Att märka ut vår mest värdefulla tillgång

Nationell säkerhet i tre EU-länders arbete med tillgängliggörandet av geodata som öppna data

Åsa Davidsson & Alexander Stagnell

FOI-R--5930--SE

Maj 2026

FOI

Åsa Davidsson & Alexander Stagnell

Att märka ut vår mest värdefulla tillgång

Nationell säkerhet i tre EU-länders arbete med tillgängliggörandet av geodata som öppna data

Titel	Att märka ut vår mest värdefulla tillgång – Nationell säkerhet i tre EU-länders arbete med tillgängliggörandet av geodata som öppna data
Title	Marking our most valuable asset – National Security and the Publication of Geodata as Open Data in Three EU Countries
Rapportnr	FOI-R--5930--SE
Månad	Maj
Utgivningsår Antal	2026
sidor	39
ISSN	1650–1942
Uppdragsgivare	Lantmäteriet
Forskningsområde	Övrigt
FoT-område	Inget FoT-område
Projektnr	E13984
Godkänd av	Anders Norén
Ansvarig avdelning	Försvarsanalys

Bild: Gustav II Adolf and His War Council at Würzburg, sketch. Konstnär Robert Wilhelm Ekman. Bild från Wikimedia.

Sammanfattning

Totalförsvarets forskningsinstitut (FOI) har på uppdrag av Lantmäteriet genomfört intervjuer med företrädare för civila och militära myndigheter från Estland, Finland och Tjeckien under 2025 och 2026. Syftet har varit att fördjupa förståelsen av öppna datadirektivets implementering i respektive land samt om länderna utför riskbedömningar innan geodata tillgängliggörs som öppna data.

Studien visar att öppenhet fortfarande är den vägledande principen i alla tre länder, även om samtliga länder bedömer att det finns risker med öppna geodata. I Finland och Tjeckien lyfts nationella säkerhetsrisker medan det i Estland framför allt finns en stor oro för medborgares integritet. En gemensam utmaning är aggregerings-problemet, det vill säga svårigheten att förutse risker som uppstår när olika datamängder kombineras. Tre exempel på riskbedömningsmetoder presenteras, samtliga från Finland.

Studien pekar sammantaget på behovet av förbättrad nationell samordning för att balansera öppna geodata, innovation, transparens och nationell säkerhet. Samtidigt väcker ökade säkerhetsutmaningar frågor om ansvarsfördelningen mellan nationell nivå och EU, samt hur en likvärdig hantering av öppna geodata mellan EU-länder ska kunna uppnås. Studien konstaterar att det finns likheter mellan Sverige och de studerade länderna, det gäller tillvaratagandet av möjligheterna med öppna geodata, men också svårigheterna att bedöma de risker som kan uppstå för nationell säkerhet.

Nyckelord: öppna datadirektivet; geodata; riskbedömning; nationell säkerhet; aggregering; Estland; Finland; Tjeckien

Summary

The Swedish Defence Research Agency (FOI), on behalf of Lantmäteriet, conducted interviews with representatives from the public sector and the armed forces in Estonia, Finland, and Czechia during 2025 and 2026. The aim was to understand if the Open Data Directive has affected the countries and whether risk assessments are carried out before geodata is made available as open data.

This study shows that despite acknowledging risks associated with open geodata, openness remains the guiding principle in all three countries. In Finland and Czechia, national security risks are emphasized, while in Estonia there are significant concerns about citizens' privacy. A shared challenge is of how to predict risks that arise from the combination of different datasets. Three Finnish risk assessment methods are presented.

The study highlights the need for improved national coordination to balance openness, innovation, and national security. Simultaneously, increasing security challenges raise questions about the division of responsibilities between the national level and the EU, and how to achieve consistent handling of open geodata across EU countries. The study points out similarities between Sweden and the countries studied, both in leveraging the opportunities of open geodata and in the challenges of assessing risks related to national security.

Keywords: Open Data Directive; geospatial data; risk assessment; national security; aggregation; Estonia; Finland; Czechia

Innehållsförteckning

1 Inledning

”Mark well the land, it is our most valuable asset.”
George Washington

Sverige har en lång tradition av öppenhet inom det offentliga, mycket på grund av tryckfrihetsförordningens offentlighetsprincip. Möjligheten att ta del av myndigheters, andra offentliga institutioners och folkvaldas arbete utgör dessutom en hörnsten i moderna liberala demokratier med målet att underlätta folkets ansvarsutkrävande gentemot dem som sitter på makten.

De liberala demokratiernas öppenhetsprinciper har på många håll stärkts av de senaste decenniernas digitalisering av samhället.[1] Bakgrunden till detta står att finna i det faktum att de data som produceras av det offentliga i allt högre grad har kommit att bli relevanta för ekonomiska intressen. Enligt EU:s egna siffror har unionens samlade dataekonomi vuxit till omkring 550 miljarder euro 2025, eller från 2,6% till 4% av EU:s totala BNP under de senaste sex åren.[2] För att främja denna växande dataekonomi beslutade Europaparlamentet och EU-rådet gemensamt under 2019 att införa *EU-direktivet (2019/1024) om öppna data och vidareutnyttjande av information från den offentliga sektorn*, hädanefter benämnt som öppna data-direktivet. Med detta direktiv uppfordras medlemsländerna att introducera processer för att alla offentligt producerade data, med vissa undantag, ska publiceras som öppna data.

Med öppna data avses i allmänhet sådana data som har tillgängliggjorts i öppna format och som därmed kan nyttjas och delas fritt av vem som helst för valfritt ändamål.[3] Begreppet introducerades under det nya millenniets första årtionde som en del i en rörelse med det uttalade målet att använda ny teknik för att öka öppenheten inom alla samhällssektorer.[4] Målet var att öppna data skulle bli normen, och att teknikutvecklingen skulle göra det möjligt att inte bara förbättra den demokratiska översynen av det offentliga, utan att detta också skulle ha demokratiserande effekter på de områden där det demokratiska inflytandet fortfarande var marginellt. Inom öppna datarörelsen sågs data i första hand som organiserade och kvantitativa datamängder som kunde processas automatiskt.[5]

---

[1] Ruijer, E. H. J. M., & Martinius, E. (2017). Researching the democratic impact of open government data: A systematic literature review. *Information Polity*, *22*(4), 233-250.
[2] European Commission. (2019). *Building a data economy - Brochure*. https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure [Hämtad 2026-03-09].
[3] Prop. 2021/22:225.
[4] Moon, M. J. (2020). Shifting from Old Open Government to New Open Government: Four Critical Dimensions and Case Illustrations. *Public Performance & Management Review*, *43*(3), 535–559. https://doi.org/10.1080/15309576.2019.1691024.
[5] Public.Resource.Org. (2007). *Open government dataprinciples*. https://public.resource.org/8_principles.html

Det öppna datadirektivet har dock valt att definiera data via det mer omfattande begreppet ’dokument’ vilket därmed också innefattar enskilda fysiska dokument. Breddandet av databegreppet, som också indikeras av direktivets titel, kommer av att öppna databegreppet har förts samman med arbetet att göra information från den offentliga sektorn tillgänglig för användning inom framför allt den privata sektorn. Det senare benämns som vidareutnyttjande. I arbetet att främja vidareutnyttjandet, som sträcker sig tillbaka långt bortom öppna datarörelsen, har transparens vad gäller offentliga data, eller snarare det bredare begreppet offentlig information, kommit att utgöra en hörnsten inom en mängd olika branscher. Detta har dock skapat förvirring när det gäller tillgängliggörandet av data som öppna data. Delvis beror detta på hur det breda databegrepp som unionen har valt att använda sig av för att främja tillväxt ska tolkas, men det handlar också om att det har visat sig att de datamängder som genererar ekonomisk vinst sällan är samma datamängder som möjliggör ett ökat demokratisk deltagande. Studier har exempelvis visat att det främst är datamängder som främjar ekonomiska intressen som har fått förtur.[6]

Ytterligare en utmaning inom öppna dataområdet berör de risker som kommer med ett fritt tillgängliggörande av data insamlade av och om det offentliga. När Sverige inkorporerade öppna datadirektivet genom *lagen (2022:818) om den offentliga sektorns tillgängliggörande av data*, hädanefter benämnd som öppna datalagen, inkluderades i lagen tre fall där offentligt producerade data inte ska publiceras som öppna data. Dessa härrör från öppna datadirektivet som fastställer att handlingar kan undantas publicering med hänvisning till bland annat skydd av nationell eller allmän säkerhet, försvarshemligheter, skydd av personuppgifter samt skydd av kritisk infrastruktur (2019/1024 kap. 1, §2). Inom ramen för den svenska öppna datalagen har öppna datadirektivet således tolkats som att det möjliggör avsteg från öppen publicering av data om det finns risker rörande informationssäkerhet, personlig integritet samt nationell säkerhet (2022:818 kap. 1, 1§).

[6] Broomfield, H. (2023). Where is open data in the Open Data Directive? *Information Polity*, 28(2), 175–188. https://doi.org/10.3233/IP-220053

1.1 Risker med tillgängliggörandet av öppna data

Enligt öppna datalagen ska således alla offentliga aktörer som producerar data ta hänsyn till dessa tre riskkategorier innan data tillgängliggörs som öppna data. Dessutom ska riskbedömningen ta hänsyn till aggregeringsmöjligheterna.[7] Aggregering innebär att kombinera en viss data med data eller information av annat slag för att därigenom extrahera ytterligare information. Det kan också innebära att data från olika tidpunkter kombineras. Det medför att även om en datamängd i sig inte innehåller information som utgör risk för Sveriges säkerhet, kan den leda till risker genom aggregering med annan data.[8] Frågan om vad som potentiellt kan utgöra en risk för Sveriges säkerhet är på många sätt komplex. Inte minst då det bland annat innebär att hänsyn behöver tas till risker som kan uppstå utanför den egna verksamheten. Därmed avviker också riskbedömningar av aggregering från en etablerad tradition inom exempelvis risk- och sårbarhetsanalyser.[9] Det finns, med andra ord, farhågor att ämnets svårgripbara natur, trots att andra åtgärdsmöjligheter finns, leder till att den offentliga sektorn väljer att kraftigt begränsa tillgängligheten till den data som produceras av det offentliga. Den mest långtgående av dessa begränsningar är att data sekretessklassificeras.

Alla inskränkningar av tillgängligheten leder till en konflikt mellan å ena sidan ekonomiska och demokratiska intressen, vilka helst ser att data tillgängliggörs som öppna data i så stor utsträckning som möjligt, och å andra sidan staters och offentliga aktörers intresse av att beakta nationell säkerhet. Därmed finns både farhågor att tillgången av data begränsas för mycket, och att nationella säkerhetsaspekter inte beaktas i tillräckligt hög grad. I skrivande stund har det inte varit möjligt att verifiera något fall där offentliga data publicerade som öppna data har använts i något försök att hota Sveriges säkerhet. Dock kan vissa paralleller gällande potentiella konsekvenser för Sveriges säkerhet dras till de konstateranden som görs i utredningen av den bristande informationssäkerheten och ”den särskilda händelsen” hos Lantmäteriet.[10]

---

[7] Prop. 2021/22:225.

[8] För genomgång av aggregering, se exempelvis Davidsson, Å., Mittermaier, E., Severin, M., Söderman, U., Winterdahl, M., Ciepielewska, M. & Stjernlöf, S. (2025a). *Riskbedömning av geodata vid tillgängliggörande som öppna data*. FOI-R--5745--SE. Totalförsvarets forskningsinstitut, Stockholm.

För exempel på aggregering, se exempelvis Winterdahl, M., Mittermaier, E., Severin, M., During, C., Gunnarson, C. (2023). *Möjliga hot och risker rörande öppna geodata - Redovisning av arbete i en förstudie*. FOI Memo 8296. Totalförsvarets forskningsinstitut, Stockholm.

[9] Davidsson m.fl. (2025a) presenterar en genomgång av vad nationell säkerhet innebär. I samma rapport görs en definition av nationell säkerhet utifrån dess användning av rapportens presenterade riskbedömningsmetod. Vidare beskrivs även komplexiteten med att genomföra riskbedömning av öppna geodata utifrån Sveriges säkerhet.

[10] Regeringskansliet. (2026). *Granskning av Lantmäteriets informationssäkerhet*. Ds 2026:2. Landsbygds- och infrastrukturdepartementet, Stockholm.

Som utredningen konstaterar är konsekvenserna för Sveriges säkerhet svåra att överblicka när det kommer till frågor som berör data, i synnerhet vad gäller aggregering. Detta gäller inte minst vad ett frisläppande av data, oavsett om det var avsikten eller ej, kan innebära på sikt.

Slutligen har också frågor om nationell säkerhet komplicerats av förändringar i relationen mellan den statliga nivån och EU. Medan Lissabonfördraget överlåter den militära och territoriella sidan av nationell säkerhet åt medlemsstaterna (2007/C 306/01, art 3A:2), har utvidgandet av begreppet nationell säkerhet, inte minst genom inkluderingen av exempelvis hybrida hot, gjort att EU i dag ägnar säkerhetsfrågor allt större uppmärksamhet. Detta kan på sikt till och med komma att utmana medlemsländernas syn på suveränitet då de inte längre har full kontroll över hur säkerhetsfrågor relaterade till nationen och dess territorium ska hanteras.[11] Till problematiken ovan bör också adderas det faktum att Rysslands invasion av Ukraina har medfört att hot mot nationell säkerhet och öppna data har fått mer uppmärksamhet än tidigare, vilket fört med sig ett ökat intresse på dessa frågor från det offentliga.[12]

1.2 Geodata

Geospatiala data, eller geodata, utgör ett fält där minskad öppenhet på grund av åtgärder för att försvara Sveriges säkerhet kan få stora konsekvenser. Detta inte minst eftersom en stor del av den data som produceras av det offentliga är av betydelse för exempelvis transportsektorn, livsmedelsproduktionen, skogsindustrin och byggbranschen. Begreppet geodata omfattar all digital information som på något sätt beskriver en företeelse med ett geografiskt läge. Geodata inbegriper således digital information om allt ifrån byggnader, infrastruktur och platser till vattendrag, vegetation och mineraltillgångar. Data om dessa företeelser kan exempelvis komma i form av ortofoto, laserdata och 3D-modeller. Därmed kan geodata användas för bland annat positionering, produktion av kartor, planering av infrastruktur och för livsmedels- och träproduktion. I Sverige tas geodata fram av en rad aktörer inom det offentliga, från kommuner och länsstyrelser till Lantmäteriet och Försvarsmakten.

Under 2023 inledde FOI på uppdrag av Lantmäteriet ett projekt avseende potentiella hot och risker som kan uppstå för Sveriges säkerhet, vid tillgängliggörande av offentligt producerade geodata som öppna data. Detta arbete har bland annat utmynnat i framtagandet av riskscenarier[13] och en metod för riskbedömning av

[11] Wetter Ryde, A. (2025). *EU:s roll om krisen eller kriget kommer – Hur bygger vi gemensam motståndskraft i EU?*. FOI-R--FOI-R--5767--SE. Totalförsvarets forskningsinstitut, Stockholm.

[12] Nikander, J., Jama, T., & Tenkanen, H. (2024). Threats Related to Open Geospatial Data in the Uncertain Geopolitical Environment. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, XLVIII-4/W12-2024, 121–126. https://doi.org/10.5194/isprs-archives-XLVIII-4-W12-2024-121-2024

[13] Winterdahl m.fl. (2023).

öppna geodata med avseende på Sveriges säkerhet, MEGS[14]. En av slutsatserna av projektets tidigare faser identifierade även behovet av att undersöka hur andra länder har påverkats av EU:s öppna datadirektiv i frågor som rör riskbedömningar av öppna geodata i relation till nationell säkerhet.[15] Därför initierades denna undersökning för att identifiera likheter och skillnader i hur offentliga aktörer i tre EU-länder har hanterat potentiella motsättningar mellan öppenhet och nationell säkerhet. Studien som här presenteras är baserad på intervjuer med företrädare för civila och militära myndigheter och departement i Estland, Finland och Tjeckien.

1.3 Syfte

Syftet med denna undersökning är att förstå hur tre EU-medlemsstater arbetar med riskbedömningar av geodata som öppna data, huruvida de har identifierat risker relaterade till nationell säkerhet som härrör från tillgängliggörandet av geodata som öppna data och hur dessa risker i sådana fall har hanterats. Två centrala frågor för studien berör hur ländernas myndigheter arbetar med riskbedömningsmetoder innan tillgängliggörande av geodata som öppna data, och huruvida genomförandet av EU:s öppna datadirektiv har påverkat myndigheternas arbetssätt i frågor som berör öppna geodata och nationell säkerhet.

1.4 Målgrupp

Målgruppen för rapporten är svenska offentliga aktörer som berörs av öppna datalagen. I första hand gäller detta statliga myndigheter som arbetar med tillgängliggörande av geodata. Rapporten kan även vara av intresse för dem som arbetar med metodutveckling inom riskbedömning av öppna geodata med avseende på Sveriges nationella säkerhet.

[14] Davidsson m.fl. (2025a); Davidsson, Å., Mittermaier, E., Severin, M., Söderman, U., Winterdahl, M., Ciepielewska, M. & Stjernlöf, S. (2025b). *Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data - Myndighetsgemensamt arbete*. FOI-R--5768--SE. Totalförsvarets forskningsinstitut, Stockholm.
[15] Davidsson m.fl. (2025a).

2 Metod

Studiens datainsamling, dokumentation och analys genomfördes med omsorg om deltagarnas anonymitet eftersom frågor kopplade till nationell säkerhet kan vara av känslig natur och identiteten hos de personer som arbetar med dessa frågor därmed inte bör röjas. Studien utgår från semistrukturerade intervjuer.

2.1 Urval

Studien inleddes med en övergripande analys av potentiellt intressanta EU-medlemsstater att undersöka. I samråd med Lantmäteriet fastställdes sedan två kriterier för urval: relativ geografisk närhet till de inblandade i kriget i Ukraina samt relativt likartad byråkratisk struktur som Sverige, med exempelvis kommunalt självstyre. I ett första steg kontaktades den svenska försvarsattachén vid beskickningarna i Estland, Finland, Frankrike, Nederländerna, Norge och Tjeckien för att underlätta kontakter med respektive nations lantmäterimyndighet samt försvarsmakt. Med utgångspunkt i studiens omfattning samt lantmäterimyndighetens intresse för geodatafrågor kopplade till nationell säkerhet valdes tre länder ut för fördjupade intervjustudier: Estland, Finland och Tjeckien.

Efter att urvalet hade genomförts kontaktades Lantmäteriets motsvarighet i respektive land. Respektive lantmäterimyndighet tillhandahölls ett informationsbrev innehållande information om studiens utförare (FOI), studiens syfte, intervjuförfarande samt kontaktperson. Informationen användes därefter av respektive lantmäterimyndighet för att identifiera relevanta civila och militära företrädare att intervjua. Genom respektive lantmäterimyndighet bjöds därefter företrädarna för såväl civila som militära myndigheter och departement in för intervjuer (översikt i tabell 1).

Urvalet av myndigheter och departement baserades på respektive lantmäterimyndighets existerande samarbeten på geodataområdet inom såväl den civila som den militära sfären. Det var upp till respektive myndighet att avgöra vilka informanter som var relevanta att inkludera i intervjun. Detta baserades bland annat på informantens ansvarsområden samt den information som myndigheten erhöll innan intervjutillfälle bokades. Alla deltagare hade flerårig erfarenhet från offentligt arbete med geodataproduktion eller tillgängliggörande av geodata som öppna data.

I Estland och i Tjeckien intervjuades endast företrädare för landets lantmäterimyndighet och dess försvarsmakt. I Estland deltog fem personer från lantmäterimyndigheten Maa- Ja Ruumiamet (Styrelsen för land- och spatialutveckling) samt två personer från den estniska försvarsmakten. I Tjeckien deltog en person från lantmäteri- och fastighetsregistermyndigheten Český úřad zeměměřický a katastrální (ČÚZK) samt en person från den tjeckiska republikens väpnade styrkor. Vid intervjuerna i Finland deltog fem personer från Lantmäteriverket, två personer från den finska försvarsmakten, en representant för miljödepartementet, tre representanter från finansdepartementet samt två företrädare för Transport- och kommuni-

kationsverket Traficom. Intervjuerna i Estland genomfördes under januari 2026. Intervjuerna i Finland och Tjeckien genomfördes under oktober 2025.

Tabell 1. Översikt av intervjurepresentanter, per representerad myndighet och land.

Antal deltagare / **Myndighet/Departement**	Estland	Finland	Tjeckien
Lantmäterimyndigheten	5	5	1
Försvarsmakten	2	2	1
Finansdepartementet		3	
Miljödepartementet		1	
Transport- och kommunikationsverket		2	

2.2 Genomförande av intervju

Efter att intervjupersonerna hade identifierats skickades information till de medverkande med uppgifter om projektets syfte och bakgrund, information om samtycke, de teman som intervjun skulle behandla samt några av de frågor som skulle kunna komma att ställas under intervjun.

Innan respektive intervju påbörjades fastställdes informerat samtycke muntligen efter att deltagarna hade fått ta del av information gällande projektets upplägg, genomförande, resultat, samt data- och personuppgiftshantering. Intervjuguiden återfinns i Bilaga A. Samtliga intervjuer inleddes med en öppen fråga om intervjupersonens/-personernas erfarenhet av arbete med geodata i allmänhet och med frågor om nationell säkerhet och öppna data i synnerhet. Frågor ställdes också kring landets historia vad gäller öppna data och nationell säkerhet. Därefter ställdes frågor som berörde följande teman:

- infrastruktur för geodata
- lagstiftning
- risk, hot och aggregering
- riskbedömningsmetod
- framtidsperspektiv

Frågorna som användes under intervjuerna var i första hand formulerade utifrån de slutsatser och identifierade utmaningar som hade lyfts i projektets tidigare rapporter.[16] Intervjuerna spelades in i sin helhet samtidigt som intervjuprotokoll fördes. Intervjuprotokollen användes för att analysera intervjuerna medan inspelningarna gjorde det möjligt att säkerställa anteckningarna.

2.3 Dataanalys

Insamlade intervjudata bearbetades med hjälp av en innehållsanalys. Vi sökte främst efter gemensamma respektive motstridiga föreställningar gällande hur geodata och potentiella risker behandlas i respektive land. Målet var också att teckna en mångsidig bild av den nuvarande situationen, samtidigt som vi önskade fånga eventuella motsättningar såväl inom som mellan offentliga aktörer som arbetar med geodata och nationell säkerhet. I det fall intervjupersonerna tog upp en existerande lag eller publikation som används i arbetet har dessa inkluderats, antingen under intervjun eller i efterhand. Insamlade intervjudata har sedan kodats in under följande sju teman:

- historia
- infrastruktur för geodata
- lagstiftning
- risk, hot och aggregering
- riskbedömning
- åtgärder för begränsningar av öppna data
- framtidsperspektiv

Dessa teman har använts som struktur för analysens presentation.

[16] Winterdahl m.fl. (2023); Davidsson m.fl. (2025a).

3 Erfarenheter från tre EU-länder

Kapitlet redogör för intervjuerna som har genomförts med representanter för civila och militära instanser. Intervjuerna presenteras separat för respektive land – Estland, Finland och Tjeckien – enligt de sju teman som presenterats i föregående avsnitt.

3.1 Estland

Estland är en parlamentarisk republik. Landet består av 79 kommuner och huvudstaden är Tallinn. Ytan utgörs av 45 336 km^2 och landet har en folkmängd om 1 369 995 personer. Estland blev EU-medlem den första maj 2004[17] och trädde in i Nato 2004[18].

3.1.1 Historia

Estland har under sin relativt korta period som självständig nation (sedan 1991) präglats av en strävan mot öppenhet.[19] Den estniska lantmäterimyndigheten, Maa- Ja Ruumiamet, har i och med varje ny teknisk landvinning valt att göra ny och mer detaljerad geodata tillgängliga som öppna data. Då Estland har gjort sig känt som ett av världens mest digitaliserade länder har även lantmäterimyndigheten haft som fokus att inte bara samla in geodata utan att också producera en rad digitala geodataprodukter som är fria att använda för allmänheten. Bland annat lanserades myndighetens första geodataportal redan 1999. Landets *Lag om offentlig information* (RT I 2000, 92, 597) trädde i kraft år 2000 och används fortsatt som en grundpelare i säkerhetsarbetet då den bland annat tillåter att myndigheten begränsar tillgängliggörandet av geodata som öppna data med hänvisning till nationell säkerhet.

I början av det nya millenniet började den estniska försvarsmakten att lägga allt större vikt vid att planera för eventuella kriser och hur den försörjning som krävs för att upprätthålla försvaret skulle säkerställas i kristider. Som ett led i detta arbete valde den estniska försvarsmakten att 2005 inrätta en egen geodatadivision med uppdrag att ta fram kartor åt samtliga försvarsgrenar. Detta beslut grundade sig också i landets Natomedlemskap som krävde andra kartstandarder än vad som var gällande i det civila. Medvetenheten inom den estniska försvarsmakten stärktes än mer i och med Rysslands invasion av Georgien 2008. De började därefter ta ett allt större ansvar för landets potentiellt känsliga geodata då en överväldigande majoritet av geodata som användes av dem producerades av civila myndigheter. Sedan ungefär tio år tillbaka analyserar den estniska försvarsmaktens säkerhetstjänst all geodata som publiceras av den estniska lantmäterimyndigheten i syfte att uppmärksamma

[17] Europeiska unionen. (u.å.a). *Estland*. https://european-union.europa.eu/principles-countries-history/eu-countries/estonia_sv [Hämtad 2026-03-11].
[18] NATO. (2024). *NATO member countries*. https://www.nato.int/en/about-us/organization/nato-member-countries [Hämtad 2026-03-11].
[19] McBride, K., Toots, M., Kalvet, T. & Krimmer, R. (2018). *Leader in e-Government, Laggard in Open Data: Exploring the Case of Estonia.* Revue française d'administration publique, 167(3), 613-625. https://doi.org/10.3917/rfap.167.0613.

myndigheten på geodata som kan innebära en säkerhetsrisk. Detta har bland annat lett till att Maa- Ja Ruumiamet har utvecklat processer för att exempelvis dölja den estniska försvarsmaktens anläggningar på digitala kartor.

Under 2025 införskaffade lantmäterimyndigheten ny utrustning för laserskanning. De nya tekniska möjligheterna – där 3D-modellernas punktdensitet gick från 18 till 80 punkter/m^2 – ledde till en sådan utbredd oro för säkerheten att myndigheten valde att inte publicera nya data innan tydliga regelverk hade utarbetats. Det främsta skälet till oron var dock personlig integritet snarare än nationell säkerhet. Samtidigt har också attacker såsom spoofing[20] mot GNSS gjort det i praktiken omöjligt för myndigheten att flyga med såväl drönare som flygplan i landets östra delar. Detta har under de senaste åren kraftigt begränsat myndighetens möjligheter att bland annat samla in nya ortofoto.

3.1.2 Infrastruktur för geodata

I likhet med Sverige och Finland åtnjuter estniska kommuner långtgående autonomi och självbestämmande, men i jämförelse med de nordiska länderna är de estniska kommunerna relativt små sett till såväl befolkningsmängd som ekonomi. Detta försvagar den formella autonomi som kommunerna besitter och gör dem exempelvis i hög grad beroende av lantmäterimyndighetens insamling av geodata för många av de uppgifter som de förväntas utföra. Detsamma gäller också för landets mer befolkningstäta storstadskommuner samt regeringens olika departement som ofta anlitar myndigheten för att genomföra geodatainsamlingsprojekt. Maa- Ja Ruumiamet producerar därmed en överväldigande majoritet av alla offentligt insamlade geodata i landet.

3.1.3 Lagstiftning

Som redan nämnts är det Estlands *Lag om offentlig information* (RT I 2000, 92, 597) som främst styr hur geodata tillgängliggörs. Lagen kom till för att garantera befolkningens tillgång till offentlig information från myndigheter och övriga offentligt finansierade verksamheter. Målet var att säkerställa ett demokratiskt och öppet land med möjligheter att övervaka hur den offentliga byråkratin och makten utför sina uppgifter. Lagen tar även upp giltiga skäl för sekretessklassificering av information, däribland möjligheten att neka tillgång till information vars utlämnande hotar det nationella försvaret eller den nationella säkerheten. Enligt civila och militära representanter har undantaget främst använts för att sekretessbelägga eller genomföra mitigerande åtgärder (såsom att minska detaljeringsgraden hos geodata) för kartor och foton som avbildar den estniska försvarsmaktens områden. Åtgärderna har också i första hand genomförts på direkt begäran från landets försvarsmakt. Under de senaste åren har även andra departement börjat begära att lantmäterimyndigheten inte ska publicera geodata som relaterar till verksamheter som faller inom respektive departements område. Begäran kommer ofta

[20] Det svenska ordet för spoofing är vilseledning och avser en signal med falsk information.

ursprungligen från en statlig myndighet eller offentlig institution. Detta, tillsammans med det hot mot personlig integritet som teknikutvecklingen anses utgöra, ledde också till att myndigheten under 2025 valde att inte publicera några nyinsamlade data utan att först få till stånd ett nytt regelverk gällande publiceringen av geodata som öppna data. Den estniska försvarsmaktens representanter menar att myndigheten för tillfället saknar stöd i lagen för att kräva begränsningar hos privata aktörer. Detta har lett till en situation där exempelvis ett militärt område avbildas med lägre upplösning i det estniska lantmäteriets karttjänst, medan samma område kan återfinnas avbildat med full upplösning i öppna tjänster tillhandahållna av privata aktörer.

Till skillnad från i Sverige, där spridningstillstånd från Lantmäteriet krävs för den som vill publicera eller på annat sätt sprida data från registreringar inhämtade med hjälp av luftfarkoster, saknar Estland denna typ av regler. Det krävs inget tillstånd, vare sig för att ta foton eller för att sprida dem. Trots detta kontaktar vissa utländska företag den estniska försvarsmakten i syfte att meddela sina intentioner att samla in och publicera geodata. Därmed har också den estniska försvarsmakten noterat ett växande intresse för att samla in data om Estland. Tillsammans med berörda myndigheter har den estniska försvarsmakten fört fram önskemål till regeringen om att införa någon typ av insamlings- eller spridningstillstånd som ska gälla för såväl privata som offentliga aktörer i landet.

3.1.4 Risk, hot och aggregering

De civila och militära representanterna menar att det sedan Rysslands invasion av Georgien 2008 har funnits en medvetenhet om risker relaterade till geodata i det estniska samhället. Denna medvetenhet stärktes ytterligare under 2014 och 2022 till följd av Rysslands anfallskrig mot Ukraina. Arbetet med att genomföra riskbedömningar och vidta åtgärder har i första hand legat på landets försvarsmakt.

Estniska lantmäterimyndigheten menar att den för närvarande mest akuta frågan gällande öppna geodata i Estland berör personlig integritet. Ett exempel på detta är den skrivelse från landets justitiekansler som myndigheten mottog under 2025. Skrivelsen innehöll kritik mot att myndighetens olika geodataprodukter erbjuder både upplösningskvalitet och uppdateringsfrekvens som potentiellt möjliggör omfattande intrång i privatlivet hos enskilda medborgare. Justitiekanslerns skrivelse framhöll därför behovet av att myndigheten inför tre nya säkerhetsåtgärder för att säkra den personliga integriteten: i) begränsa upplösningen, ii) fördröja publiceringen av nyproducerade data, och iii) införa autentiseringsprocedurer. Uppmärksamheten för frågan har också lett till att myndigheten under de senaste åren fått in en ökad mängd förfrågningar från allmänheten om att dölja framför allt privatägda hus och tomter på digitala karttjänster. För tillfället finns dock inte legala möjligheter för myndigheten att genomföra detta, vilket har lett till att sådana förfrågningar har avslagits.

Från myndighetens sida framhålls i nuläget personlig integritet snarare än nationell säkerhet som den största utmaningen för framtidens teknikutveckling på området. En av anledningarna är att informanterna anser att den existerande tekniska nivån redan erbjuder en tillräcklig detaljrikedom för att en antagonistisk stat ska ha möjlighet att planera eventuella attacker. Därför menar de att högre upplösning och ökad uppdateringsfrekvens främst är någonting som bör analyseras ur ett integritetsperspektiv. Samtidigt uttrycks också en oro för att de föreslagna åtgärderna (framför allt att senarelägga publiceringen av nyproducerade data) skulle kunna leda till att aktörer istället väljer privata alternativ och på så sätt ändå kringgår eventuella regler som införs.

3.1.5 Riskbedömning

I och med att den estniska lantmäterimyndigheten under 2025 upphörde med att omedelbart publicera nyproducerade laserdata (LiDAR) som öppna data, menar representanterna att det har uppstått en situation där myndigheten måste utreda och svara på ett större antal förfrågningar om att få ta del av insamlade data. Utredningarna görs i samverkan med myndighetens juridiska avdelning, men myndigheten saknar en särskilt utvecklad metod eller process för riskbedömning.

Det saknas också samordning på en högre nivå gällande bedömning av geodata vid tillgängliggörandet som öppna data. Företrädare för såväl Estlands försvarsmakt som civila myndighet uttrycker att arbetet idag sker lokalt, att olika aktörer har sina egna processer och kriterier samt att landet är i behov av en gemensam och samordnad strategi vad gäller dessa frågor. Den estniska försvarsmakten och berörda myndigheter har nyligen gått samman och önskat tydligare reglering från regeringen. Företrädare lyfter även behovet av samordning på EU-nivå gällande frågan.

3.1.6 Åtgärder för begränsning av öppna data

I en strävan efter att ligga i framkant framhåller representanterna att Maa- Ja Ruumiamet tar som sin utgångspunkt att myndigheten alltid ska försöka samla in så många och så högkvalitativa geodata som möjligt samt att göra dessa tillgängliga öppet. Det ska sedan vara upp till departementen och övriga myndigheter att begränsa lantmäterimyndighetens spridning av dessa geodata med hänvisning till exempelvis nationell säkerhet eller personlig integritet. Detta handlar främst om att myndigheten inte anser sig besitta den specialistkunskap som krävs för att genomföra nödvändiga riskbedömningar inklusive bedöma aggregeringsmöjligheter.

Det faktum att Estlands försvarsmakt har huvudansvaret för frågor om nationell säkerhet skapar också en situation där civila myndigheter inväntar besked från dem om åtgärder ska vidtas inför publicerandet av nyproducerade geodata som öppna data. I dagsläget finns därför en upparbetad struktur där landets försvarsmakt inkommer med begränsningar inför att lantmäterimyndigheten påbörjar sina årliga flygningar för ortofoto och laserskanning.

3.1.7 Framtidsperspektiv

Inför framtiden ämnar den estniska lantmäterimyndigheten formalisera och utveckla sitt arbetssätt med att riskbedöma utlämnandet av geodata. Det anses vara nödvändigt, inte minst om myndigheten fortsatt stoppar all publicering av nyproducerade geodata i väntan på reglering från departementet. Fokus ligger dock främst på frågor som berör personlig integritet. Respondenterna exemplifierar med att det finns händelser där mer detaljerade geodata gör det möjligt för bedragare att vara mer specifika i sina bedrägeriförsök. Respondenterna uttrycker också en oro över att öppna geodata kan komma att användas i aggressiva marknadsföringskampanjer. Detta gäller inte minst de 3D-modeller som myndigheten har börjat skapa med hjälp av mer detaljerade laserskanningsdata. I samband med detta har också frågor om nationell säkerhet lyfts och lämnats vidare till den estniska försvarsmakten.

3.2 Finland

Finland är en parlamentarisk republik. Landet består av 309 kommuner och huvudstaden är Helsingfors. Ytan utgörs av 338 363 km^2 och landet har en folkmängd om 5 635 971 personer. Finland blev EU-medlem den första januari 1995[21] och trädde in i Nato 2023[22].

3.2.1 Historia

Finland beskrivs ofta som en föregångare vad gäller offentlig transparens och öppna data. Exempelvis har landet sedan nittiotalet haft en mycket långtgående lagstiftning på området, *Lag om offentlighet i myndigheternas verksamhet* (621/1999), vilken föreskriver myndigheterna omfattande skyldigheter att främja tillgång till information. Denna lagstiftning kompletterades 2019 med en mer specifik lagstiftning kring publiceringen av öppna data (712/2021). Mycket av Lantmäteriverkets data var avgiftsbelagd fram till 2012, då majoriteten av myndighetens topografiska data, kartor och ortofoton tillgängliggjordes samt avgiftsbefriades. Geodata som har tillgängliggjorts som öppna data har från och med 2012 också riskbedömts via en omfattande process. I utarbetandet av denna process tog Lantmäteriverket bland annat hjälp av den finska försvarsmakten för att utveckla en modell för riskbedömningar. Det fanns flera anledningar till att öppna data blev en viktig fråga i landet under den här perioden. Det fanns en stark politisk vilja till öppenhet och en idé om att ett öppet delande av data som hade tagits fram av det offentliga, skulle effektivisera dataanvändningen inom såväl offentliga som privata verksamheter. Dessutom fanns det anledningar som var direkt kopplade till Lantmäteriverkets uppdrag. Lantmäteriverkets tid upptogs där och då i hög grad av att administrera de licenser som datahanteringen krävde. Därutöver fanns det inom myndigheten en stark oro att

[21] Europeiska unionen. (u.å.b). *Finland*. https://european-union.europa.eu/principles-countries-history/eu-countries/finland_sv [Hämtad 2026-03-11].
[22] NATO. (2024).

offentliga aktörer skulle börja att använda gratiskartor av lägre kvalitet om myndigheten hade fortsatt att ta ut avgifter för geodata och geodataprodukter.

Företrädare för en rad finska myndigheter samt för landets försvarsmakt framhåller en medvetenhet inom såväl politiken som offentligheten om att krig återigen kan drabba landet. Flera av informanterna noterade att befolkningen fortfarande bär ett historiskt minne av krig, någonting som man menar syns i dess stöd för försvarsstärkande åtgärder, även om dessa kan ha negativa effekter på andra samhällssektorer.

3.2.2 Infrastruktur för geodata

Det finska finansdepartementet har under ett antal år drivit ett projekt på nationell nivå som berör det offentligas arbete med risker kopplade till öppna data, inklusive geodata. Departementet kan dock inte erbjuda kommunerna mer än rekommendationer, eftersom det i sådana fall skulle innebära att departementet tar över ansvaret för kommunernas hantering av sina data. En informant beskriver att det är en av anledningarna till att de driver en process för att hjälpa kommunerna i landet att själva utveckla sitt säkerhetsarbete gällande datahantering. Ytterligare anledningar till att kommunerna ska utveckla sitt eget säkerhetsarbete är den totala autonomi som kommunerna åtnjuter vad gäller stadsplanering samt de stora skillnader som finns mellan kommunerna. Dessa skillnader går i hög grad att förklara utifrån kommunernas storlek och ekonomiska förutsättningar, och att få stöd i processen kan inte minst vara av nytta i de fall då en mindre kommun får in många förfrågningar om att lämna ut geodata. Sådana situationer har också lett till att vissa kommuner ibland valt att avpublicera alla öppna geodata, medan andra har valt att fullt tillgängliggöra sina öppna data.

Ett flertal intervjupersoner framhöll att det finska systemet i hög grad är beroende av informella kontakter mellan offentliga aktörer, inte minst mellan myndigheter och departement. Samtidigt tillskriver systemet varje aktör en hög grad av autonomi, vilket gör att slutgiltiga beslut rörande exempelvis säkerhetsåtgärder och -praktiker samt riskbedömningar alltid ligger hos det enskilda samhällsorganet. I avsaknad av direkta styrningsmöjligheter försöker såväl Lantmäteriverket som Finansministeriet att hjälpa de offentliga aktörerna genom att utveckla nationella rekommendationer och riskprocesser. Den finska försvarsmakten spelar en viktig roll i framtagandet av dessa rekommendationer.

3.2.3 Lagstiftning

I Finland regleras öppna data i första hand av *Lag om offentlighet i myndigheternas verksamhet* (621/1999) samt *Lag om vidareutnyttjande av data som innehas av företag som producerar vissa allmännyttiga tjänster* (712/2021). Den förstnämnda lagen fastställer en rad omständigheter under vilka handlingar kan sekretessbeläggas, bland annat omfattar dessa handlingar som rör skyddsarrangemang för byggnader och inrättningar samt den finska försvarsmaktens verksamheter. Myndigheter och

departement har valt att tolka lagen på ett sätt som gör att geodata innefattas i denna lagstiftning vilket gör det möjligt att begränsa publiceringen av, eller modifiera vissa typer av geodata som öppna data. Lagstiftningen i Finland har dock varit ämnad att i mesta möjliga mån göra offentligt producerade data tillgängliga som öppna data. Flera myndigheter menar att det är en intention som kraftigt har reducerat möjligheterna att begränsa tillgängliggörandet av offentliga data som öppna data. Sedan 2024 pågår ett arbete med att revidera *Lag om offentlighet i myndigheternas verksamhet*. Revideringen görs för att anpassa lagen till dagens behov, bland annat för att i högre grad anpassa lagen till digitala data.

3.2.4 Risk, hot och aggregering

Lantmäteriverket har sedan ett knappt decennium tillbaka sett en ökning av incidenter relaterat till geodata och geodatasystem, med allt ifrån systematisk insamling av öppna geodata till så kallad spoofing av globala satellitnavigeringssystem, GNSS. Aggregering av data lyfts också fram som ytterst problematiskt av samtliga intervjupersoner då det i princip är omöjligt att bedöma vilka aggregeringar som kan ske samt potentiella följdeffekter. Ett exempel på en utmaning är att olika ortofoton kan avslöja lokalisering av transformatorstationer. Tillsammans med insamling av information från andra källor, såsom Google Street View samt källor för namn och telefonnummer, kan modelleringar göras för att skapa underlag för en eventuell antagonistisk handling.

Det ökande antalet incidenter ledde till att Lantmäteriverket initierade ett mer omfattande säkerhetsarbete med bland annat träning och säkerhetsprövning av personalen. Myndigheten tog också hjälp av ett universitet för att utveckla en riskbedömningsprocess med förhoppningen att en utomstående part skulle bidra till att Lantmäteriverket varken över- eller underreagerade på den förändrade hotsituationen. Tillsammans med försvarsdepartementet har Lantmäteriverket dessutom under samma tidsperiod successivt växlat upp arbetet med att öka säkerhetsmedvetenheten hos övriga offentliga institutioner. Från Lantmäteriverkets sida framhålls också att man idag kan se stora förbättringar på området jämfört med för tio år sedan.

3.2.5 Riskbedömning

Det finns en samsyn mellan finska försvarsmaktens och civila myndigheters representanter vad gäller såväl samarbetsformer som ansvarsområden och framtidsutsikter. Det finns också överlag en gemensam syn på att lagändringar och försök att begränsa tillgängliggörandet av geodata som öppna data inte är den viktigaste vägen framåt, då mycket data redan finns tillgängliga eller kan införskaffas via andra kanaler än via offentliga aktörer.

Finlands försvarsmakt agerar i första hand i en rådgivande funktion till de civila myndigheterna. Dessutom har de deltagit i framtagandet av existerande modeller och instruktioner för riskbedömning samt bidrar med expertkunskap när den efterfrågas.

Den finska försvarsmakten mottar också all geodata som används militärt från de civila myndigheterna.

De finska myndigheterna utför ett omfattande arbete med att utveckla riskbedömningsmetoder och med att genomföra riskbedömningar av data innan de tillgängliggörs som öppna data. Nedan presenteras Lantmäteriverkets, Finansministeriets och Miljöministeriet respektive arbetssätt med riskbedömning av geodata.

3.2.5.1 Lantmäteriverket

Sedan 2012 har Lantmäteriverket riskbedömt geodata i och med att de flesta av Lantmäteriverkets topografiska data, kartor och ortofoton gjordes tillgängliga som öppna data i enlighet med nuvarande lagstiftning. Detta har skett i nära samarbete med Försvarsmakten. Sedan 2012 görs en uppdelning i tre kategorier för Lantmäteriverkets laserdata: öppna, publika och begränsade data. Detta är ett sätt att bemöta potentiella hot där öppna data används[23] och illustrerar ett alternativ till sekretessklassning. Dessa förklaras nedan.

I kategoriseringen av laserdata gäller den första kategorin, öppna data, avgiftsfria nationella laserdata med punktdensiteten 0,5 mätpunkter per m^2 i öppen terräng.[24] För att få tillgång till dessa öppna data kräver systemet endast att användaren uppger en e-postadress. Den andra kategorin, publika data, är tillgängliga för personer med finsk id-legitimation. Denna kategori omfattar nationella laserdata med punktdensiteten 5 mätpunkter per m^2 i öppen terräng. För att få tillgång till dessa data måste en användare även avlägga en mindre avgift och acceptera systemets användarvillkor.[25] Användarvillkoren inbegriper bland annat att data inte ska laddas ner utanför Finland. Det är även möjligt för myndigheten att i systemet övervaka vad som laddas ner och av vem. Under 2026 kommer det bli möjligt att som publika data ta del av punktdensiteten 20 mätpunkter per m^2 i öppen terräng. Den tredje kategorin, begränsade data, avser bland annat myndighetsdata samt sekretessklassificerade data.

De kommuner som producerar egna laserdata ger i vissa fall ut mer detaljerade data än Lantmäteriverket. Kommunerna är dock medvetna om att detta arbetssätt kommer med vissa risker varpå efterfrågan finns om stöd från myndigheten för att avgöra om detaljerade data kan göras tillgängliga som öppna data.

Under 2025 införde Lantmäteriverket en ny riskbedömningsmetod som stöd för bedömningen av geodata som öppna data. Metoden baseras på en högskoleingenjörs

[23] Nikander, J. Jama, T. & Tenkanen H. (2023). *Selvitys Maanmittauslaitoksen avoimiin peruspaikkatietoihin liittyvistä uhkista*. Aalto-yliopisto.

[24] I skogklädd terräng kan punktätheten vara högre. Lasermätpunkter återfinns normalt både i träd och på marken och antalet mätpunkter inom en m^2 kan i genomsnitt bli fler än 0,5 stycken.

[25] National Land Survey of Finland. (u.å.). *Laser scanning data 5 p terms of use*. https://www.maanmittauslaitos.fi/en/laser-skanning-data/terms-of-use [Hämtad 2026-02-25].

uppsats[26] från samma år. I stort handlar metoden om att bedöma risker *och* möjligheter med en datamängd, eftersom dessa anses vara sammanlänkade då datamängder kan orsaka risker men också generera möjligheter. Risk i detta sammanhang likställs med konsekvenser. En risk kan vara någonting negativt som inträffar till följd av att data tillgängliggörs. Risken kan även vara något positivt som *inte* realiseras, alltså att en möjlighet förhindras i och med att data inte tillgängliggörs. Med andra ord innebär det att riskbedömningen ska utröna om konsekvenser *kan uppstå* om data tillgängliggörs *samt* om möjligheter kan gå förlorade om data *inte* tillgängliggörs. Exempel på möjligheter som data kan generera är tekniska innovationer. Skalan för potentiella risker är bred och inkluderar alltifrån hot mot nationens säkerhet till att exempelvis en ambulans inte får korrekt färdriktning vid en utryckning.

För att göra en bedömning av risker och möjligheter används fem kategorier: byggnader och strukturer, transport, terräng och markanvändning, hydrografi samt kabel- och specialanvändningszoner. Kategorierna bedöms genom fem kriterier som även dessa är identiska för både risk- och möjlighetsvariablerna: integritet, tillgänglighet, regional påverkan, geometrisk information samt attributinformation.[27]

Metoden poängterar även aggregeringsaspekten. Dock finns det inte någon universallösning för hur aggregering ska inkluderas utan metoden lyfter endast att aggregering ska beaktas. Det är därför upp till den som utför riskbedömningen att reflektera kring aggregeringsmöjligheter.

Resultatet från metoden blir ett slags risk-möjlighets-index, alltså en jämförelse mellan risk och möjlighet. Jämförelsen kan visualiseras med hjälp av en matris där risknivån sätts ut på ena axeln, och möjlighetsnivån sätts ut på den andra. Genom denna jämförelse kan det sedan göras en bedömning av om en risk är acceptabel med tanke på de möjligheter som en öppen datamängd skulle kunna generera. Informanterna påpekar att i majoriteten av fallen är det möjligheterna som överväger, trots att risker existerar. Fördelen med att använda en strukturerad metod samt möjligheten att visualisera risk- och möjlighetsaspekter är, enligt informanterna, att den ger ett välgrundat underlag som underlättar redogörelsen för en bedömning.

Metoden används både på nyproducerade data som ska tillgängliggöras och på data som redan är tillgängliggjorda. Vidare upprepas bedömningen om det sker förändringar eller uppdateringar i en redan bedömd datamängd.

[26] Mokhtari, A. (2025). *Menetelmä Maanmittauslaitoksen paikkatietoaineistojen riskienarviointiin*. Metropolia Ammattikorkeakoulu.

[27] För närmare beskrivning av kategorier och kriterier, se Mokhtari. (2025).

3.2.5.2 Finansministeriet

Finansministeriet arbetar med ett projekt gällande bedömning av öppna data som berör kritisk infrastruktur och potentiell risk för nationell säkerhet. Projektet sker i samverkan med flera myndigheter, departement och kommuner, där bland annat uppgiften att arbeta fram en riskbedömningsmodell ingår. Riskbedömningsmodellen ska stötta aktörer i att bedöma öppna data relaterade till kritisk infrastruktur med relevans för nationell säkerhet. I samma projekt ingår också att arbeta fram riktlinjer för bedömning av öppna data. Preliminärt kommer projektet att vara färdigt under 2026.

Riskbedömningsmodellen är en del i en större helhet som utgör en riskhanteringsprocess för spatiala data, vilken publicerades 2024.[28] Processen består av fem områden: i) definition av verksamhetsmiljön, ii) riskbedömning, iii) definition av publiceringsprinciper, iv) publicering av data och v) användning och hantering av data samt bedömning av avvikelser. I det andra steget, riskbedömning, ska hänsyn tas till både risk *och* möjligheter relaterade till öppet tillgängliga data.

Vid bedömning av geodata enligt modellen ska särskild hänsyn tas till kritisk infrastruktur och till andra funktioner av särskild betydelse för samhället. I detta sammanhang definieras kritisk infrastruktur som grundläggande strukturer, tjänster och relaterade funktioner som är avgörande för att upprätthålla samhällets vitala funktioner. Kritisk infrastruktur omfattar både fysiska anläggningar och strukturer samt digitala funktioner och tjänster. Exempel på kritisk infrastruktur är vatten- och avfallshantering samt energiproduktion.[29]

En del av modellen handlar om att hitta de frågor som behöver ställas för att identifiera data vars öppna tillgängliggörande kan leda till hot mot nationens säkerhet. Till exempel ska användaren av modellen identifiera ytterligare information om vad en identifierad risk i praktiken innebär och hur denna risk kan avvärjas. Framför allt handlar det om att modellen ska skapa en känsla av trygghet för bedömaren då motstrategier för identifierade risker ska skrivas fram.

Trots att kommunerna efterfrågar listor på data som bör skyddas, har Finansministeriet valt att skapa en modell som aktören själv kan använda. Anledningen till detta är att departementet anser att listor riskerar att behandlas som ett facit eller som en lag för vad som ska vara öppet eller ej, en situation som intervjupersonerna säger sig vilja undvika. En riskbedömningsmodell kan även hjälpa till att skapa en balans mellan öppna och sekretessklassade data, för att på så sätt värna transparens och demokratiska värden, utöver de möjligheter som öppna data medför i form av innovationsmöjligheter. Ännu en anledning att verka för införandet av en modell är att samma modell ska kunna användas på lokal och regional nivå, för att sedan

[28] Modellen samt förslag på åtgärder presenteras i promemoria: Finansministeriet. (2024). *Paikkatiedon kansallisen riskiarvion työryhmän muistio (julkinen)*. Finansministeriet, Helsingfors.
[29] Finansministeriet. (2024).

kunna utgöra en grund för en nationell översikt av de potentiella risker som finns kopplade till öppna geodata.

En del i projektet har bestått av en pilotstudie som genomfördes med 290 av landets 308 kommuner. Kommunerna mottog ett brev med information och en enkät som uppmuntrade varje kommun till att göra riskbedömningar av all sin öppna data, inklusive geodata. Enkäten rörde dock generell risk och inte bara nationell säkerhet. Av 290 tillfrågade kommuner svarade 70 stycken. De områden som rapporterades ha högst risk i relation till öppna data återfanns inom sektorerna vattenförsörjning, digital infrastruktur och energi. Hela 65 av 70 kommuner ansåg att störningar i vattenförsörjningen var den mest signifikanta risken. Senare genomfördes ytterligare en studie[30] med fem städer av olika storlek och geografisk fördelning för att fördjupa förståelsen av riskbedömning av öppna data som är relevanta för vattenförsörjning.

3.2.5.3 Miljöministeriet

Miljöministeriet riskbedömer miljörelaterade data som ska tillgängliggöras som öppna data. En anledning till att riskbedömningar har blivit en viktig fråga på departementet är att miljödata numera ska vara digital för att vara tillgänglig på nationell nivå. Detta har lett till ett omfattande arbete med såväl insamling av ny data som omvandling av analoga till digitala data. Miljöministeriet anser att miljödata generellt sett inte utgör risker för nationell säkerhet. Dock problematiserar informanten detta genom att peka ut att data som samlas på nationell nivå kan skapa ytterligare risker på grund av aggregering. Samtidigt finns det även en stor efterfrågan på specifika riktlinjer från kommunerna vad gäller miljörelaterade geodata. Dessa tillhandahålls inte av Miljöministeriet.

Ett arbete pågår hos Miljöministeriet för att formulera en gemensam förståelse av vilka data som ska vara öppna. En grundregel är att data som härrör från områden under mark inte ska vara tillgängliga för allmänheten. Arbetet följer inte en strukturerad metod utan är istället utformat som diskussionsmöten där olika kompetenser från exempelvis den finska säkerhetspolisen och landets försvarsmakt samlas. På mötena samlas människor med god fantasi, kunskaper om geografiska informationssystem (GIS) och nationell säkerhet, samt med god förståelse av både risker och möjligheter med öppna data. En sådan gruppsammansättning gör det möjligt att genomföra riskbedömningar av en datamängd. Dock kan det vara komplicerat med en sådan konstellation av personer och kompetenser eftersom olika bakgrund och preferenser kan leda till att risker bedöms olika. Dessutom skiljer sig risktoleransen åt mellan deltagarna. En lärdom som har dragits av detta arbetssätt är att det bör ingå ett lärandeperspektiv där deltagarna strävar mot att förstå varandra och varandras utgångspunkter. Under dessa möten bedöms respektive datamängd utifrån risk, sannolikhet och effekt. Informanten poängterar att det är viktigt att beskriva

[30] För ytterligare beskrivning av genomförd studie, se Finansministeriet. (2025). *Kriittisen infrastruktuurin tietojen avoin jakaminen arvioidaan uudelleen huomioiden kansallinen turvallisuus*. Finansministeriet, Helsingfors.

bedömningen med hög detaljrikedom för att på så sätt kunna motivera varför och hur ett beslut om öppna data och potentiell risk har tagits.

Informanten lyfter även vikten av att deltagarna måste acceptera att viss risk kvarstår efter dessa riskbedömningar, då det inte är möjligt att förhindra eller förutse alla risker. I bedömningen handlar det om att avgöra vilken betydelse respektive aktörs egna datamängder har för att kunna avgöra hur risken kan minskas.

Vid riskbedömning av en datamängd tas även hänsyn till data som redan finns öppna via andra källor. Informanten ansåg att aggregeringsfrågan är komplex och att det finns stora svårigheter med att identifiera risker utifrån de oändliga aggregerings-möjligheterna.

Den data som tillgängliggörs som öppna data kräver ingen inloggning. Det är dock möjligt med övervakning av IP-adresser och loggning av vilka data som laddas ner. Enligt informanten finns det exempel på incidenter där stora mängder nerladdningar av data har skett, men det finns en oklarhet rörande vilka åtgärder som ska vidtas mot sådana situationer, samt vad som ska ses som misstänkt beteende och som därmed kräver ytterligare utredning.

Utöver öppna data finns myndighetsinloggningar där personer som arbetar med miljörelaterade frågor kan komma åt ytterligare data. Myndighetsdata och öppna data är placerade på olika servrar för att öka säkerheten.

3.2.6 Åtgärder för begränsning av öppna data

Lantmäteriverket har, som tidigare nämnts, valt att klassificera laserdata i tre kategorier: öppna, publika och begränsade data. Mellansteget – publika data – tillåter myndigheterna att inkludera ett antal säkerhetsåtgärder vid tillgängliggörandet, såsom identitetskontroller och användarvillkor. Denna praktik är ännu inte explicit reglerad i finsk lag, och kan därför kräva avgörande i domstol (praxis). En fråga som den omarbetade offentlighetslagen ska ta sig an är kommunernas önskan om större möjligheter att klassificera eller begränsa tillgången till öppna data. Flera myndighetsföreträdare menar dock att det redan i gällande lag finns utrymme för denna typ av åtgärder, men att kommunerna fruktar att de ska dras inför rätta om det uppstår tvister kring hur lagen ska tolkas. Överlag framhåller dock alla informanter, oavsett tillhörighet, att det finns en stark övertygelse hos offentliga aktörer att offentligt producerade data i så hög grad som möjligt ska tillgängliggöras som öppna data.

Gällande frågan om åtgärder menar flera informanter att begränsningar av data, såsom att dölja områden eller att sekretessklassa geodata, endast minskar risken i ett antal specifika fall. Detta då en stor del av den geodata som produceras, även sådant som i vissa fall borde ha sekretessklassats, i dag kan införskaffas från privata aktörer. Flera informanter framhåller därför att exempelvis försöken att skydda kritisk infrastruktur ovan jord genom att dölja associerade data på ortofoton, karttjänster eller satellitbilder snarare skapar fler problem och utmaningar. De ser därför att man i första hand bör arbeta med fysiskt skydd snarare än sekretessklassning, ett

förhållningssätt som också ofta motiveras med utgångspunkt i bevarandet av demokratiska värden såsom öppenhet och transparens. Det framkommer också att flera aktörer som har ansökt om att få begränsa tillgången till vissa data, ofta drar tillbaka sina ansökningar när den ansvariga myndigheten förklarar att en sådan åtgärd i flertalet fall gör det lättare att exempelvis lokalisera kritisk infrastruktur.

3.2.7 Framtidsperspektiv

Arbetet med att anpassa nuvarande lagar som berör öppna data fortsätter, samtidigt som myndigheter och departement försöker stödja kommunernas arbete med att ta fram processer för att riskbedöma öppna geodata. Finska myndigheter undersöker även andra sätt att skydda bland annat kritisk infrastruktur utöver att införa åtgärder på geodata såsom sekretessklassning. Myndigheterna upplever också ett stort stöd hos allmänheten för sitt arbete, och ännu har inga direkta protester hörts mot redan genomförda begränsningar såsom exempelvis i fallet med publika laserdata.

3.3 Tjeckien

Tjeckien bildades vid delning av Tjeckoslovakien 1993 och är en parlamentarisk republik. Landet utgörs av 14 regioner och huvudstaden är Prag. Ytan består av 78 871 km^2 och landet har en folkmängd om 10 909 500 personer. Tjeckien blev EU-medlem den första maj 2004[31]och trädde in i Nato 1999[32].

3.3.1 Historia

Berlinmurens fall och den liberalisering som skedde i landet under 1990-talet har i mycket hög grad format Tjeckiens inställning till att tillgängliggöra data som öppna data. Denna utveckling har därmed också präglat det offentligas arbete med geodata. Efter att under lång tid ha tillåtit militären att hemligstämpla alla kartor – tillsammans med underliggande geodata – har landet sedan självständigheten 1993 lagt stor vikt vid öppenhet och transparens gällande geodata.

3.3.2 Infrastruktur för geodata

Tjeckiens kommuner är i stor utsträckning självstyrande. Trots detta är det vid sidan av privata aktörer främst det tjeckiska lantmäteriet (ČÚZK) som genomför insamling och produktion av nya geodata samt tillhandahåller dem som öppna data via sin geodataportal Digital Technical Maps. Vissa storstadskommuner, framför allt Prag, erbjuder egna geodataportaler, karttjänster och andra produkter baserade på geodata, men en stor del av underliggande grunddata hämtas från ČÚZK:s nationella databas.

[31] Europeiska unionen. (u.å.c). *Tjeckien*. https://european-union.europa.eu/principles-countries-history/eu-countries/czechia_sv [Hämtad 2026-03-11].
[32] NATO. (2024).

Lantmäterimyndigheten använder sig också av privata underleverantörer inom exempelvis laserskanning för att producera nya geodata. Vid sidan om detta har även den tjeckiska försvarsmakten en geodataavdelning som producerar data som dock uteslutande används inom myndigheten.

3.3.3 Lagstiftning

Likt många andra länder införde Tjeckien i slutet av 1990-talet lagstiftning om öppenhet i det offentliga, framför allt genom *Lagen* (106/1999 Sb) *om fri tillgång till information*. Några år senare kompletterades denna med *Lagen* (412/2005 Sb) *om skydd av sekretessbelagda uppgifter och säkerhetsprövning* som gör det möjligt att sekretessklassa information som kan skada landets intressen. Tjeckien införde ingen särskild lagstiftning med anledning av EU:s öppna datadirektiv. Detta har främst att göra med att tidigare geodatainsamlingsprojekt i landet i de flesta fall har finansierats av EU och därmed har öppna geodata sedan länge varit en norm. Både civila och militära informanter betonar att det främsta verktyget för att begränsa tillgängliggörandet av geodata finns i *Samlingsförordning om den digitala tekniska kartan över regionen* (393/2020). Denna förordning, som har tagits fram av ČÚZK, består av en lista av datatyper vilka är sekretessklassificerade enligt en skala från ’Begränsad av första graden’ till ’Topphemligt’. Alla tjeckiska myndigheter kan föreslå tillägg till listan, och när en typ av geodata har lagts till ansvarar också föreslående myndighet för att denna typ av geodata skyddas.

3.3.4 Risk, hot och aggregering

De civila och militära representanterna förklarar att det hos såväl de styrande inom Tjeckiens lantmäteri, som hos landets nationella politiker och hos allmänheten, finns en övertygelse om att öppenheten ska sättas i främsta rummet. Det råder konsensus hos informanterna om att det tjeckiska folket i liten grad oroar sig för krig på nationens territorium, någonting som man menar också leder till att frågan om risker med öppna geodata är lågt prioriterat inom den nationella politiken. Det lyfts även ett önskemål om att samordna frågan om potentiella risker gällande öppna geodata på EU-nivå. Det uppges vara svårt för den tjeckiska försvarsmakten, liksom för ČÚZK, att få ekonomiskt stöd och gehör för att utveckla riskarbetet.

Den militära representanten menar att det inom Tjeckiens väpnade styrkor finns en uppfattning om att den öppenhet som råder i landet vad gäller geodata har lett till en situation där motåtgärder för att skydda nationell säkerhet har relativt liten effekt. Framför allt i jämförelse med de ekonomiska förluster som begränsningar i tillgången till data kan leda till. Istället för att till exempel dölja den tjeckiska försvarsmaktens anläggningar på landets officiella karttjänster försöker de finna andra metoder för att skydda viktig militär infrastruktur.

3.3.5 Riskbedömning

Det finns inget lagstadgat krav på att riskbedömning ska ske innan data görs tillgängligt som öppna data. Majoriteten av ČÚZK:s data är därför öppna för

allmänheten. Exempelvis gäller detta för den laserskanningsdata över landet som ČÚZK har samlat in sedan 2010. Denna data, liksom all rådata från laserskanningen, är tillgänglig för nerladdning. ČÚZK har, framförallt i sina laserskanningsprojekt, mottagit ekonomiskt stöd från EU. Sådant stöd erbjuds dock endast under villkoret att insamlade data publiceras som öppna data. Då detta har pågått under lång tid, har EU:s öppna datadirektiv haft en förhållandevis liten inverkan på det offentligas datapraktiker i Tjeckien. För lantmäterimyndigheten kom öppna datadirektivet framför allt att innebära att myndigheten inte längre kunde ta ut avgifter för att dela med sig av data. Påverkan på myndigheten har dock varit minimal, då avgifterna som tidigare betalades in gick direkt till statskassan istället för att användas för att driva myndigheten.

Informanterna lyfter att myndigheten har givits ansvaret för den förordning som styr över säkerhetsklassning av data men att ČÚZK saknar både ekonomiska resurser och tekniska infrastruktur för att själva hantera en ökad mängd sekretessklassade data. Utvärderingar och beslut om att begränsa tillgången till insamlade geodata som bör vara sekretessklassade är i praktiken omöjligt för myndigheten att genomföra, och man arbetar därför inte heller för att tilldelas sådana befogenheter.

3.3.6 Åtgärder för begränsning av öppna data

Sommaren 2024 lanserade ČÚZK dataportalen Digital Technical Maps. Portalen samkör omkring 14 olika databaser från olika ägare, inklusive ČÚZK, och innehåller en mängd olika typer av data såsom ortofoton, laserdata och 3D-modeller över landet. Portalen är ett pågående arbete som planeras att fortsätta under flera år framåt och den ska på sikt bland annat utvecklas till en central databas. I och med att det utgör ett pågående omfattande arbete ligger prioritering i första hand på fortsatt utveckling av databasen. Eftersom det inte finns krav på att riskbedömning ska ske innan data tillgängliggörs, finns inte nog med resurser för att utföra arbete utöver det som är prioriterat.

Majoriteten av data i databasen är öppen för alla användare att ladda ner och kräver ingen typ av inloggning. Attribut kopplat till kritisk infrastruktur har dock plockats bort. Tidigare nämnda förordning *Samlingsförordning om den digitala tekniska kartan över regionen* (393/2020) reglerar bland annat vilka attribut som ska sekretessklassificeras. Utöver det som nämns i förordningen är det upp till respektive aktör som tillhandahåller data till den gemensamma databasen att avgöra vad som inte ska tillgängliggöras. Det finns heller ingen formell process att följa innan geodata tillgängliggörs som öppna data. Detta, menar intervjupersonerna, gör det svårt att avgöra vilka data som ska klassificeras, utöver vad förordningens krav säger.

Som nämnts är majoriteten av data tillgänglig för alla. Dock finns viss reglering där särskilda aktörer kan få tillgång till mer data. Medan öppna geodata görs tillgängliga helt utan användarverifikation kräver offentliga data att användare identifierar sig med ett tjeckiskt elektroniskt ID-kort. På så vis är det möjligt för vissa aktörer att få tillgång till geodata som berör samhällelig infrastruktur, vilka är nödvändiga för

exempelvis fastighetsutveckling. Detta arbetssätt har också gjort det möjligt för lantmäterimyndigheten att i viss mån övervaka användare för att identifiera misstänkta beteenden. Intervjupersonerna säger samtidigt att det är oklart hur detta ska användas och hur effektivt det är med övervakning eftersom en hotaktör kan använda sig av mellanhänder för att införskaffa önskade data. Representanten för Tjeckiens väpnade styrkor framhåller vikten av en balanserad hantering av geodatafrågor. De tjeckiska väpnade styrkorna har möjlighet att hindra vissa typer av data från att tillgängliggöras öppet, men de kan inte bestämma om tillgången till specifika datamängder ska begränsas då detta är beroende av hur datamängden typifieras. Samtidigt menar företrädaren för Tjeckiens väpnade styrkor att sekretessklassificering av geodata inte utgör huvudspåret in i framtiden. Detta exemplifieras med att geodata erbjuds från såväl privata som offentliga aktörer, vilket innebär att möjligheterna att hindra data från att hamna i fel händer är högst begränsade. Samtidigt är förlusterna vad gäller innovation och utveckling potentiellt högre jämfört med de risker som undviks om man skulle välja att inte publicera insamlade data öppet. Istället framhålls andra alternativ, framförallt vad gäller skydd och övervakning av kritisk infrastruktur. Den tjeckiska försvarsmaktens representant menar att det även borde finnas ytterligare alternativ mellan öppna data och sekretessklassning, för att på så sätt kunna begränsa vem som får tillgång till vissa typer av data. En sådan åtgärd skulle exempelvis bestå av att data är tillgänglig för landets medborgare eller aktörer som verkar inom EU, men inte för resten av världen. Den förordning som reglerar vilken data som ska sekretessklassificeras ger ett visst stöd, men informanten menar att det borde finnas fler möjligheter för att begränsa vem som får tillgång utan att behöva använda sig av sekretess. Dessutom skrevs lagen innan kriget i Ukraina utbröt, vilket gör att världsbilden som styrde arbetet var annorlunda jämfört med den man har i nuläget.

Uppfattningen hos de civila och militära representanterna är att den allmänna synen på att Tjeckien inte befinner sig under ett direkt krigshot också leder till att den tjeckiska försvarsmaktens ställning fortsatt är relativt svag. Detta inte minst efter de många nedskärningar som har skett inom myndigheten sedan 1990-talet. Mellan ČÚZK och Tjeckiens väpnade styrkor finns också vissa skillnader i synen på utmaningarna vad gäller möjligheterna att begränsa spridningen av geodata som öppna data. Medan representanten för lantmäterimyndigheten gärna ser ökade lagliga befogenheter, menar den tjeckiska försvarsmaktens representant att det i första hand måste finnas andra alternativa tillvägagångssätt för att skydda kritisk infrastruktur. Det finns dock en samsyn mellan den civila och den militära sidan att vägen framåt inte är mer sekretessklassad data.

3.3.7 Framtidsperspektiv

I den närmaste framtiden kommer ČÚZK fortsatt att i första hand fokusera på att tillhandahålla öppna geodata, både genom ny och mer detaljerad laserskanning av landet och genom utveckling av dataportalen Digital Technical Maps.

4 Diskussion

Föreliggande rapport har ett tredelat syfte. Det övergripande syftet handlar om att öka vår förståelse av hur tre europeiska länder arbetar med riskbedömningar av geodata tillgängliggjorda som öppna data. Dessutom ämnar studien också bidra till att bättre förstå huruvida dessa länder har identifierat risker relaterat till nationell säkerhet vid tillgängliggörandet av geodata som öppna data, samt hur eventuella identifierade risker har hanterats.

Samtliga tre studerade länder bedömer att det finns risker med öppna geodata. Dock skiljer det sig något åt beroende på om riskerna bedöms utgöra hot mot nationens säkerhet eller ej. Estland lyfter en större oro för att detaljerade data kan skada medborgares integritet. Tjeckien uttrycker oro för den nationella säkerheten, men att det inte finns utrymme för att genomföra ett mer utförligt riskbedömningsarbete då det inte är något som efterfrågas i exempelvis lagstiftning, från politiken eller från allmänheten. Även Finland lyfter oro för nationell säkerhet. Här utförs ett omfattande arbete med att bedöma hur öppna geodata kan utgöra risker för den nationella säkerheten. Sammanfattningsvis kan sägas att samtliga intervjuade representanter, i respektive land, instämmer rörande de utmaningar som finns med aggregeringsproblematiken och det omöjliga i att förutse de risker som rimligen kan uppstå när data och information kombineras med varandra och över tid.

För syftets andra del och frågan gällande hur eventuella risker hanteras finns en del lärdomar som Sverige kan dra från Finlands arbete med risker om öppna geodata. Inget av de studerade länderna har i lagtext uttryckt att riskbedömning ska genomföras eller att hänsyn ska tas till nationell säkerhet innan data ges ut som öppna data. Trots avsaknad av lagstiftning pågår i Finland ett brett arbete med att identifiera och hantera risker relaterade till öppna geodata och nationell säkerhet. Lantmäteriverket, Finansministeriet och Miljöministeriet arbetar alla enligt något slags strukturerat arbetssätt för att hitta geodata som skulle kunna användas för att hota nationens säkerhet. Att flera myndigheter och departement genomför detta arbete, och samarbetar med andra offentliga aktörer för att skapa metoder, samt stöttar kommunerna i deras riskbedömningsarbete, visar på den otroliga mängd resurser som riskbedömning av öppna geodata kräver. Från svenskt lagstiftningsperspektiv ska tilläggas att riskbedömning av öppna data avser all data, inte endast geodata.

4.1 Lärdomar

Bakgrunden till denna studie står att finna i det tidigare arbete som FOI har utfört på uppdrag av Lantmäteriet. Där identifierades bland annat behovet av att förbättra myndighetens förståelse av hur dessa frågor hanteras inom EU. Detta uppdrag var tänkt att stödja arbetet med att förbättra den riskbedömningsmetod, MEGS, som tagits fram för att identifiera risker med öppna geodata med avseende på Sveriges säkerhet.[33] Eftersom metoden är den första i sitt slag i Sverige fordras därmed vidareutveckling. Exempel på detta är att inkludera möjligheter. Tre instanser i Finland poängterar att de i sina riskbedömningsmetoder, utöver risk, också inkluderar variabeln ’möjligheter’ vid bedömning av en datamängd. En annan potentiell utveckling av MEGS gäller definitionen av nationell säkerhet. MEGS följer och utvecklar den juridiska förståelsen av Sveriges säkerhet med fokus på inre och yttre säkerhet, medan myndigheterna i Finland framför allt utgår från kritisk infrastruktur i sina riskbedömningar. Det är oklart vad skillnaden i praktiken kan innebära, men en potentiell utmaning är att olika definitioner av nationell säkerhet kan försvåra samarbete över landsgränser. Samtidigt är det naturligt att olika angreppssätt och definitioner uppstår i och med att varje land skapar sina egna riskbedömningsstrukturer och -metoder för öppna geodata.

Eftersom öppna datadirektivet inte lämnar utrymme för att begränsa tillgången på data om data kan tillgängliggöras som öppna data, är sekretessklassning det enda alternativ som finns att tillgå för svenska myndigheter. Sekretessklassning är problematiskt då det medför en större arbetsbörda genom att ställa krav på tillgång till särskilt anpassade datorer, lokaler och personal. Sekretessklassning är samtidigt, enligt såväl militära som civila instanser, inte den lösning som främst ska användas för att hindra tillgängliggörande av data. I relation till detta lyfte även samtliga informanter återkommande betydelsen av att bevara öppenheten i samhället. De framhöll att data inte ska stängas in utan att det istället behövs möjlighet att upprätta en balans där data kan gynna utveckling och innovation, samtidigt som det är säkerställt att datas tillgängliggörande inte kan användas för att hota den nationella säkerheten. Något som efterfrågas av Tjeckien, och som delvis redan används av den finska lantmäterimyndigheten med avseende på laserdata, är ett tredje alternativ till öppna data och sekretess – i Finland benämnt publika data. Det tredje alternativet skapar en möjlighet att begränsa spridningen av öppna data, utan att använda sekretessklassning, samtidigt som data finns att tillgå för landets medborgare. Däremot är detta tredje alternativ inte i linje med vad öppna datadirektivet har specificerat om hur öppna data ska vara tillgängliga. Detta är myndigheterna i Finland medvetna om, och tillvägagångssättet är inte heller prövat i domstol. Ett förslag är att Sverige ser över om något liknande arbetssätt vore möjligt att inkorporera i de fall där det är ett rimligt åtgärdsalternativ.

[33] Davidsson m.fl. (2025b).

I studien har vi inte märkt av den potentiella konflikt som just nu kan sägas växa fram mellan frågor som behandlas på EU-nivå, inom områden såsom handel och konkurrens, och säkerhetsfrågor som traditionellt hanteras på nationell nivå och som berör territoriets bevarande och statens suveränitet.[34] Traditionellt har medlemsländerna överlämnat beslut om handelsfrågor till EU medan militära eller territoriella säkerhetsfrågor har hållits kvar på respektive lands nationella nivå. Detta kan nu komma att förändras, någonting som reflekteras i två inflytelserika rapporter från de senaste åren. Såväl Draghi-rapporten (2024), som behandlar EU:s framtida ekonomiska konkurrenskraft, och Niinistö-rapporten (2024), om EU:s militära och civila beredskap, framhåller att europeiska ekonomiska och säkerhetsmässiga problem i dag endast kan hanteras med hjälp av gemensamt utvecklade lösningar. Vissa säkerhetsfrågor har redan flyttats från nationell nivå upp till EU-gemensam nivå, och än fler kan komma att genomföra samma resa om rapporternas förslag blir till verklighet.[35] Samtidigt ökar detta ytorna på vilka konflikten mellan, å ena sidan, konkurrens och utveckling och, å andra sidan, säkerhet kan utspela sig. Tidigare har EU främst arbetat för att främja konkurrens och utveckling genom initiativ som öppna datadirektivet, samtidigt som frågor om säkerhet nästan helt lämnats över till medlemsstaterna. Det är istället på den nationella nivån, exempelvis genom Sveriges lagstiftning om riskbedömning av data utifrån nationell säkerhet, som motsättningen mellan ekonomisk vinning och säkerhet infunnit sig. Risken är dock att denna konflikt i framtiden också kommer att återfinnas på EU-nivå. Potentiellt innebär de olika intressenivåerna och relationen mellan EU och Sverige, att ytterligare börda läggs på de aktörer som genomför riskbedömningar, där inte bara Sveriges, utan hela EU:s säkerhet ska inkluderas innan tillgängliggörandet av data som öppna data.

I tidigare studier[36] har det framkommit behov av samverkan på nationell nivå för att stötta aktörerna i riskbedömningsarbetet. Omvärldsbevakningen som presenteras i denna rapport visar att samma önskemål om nationell samordning existerar i samtliga studerade länder. Vidare framkommer ett starkt önskemål om att lyfta frågan till EU-nivå för att underlätta etablerandet av en samsyn kring hur länder identifierar potentiella risker med öppna data. Denna önskan stämmer väl överens med Niinistö-rapportens slutsatser[37] som framhäver att EU bör ta ett större grepp om säkerhetspolitiska kriser och ytterst krig och därmed kunna förebygga krisers uppkomst, istället för att som i dagsläget svara reaktivt. En motiverande faktor är medlemsstaternas täta sammankoppling vilken medför att om en medlemsstats säkerhet hotas kan detta skapa problem för övriga stater samt för EU som helhet.

Slutligen kan här konstateras att det finns flertalet likheter mellan de studerade länderna och mellan dem och Sverige. De intervjuade var alla överens om

[34] Ingemarsdotter, J., & Wetter Ryde, A. (2024b). *Niinistö-rapporten: På väg mot ett europeiskt civilt försvar?* FOI Memo 8743.
[35] Ingemarsdotter, J., & Wetter Ryde, A. (2024a). *Draghi-rapporten: Villkoren för Europas självbevarelse?* FOI Memo 8658.; Ingemarsdotter & Wetter Ryde. (2024b).
[36] Davidsson m.fl. (2025a).
[37] Ingemarsdotter & Wetter Ryde. (2024b).

möjligheterna som öppna data kan generera, men poängterade också att hanteringen av de risker som kan uppstå inte har givits tillräckliga resurser. Studien har visat att personer som arbetar inom geodatasektorn sitter med samma typ av frågor, men i olika delar av Europa. Projektets intervjubesök togs emot med inställningen att detta är viktiga frågor som behöver lyftas, samt att länderna som ingår i unionen behöver samarbeta för att lära av varandra och skapa likvärdiga riskbedömningar av öppna geodata. Det som upplevs som det svåraste problemet består i att lösa de utmaningar som gäller aggregering av data. Här finns ännu ingen lösning, men det är en fråga som framstår som väl värd att hantera enligt intervjupersonerna. Inte minst då potentiella risker som kan uppstå på grund av aggregering också kan röra sig över landsgränser. Aggregering kan ske globalt och därmed också påverka säkerheten bortom nationalstaten.

5 Referenser

Broomfield, H. (2023). Where is open data in the Open Data Directive? *Information Polity*, 28(2), 175–188. https://doi.org/10.3233/IP-220053

Davidsson, Å., Mittermaier, E., Severin, M., Söderman, U., Winterdahl, M., Ciepielewska, M. & Stjernlöf, S. (2025a). *Riskbedömning av geodata vid tillgängliggörande som öppna data*. FOI-R--5745--SE. Totalförsvarets forskningsinstitut, Stockholm.

Davidsson, Å., Mittermaier, E., Severin, M., Söderman, U., Winterdahl, M., Ciepielewska, M. & Stjernlöf, S. (2025b). *Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data -Myndighetsgemensamt arbete.* FOI-R--5768--SE. Totalförsvarets forskningsinstitut, Stockholm.

Direktiv 2007/2/EG. *EU:s infrastruktur för rumslig information (Inspire)*.

Draghi, M. (2024). *The future of European competitiveness – A competitiveness strategy for Europe*. European Commission.

EU 2019/1024. *Direktiv om öppna data och vidareutnyttjande av information från den offentliga sektorn*.

European Commission. (2019). *Building a data economy - Brochure*. https://digital-strategy.ec.europa.eu/en/library/building-data-economy-brochure [Hämtad 2026-03-09].

Europeiska unionen. (u.å.a). *Estland*. https://european-union.europa.eu/principles-countries-history/eu-countries/estonia_sv [Hämtad 2026-03-11].

Europeiska unionen. (u.å.b). *Finland*. https://european-union.europa.eu/principles-countries-history/eu-countries/finland_sv [Hämtad 2026-03-11].

Europeiska unionen. (u.å.c). *Tjeckien*. https://european-union.europa.eu/principles-countries-history/eu-countries/czechia_sv [Hämtad 2026-03-11].

Finansministeriet. (2024). *Paikkatiedon kansallisen riskiarvion työryhmän muistio (julkinen)*. Finansministeriet, Helsingfors.

Finansministeriet. (2025). *Kriittisen infrastruktuurin tietojen avoin jakaminen arvioidaan uudelleen huomioiden kansallinen turvallisuus*. Finansministeriet, Helsingfors.

Ingemarsdotter, J., & Wetter Ryde, A. (2024a). *Draghi-rapporten: Villkoren för Europas självbevarelse?* FOI Memo 8658.

Ingemarsdotter, J., & Wetter Ryde, A. (2024b). *Niinistö-rapporten: På väg mot ett europeiskt civilt försvar?* FOI Memo 8743.

McBride, K., Toots, M., Kalvet, T. & Krimmer, R. (2018). Leader in e-Government, Laggard in Open Data: Exploring the Case of Estonia. *Revue française d'administration publique*, 167(3), 613-625. https://doi.org/10.3917/rfap.167.0613.

Mokhtari, A. (2025). *Menetelmä Maanmittauslaitoksen paikkatietoaineistojen riskienarviointiin*. Metropolia Ammattikorkeakoulu.

Moon, M. J. (2020). Shifting from Old Open Government to New Open Government: Four Critical Dimensions and Case Illustrations. *Public Performance & Management Review*, *43*(3), 535–559. https://doi.org/10.1080/15309576.2019.1691024

NATO. (2024). *NATO member countries*. https://www.nato.int/en/about-us/organization/nato-member-countries [Hämtad 2026-03-11].

National Land Survey of Finland. (u.å.). *Laser scanning data 5 p terms of use*. https://www.maanmittauslaitos.fi/en/laser-skanning-data/terms-of-use [Hämtad 2026-02-25].

Niinistö, S. (2024). *Safer Together: Strengthening Europe's Civilian and Military Preparedness and Readiness*. European Commission.

Nikander, J. Jama, T. & Tenkanen H. (2023). *Selvitys Maanmittauslaitoksen avoimiin peruspaikkatietoihin liittyvistä uhkista*. Aalto-yliopisto.

Nikander, J., Jama, T., & Tenkanen, H. (2024). Threats Related to Open Geospatial Data in the Uncertain Geopolitical Environment. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, *XLVIII-4/W12-2024*, 121–126. https://doi.org/10.5194/isprs-archives-XLVIII-4-W12-2024-121-2024.

Prop. 2021/22:225. *Den offentliga sektorns tillgängliggörande av data*.

Public.Resource.Org. (2007). *Open government data principles*. https://public.resource.org/8_principles.html. [Hämtad 2026-03-23].

Regeringskansliet. (2026). *Granskning av Lantmäteriets informationssäkerhet*. Ds 2026:2. Landsbygds- och infrastrukturdepartementet, Stockholm.

Ruijer, E. H. J. M., & Martinius, E. (2017). Researching the democratic impact of open government data: A systematic literature review. *Information Polity*, *22*(4), 233–250.

SFS 2022:818. *Lag om den offentliga sektorns tillgängliggörande av data*.

Wetter Ryde, A. (2025). *EU:s roll om krisen eller kriget kommer – Hur bygger vi gemensam motståndskraft i EU?*. FOI-R--5767--SE. Totalförsvarets forskningsinstitut, Stockholm.

Winterdahl, M., Mittermaier, E., Severin, M., During, C., Gunnarson, C. (2023). *Möjliga hot och risker rörande öppna geodata - Redovisning av arbete i en förstudie*. FOI Memo 8296. Totalförsvarets forskningsinstitut, Stockholm.

Bilaga A: Intervjuguide

This study refers to geospatial datasets. This means data that identifies the geographic location, extent, and characteristics of natural or human-made features on the Earth. It combines spatial information (e.g., coordinates, geometry, topology) with attribute information (e.g., name, type, or classification of the feature). When referring to geodata, the study in particular refers to datasets intended to be made publicly available with reference to the EU Open Data Directive (2019/1024).

This study also refers to geodata aggregation. This means the act of compiling geodata from different datasets in order to extract larger-scale units. Aggregation can be done with all kinds of information in addition to geodata.

Questions concerning geodata infrastructure

Background: The ways in which primary geodata infrastructure is constructed, owned, serviced, and monitored sets certain limits and offer certain possibilities when it comes to security measures. In order to understand the specific circumstances shaping geodata production and potential risks related to it in your country, we would like to begin with questions concerning your nation's geodata infrastructure.

- What kinds of geodata is, generally, produced?
- What actors produce high-value datasets (according to EU Open Data Directive 2019/1024)?
- What geodata is made publicly available? High valuable data?
- In what ways are geodata made publicly available?
- What actors builds, owns, services, and monitors geodata infrastructure?
- What actors host geodata portals?
- (For agencies that does not produce their own data) From whom does your agency procure geodata?
- Has any geodata been restricted as a result of the EU Open Data Directive?
  a) In what ways have this geodata been restricted?
  b) What are the motives behind the restrictions?
- Which institutions have the mandate to restrict geodata?

Question concerning risks, threats, and aggregation

Background: The EU directive was introduced with the aim of facilitating development. However, it can also create challenges related to the availability of datasets. In Sweden, there are requirements for data to undergo a risk assessment before being made publicly accessible. One reason for this assessment is that the aggregation of different datasets can generate new information that may be exploited by a potential antagonist. Therefore, we would like to ask you some questions about how you handle risk assessment and the issue of data aggregation.

- Are there any (legal) requirements to carry out a risk assessment before making data available?
- Have new risks and threats been identified in the process of making geodata available?
- Have any real threats or suspicious activities been identified? Could you share examples?
- Have any threat scenarios been included in the risk assessment process?
- Are there any threat scenario analysis and who/what agency provides it?
- Are you familiar with any technology that, when combined with geodata, could be significant for an antagonist?
- How are the threats related to the aggregation of geodata being addressed?
- Are there any existing or ongoing inquiries into handling threat assessments concerning aggregation?
- Are authorities/institutions etc. working together to identify risks and threats related to aggregation?

Questions concerning risk assessment methodology

Background: Sweden requires that data be risk assessed to determine whether it may pose a threat to national security before it is made available. However, Swedish legislation does not specify how this risk assessment should be conducted, and no standardized method or procedure has been developed for this purpose. As a result, FOI was tasked with developing a method to support the risk assessment of geodata based on Sweden's security needs. This was a major undertaking that requires continuous development. Therefore, we are interested in learning from you and whether you follow any particular method or standardized approach in your risk assessment work.

- Do you follow any methodology when assessing risks and threats related to geodata?
- What actors were involved in designing the methodology?
- How is this methodology designed?
- Which institutions took part in developing any existing geodata security measures?
- Are users of geodata monitored? How? By whom?
- Does the methodology include aggregation of different data sets?
- Has the methodology been tested?
- What are the experiences of using it?
- Can we take part of the methodology?

Questions concerning legal frameworks

Background: The ways in which the EU open data directive has been interpreted by nations differ. We would therefore like to ask questions concerning how the directive has been adapted into national law or other legal frameworks.

- Did the EU directive result in major changes for you compared to how accessible geodata was to the public before it came into effect? How?
- What national regulation regarding geodata exists today, and how does it relate to the EU open data directive?
- In accordance with which laws, directives, or regulations is geodata evaluated for restrictive usage?
- Is there anything missing in the national legislation?
- Do you see any other challenges in the implementation of the EU directive?

Questions concerning the future of geodata

Background: It is predicted that geodata will play an increasingly important role in society over the coming decade. We would like to end this interview by asking questions concerning your opinions regarding the future of geodata security.

- What technological advances do you think will have the greatest impact on geodata management over the next 5-10 years?
- What advice would you give to Sweden regarding geodata and potential risks?

Other

- What kinds of geodata infrastructure is operative?
- How is the infrastructure connected (fibre cable, cell phone network etc.)?
- What are the purposes behind collecting geodata?

FOI

ISSN 1650-1942

www.foi.se