹ Undervattenskablar i Östersjön har under de senaste åren varit föremål för misstänkt sabotage av främmande statsaktörer, vilket har aktualiserat deras betydelse för nationell och regional säkerhet. Undervattenskablar ägs av privata företag som ansvarar för drift, underhåll och reparationer. Det råder brist på svenska aktörer med fartyg som kan lägga och reparera undervattenskablar.¹²

EU tillkännagav i början av 2025 en handlingsplan med åtgärder för att stärka el- och telekominfrastruktur under vatten. I den ingår ett initiativ att bygga upp och stärka regionala nav för övervakning av undervattenskablar, vilket syftar till att främja situationsmedvetenhet och detekteringsförmåga.¹³ Regeringen gav under 2025 bland annat MSB, PTS och Kustbevakningen uppdraget att gemensamt vidta åtgärder för att stärka

¹⁰ https://defence-industry-space.ec.europa.eu/iris2-european-commission-awards-concession-contract-spacerise-consortium-2024-10-31_en

¹¹ Se exempelvis *ENISA:s rapport Undersea Cables – What is at stake?*.

¹² <https://www.sjofartstidningen.se/branschen-ett-fartyg-racker-inte/>

¹³ <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025JC0009>

förmågan att upptäcka och rapportera incidenter och störningar på undervattensinfrastruktur. Uppdraget är slutredovisat till regeringskansliet.

Inom ramen för NATO finns initiativet *Baltic Sentry* som, genom ökad militär närvaro i Östersjön, syftar till att bättre kunna skydda kritisk undervattensinfrastruktur. Kustbevakningen utgör operativ kontaktpunkt mot NATO-nätverket *Critical Undersea Infrastructure Network* (CUIN). Nätverket för samman bland annat militära aktörer, civila myndigheter och industripartners i syfte att stärka informationsspridning och samarbetet kring kritisk undervattensinfrastruktur. Kustbevakningens uppdrag genomförs i nära samarbete med Försvarsmakten och samverkan sker med andra myndigheter och privat sektor. NATO har även centret *Maritime Centre for Security of Critical Undersea Infrastructure* som koordinerar insatser mellan NATO-allierade, partners och privat sektor. Sverige har tillsammans med andra länder i Östersjöregionen uttryckt vikten av ökat samarbete kring undervattensinfrastrukturen.¹⁴

DNS

Det finns fler än 1 300 rotserverinstanser över hela världen, vilka förvaltas och utvecklas av tolv organisationer i fyra länder koordinerade av ICANN. I Sverige står en av totalt 13 rotserverar för DNS i världen.

- **DNS Tapir** är ett open source-projekt för integritetssäker analys av DNS-trafikdata. Genom att göra resultaten allmänt tillgängliga syftar projektet till att förbättra DNS-säkerheten för hela samhället. DNS Tapir har erhållit finansiering av PTS och Internetstiftelsen och drivs av representanter från bland annat Edvina AB, Internetstiftelsen, Netnod AB och Sunet.
- **DNS-Labs** är en del av Internetstiftelsen och arbetar med att göra det svenska DNS-systemet säkrare. DNS-Labs består av ett forsknings- och utvecklingsteam som utvecklar nya tekniska lösningar för DNS, engagerar sig i internationellt på området, samt samarbetar med svenska universitet och myndigheter i syfte att främja utvecklingen av och säkerheten kring DNS.

Analys av nulägesbild

Sverige har en överlag välutbyggd internetinfrastruktur som når i princip alla, medborgare såväl som organisationer. Nationella telesamverkansgruppen, med representation från både myndigheter och centrala privata aktörer, ökar förmågan att hantera allvarliga samhällsstörningar genom samordning av berörda parter. Det finns vidare väletablerade nätverk och samverkansföretag för verksamheter som tillhandahåller internetinfrastruktur. Ansvarsförhållandena vad gäller nätens drift, underhåll och reparation i fredstid och ordinära krissituationer är förhållandevis tydliga i ljuset av lagregleringen, ansvarsprincipen och existerande föreskrifter. Den nya cybersäkerhetslagen förväntas vidare förstärka den öppna kärnans motståndskraft ytterligare genom utökad kravställning. Verksamheter som är viktiga för den öppna kärnan kommer att behöva vidta ytterligare säkerhetsåtgärder,

¹⁴ *Joint statement, Nordic and Baltic Ministers of Digitalisation*, publicerat den 20 november 2024 på regeringens hemsida.

rapportera incidenter och informera mottagare av deras tjänster om betydande incidenter och cyberhot som kan påverka dem. Följande allmänna brister har identifierats:

- Ansvarsprincipen är i praktiken otillräcklig för att säkerställa resiliens vid extraordinära situationer, såsom exempelvis krig. Detta för att det är orimligt att förvänta sig att verksamhetsutövaren har förmåga att fullgöra sin verksamhet under så pass radikalt förändrade förutsättningar som sådana situationer kan innebära (även om t.ex. Stadsnätets förenings beredskapsuppdrag i viss mån lindrar den här problematiken).

Trådlös kommunikation

5G- och 4G-näten har hög tillgänglighet i Sverige och den stora mängden basstationer skapar en god redundans i den trådlösa nätinfrastrukturen. 5G-nätets förmåga att hantera en stor mängd uppkopplade enheter gör nätet mindre känsligt för överbelastning. Risken för avbrott i dataöverföringen är således lägre än i tidigare generationers nät. Det är positivt att Telia under perioden förskjuter utfasningen av 2G eftersom många system fortfarande förlitar sig på den tekniken. Följande brister har identifierats:

- Det är en svaghet att basstationer är lätta att identifiera och sabotera av antagonistiska hotaktörer. En konsekvens av detta är att de trådlösa näten kan slås ut i avgränsade områden. Orsaken till detta är att basstationerna är fysisk infrastruktur som måste placeras öppet på allmänt tillgängliga platser för att önskad effekt i näten ska uppnås.

Fiberoptiska kabelnät

Det svenska fibernätet är välutbyggt och når ut till den stora majoriteten av befolkningen, även ute i glesbygderna. Stadsnätets modellen ger ett decentraliserat ansvar där (ofta kommunala) nätägare på lokal och regional nivå väl känner till sina nät och vid behov snabbt kan åtgärda problem. Stadsnätets förenings beredskapsuppdrag bidrar till att den digitala infrastrukturen klarar större påfrestningar till följd av kris och konflikt. Telekombolagen som äger fibernät är flera till antalet (till skillnad från ett stort bolag som har monopolställning på den privata nätägarmarknaden), vilket är en styrka eftersom flera parallella nät och ansvariga nätägare ger högre redundans i infrastrukturen överlag. Branschgemensam certifiering och vägledning för byggnationen av robusta fibernät bidrar till att framtidens nät håller hög standard. Följande brister har identifierats:

- Det är en svaghet att den fiberoptiska nätinfrastrukturen är lätt att identifiera och sabotera av antagonistiska hotaktörer. En konsekvens av detta är att den kan slås ut i avgränsade områden. Orsaken till detta är att fiberoptiska nät är fysisk infrastruktur som måste anläggas på allmänt tillgängliga områden.

Undervattenskablar

Redundansen i den digitala undervattensinfrastrukturen förstärker tillgängligheten i den öppna kärnan i händelse av kabelbrott till följd av olyckor eller uppsåtlig åverkan. Det finns internationella samarbeten inom NATO och EU, samt multilaterala initiativ på olika

Myndigheten för samhällsskydd och beredskap

Postadress:
651 81 Karlstad

Telefon: 0771-240 240
Fax: 010-240 56 00

registrator@msb.se
www.msb.se

Org.nr: 202100-5984

nivåer, vilket bidrar till att förmågan att hantera incidenter och sabotage och skapar resiliens i undervattenskabelsystemet. Följande sårbarheter och brister har identifierats:

- Undervattenskablarnas geografiska utbredning på internationellt vatten utgör en sårbarhet eftersom det underlättar för en antagonistisk hotaktör som vill sabotera infrastrukturen.
- Det råder brist på svenska aktörer som har kapacitet att reparera undervattensinfrastruktur. Detta innebär att det kan ta lång tid att laga kablar om flera skulle kapas parallellt i händelse av konflikt eller krig.

Satellit

IRIS² kommer förbättra tillgängligheten till säkra satellitkommunikationer i hela EU. Systemet kommer dessutom vara anpassat för militära behov och krissituationer för att stärka motståndskraften och tillgängligheten vid extraordinära händelser. En unionsgemensam satellitkonstellation skapar redundans och minskar beroendet av andra aktörer för alternativa kommunikationsmedel vid avbrott i andra delar av den digitala infrastrukturen. Följande brister har identifierats:

- Sverige har en satellit men vi är i hög grad beroende av utländska kommersiella satellittjänster för digital kommunikation. Detta utgör en sårbarhet eftersom utländska kommersiella tjänster kan stängas av till följd av exempelvis politiskt tryck och vi kan således förlora stora delar av förmågan i kristider.
- Sverige saknar statliga markstationer för överföring av data till och från satelliter. Detta gör staten beroende av andra nationers markstationer och övrig infrastruktur för vidareöverföring av datan till Sverige över svenska gränsen.
- De kommersiella satellittjänsterna riktar sig primärt till den civila marknaden och är inte särskilt anpassade för kris- och krigsförhållanden. Detta är en potentiell sårbarhet eftersom kapaciteten i tillgängliga kommersiella tjänster kan visa sig otillräcklig i extraordinära situationer.
- IRIS² beräknas vara i drift och tillgängligt först 2030. Fram till dess är Sverige och EU beroende av kommersiella aktörer (enligt ovan).

DNS

De svenska initiativen DNS Tapir och DNS-Labs bidrar till utvecklingen och säkerheten kring DNS och kan genom sina samarbeten i och utanför Sverige bidra till robustheten och motståndskraften i svensk DNS. Sverige har en rotserver för DNS och har därmed inte något externt beroende för tillgång till listor över auktoritativa namnservrar. Följande brister har identifierats:

- Befintliga säkra DNS-lösningar implementeras inte alltid. Detta gör DNS mer sårbart för angrepp och handhavandefel, vilket kan påverka tillgängligheten i den offentliga kärnan. Orsaken till detta är att säkra DNS-lösningar kan vara kostsamma och komplicerade att införa.