Riskbedömning av geodata vid tillgängliggörande som öppna data

Åsa Davidsson, Eva Mittermaier, Minna Severin,
Ulf Söderman, Mathias Winterdahl

Maria Ciepielewska, Sofia Stjernlöf

FOI-R--5745--SE

Maj 2025

FOI

Åsa Davidsson, Eva Mittermaier, Minna Severin, Ulf Söderman, Mathias Winterdahl.

Maria Ciepielewska, Sofia Stjernlöf.

Riskbedömning av geodata vid tillgängliggörande som öppna data

Titel	Riskbedömning av geodata vid tillgängliggörande som öppna data.
Rapportnummer	FOI-R--5745--SE
Månad	Maj
År	2025
Antal sidor	62
ISSN	1650-1942
Uppdragsgivare	Lantmäteriet
Forskningsområde	Övrigt
Projektnummer	E13927
Godkänd av	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys
Omslagsbild:	Shutterstock

Figurer: Åsa Davidsson, Kristina Gavhed, Patric Karlsson, Minna Severin, Mathias Winterdahl (FOI).

Sammanfattning

Totalförsvarets Forskningsinstitut (FOI) och Lantmäteriet har under 2024 och 2025 tagit fram förslag till en metod för riskbedömning vid tillgängliggörande av geodata avseende Sveriges säkerhet. Det sker efter att Lantmäteriet upptäckt behovet enligt krav i lagen (2022:818) om den offentliga sektorns tillgängliggörande av data, även kallat öppna datalagen, som trädde i kraft under 2022. I förarbetet till lagen uttrycks dessutom att riskbedömningen ska ta hänsyn till aggregering, en relevant utmaning då antalet aggregeringar som kan ske är oändligt. Projektet har utvecklat ett utkast till en metod för riskbedömningar vid tillgängliggörande av geodata som öppna data med avseende på Sveriges säkerhet.

Riskbedömningar utgår ofta från bedömning av sannolikhet och konsekvens. Men för komplexa risker, är detta tillvägagångssätt inte tillämpbart. Den risk som ska bedömas i detta sammanhang är dessutom relaterad till Sveriges säkerhet, och för Sveriges säkerhet finns varken tydliga kriterier eller konsekvenser definierade. För att bemöta detta har här istället för sannolikhet begreppet *relevans* införts. För konsekvenserna har projektet testat en ansats med konsekvensnivåer utifrån en möjlig innebörd av Sveriges säkerhet. I det föreslagna utkastet till riskbedömningsmetod används relevans, konsekvensnivåer och utkast till kriterier för dessa nivåer.

Rapporten presenterar framtagandet av metoden samt de avväganden som ligger bakom utformningen. Tillämpningen av metoden beskrivs i en separat publikation *Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data*.

Nyckelord: riskbedömning, myndighetssamverkan, geodata, digitalisering, öppna datalagen, konsekvens, relevans, tillgängliggörande, Sveriges säkerhet.

Summary

The Swedish Defence Research Agency (FOI) and the Swedish Mapping, Cadastral, and Land Registration Authority (Lantmäteriet) have developed a draft risk assessment method, MEGS, to evaluate the impact of making geodata available as open data on Sweden's security. This work, *Method for Risk Assessment of Geodata when Making them Available as Open Data*, undertaken between 2024 and 2025, aligns with the Open Data Act, which came into effect in 2022. The law requires that risk assessments account for aggregation, where potential combinations are infinite.

Risk assessments often rely on evaluating probability and consequences. However, for complex risks, this approach is not applicable since there is no data to assess the probability. Since the security of Sweden is involved, with no clear criteria or defined consequences, the method introduces *relevance* instead of probability. For assessing consequences, the project has tested developing consequence levels based on interpretations of Sweden's security. Relevance, consequence levels, and their criteria for Sweden's security are used in the proposed risk assessment method, MEGS.

The report outlines MEGS's development and design considerations, with a separate publication detailing its application *Proposed Process Support for Risk Assement of Geodata when Making them Available as Open Data – A Collaborative Effort by Government Agencies*.

Keywords: risk assessment, collaboration between authorities, geodata, digitalisation, open data law, consequence, relevance, accessibility.

Förord

Geodata, data om den fysiska verkligheten, är en avgörande del i den pågående digitaliseringen. I en tid av ökande geopolitiska utmaningar och växande klimatförändringar är tillförlitliga geodata viktiga för Sveriges säkerhet och beredskap. Omvärldsläget har förändrats kraftigt och är mer oförutsägbart. Händelser som undervattenssabotage, Malmbanans urspårning, skredet vid E6:an i Stenungsund, kriget i Ukraina, förändringar i världshandeln, upprustning i Europa och olika former av valpåverkan är företeelser som måste beaktas när vi ska avgöra om vår geodata är lämplig att göras öppen, tillgänglig och användbar för alla.

Risker kring aggregering av data har varit föremål för en diskussion under mer än tio års tid inom den offentliga sektorn. Flera myndigheter har under åren påpekat aggregeringsriskerna med geodata och att kombinationer av öppna data kan innebära att ny information uppstår och innehåller uppgifter omfattade av totalförsvarssekretess. Det är dock svårt att få grepp om frågeställningen som sådan och det finns få exempel att hänga upp diskussionen på.

Enligt 2 kap. 1 § öppna datalagen (2022:818), ska myndigheter göra en riskbedömning för bland annat Sveriges säkerhet, om data ska tillgängliggöras enligt lagen. Det innebär att uppgifter som inte omfattas av sekretess men som aktualiserar risker för Sveriges säkerhet, inte ska tillgängliggöras som öppna data. Riskerna med aggregering ska särskilt beaktas. I förarbetena uttrycks även att det kan vara lämpligt att en myndighet samråder med andra myndigheter och eventuellt söker ytterligare vägledning i frågor som rör tillgängliggörande av data för vidareutnyttjande. Då det saknas en vedertagen metod för denna riskbedömning har Lantmäteriet därför tagit hjälp av FOI, Geodatarådet och ytterligare ett antal myndigheter och kommuner, för att ta fram ett förslag till metodstöd, för att möjliggöra för myndigheter att gemensamt bedöma riskerna. Arbetet har pågått sedan vintern 2024 och har finansierats med 2:4-medel från Myndigheten för samhällsskydd och beredskap.

Vi är enormt tacksamma över att statliga myndigheter och kommuner har tagit sig tid och delat med sig av sin kunskap och sina erfarenheter i projektet. Ert bidrag i detta arbete har varit avgörande och vi vill rikta ett stort tack till er och era myndigheter.

Det har varit ett komplext och spännande uppdrag och vi ser att detta bara är början och att det finns ett stort behov av att fortsätta jobba med frågorna. Förslaget till metod behöver testas, utvärderas och fortsatt utvecklas för att säkerställa att den fyller sitt syfte. Vi hoppas därför på ett fortsatt gott samarbete, dialog och vidareutveckling i dessa frågor med berörda aktörer.

Sofia Stjernlöf
Projektledare Lantmäteriet

Minna Severin
Projektledare FOI

Innehållsförteckning

Begreppslista

I rapporten återkommer en del begrepp som kan ha olika betydelser eller som behöver förklaras närmare. Nedan följer de definitioner som avses i rapporten.

Ackumulering

Sammanställning av samma typ av data- eller informationsmängder, exempelvis över tid. Är ett specialfall av aggrgering.

Aggregering

Sammanställning av flera data- eller informationsmängder.

Analysobjekt

Den geodatamängd som man ämnar tillgängliggöra som öppna data och för vilken riskbedömningen ska göras.

Data

Representation av bland annat fakta och idéer i en form lämpad för överföring och bearbetning av människor eller av automatiska hjälpmedel, exempelvis siffror, alfabetiska tecken, figurer, bilder och ljudvågor.

Geodata (geografiska data)

Digitala data som relaterar till en geografisk position.

Geodatamängd

En samling geodata som används för att beskriva och analysera geografiska företeelser.

Hot

Möjlig händelse, aktivitet eller företeelse som kan leda till förlust av eller skada på, eller till förväntan om förlust av eller skada på, förmåga, funktion, information eller materiella och personella resurser.

Hotaktör

Aktör som har intention och förmåga att med avsikt utföra handlingar som leder till förlust av eller skada på, eller till förväntan om förlust av eller skada på, förmåga, funktion, information eller materiella och personella resurser. Antagonist används här synonymt med hotaktör.

Information

Det budskap eller den innebörd, andemening eller tolkning som bland annat data förmedlar till en människa, såsom tolkning av text och matematiska tal eller innebörd av språkliga eller visuella beskrivningar. I huvudsak, men inte nödvändigtvis, sådant som är meningsfullt för individen.

Initierande aktör

Den offentliga aktör som önskar tillgängliggöra analysobjektet som öppna data och följaktligen inleder riskbedömningsprocessen.

Offentlig aktör

Offentlig organisation som omfattas av lag (2022:818) om den offentliga sektorns tillgängliggörande av data.

Processledare

Den befattningshavare som är ansvarig för att leda riskbedömningsprocessen vid en offentlig aktör.

Risk

En situation, händelse eller skeende med osäker, negativ konsekvens för Sveriges säkerhet vilken kan bli resultatet av tillgängliggörande av öppna geodata.

Riskbedömning

Metod för att identifiera, analysera och värdera de eventuella risker för Sveriges säkerhet som tillgängliggörande av geodata som öppna data kan medföra.

Sveriges säkerhet

Avser Sveriges territoriella suveränitet, politiska självständighet, demokratiska statsskick och samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå.

Säkerhetskänslig verksamhet

Sådan verksamhet som enligt säkerhetsskyddslagen (2018:585) ”är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktigande internationellt åtagande om säkerhetsskydd”.

Workshop

Arrangemang för verksamhet i grupp med tillfälle att samverka, sammanföra olika kompetenser, överföra kunskap samt dela med sig av erfarenheter.

Öppna data

Digitala data som tillhandahålls av offentliga aktörer i öppna format och som kan vidareutnyttjas för valfritt ändamål. och delas fritt i enlighet med *lag (2022:818) om den offentliga sektorns tillgängliggörande av data*.

1. Inledning

I dagens digitaliserade samhälle är vi beroende av stora mängder information för att sköta funktioner såsom trafikplanering och miljöövervakning. En viktig informationsmängd är geoinformation och geodata.[1] Med geodata avses alla data som är knutna till en geografisk position och relaterar till specifika punkter, sträckor eller områden. De kan symbolisera både fysiska objekt och administrativa enheter som byggnader, personers eller fordons rörelser, fastigheter, sjöar, vattendrag och kommuner. Vanligen består geodata även av annan information än endast position och utsträckning och kan representera jordarter, vegetationstyper och befolkningstäthet för ett geografiskt område eller beskriva den verksamhet som bedrivs i området. Geodata kan även utgöra avbildningar av jordytan i form av bilder eller topografisk representation.

I dagens moderna samhälle är geodata en nyckelresurs som bidrar med stor samhällsnytta. Här finns exempelvis den information som redovisas i fastighetsregister som innehåller geografiska data om fastigheters position, fastighetsbeteckning, ägarskap med mera. Denna typ av data utgör grund för en stor del av de ekonomiska transaktioner som sker rörande fast egendom. De behövs exempelvis för att du ska kunna bevisa att du är rättmätig ägare för att kunna sälja eller belåna en fastighet. Andra exempel är de data som med alltmer förfinade tekniska metoder samlas in för att beskriva topografin i ett landskap. Dessa används bland annat för att undersöka hur vattennivåer förändras vid översvämningar och hur detta i sin tur kan påverka byggnader, infrastruktur och framkomlighet.

Under 2022 implementerades EU-direktivet (2019/1024) om öppna data och vidareutnyttjande av information från den offentliga sektorn[2] (hädanefter benämnt öppna datadirektivet), genom *lagen (2022:818) om den offentliga sektorns tillgängliggörande av data* (hädanefter benämnd öppna datalagen). Enligt öppna datadirektivet ska offentliga aktörer inom EU tillgängliggöra data som har samlats in med offentliga medel.

Både öppna datalagen och *kommissionens genomförandeförordning (EU) av den 21.12.2022 om fastställande av en förteckning över särskilda värdefulla dataset och arrangemangen för offentliggörande och vidareutnyttjande av dessa* (hädanefter benämnd genomförandeförordningen) innehåller särskilda regler för så kallade värdefulla datamängder. Syftet är att säkerställa att offentliga data med högsta socioekonomiska potential görs tillgängliga för vidareutnyttjande med minimala rättsliga och tekniska begränsningar och utan avgift. De värdefulla datamängder som pekas ut i genomförandeförordningen är administrativ indelning, adresser, byggnader, fastighetsområden, hydrografi, markhöjdmodell, marktäcke och ortofoton. Genomförandeförordningen ställer krav på innehåll och på hur värdefulla datamängder ska göras tillgängliga, bland annat i form av API (direktåtkomst) och bulknedladdning (möjlighet att ladda ner stora mängder data samtidigt), och att de ska tillgängliggöras enligt licensen CCBY 4.0[3] eller lägre.

Enligt 2 kap. 1 § i öppna datalagen ska en riskbedömning avseende Sveriges säkerhet genomföras innan datamängder görs tillgängliga. Dessutom specificeras det i förarbetena[4] att riskbedömningen ska ta hänsyn till möjligheterna till aggregering, det vill säga att kombinera geodata med andra data eller informationsmängder för att på så sätt extrahera ny information. Detta innebär att separata geodatamängder inte behöver förmedla information som innebär risk för Sveriges säkerhet, men genom aggregering kan risk uppstå. Antalet kombinationsmöjligheter som kan uppstå genom aggregering är oändligt.

1 Hahmann, S., & Burghardt, D. (2013). How much information is geospatially referenced? Networks and cognition. *International Journal of Geographical Information Science*, 27(6), 1171–1189. https://doi.org/10.1080/13658816.2012.743664

2 Kommissionens genomförandeförordning (EU) av den 21.12.2022 om fastställande av en förteckning över särskilda värdefulla dataset och arrangemangen för offentliggörande och vidareutnyttjande av dessa, Pub. L. No. C(2022) 9562.

3 För information som skapas hos myndighet som är föremål för upphovsrättsligt skydd som verk eller prestation rekommenderas licensen CC BY 4.0. Se DIGG:s sida avseende Vägledning för att tillgängliggöra information, https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktörer/vagledning-for-att-tillgangliggora-information#h-Valjvillkorforanvandning

4 Prop. 2021/22:225.

Vad som *inte* framkommer i lagstiftningen om tillgängliggörande av data, är hur riskbedömningen ska genomföras. Under 2023 genomfördes en förstudie gällande möjliga säkerhetshot och risker med tillgängliggörande av öppna geodata.[5] Förstudien konstaterar att orsakerna till hot och risker kan delas in i följande tre övergripande kategorier:

1. Genom att tillgängliggöra en stor mängd detaljerad data, som annars skulle kräva resurser att hämta in, underlättas arbetet för hotaktören.
2. Tillgången på öppna geodata möjliggör avancerade rumsliga (geospatiala) analyser som annars hade varit komplicerade eller omöjliga att utföra.
3. Genom aggregering av olika typer av data kan hotaktören i vissa fall erhålla säkerhetskänslig information.

Förstudien visade på behovet av en metod för att bedöma risker med geodata som kan komma att tillgängliggöras, eller redan är tillgängliggjorda, som öppna data. Detta projekt har undersökt *hur* ett sådant riskarbete kan genomföras, på ett sådant sätt att myndigheterna inte bara uppfyller den lag de förväntas efterleva, utan att det även sker ett arbete där riskerna för Sveriges säkerhet minimeras. Här presenteras det arbete som ligger bakom framtagandet av ett utkast till metod för hur riskbedömningar av geodata kan gå till. För att underlätta för läsaren har vi valt att benämna förslaget till metoden för MEGS (Metod för riskbedömningar av öppna geodata med avseende på Sveriges säkerhet). Rapporten presenterar metodens innehåll och hur den utvecklats. Hur MEGS ska tillämpas i praktiken beskrivs utförligt i en separat publikation.[6]

1.1 Syfte och målgrupp

Syftet med denna rapport är att redovisa resultat från ett genomfört samverkansprojekt mellan FOI och Lantmäteriet. Syftet med projektet var att utveckla en metod för att kunna bedöma vilka risker för Sveriges säkerhet som kan uppstå vid tillgängliggörande av geodata som öppna data. Vidare syftar rapporten till att presentera hur projektgruppen har arbetat samt identifierade svårigheter som föreligger för offentliga aktörer att utföra riskbedömningar av data med avseende på Sveriges säkerhet. FOI har genomfört projektet på uppdrag och i samarbete med Lantmäteriet.

MEGS syftar till att möjliggöra för offentliga aktörer att i samverkan göra regelbundna bedömningar av riskerna för Sveriges säkerhet med öppna geodata med särskilt beaktande av aggregeringsproblematik. Metoden är tänkt att användas av offentliga aktörer i samverkan för att uppnå enhetliga och konsekventa bedömningar och för att involvera bredast möjliga kompetens vid riskbedömningarna.

Målgruppen för rapporten är offentliga aktörer, i första hand statliga myndigheter, som berörs av öppna datalagen, främst gällande tillgängliggörande av geodata. Rapporten kan även vara av intresse för de som arbetar med metodutveckling inom riskbedömning av öppna data eller andra typer av riskbedömningar avseende Sveriges säkerhet.

1.2 Avgränsningar

Enligt öppna datalagen ska tillgängliggörande av geodata som öppna data endast ske så länge informationssäkerhet kan garanteras, skydd av personuppgifter upprätthålls och det inte medför risker för Sveriges säkerhet. I projektet har varken informationssäkerhet[7] eller skydd av personuppgifter[8] beaktats eftersom syftet med projektet var att utveckla en metod för att bedöma risker för Sveriges säkerhet. Det är emellertid lämpligt att riskbedömningen

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

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

7 MSB (2025). *Metodstöd för informationssäkerhetsarbete*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/metodstod-for-informationssakerhetsarbete/ [Hämtad 2025-05-13].

8 Integritetsskyddsmyndigheten (2021). Vad är personuppgifter? https://www.imy.se/privatperson/dataskydd/introduktion-till-gdpr/vad-ar-personuppgifter/ [Hämtad 2025-05-13].

utförs kombinerat eller parallellt med de offentliga aktörernas etablerade metoder för att säkerställa informationssäkerhet och skydd av personuppgifter.

Ett av de grundläggande skälen till öppna datadirektivet är att offentlig producerade och bekostade data ska bidra till ökad nytta för samhället, exempelvis genom datadriven innovation. Den potentiella nyttan med olika geodatamängder har inte berörts inom projektet då det inte är möjligt att identifiera all potentiell framtida samhällsnytta och då nytta inte uppväger risker för Sveriges säkerhet.

MEGS är utformad för att bedöma risker vid tillgängliggörande av geodata som öppna data. Det är emellertid troligt att delar av MEGS kan återanvändas vid riskbedömningar av andra typer av data som också omfattas av öppna datalagen.

1.3 Disposition och läsanvisningar

Denna rapport är uppdelad i sju kapitel och en bilaga. Det första kapitlet är en kort inledning till rapportens innehåll, och redogör för dess syfte och målgrupp. Kapitel 2 redogör för bakgrunden till varför en riskbedömningsmetod avseende Sveriges säkerhet inför tillgängliggörande av geodata behövs. Kapitlet beskriver även problembilden och förutsättningarna för att skapa en sådan metod. Kapitel 3 beskriver hur projektet har genomförts och hur MEGS har utvecklats. Kapitel 4 och 5 redogör för projektets resultat. Kapitel 4 består av en övergripande presentation av MEGS medan kapitel 5 redogör för hinder och behov för att genomföra riskbedömningar av geodata. Diskussion, slutsatser och referenser redovisas i kapitel 6–8.

Utöver denna rapport finns en separat processtöd som i helhet presenterar riskbedömningsmetoden.[9] Syftet med processtödet är att beskriva hur MEGS kan användas för att göra riskbedömningar av geodata med avseende på Sveriges säkerhet. Författarnas förhoppning är att den både ska fungera som övergripande beskrivning av metoden och som stöd att vända sig till under det praktiska arbetet med riskbedömningar. Processtödet innehåller även mallar som kan användas vid tillämpning av MEGS. Både denna rapport och rapporten med processstödet kan läsas separat.

9 Davidsson m.fl. *(2025)*.

2. Bakgrund och problembeskrivning

I detta kapitel redogörs för de förutsättningar som råder för att kunna bedöma om ett tillgängliggörande av geodata utgör en risk för Sveriges säkerhet. För att förstå den komplexa kontexten där denna typ av riskbedömning hamnar krävs en bred bakgrund. För att kunna utveckla en metod för riskbedömningen avseende Sveriges säkerhet behöver det först redas ut vad som menas med Sveriges säkerhet. Vidare behöver man förstå vilka krav som ställs på svensk förvaltning utifrån geodata. För att förstå dessa krav beskrivs den juridik som är relevant för öppna datadirektivet och dess genomförande i Sverige. Juridiken lyfter att samverkan är av betydelse vid riskbedömning samt att hänsyn till aggregering ska tas. Därav finns avsnitt som berör just samverkan och förvaltningen av Sverige, samt ett avsnitt om aggregeringsproblematiken. Eftersom metoden handlar om riskbedömning finns ett avsnitt om vad om krävs av en användbar riskbedömningsmetod. Slutligen beskrivs den ansats som denna rapport tar för att göra det möjligt att utveckla en riskbedömningsmetod avseende Sveriges säkerhet enligt öppna datalagen.

2.1 Sveriges säkerhet

En första fråga, är att reda ut vad som menas med Sveriges säkerhet samt vad som kan utgöra ett hot. Ett exempel på vad som anses omfatta Sveriges säkerhet kan hittas i 1 kap. 1 och 2 § i säkerhetsskyddslagen:

> Verksamhet som är av betydelse för Sveriges säkerhet eller som omfattas av ett för Sverige förpliktande internationellt åtagande om säkerhetsskydd (säkerhetskänslig verksamhet) (1 kap.1§) och preciserar sig till säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Med säkerhetsskyddsklassificerade uppgifter avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) eller som skulle ha omfattats av sekretess enligt den lagen om den hade varit tillämplig.

Dock har begreppet ”Sveriges säkerhet” – tidigare ”rikets säkerhet” – aldrig definierats uttryckligen, för att inte ge antagonistiska aktörer sådan detaljerad information, eller låsa fast sig vid en enskild definition då förutsättningarna förändras över tid.[10] Sveriges säkerhet anses emellertid bestå av två delar: den yttre och den inre säkerheten.[11]

I totalförsvarspropositionen 2024/25:34 skriver regeringen:[12]

> Försvarsberedningen konstaterar att stater i större utsträckning än tidigare använder sig av olika typer av antagonistiskt agerande som kan användas i stället för, i kombination med eller som förberedelse till militärt våld. Maktmedel såsom otillbörlig informationspåverkan, desinformation, politiska påverkansoperationer, ekonomiska åtgärder, cyberangrepp, illegal underrättelseinhämtning, utnyttjande av juridiska sårbarheter samt fysiskt sabotage kan användas för att påverka andra staters politik och samhällen. Detta gör det svårt att dra en gräns mellan inre och yttre säkerhet samt mellan militära och icke-militära hot, vilket kräver ett nära samarbete mellan samtliga underrättelse- och säkerhetstjänster oavsett om de är satta att hantera yttre eller inre hot. Den nationella samverkan behöver därför fortsatt fördjupas.

Den yttre säkerheten har tidigare främst utgått från totalförsvaret men har i och med insikten att även andra verksamheter är centrala för landets funktion breddats. Exempelvis har det tidigare ansetts att Sveriges yttre säkerhet ska vara ”till skydd för Sveriges försvarsförmåga, politiska oberoende och territoriella suveränitet” och utgöra ”skyddet för Sveriges oberoende – i betydelsen självständighet och suveränitet – och bestånd”.[13]

10 Prop. 2017/18:89.

11 Prop. 1995/96:129, prop. 2017/18:89.

12 Prop. 2024/25:34. Totalförsvaret 2025–2030.

13 Prop. 2017/18:89.

I prop. 2017/18:89 preciseras begreppets nutida betydelse som att den yttre säkerheten utgörs av två dimensioner, *territoriell suveränitet* och *politisk självständighet*:

> Sveriges yttre säkerhet kan delas in i territoriell suveränitet och politisk självständighet. En viktig beståndsdel är den nationella försvarsförmågan av Sveriges territorium […]. I den uppgiften ligger att kunna försvara Sverige och främja svensk säkerhet, upptäcka och avvisa kränkningar av det svenska territoriet samt värna om Sveriges suveräna rättigheter och nationella intressen inom Försvarsmaktens verksamhet […]. Utöver Försvarsmakten finns andra verksamheter, t.ex. inom försvarsindustrin, som är viktiga […]. Sveriges oberoende och handlingsfrihet, politisk självständighet, handlar om att upprätthålla förmågan att förebygga och avvärja brott enligt framförallt spionerilagstiftningen […][14]

Vad som avses med den inre säkerheten preciseras också i prop. 2017/18:89:

> Sveriges inre säkerhet rör påverkan på förmågan att upprätthålla och säkerställa Sveriges statsidé avseende funktion, handlingsfrihet och oberoende. Säkerhetsskyddet för Sveriges inre säkerhet handlar till stor del om att skydda särskilt kritiska anläggningar, funktioner och informationssystem för Sveriges demokratiska statsskick, rättsväsende eller brottsbekämpande förmåga. […] samhällsviktig verksamhet kan bedömas röra Sveriges säkerhet. Verksamheter som […] definieras som samhällsviktiga finns ofta inom sektorerna energiförsörjning, livsmedelsförsörjning, elektroniska kommunikationer, vattenförsörjning, transporter och finansiella tjänster. Avgörande för om sådan verksamhet kan anses röra Sveriges säkerhet bör vara om en antagonistisk handling (exempelvis spionerі, sabotage eller terroristbrott) skulle kunna medföra skadekonsekvenser på nationell nivå. Sådana skadekonsekvenser kan t.ex. vara störningar i eller bortfall av leveranser, tjänster och funktioner som är nödvändiga för samhällets funktionalitet ur ett nationellt perspektiv.[15]

Även den inre säkerheten kan alltså anses bestå av två dimensioner: skydd för det *demokratiska statsskicket* och *skydd av samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå*. Exempel på vad som kan utgöra hot mot den inre säkerheten presenteras i prop. 1995/96:129:

> Ett exempel är försök att ta över den politiska makten genom uppror, men också användning av våld, hot eller tvång mot statsledningen i syfte att påverka politikens utformning. Försök att systematiskt hindra medborgarna från att utnyttja sina demokratiska fri- och rättigheter bör också räknas till hoten mot rikets inre säkerhet. Det förtjänar i detta sammanhang att framhållas, att det skall röra sig om kriminella aktiviteter […][16]

> Ett hot mot rikets säkerhet som säkerhetsskyddsförordningen skall förebygga är omstörtande verksamhet, dvs. sådan subversiv eller underminerande verksamhet som syftar till att undergräva förtroendet för vårt politiska system eller för att förbereda ett maktövertagande med illegala metoder. Denna verksamhet kan vara såväl ett led i inhemska gruppers eller organisationers strategi, som initierad och finansierad av främmande makt i syfte att bereda vägen för en militär intervention.[17]

Notera att här används begreppet *rikets säkerhet* medan det i nyare författningar har övergått till *Sveriges säkerhet*. De två begreppen ska uppfattas som synonyma (liksom *nationell säkerhet* som endast används i direkt överföring från EU-lagstiftning).[18]

Eftersom det saknas en entydig definition av Sveriges säkerhet används ovanstående som ett sätt att förklara dess innebörd. Detta eftersom riskbedömning av Sveriges säkerhet enligt öppna datalagen kräver att Sveriges säkerhet kan förstås och beskrivas. Utifrån ovanstående juridiska redogörelse kan alltså Sveriges säkerhet bedömas utifrån fyra dimensioner: *politisk självständighet, territoriell suveränitet, landets demokratiska statsskick och samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå*. Det är noterbart att ingen av dimensionerna av Sveriges säkerhet egentligen tar hänsyn till förlust av människoliv. Det betyder att en händelse som inte direkt leder till förlust av människoliv kan klassificeras som ett allvarligare hot mot Sveriges säkerhet än en händelse där många människoliv förgås. Eftersom rätten till liv kan anses vara en grundläggande rättighet så skulle en sådan aspekt kunna anses ingå

14 Prop. 2017/18:89.
15 Prop. 2017/18:89.
16 Prop. 1995/96:129.
17 Prop. 1995/96:129.
18 Prop. 2017/18:89.

i dimensionen Sveriges demokratiska statsskick men undersökta förarbeten ger ingen vägledning i detta fall. Vidare innebär ovanstående att det som utgör ett hot mot de fyra dimensionerna är av antagonistisk karaktär. Därför är antagonistiska risker i fokus för denna rapport. De fyra dimensionernas innebörd utvecklas och definieras i kapitel 4 för att vara användbara i den presenterade riskbedömningsmetoden. Öppna datalagen och tillhörande lagstiftning presenteras i nästa delkapitel.

2.2 Öppna datalagen förutsätter riskbedömning

Under 2022 implementerades EU-direktivet om öppna data och vidareutnyttjande av information från den offentliga sektorn (2019/1024). Enligt öppna datadirektivet ska offentliga aktörer inom EU öppet tillgängliggöra de digitala data som aktörerna producerar och på så sätt ”ta itu med hinder för ett brett vidareutnyttjande av information från den offentliga sektorn och offentligt finansierad information i hela EU”.[19] Den svenska lag som genomför EU-direktivet, lag (2022:818) om den offentliga sektorns tillgängliggörande av data, innehåller krav på en riskbedömning som tar sikte på bland annat Sveriges säkerhet. Öppna datalagen anger följande i 2 kap. 1 och 2§§:

> Tillgängliggörande ska ske i den utsträckning som krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och under förutsättning att det inte innebär risker för Sveriges säkerhet.
>
> Data ska tillgängliggöras i det befintliga formatet eller, om sökanden begär det och det är lämpligt samt praktiskt och tekniskt möjligt, i ett format som är öppet, maskinläsbart, och i förekommande fall, tillgängligt och sökbart, tillsammans med tillhörande metadata.[20]

I förarbetena skriver regeringen följande:[21]

> En risk kan vara av sådan karaktär att den inte fullt ut går att konkretisera men likväl sådan att det kan befaras att ett tillgängliggörande av vissa data kan innebära risker för informationssäkerheten, skyddet av personuppgifter eller Sveriges säkerhet. Det saknar betydelse om den eventuella risken kan antas inträda direkt vid tillgängliggörandet eller vid en annan tidpunkt. Vid en prövning av om data kan tillgängliggöras behöver emellertid den risk som förutses kunna beskrivas på en övergripande nivå och göras begriplig för en vidareutnyttjare.
>
> En myndighet eller ett offentligt företag ska alltså inte tillgängliggöra data för vidareutnyttjande om det finns en risk för att detta inkräktar på något av de uppräknade skyddsintressena. Riskerna gör sig särskilt gällande när data aggregeras och sedan bearbetas. Med aggregering avses bland annat att olika uppgifter, som var för sig inte omfattas av sekretess, tillsammans får ett nytt skyddsvärde. Vid bedömningen av om ett tillgängliggörande av data kan innebära risker för Sveriges säkerhet ska det beaktas om det kan medföra att information som är av betydelse för Sveriges säkerhet görs tillgänglig. Det kan avse stora mängder uppgifter som inte är säkerhetsskyddsklassificerade, men som av andra skäl är av betydelse för Sveriges säkerhet. Även uppkomsten av kombinatoriska effekter när data från olika källor sambearbetas bör uppmärksammas. I detta sammanhang behöver också risken att data ackumuleras och aggregeras för underrättelseinhämtning särskilt beaktas. En myndighet eller ett offentligt företag behöver alltså göra en allsidig bedömning utifrån de data som ska tillgängliggöras.

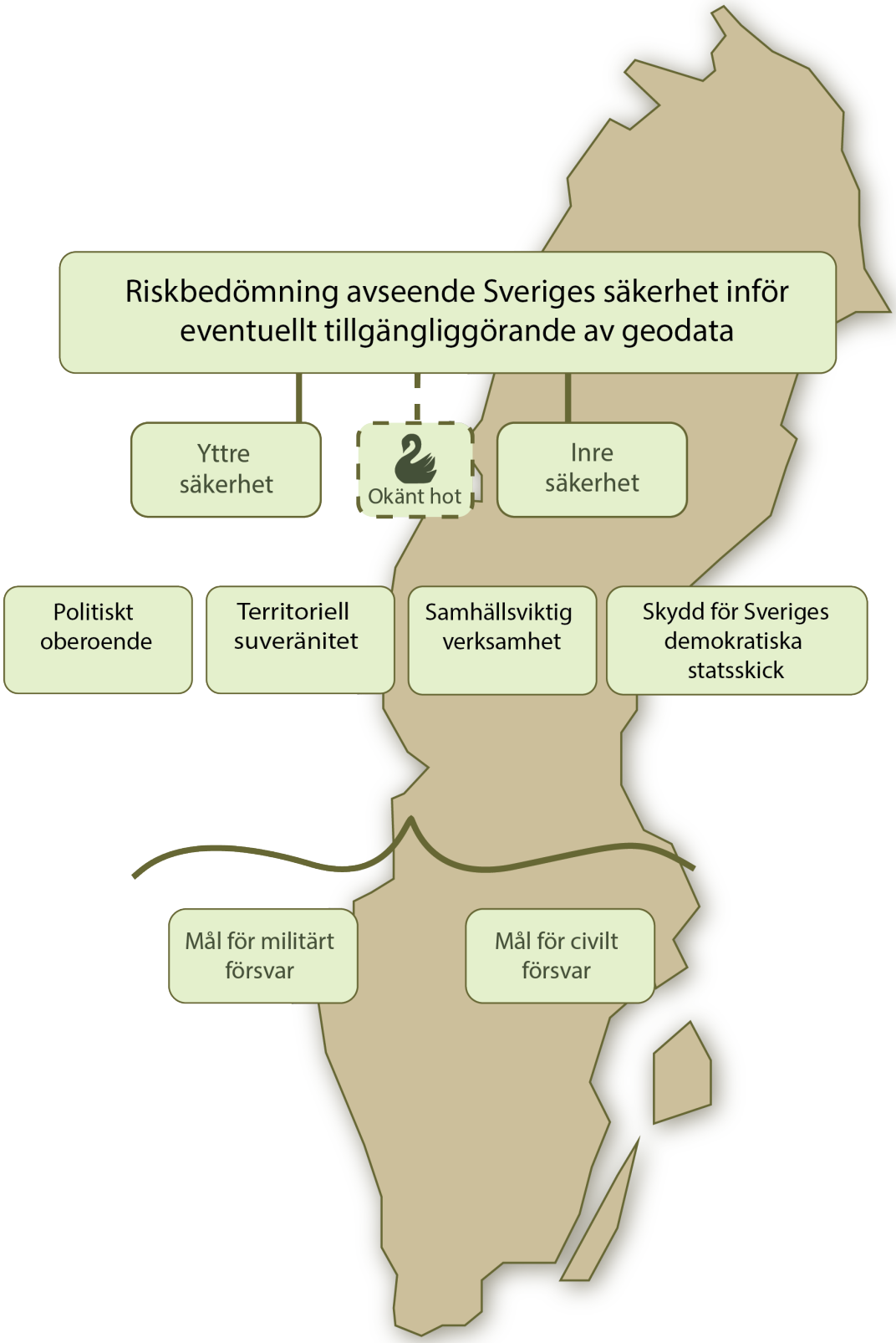
I förarbetena till öppna datalagen konstateras bland annat att en myndighet eller ett offentligt företag som avser att tillgängliggöra data för vidareutnyttjande bör göra en allsidig riskbedömning innan ett tillgängliggörande sker.[22] I en sådan bedömning bör riskerna med att tillgängliggöra data identifieras, analyseras och värderas. Om en myndighet bedömer att krav på informationssäkerhet och skydd av personuppgifter inte kan upprätthållas om vissa data tillgängliggörs för vidareutnyttjande, bör dessa inte göras tillgängliga. Detsamma gäller om ett tillgängliggörande av data kan innebära risker för Sveriges säkerhet (Figur 1). Riskbedömningsmetoden som presenteras i kapitel 4 avser riskbedömning av Sveriges säkerhet enligt öppna datalagen. Den inkluderar ej annan lagstiftning.

19 Europaparlamentets och rådets direktiv (EU) 2019/1024.

20 Befintligt format betyder något av de digitala format som data bearbetas eller lagras i hos den offentliga aktören. Om data är lagrat i olika format är det befintliga formatet något av de formaten som den lagras i (Prop. 2021/22:225. *Den offentliga sektorns tillgängliggörande av data*. s.82).

21 Prop. 2021/22:225.

22 Prop. 2021/22:225.



Figur 1: Figuren visar exempel på den bredd som de offentliga aktörerna behöver ta hänsyn till vid tillgängliggörande, gällande riskbedömning avseende Sveriges säkerhet. Målen kommer från regeringens proposition 2024/25:34 Totalförsvaret 2025–2030. De dimensioner som här anses utgöra Sveriges säkerhet är politiskt oberoende, territoriell suveränitet, landets demokratiska statsskick och samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå.

2.3 Olika risker utifrån olika lagstiftningar

Som nämnts i föregående delkapitel inkluderar rapportens riskbedömningsmetod inte andra risker än de som är kopplade till Sveriges säkerhet enligt öppna datalagen. För kännedom görs ändå en kortfattad genomgång av annan lagstiftning som kan vara relevant att ta hänsyn till. Detta ska dock inte ses som uttömmande, utan varje aktör behöver göra en omvärldsbevakning och identifiera den lagstiftning som berörs.

Samhällets aktörer hanterar en rad typer av risker, alltifrån naturolyckor till antagonistiska hotaktioner och vad som är gemensamt för denna typ av riskarbete är att arbetet begränsas till en specifik verksamhet. Exempelvis genomför en kommun risk- och sårbarhetsanalyser för just sitt geografiska område.[23] Ett annat exempel är en myndighet som genomför riskbedömning inom informationssäkerhet.[24] För flera av dessa risker finns vägledningar och annat sorts stödmaterial för att underlätta riskarbetet.

En förutsättning för att tillgängliggörande av geodata ska vara möjligt är att tillgängliggörandet sker enligt gällande rätt. Det får alltså inte finnas hinder enligt offentlighets- och sekretesslagen, integritetsskyddslagstiftning eller annan relevant lagstiftning för att tillgängliggöra informationen. Relevanta skyddskrav ska ha bestämts för informationen i samband med myndighetens informationssäkerhetsarbete enligt MSB:s föreskrifter och i relevanta fall enligt säkerhetsskyddslagen.

Att myndigheter ska bedriva ett riskbaserat och systematiskt informationssäkerhetsarbete framgår redan av andra författningar. Informationen ska bland annat vara placerad i informationssäkerhetsklass utifrån aspekterna konfidentialitet, riktighet och tillgänglighet för att identifiera konsekvenser av ett otillräckligt skydd vid och under tillgängliggörandet. Utifrån genomförd placering i informationssäkerhetsklass och riskbedömning ska ändamålsenliga och proportionella säkerhetsåtgärder införas.[25]

I säkerhetsskyddslagen finns det bestämmelser om säkerhetsskyddsklassificering av uppgifter utifrån den skada som ett röjande av uppgiften kan medföra för Sveriges säkerhet.[26] För personuppgifter finns det särskilda regler kring konsekvensbedömning av den planerade behandlingen som sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.[27]

Bedömning av risk vid tillgängliggörande av geodata är inte fråga om en tillämpning av säkerhetsskyddslagen eller en bedömning av sekretess då dessa redan ska hanteras enligt utarbetade metoder och med stöd av berörda tillsynsmyndigheter. Men, den sorts riskbedömning som i detta sammanhang blir aktuell rör sig inom flera riskområden. I och med att geodata omfattas av informationssäkerhet innebär det att informationslagstiftning kan beröras. Den potentiella risk som uppstår kan vara av fysisk karaktär såsom en antagonistisk handling, exempelvis att spränga broar. Det innebär att risken berör flera geografiska områden samtidigt, från lokala till nationella risk- och sårbarhetsanalyser. Dessutom, när det gäller information som är av betydelse för totalförsvaret, såsom uppgifter om skyddsobjekt, finns säkerhetsskyddslagen och utarbetade metoder för säkerhetsskyddsklassificering. Grundläggande kunskap när det gäller säkerhetsskydd kan sökas i Säpos vägledning i ämnet.[28] MSB ger ut vägledningar för informationssystem och säkerhet.[29] När det gäller digitalisering och informationssäkerhet sker genomförande genom de så kallade NIS2- och CER-direktiven som implementeras i svenskt lag under 2025.[30] Detta innebär att riskbedömning av geodata behöver reda ut vilka avgränsningar som föreligger sett till säkerhetsskyddslagen och informationslagstiftning. Rapportens föreslagna metod omfattar inte detta arbete.

När det kommer till riskbedömning enligt öppna datalagen och öppna datadirektivet är det inte möjligt att avgränsa potentiella risker eller riskarbetet till den egna verksamheten, oavsett om det är en kommun, länsstyrelse, myndighet eller ett företag. Geodata kan tillgängliggöras om det inte föreligger risk för Sveriges säkerhet samt om aggregeringsproblemtiken har beaktats.

23 Lag (2006:544) om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.

24 MSBFS 2020:6.

25 Se 4 och 6 §§ MSBFS 2020:6 och MSBFS 2020:7, MSB:s föreskrifter om informationssäkerhet för statliga myndigheter.

26 Se 5§ säkerhetsskyddslagen.

27 Se artikel 35 i den allmänna dataskyddsförordningen.

28 Säkerhetspolisen (2023b). *Vägledning i säkerhetsskydd, Säkerhetsskyddsanalys*.

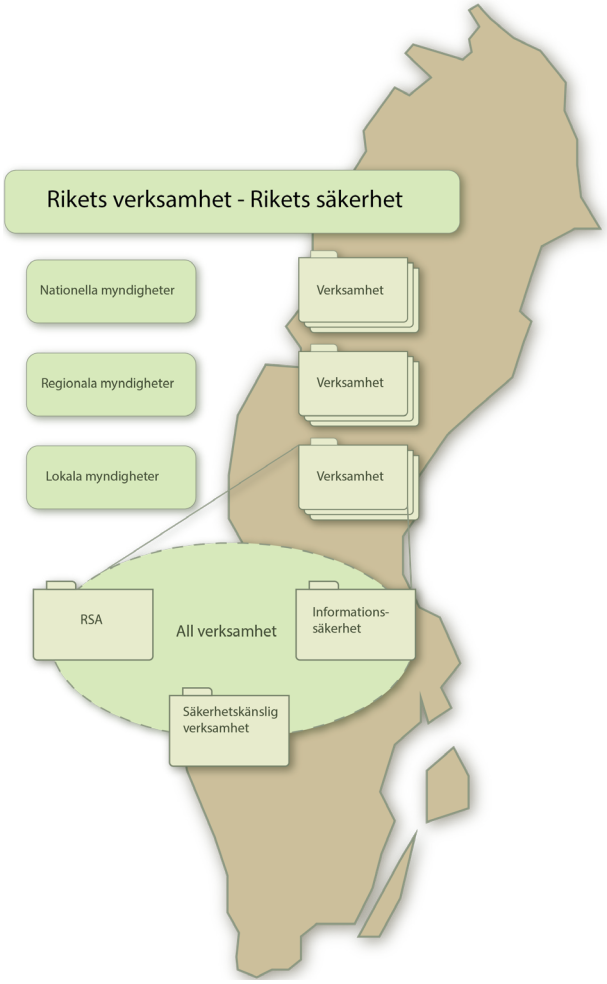
29 MSB (2023). *Vägledning, Säkerhetsåtgärder i informationssystem.* MSB2032.

30 SOU 2024:64 *Motståndskraft i samhällsviktiga tjänster*.

Detta innebär framför allt att:

- Den aktör som ska avgöra om en geodatamängd kan tillgängliggöras måste ta hänsyn till data hos andra aktörer på allt från lokal till nationell nivå för att avgöra om aggregering kan utgöra risk för Sveriges säkerhet.
- Risken hamnar eventuellt inte hos den aktör som innehar geodatamängden. Exempelvis kan en aktör som bedriver samhällsviktig eller säkerhetskänslig verksamhet (*aktör a*) få sin verksamhet hotad genom att en annan aktör (*aktör b*) tillgängliggör data som på något sätt berör den säkerhetskänsliga verksamheten (*aktör a*). (Detta innebär också att aktörer som inte alls innehar geodata, inte innehar data som innebär risk för Sveriges säkerhet, eller inte bedriver samhällsviktig eller säkerhetskänslig verksamhet, kan vara den som blir utsatt för risken på sådan nivå att det omfattar Sveriges säkerhet.)

Som tidigare nämnts är det inte möjligt att avgränsa potentiella risker eller riskarbetet till den egna verksamheten när det gäller riskbedömning av geodata. När riskbedömning ska ske avseende Sveriges säkerhet inför tillgängliggörande av geodata innebär det att riskbedömningen ska göras långt utanför den egna verksamheten. Riskbedömningen ska, utöver att omfatta den egna verksamheten, omfatta ett nationellt perspektiv (figur 2). Det innebär att om *länsstyrelse a* tillgängliggör geodata, skulle denna geodata kunna aggregeras med geodata från *länsstyrelse b* och *c*, samt med *myndighet d* och *e*. Den samlade mängden geodata innehåller information som tillsammans kan utgöra en risk för Sveriges säkerhet. Riskbedömningsmetoden som föreslås i kapitel 4 söker skapa förståelse för helheten på nationell nivå inklusive både verksamheter och relationer mellan alla dessa och deras respektive geodata.



Figur 2. Figuren illustrerar hur verksamheter på olika nivåer i samhället enskilt ansvarar för respektive arbete med risk- och sårbarhetsanalyser, informationssäkerhetsarbete och skydd för säkerhetskänslig verksamhet. Riskbedömningarna enligt öppna datalagen finns inte med i figuren.

2.4 Bra tillförlitlighet och begriplighet

Då denna rapport presenterar ett förslag på en metod för riskbedömning rörande Sveriges säkerhet behöver hänsyn tas till hur en metod ska utformas för att vara användbar för utövaren. Med en metod menas vanligen ett ”planmässigt tillvägagångssätt” för att systematiskt uppnå ett avsett resultat.[31] Eftersom metoder har studerats under lång tid finns riktlinjer för vad som utmärker tillförlitliga och passande metoder. Lämpliga metoder har såväl hög reliabilitet (att den ger samma resultat oavsett vem som använder metoden) som validitet (att den ger ett korrekt resultat för det som är avsett, till exempel att det verkligen mäter det som man vill mäta).[32] Idealt ska en metod alltså vara konsekvent.

En tredje aspekt är metodens användbarhet (eng. *utility*).[33] Om användbarheten är låg tenderar användarna att låta bli att använda metoden då den anses för krånglig och svår eller tar för lång tid. Därför är användbarheten något som måste tas hänsyn till när en metod utvecklas. Inom en verksamhet sker arbetet med risker genom ett

31 Svenska akademins ordlista SAOL 2021.

32 Bannigan, K., & Watson, R. (2009). Reliability and validity in a nutshell. Journal of Clinical Nursing, 18(23), 3237–3243. https://doi.org/10.1111/j.1365-2702.2009.02939.x

33 Bannigan & Watson, (2009).

övergripande och samlat riskhanteringsarbete som inkluderar samtliga aktiviteter och funktioner genom att vara en integrerad del i organisationens ledningsstruktur och aktiviteter.[34] Riskbedömningar sker inom avgränsade områden av en verksamhet. Detta innebär att en riskbedömning inom ett specifikt område ska vara en del av organisationens riskhantering och ta del av mål, strategier och kultur som gäller för riskhanteringen. Det råder viss förvirring kring begreppsanvändningen av vad en *riskbedömning* avser. Exempelvis använder MSB orden riskbedömning och riskanalys synonymt med betydelsen *ett strukturerat arbetssätt för att identifiera förhållanden som kan hindra organisationen från att uppnå sina mål*. Vilka dessa mål är, varierar beroende på organisation och vilken del av organisationens verksamhet det är som ska riskbedömas. I denna studie är ett av målen att inte tillgängliggöra geodatamängder som innebär en risk för Sveriges säkerhet, enligt öppna datalagen. På grund av den inkonsekvens som råder gällande betydelsen av begrepp kopplade till arbete med att identifiera och bemöta risker, har vi valt att begränsa användningen av dem. Den presenterade riskbedömningsmetoden (kapitel 4) omfattar innebörden av begrepp såsom riskidentifiering, riskanalys och riskvärdering. Men istället för att använda dessa och andra begrepp, har vi valt att göra beskrivningar av de olika delar som metoden inkluderar. Detta sker med tanke på att metoden ska vara användbar för flera aktörer och förhoppningsvis passa in i respektive aktörs riskhanteringsarbete, oavsett begreppsanvändning och definition. Riskbedömningsmetoden syftar dock fortfarande till att besvara grundläggande frågor om risker: Vad kan hända? Vad blir konsekvenserna? Hur kan vi minska risken?

Vetenskapliga metoder kan delas in kvantitativa respektive kvalitativa metoder. Kvantitativa metoder kan vara enklare att standardisera och förbättra avseende reliabilitet men behöver inte ha hög validitet. Det är exempelvis vanligt att mäta och studera indikatorer som är lätta att mäta men utan att säkerställa om dessa indikatorer egentligen är tillförlitliga mått på det som man är intresserad av.[35] Forskning har visat att algoritmer ger bättre resultat än fria bedömningar då de senare påverkas av såväl bias som variabilitet, vilket de förra inte gör. Vid sådana riskbedömningar som avhandlas i detta arbete är det emellertid svårt att hitta rättvisande kvantitativa representationer och då blir algoritmer svåra, eller omöjliga, att tillämpa. Det är exempelvis inte möjligt att uppskatta objektiva sannolikheter för att riskerna ska realiseras utan man hänvisas till subjektiva uppskattningar av sannolikheterna. Dessa är vanligtvis varken särskilt träffsäkra eller rättvisande.[36] Människor har även svårt att överblicka konsekvenserna – framförallt de indirekta och de långsiktiga – av olika omvälvande händelser varför konsekvensbedömningar vanligtvis blir mycket osäkra. Det är inte ovanligt med metoder, särskilt kvalitativa metoder, som bygger på mänskliga bedömningar. Denna typ av metod är dock förenad med betydande brister avseende både reliabilitet och validitet.[37]

Den metod som presenteras i rapporten är baserad på mänskliga bedömningar i och med att det saknas underlag för att göra kvantitativa beräkningar. Syftet är också att den ska minska bias så mycket som möjligt och försöka klargöra vilka komponenter såsom vilka kompetenser och individer som behövs för att utföra en bedömning. Utgångspunkten är därför att riskbedömningarna görs i diskussion mellan olika aktörer, att slutsatser, rekommendationer och beslut motiveras och dokumenteras väl samt att alla som är inblandade i processen tar ansvar för att löpande testa, lära sig och bidra till metodens utveckling. Det kan göras genom att rangordna ett antal händelser efter konsekvensnivå. En sådan bedömning kan dock präglas av deltagarnas tidigare upplevelser, förutfattade meningar och fakta, alltså vilken riskperception som individerna har. Några faktorer som påverkar riskperceptionen är 1) om risken är känd eftersom en ny risk ofta bedöms som mer allvarlig jämfört med en tidigare känd risk, 2) om risken är observerbar, eftersom en osynlig risk bedöms som mer allvarlig, och 3) om rädslan för risken är stor, eftersom risker som innebär mycket lidande eller många döda bedöms som mer allvarliga jämfört med en risk med låg konsekvens men hög sannolikhet. Även egenskaper och förutsättningar hos individen påverkar hur risken uppfattas. Ålder, kön, socioekonomiska förutsättningar och erfarenheter påverkar hur en individ väljer att fatta ett beslut.

Något annat som kan påverka hur en person väljer att agera vid en risk, är vilken koppling som personen har till det ord som avser händelsen. Till exempel väljer vi att spela på lotto eller hästar, trots låg sannolikhet att vinna, eftersom det är vinsten som förknippas med risken. Samma resonemang förklarar varför det är svårt att motverka

34 Svenska institutet för standarder. (2022). *Informationssäkerhet, cybersäkerhet och integritetsskydd – Vägledning om riskhantering inom informationssäkerhet* (ISO/IEC 27005:2022, IDT) Svenska institutet för standarder. (2018). *Riskhantering – Vägledning* (ISO 31000:2018, IDT). MMSB (2024). *Riskhantering*. https://metodstod-informationssakerhet.msb.se/sv/utforma/riskhantering/ [Hämtad 2025-05-13].

35 James, P. (2015). *Urban Sustainability in Theory and Practic*e. Abingdon: Routledge.

36 Se t.ex. Taleb, N. N. (2010). *The Black Swan. The Impact of the Highly Improbable* (2nd ed.). New York: Random House.

37 Kahneman, D., Sibony, O., & Sunstein, C. R. (2021). *Noise: A Flaw in Human Judgment.* New York: Little Brown & Co.

en oro hos allmänheten gällande risker med mycket liten sannolikhet att inträffa. Exempelvis upplever många personer kraftig oro inför att flyga eftersom flygningen kopplas till en flygolycka.[38]

Att riskperceptionen påverkar bedömning och beslutsfattande är ofrånkomligt. Däremot är experter ofta bättre på att väga in fakta jämfört med gemene man.[39] Dessutom, när beslut ska tas utifrån otillräckliga underlag, kan personer med erfarenhet inom ett område *använda* sin heuristik (egna tumregler och metoder) för att fatta ett beslut baserat på en begränsad mängd information. Det är inte helt ovanligt att detta sker, men det är sällan som det medges. Ofta efterfrågas matematiskt underlag. Men om det exempelvis inte finns data nog för att kvantifiera ett utfall så kan inte heller en matematisk linjär modell ge ett mer välgrundat svar än svaret från en person med erfarenhet som använder sin heuristik.[40]

Sammantaget medför de avvägningar och komplikationer som har beskrivits ovan att riskbedömningen oundvikligen präglas av stora osäkerheter. Liksom all verksamhet som har sitt fokus i framtiden är dessa osäkerheter oundvikliga.[41] Det finns olika metoder för att försöka hantera sådana osäkerheter, och även om vissa av dessa utgår från data och mekanistiska samband, exempelvis olika modellverktyg, baseras de flesta på mänskliga bedömningar.[42] Det finns dock några faktorer att ta hänsyn till för att skapa en sund bedömningskultur, exempelvis:

- Bedömningarna blir vanligen bättre om de görs av de som har den största kompetensen i frågan som avhandlas.[43]
- Relativa bedömningar (dvs. att rangordna bedömningsobjekten) är vanligen mer robusta än absoluta bedömningar men kan ge orimliga resultat om det man rangordnar egentligen symboliserar absoluta egenskaper.[44]

Ovanstående två faktorer har den föreslagna metoden försökt att inkludera.

2.5 Aggregeringsproblematik

En särskild utmaning vid riskbedömning är att avgöra om någon utomstående har möjlighet att kombinera viss geodatamängd, hädanefter benämnt analysobjektet, med andra datamängder så att nya data eller ny information uppstår, vilka i sin tur kan innebära en risk.[45] Generellt kan det handla om vilken data som helst, exempelvis andra öppna data, kommersiella data, data bearbetade eller helt skapade med AI-teknik[46] eller till och med känsliga datamängder anskaffade på illegal väg. Dessa data kan också representera uppgifter inom vitt skilda områden såsom beskaffenhet hos terrängen, livsmedelsproduktion, transportmöjligheter, uppgifter om anläggningar på strategiska platser vilka är viktiga för försvarsförmågan eller känsliga personuppgifter.

Att lägga samman och kombinera data- eller informationsmängder brukar allmänt benämnas aggregering. I de fall sammanläggningen är avgränsad till enbart samma typ av data- eller informationsmängder, till exempel samma typ av data men från olika tidpunkter, används ofta begreppet ackumulering.

I det arbete med riskbedömningar som rapporteras här utgörs analysobjekten av geografiska data. Att analysobjektet är av en viss typ innebär dock inte någon begränsning vad gäller de typer av datamängder som kan bli aktuella vid aggregering. För att en sammanläggning ska vara meningsfull och inte bara medföra en ännu större datamängd, där stora delar är orelaterade, bör det finnas någon meningsfull koppling eller relation mellan enskilda dataelement. Sammanläggningar som baseras på mer eller mindre artificiella relationer, till exempel en koppling mellan adresser och färgtoner hos målarfärger baserad på deras begynnelsebokstav, är föga meningsfulla även om de är teoretiskt möjliga.

38 Slovic, P., Peters, E., Finucane, M. L. & MacGregor, D. G. (2005). Affect, risk, and decision making. *Health Psychology* 24(4), 35-40. 10.1037/0278-6133.24.4.S35. Breakwell, G. M. (2007). *The psychology of risk*. Cambridge: Cambridge University Press.

39 Slovic, P. m.fl. (2005). Breakwell, G. M. (2007).

40 Mousavi, S., & Gigerenzer, G. (2014). Risk, uncertainty, and heuristics. *Journal of Business Research*, 67(8), 1671-1678. 10.1016/j.jbusres.2014.02.013

41 Clardy, A. (2022). What can we know about the future? Epistemology and the credibility of claims about the world ahead. *Foresight*, 24(1), 1–18. https://doi.org/10.1108/FS-01-2021-0020

42 Beard, S., Rowe, T., & Fox, J. (2020). An analysis and evaluation of methods currently used to quantify the likelihood of existential hazards. *Futures*, 115, 102469. https://doi.org/10.1016/j.futures.2019.102469

43 Kahneman, D., Sibony, O., & Sunstein, C. R. (2021).

44 Kahneman, D., Sibony, O., & Sunstein, C. R. (2021).

45 Prop. 2021/22:225.

46 Artificiell intelligens avser system som uppvisar intelligent beteende genom att analysera sin miljö och vidta åtgärder – med viss grad av självständighet – för att uppnå särskilda mål." Artificiell intelligens för Europa, meddelande från kommissionen till europaparlamentet, europeiska rådet, rådet, europeiska ekonomiska och sociala kommittén och regionkommittén. Bryssel den 25 april 2018.

Riskbedömningen av analysobjektet behöver ta i beaktande att aggregering i princip kan ske med vilka datamängder som helst så länge sammanslagningen är någorlunda meningsfull. Risken är därmed stor att arbetet med analys av potentiella aggregeringar och konsekvenser snabbt kan bli omfattande och till och med upplevas helt oöverblickbart. Antalen möjliga aggregeringar av ett analysobjekt med en eller flera datamängder är i princip obegränsad och en fullständig genomgång av alla kombinationer är inte praktiskt möjlig.[47]

Riskbedömningen av analysobjektet behöver också avgöra analysobjektets roll och relevans i de fall den sammanslagna datamängden resulterar i ny information som innebär en risk. Med andra ord behöver man avgöra om analysobjektet är oersättligt för att information som innebär en risk ska uppstå och därmed utgör en kritisk datamängd. En *kritisk datamängd* är en datamängd där en aggregation av datamängden med några övriga datamängder utgör en risk samtidigt som de övriga datamängderna vare sig enskilt eller tillsammans utgör en risk, det vill säga att om den kritiska datamängden avlägsnas från aggregationen så upphör risken. Det kan uttryckas mer koncist som ett logiskt uttryck, se uttrycket (figur 3). I riskbedömningen innebär analys av aggregering att man ska kunna avgöra om uttrycket är uppfyllt, det vill säga är sant eller inte. Uttrycket läses så här: det existerar en delmängd av universumet av datamängder sådan att delmängden tillsammans med analysobjektet utgör en risk samtidigt som delmängden själv inte utgör en risk.

$$\mathrm{P} = \exists A\,[(A \cup \{ao\} \rightarrow r) \wedge (A \rightarrow \neg r)] \quad \text{där } A = \{x \mid x \in I \wedge x \neq ao\}$$

I	Universum av data- eller informationsobjekt
A	Delmängd av I där ao ej ingår
$ao \in I$	Analysobjektet
$r \in \{\mathcal{T}, \mathcal{F}\}$	Risk (sant eller falskt)

Figur 3 En kritisk datamängd är en datamängd sådan att en aggregation av datamängden med några övriga datamängder utgör en risk samtidigt som de övriga datamängderna tillsammans inte utgör en risk, det vill säga om den kritiska datamängden avlägsnas från aggregationen så upphör risken. Det här kan uttryckas med det logiska uttrycket P. Uttrycket har tagits fram av projektgruppen i syfte att förstå problembilden ytterligare.

För att analysen av aggregering och dess konsekvenser i riskbedömningen inte ska bli ohållbart omfattande behöver det praktiska arbetet fokuseras. En lämplig utgångspunkt är att rikta fokus mot aggregeringar som bedöms meningsfulla med beaktande av analysobjektet självt och det aktuella säkerhetsläget inom vilken riskbedömningen sker. Potentiella datamängder för aggregering bör sökas på bredast möjliga sätt och med beaktande av att kunna forma meningsfulla aggregeringar med analysobjektet. I det arbetet kan samverkan med utomstående experter och befattningshavare med ansvar för framtagning och hantering av data och information inom andra organisationer än där analysobjektet har sin hemvist vara av stort värde. Tillsammans i grupp har man större möjligheter att identifiera och uppmärksamma potentiella datamängder för aggregering vilket minskar risken att något väsentligt förblir oprövat.

I riskbedömningen arbetar man med att identifiera aggregeringar som kan komma att innebära risker. Som ett stöd i arbete kan man formulera och besvara olika frågor relaterade till analysobjektet och säkerhetsläget.

47 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*, 48, 121-126. 10.5194/isprs-archives-XLVIII-4-W12-2024-121-2024. Prop. 2021/22:225, s.34.

Nedan presenteras några exempel på frågor. Listan ska bara ses som exempel och kan behöva modifieras.

- Går det att utläsa förhållanden om bevaknings- eller andra säkerhetsåtgärder?
- Går det att utläsa uppgifter om användning av eller verksamhet vid skyddade anläggningar?
- Går det att utläsa uppgifter om samhällsviktig verksamhet?
- Kan uppgifter möjliggöra eller kraftigt underlätta terrorism?
- Finns det uppgifter om stora ekonomiska, miljörelaterade eller andra samhälleliga värden?
- Kan uppgifter främja utbredning och befästande av organiserad brottslighet?
- Röjs uppgifter, direkt eller indirekt, som individer eller verksamheter behöver kunna skydda mot allmän kännedom?

Nedan följer ett påhittat scenario för att exemplifiera vad aggregering av flera olika typer av datamängder skulle kunna medföra.

Exempelscenario:
En antagonist har etablerat ett IT-system som kontinuerlig bevakar och tar hem alla öppna data som svenska myndigheter och andra organ tillgängliggör på internet. Systemet är utformat för att upptäcka när data uppdateras eller nya data tillkommer, varpå den datamängden laddas hem. Därefter bearbetas data med automatiska metoder, bland annat med automatiserad mönsterigenkänning med stöd av artificiell intelligens, AI. Resultaten av analysen sparas och med jämna mellanrum sker en genomgång manuellt och resultaten värderas. Värderingen återmatas till AI-systemet för att förstärka sökande efter sådant som kan anses relevant och undertrycka sådant som bedöms vara av mindre intresse.

Bland resultaten framkommer information om ett avvikande mönster i data på en plats *långt ute i skogen*. Analysen har använt Lantmäteriets fastighetsdata och ortofoto, Skogsstyrelsens skogliga data och Naturvårdsverkets marktäcke och andra naturdata. Då fastighetsdata innehåller skogsfastigheternas gränser finns också indirekt information om avstånd mellan fastigheter och om vilka fastigheter som är grannar. Baserat på alla dessa data har systemet noterat ett avvikande mönster i en region med många mindre och mellanstora skogsfastigheter. Hos ett litet antal direkt angränsande skogsfastigheter uppvisar skogen exakt samma karaktär, till exempel ålder- och höjdfördelningar samt skötselmönster. Det som står ut är bland annat att fastigheterna karaktäriseras av väldigt liten aktivitet vad gäller skötselåtgärder och att det som faktiskt genomförs verkar vara precis samma åtgärd och utförs vid samma tidpunkt. Det verkar som att den ringa skötsel som genomförs är mycket väl samordnad och genomförs av samma aktör. Detta skiljer ut dessa fastigheter i den aktuella regionen. Systemägaren undrar vad det här kan betyda, finns det något på den här platsen som påverkar hur skogen sköts och utvecklas, något som inte finns markerat på några kartor?

Antagonisten går vidare och med hjälp av Lantmäteriets gratis online-tjänst tar man enkelt reda på vem som äger fastigheterna och var de bor. Ägarna visar sig vara utspridda över landet och ingen direkt koppling verkar finnas. Men med stöd av ägarnas namn och adress söker man vidare på internet och sociala medier. Data samkörs och återigen används mönsterigenkänning. Snart framkommer flera intressanta mönster och kopplingar. Alla personerna visar sig ha ett större intresse för försvarsfrågor än genomsnittet, bland annat med egna inlägg på sociala medier, verkar vara följare till influensers inom försvarsfrågor och har många gilla-markeringar för den typen av innehåll. Det finns också direkta länkar mellan några av personerna, man är följare eller vänner till varandra på sociala medier. Antagonisten hittar också information som pekar på att några verkar ha förflutet med anställningar som rör försvaret. Har man försök dölja något genom att dela ett större markområde på flera fastigheter och registrera dessa på några till synes helt orelaterade personer som ägare? Resultatet är att antagonisten beslutar att skicka personal till platsen för att rekognosera och samla mer information.

Det här exemplet, som är helt påhittat, syftar här till att peka på potentialen att hitta ny information vid aggregering av stora datamängder. Redan idag, med den teknik som finns allmänt tillgänglig är det relativt enkelt att kontinuerligt bevaka och ladda hem stora datamängder, lägga ihop data och med helt automatiska metoder leta efter mönster med AI-baserade metoder. Vilka möjligheter som den pågående kraftfulla utvecklingen inom artificiell intelligens öppnar för kan vi bara sia om. Helt klart är dock att aggregering och samkörning av mycket stora mängder data inte längre är science fiction. Avancerade metoder för automatiserad mönsterigenkänning i

stor skala används redan idag av de stora teknikbolagen[48] och de kommer bli allt mer sofistikerade och enklare att använda i framtiden. En jämförelse går att göra med utvecklingen av språkmodeller som nu erbjuder möjligheter till avancerade dialoger eller system för att automatiskt generera realistiska sekvenser med rörliga bilder som är svåra att skilja från riktiga filmer. Samhället behöver ta detta i beaktande och vara berett på att information, som kanske borde vara skyddad, kommer att kunna upptäckas och kartläggas på distans med de data som vi själva tillhandahåller.

2.6 Samverkan och samråd

I förarbetena uttrycks också att det kan vara lämpligt att en myndighet, vid bedömningen av om data som härrör från en annan myndighet kan göras tillgängliga, samråder med den myndighet som aktuella data kommer ifrån. Det kan även finnas behov av ytterligare vägledning i frågor som rör tillgängliggörande av data för vidareutnyttjande.[49]

I öppna data-utredningen[50] uttrycks att det finns en medvetenhet om de risker som aggregering (aggregering förklarades i föregående avsnitt) av olika datamängder kan ge upphov till. Utredningen menar att ett gediget förebyggande och strukturerat säkerhetsarbete är en nödvändig förutsättning för tillgängliggörande av öppna data. Hur detta arbete ska kunna ta hänsyn till alla potentiella risker som tillkommer eller påverkas genom tillgången till en stor mängd öppna data klargörs emellertid inte. Utredningen nöjer sig med att deklarera att ”vikten av samverkan mellan aktörerna betonas när det gäller att skaffa sig underlag för identifiering och analys av potentiella risker med tillgängliggörande av olika typer av information”.[51]

Samverkan lyfts fram vid lagstiftningen om tillgängliggörande av data. I förarbetena skriver regeringen följande:[52]

> En myndighet eller ett offentligt företag som avser att exempelvis göra en större datamängd direkt tillgänglig via internet för vidareutnyttjande bör lämpligen dokumentera sin analys och bedömning av om krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och inte innebär risker för Sveriges säkerhet. Vid behov kan en myndighet eller ett offentligt företag samråda med eller inhämta synpunkter från myndigheter eller andra aktörer vars verksamhet kan påverkas av det aktuella tillgängliggörandet. Det kan vara särskilt relevant om de data som en myndighet avser att tillgängliggöra härrör från en annan myndighet. Sådana kontakter kan även vara nödvändiga för att avgöra risker med att vissa data blir känsliga genom att de läggs samman med andra data som har gjorts tillgängliga av myndigheten eller av en annan aktör. För att bedöma eventuella risker med ett tillgängliggörande kan även kontakter med relevanta expertmyndigheter vara nödvändiga.

Eftersom samverkan återkommande lyfts fram som en del i att hantera aggregeringsproblematiken samt för att identifiera risker, är den presenterade metoden i kapitel 4 starkt präglad av samverkan.

2.7 Att dela information

Samverkan betonas som en viktig aspekt vid riskbedömning samt för att hantera aggregeringsproblematiken, men det finns en rad frågetecken som lagstiftningen inte förklarar hur de ska hanteras. Ett avgörande sådant är hur myndigheter kan dela information sinsemellan. I den svenska förvaltningsmodellen styrs myndigheterna av regeringen som också ansvarar för deras verksamhet. Myndigheterna är organisatoriskt fristående, vilket betyder att departementen och myndigheterna inte sitter ihop organisatoriskt. Det finns dock frågor som myndigheterna hanterar självständigt utan att vare sig regeringen eller enskilda ministrar får lägga sig i. Detta förbud mot påverkan omfattar även andra samhällsorgan och gäller hur myndigheterna i ett särskilt fall 1) ska besluta i ett ärende som rör myndighetsutövning mot en enskild eller mot en kommun, och 2) tillämpa lag.[53]

I den svenska rättsordningen är offentlighetsprincipen central. Den innebär att allmänheten, ofta enskilda individer och företrädare för media, har rätt till insyn i och tillgång till information om statens och kommunernas verksamhet, bland annat genom så kallade allmänna handlingars offentlighet. Denna rätt att ta del av allmänna

48 Ingemarsdotter, I., Eidenskog, D. & Hedtjärn Swaling, V. (2020), *Vilse i lasagnen? En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*, FOI-R--4814--SE. Stockholm, Totalförsvarets forskningsinstitut.

49 Prop. 2021/22:225.

50 SOU 2020:55. *Innovation genom information (Öppna data-utredningen)*.

51 SOU 2020:55 s. 35lff. *Innovation genom information (Öppna data-utredningen)*.

52 Prop. 2021/22:225.

53 www.regeringen.se [hämtad 2025-03-18].

handlingar kan begränsas genom sekretess. Bestämmelser om sekretess finns framför allt i offentlighets- och sekretesslagen (2009:400). Varje myndighet ansvarar för att den information som myndigheten hanterar omfattas av ett arbete med att skydda och klassificera information. Exempelvis ska information som omfattas av försvarssekretess placeras i säkerhetsskyddsklass. För att underlätta för samverkan och delning av information skulle det behövas tydligare regler och kring hur denna informationsdelning bör ske.

2.7.1 Samverkan i Sverige - exempel inom försvar och krisberedskap

För att underlätta samverkan mellan myndigheter har dock insatser skett inom försvars- och krisberedskapsområdet. Inom MSB har arbete bedrivits för att ta fram ett gemensamt sätt att tänka och arbeta på, för att stödja samverkan och ledning för att på så sätt ge en gemensam grund. I exempelvis MSB:s *Gemensamma grunder för samverkan och ledning vid samhällsstörningar* anges att funktionerna samverkan och ledning tillsammans ska bidra till att skapa effekt i form av inriktning och samordning.[54] Samverkan har stor betydelse när det handlar om sidoordnade aktörer där ingen har nyttjat något befintligt mandat eller på annat sätt har givits i uppdrag att bestämma över någon annan. Aktörerna måste då komma överens, och dialog är en förutsättning för att detta ska ske. Skyldigheten att stödja och samverka med andra aktörer följer av den så kallade ansvarsprincipen.

Samverkan är viktig inom cybersäkerhet och informationssäkerhet, där samverkan mellan offentliga och privata aktörer är av avgörande betydelse.[55] Inom detta område har samverkan genom det nationella cybersäkerhetscentret fått en fysisk samlokalisering där flera aktörer samverkar tillsammans på plats. Propositionen betonar behovet av att underlätta civil-militär samverkan och omvärldsbevakning på grund av den snabba och omfattande teknikutvecklingen som sker i den civila sektorn.

Inom försvaret finns flera exempel på samverkan, där civil-militär samverkan har varit och är viktig inom internationella insatser och generellt inom utvecklingen av totalförsvaret och där man måste dela information som är säkerhetskänslig eller sekretessbelagd. I FOI-rapporten *Civil och militär regional ledning och samverkan vid samordning av samhällets resurser i extraordinära situationer* anges att samverkan är ett medel för att åstadkomma samordning och detta kan ske på olika sätt genom personsammanträffande, via kommunikationsmedel eller genom ömsesidig information.[56]

Under pågående uppbyggnad av totalförsvaret har i rapporten *Handlingskraft* redovisats en modell för informationsdelning mellan aktörerna vilken bygger på sektionering.[57] Se figur 2 i *Handlingskraft* avseende informationsdelning på tre nivåer. Sektionering innebär regler för hur information ska delas, vilket innebär att ingen får ha all information. Sektioneringen kan ha geografisk, sektorsvis eller behovsvis indelning. När man väl har bestämt detta kan man välja metod för hur information ska spridas. Exempel på metoder och former är arbetsmöten, spel, remisser, och så kallade Silent periods (vanligt inom informationssäkerhetsområdet och där man måste höra av sig i de fall man har synpunkter och invändningar).

Detta projekt har tagit fäste på betydelsen av samverkan inom svensk förvaltning och betoningen av samverkan inom lagstiftningen om tillgängliggörande av data. Därför är riskbedömningsmetoden som rapporten presenterar i kapitel 4, starkt präglad av samverkan mellan myndigheter och aktörer.

2.8 Utmaningar med riskbedömningar

I den vetenskapliga litteraturen finns många olika definitioner av risk beroende på syfte och kontext.[58] Ofta operationaliseras risk som kombinationen av sannolikhet och konsekvens. Författarna till denna rapport anser, i överensstämmelse med Säkerhetspolisens vägledning för säkerhetsskydd,[59] att denna operationalisering är olämplig för att bedöma vilka risker för Sveriges säkerhet tillgängliggörande av geodata medför. Säkerhetspolisen

54 MSB (2018). *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. MSB777.

55 Se bland annat totalförsvarspropositionen 2024/25:34.

56 Carlbom, O., Douglas, D., Larsson, P. & Lindgren, R. (2001). *Civil och militär regional ledning och samverkan vid samordning av samhällets resurser i extraordinära situationer.* FOI-R--0064--SE. Totalförsvarets forskningsinstitut, Stockholm.

57 Försvarsmakten & MSB (2021). *Handlingskraft. Handlingsplan för att främja och utveckla en sammanhängande planering för totalförsvaret 2021-2025.* FM2021-17683:2, MSB2020-16261-3.

58 T.ex. Hansson, S. O. (2004). Philosophical Perspectives on Risk. Techné, 8(1), 10–35; Aven, T., Renn, O., & Rosa, E. A. (2011). On the ontological status of the concept of risk. *Safety Science,* 49(8), 1074–1079. https://doi.org/10.1016/j.ssci.2011.04.015; Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023; Aven, T., Ben-Haim, Y., Boje Andersen, H., Cox, T., Droguett, E. L., Greenberg, M., m. fl. (2018). *Society for Risk Analysis Glossary*. Retrieved March 6, 2024, from https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf

59 Säkerhetspolisen, (2023b). Vägledning i säkerhetsskydd. Säkerhetsskyddsanalys.

skriver i sin vägledning att: ”Ytterligare en viktig distinktion är att säkerhetsskyddsanalysen inte tar hänsyn till den bedömda sannolikheten för att olika händelser ska inträffa, och inte heller till kostnaderna för de åtgärder som ska vidtas, vilket riskanalyser vanligtvis behöver förhålla sig till.”[60]

Osäkerheter[61] är en naturlig del av riskbedömning eftersom risk i sig innebär att det inte går att säga med säkerhet att en händelse kommer att inträffa eller vad dess konsekvenser blir. Hur stor osäkerheten är beror på tillgången till, och kvaliteten på, relevant information och data.[62] Att det finns ett tydligt samband mellan orsak och verkan kan räcka för att bedöma en så kallad enkel risk. För att kunna göra denna bedömning krävs att det finns ett gott underlag, att de negativa konsekvenserna av en händelse är kända, att osäkerheten i bedömningarna är låg samt att det finns en överensstämmelse bland experter om ämnesområdet. Ofta finns då ett omfattande underlag som möjliggör statistiska analyser av sannolikhet och konsekvensbedömningar kan göras baserat på tidigare inträffade händelser.[63]

De risker som däremot inte har ett tydligt eller linjärt samband mellan orsak och verkan, och inte heller kan mätas numeriskt, är så kallade komplexa risker. För dessa risker saknas kunskap och erfarenhet om konsekvenserna. Detta är händelser som omfattas av stor osäkerhet och svårighet att på förhand identifiera dem eller händelsekedjan bakom.[64] Risker orsakade av geodata med avseende på Sveriges säkerhet, kan antas vara en komplex risk.

Tidsperspektivet är en annan komplicerande faktor för att riskbedöma geodata. Tidsperspektivet är viktigt, men svårt att fastställa då samhällets förändringar kan påverka risker. Längre tidsperspektiv innebär ökad komplexitet, då bedömningen kan baseras på dagens eller ett framtida samhälle. Teknisk, social och ekonomisk utveckling påverkar riskens utveckling.[65] Det är svårt att definiera en relevant tidsaspekt vid geodataanalyser, då utvecklingen går snabbt och en all-risk-ansats där alla potentiella risker identifieras och analyseras inte är möjlig. Men det finns heller inte, enligt vår uppfattning, någon egentlig rekommendation om rimlig tidsaspekt att utgå ifrån. Förarbetena till öppna datalagen nämner angående tidsaspekten att ”Det saknar betydelse om den eventuella risken kan antas inträda direkt vid tillgängliggörandet eller vid en annan tidpunkt”.[66] Vi konstaterar att bedömningar om framtiden innehåller stora osäkerheter.

I likhet med risker i vissa andra discipliner – exempelvis sådana som uppskattar existentiella risker[67] – saknas tillförlitliga data för att kunna kvantifiera sannolikheten för många av de risker som behöver beaktas i en riskbedömning med avseende på Sveriges säkerhet. För andra risker är sannolikheterna snedvridna på grund av att dessa händelser underrapporteras eller inte upptäcks. De flesta risker som ska bedömas gällande öppna geodata är okända och kommer förmodligen aldrig att realiseras, och även om så skulle ske är det inte säkert att de upptäcks, till exempel för att antagonisten håller sig dold. Jämför med cyberrisker där en antagonist inte nödvändigtvis ger sig till känna vilket innebär att risken är ett faktum men att den angripne inte vet om det.

Inte heller konsekvenserna av de händelser eller skeenden som behöver beaktas är i allmänhet möjliga att kvantifiera då de rör politiska värden på nationell nivå som territoriell integritet, politisk självständighet och det demokratiska statsskicket. Det finns visserligen exempel då sådana värden kvantifieras, eller snarare ges semikvantitativa form, men då oftast i syfte att rangordna värden, exempelvis för att jämföra länder utefter demokratisk mognad.[68] Därför behöver konsekvenserna, det vill säga negativ påverkan på Sveriges politiska självbestämmande och demokratiska statsskick samt samhällets funktionalitet, uttryckas och hanteras på annat sätt i metoden för att kunna avgöra om tillgängliggörande av geodata leder till risker för Sveriges säkerhet.

Här definierar vi risk som *en potentiell situation, händelse eller ett skeende med, negativ konsekvens för Sveriges säkerhet vilken kan uppstå eller förvärras som resultat av tillgängliggörande av öppna geodata*. Definitionen tydliggör att de risker som ska bedömas medför en negativ, men möjligtvis oklar, konsekvens för Sveriges säkerhet. Dessutom

60 Säkerhetspolisen (2023b), s. 7.

61 Hansson, S. O. (2022). Can uncertainty be quantified? *Perspectives on Science*, 30(2), 210-236. /10.1162/posc_a_00412

62 Winehav, M. & Nevhage, B. (Red.), (2011). *FOI:s modell för risk- och sårbarhetsanalys (FORSA)*. FOI-R--3288--SE. Totalförsvarets forskningsinstitut, Stockholm, Sverige.

63 Sonnsjö, H. & Mobjörk, M,. (2013). *Om indirekta, komplexa och oönskade händelser. Att analysera risker med stor osäkerhet.* FOI-R--3649--SE. Totalförsvarets forskningsinstitut, Stockholm.

64 Sonnsjö, H. & Mobjörk, M,. (2013).

65 Winehav, M., & Nevhage, B,. (2011).

66 Prop. 2021/22:225.

67 Beard et al., 2020; Baum, S. D. (2020). Quantifying the probability of existential catastrophe: A reply to Beard et al. *Futures*, 123, 102608. https://doi.org/10.1016/j.futures.2020.102608

68 Coppedge, M., Gerring, J., Altman, D., Bernhard, M., Fish, S., Hicken, A., et al. (2011). Conceptualizing and Measuring Democracy: A New Approach. *Perspectives on Politics*, 9(2), 247–267. https://doi.org/10.1017/S1537592711000880

signalerar ordet ”kan” att tillgängliggörande av en viss geodatamängd möjligtvis orsakar eller på annat sätt bidrar till de situationer, händelser och skeenden som utgör risker. Det finns alltså åtminstone två källor till osäkerhet knutet till möjliga risker: osäkerhet angående den kausala kopplingen mellan tillgängliggörande av en geodatamängd och de situationer, händelser och skeenden som kan leda till negativa konsekvenser, samt osäkerhet gällande konsekvensernas natur.

I detta kapitel har en rad svårigheter framkommit gällande möjligheten att genomföra en riskbedömning avseende Sveriges säkerhet inför tillgängliggörande av geodata: i) den som utsätts för risken är inte nödvändigtvis den aktör som tillgängliggör data, ii) hänsyn ska tas till aggregering, iii) tidsperspektivet är oklart, iv) att uppskatta sannolikhet är inte relevant vid bedömning av risker för Sveriges säkerhet, v) begreppet Sveriges säkerhet är inte definierat, varpå vi) konsekvenserna för Sveriges säkerhet eventuellt inte går att bedöma.

För att bemöta dessa svårigheter med att riskbedöma Sveriges säkerhet presenteras i denna rapport ett alternativt angreppssätt. Kapitel 4 presenterar en utvecklad metod för att göra riskbedömning avseende Sveriges säkerhet inför tillgängliggörande av geodata. För att hantera avsaknaden av data att basera bedömningarna på, har här istället för sannolikhet begreppet *relevans* införts. För konsekvenserna har projektet testat att göra en ansats att utveckla konsekvensnivåer utifrån en möjlig innebörd av Sveriges säkerhet. Utvecklingen av relevans och konsekvensnivåer presenteras i kapitel 3.

3. Projektets genomförande

Utifrån redovisningen i föregående kapitel om den kravbild som ges i lagstiftningen om tillgängliggörande av öppna geodata med stöd av en riskbedömning, har projektgruppen tagit på sig uppgiften att söka efter ett sätt att genomföra en sådan riskbedömning som fyller dessa krav. Här finns två stora utmaningar. Det gäller dels att förstå konsekvenserna för Sveriges säkerhet av tillgängliggörandet, något som inte är helt utrett (vad vi har kunnat utröna). Dels gäller det behovet av att arbetet ska ske i samverkan, vilket skapar utmaningar då vi rör oss inom ett område där information som behöver delas mellan aktörer kan vara eller bör vara sekretessbelagd. Sammanfattningsvis befinner vi oss inom ett omoget område där det finns stora behov av vidare fördjupningsarbete och klargöranden.

Arbetet i projektgruppen har, utöver utveckling av metod, till stor del handlat om att sätta syftet i en kontext, redogöra för det material som finns, förstå utmaningarna och vad som behövs för att uppfylla öppna datalagens krav.[70] Projektets resultat i form av en metod har utvecklats för att passa in i Lantmäteriets processer. I och med att arbetet har bedrivits parallellt med Lantmäteriets egen underlagsframtagning inför beslut om tillgängliggörande av specifika, så kallade värdefulla, datamängder den 3 februari 2025 har Lantmäteriets arbetsinsatser i projektet berört högst aktuella och relevanta frågor.

Kapitel 3 beskriver delarna i projektets genomförande. De har bestått av litteraturstudier, skapande av ett första utkast till metod, samt planering, genomförande och utvärdering av workshoppar med offentliga aktörer.

Metoden finns beskriven mycket översiktligt i kapitel 4. Metoden i dess helhet med tillhörande instruktion kring hur metoden är tänkt att genomföras finns som ett förslag till processtöd i en separat publikation *Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data* (2025).

3.1 Litteraturstudier

Litteraturinsamling har gjorts för att identifiera vilket material som redan finns och vad som saknas gällande stödmaterial för att riskbedöma data inför ett tillgängliggörande. Sökning efter vetenskapliga artiklar har skett utifrån sökord på engelska som *geospatial data* i kombination med begreppen *risk*, *risk management*, *risk analysis* och *threat*. Projektgruppen har även, utan framgång, gjort sökningar efter internationell litteratur från myndigheter för att få kunskap om hur riskhanteringen rörande geodata går till i andra länder.

Vidare har projektgruppen tagit del av det stödmaterial som svenska myndigheter har producerat inför tillgängliggörande av datamängder. Detta stödmaterial har dock varit begränsat, både gällande vilka som erbjuder stödmaterial samt hur innehållsrikt och tillämpligt materialet har varit. För att identifiera denna typ av litteratur har projektgruppen haft dialog med andra myndigheter rörande tillgängliggörande av öppna geodata, informationsdelning och relaterade frågor. Detta har skett för att förstå hur andra myndigheter har valt att ta sig an det arbete som öppna datalagen innebär. Gruppen har efterfrågat och fått ta del av underlag i form av arbetshandlingar med information från bland annat Myndigheten för digital förvaltning (DIGG), Myndigheten för samhällsskydd och beredskap (MSB), Sveriges geologiska undersökning (SGU), Stockholm stad samt Havs- och vattenmyndigheten (HaV). Muntlig insamling av information har också gjorts i form av webbmöten med andra informationsinsamlande myndigheter och med DIGG. Vägledningar rörande informationssäkerhet har inhämtats från MSB och Säkerhetspolisen. Vidare har sekretessområdet också berörts, varpå litteratur har inhämtats.

Ett närbesläktat område där arbetsmaterial har inhämtats är arbetet med risk- och sårbarhetsanalyser. Detta har skett genom att utgå från FOI:s modell för risk- och sårbarhetsanalys (FORSA), en metod som handlar om att bedöma risker för organisationer. FORSA-metoden beskrivs i en FOI-rapport[71] och bygger på en rad genomförda risk- och sårbarhetsanalyser för olika uppdragsgivare. FORSA togs fram för att stödja de svenska krisberedskapsaktörerna.[72] Det existerar även andra metoder i Sverige som används på liknande sätt.[73] Även ytterligare litteratur om riskbedömning och riskhantering har insamlats för att komplettera riskförståelsen utifrån detta projekts syfte.

70 Projektgruppen har bestått av två medarbetare från Lantmäteriet och fem från FOI, vilka har träffats löpande. Gruppmedlemmarna från FOI är experter inom geodata, teknik för inhämtning av sådan information samt personer med erfarenheter av risk- och sårbarhetsanalys från andra områden än geodata. Lantmäteriets medarbetare har lång erfarenhet av att bedöma risker kopplade till den information som myndigheten ansvarar för.

71 Winehav, M., & Nevhage, B. (2011).

72 Winehav, M., & Nevhage, B. (2011).

73 Eriksson, C., Denward, C., Mickelsson, L. & Hedtjärn Swaling, V. (2020). *Kunskap för beredskap: Vad har risk- och sårbarhetsanalys gett för effekt hittills och hur kan nyttan öka?* FOI-R--4804--SE. Stockholm, Totalförsvarets forskningsinstitut.

3.2 Skapande av ett första utkast till metod

Det första utkastet till metod togs fram genom interna diskussioner i projektgruppen. Inspiration till metoden inhämtades även från befintliga metoder för risk- och sårbarhetsanalys, såsom den nämnda FORSA-metoden.[74] I denna ingår steg som handlar om att beskriva den verksamhet som är föremål för analysen, identifiera och bedöma händelser som kan medföra risker för verksamheten och hur konsekvenserna då kan se ut samt vilka åtgärder som kan vidtas för att begränsa konsekvenserna.

För det nya fält som beskrivs ovan har projektgruppen diskuterat möjliga ingående steg och hur man kan se på de begrepp som används inom risk- och sårbarhetsanalyser men även inom området systematiskt informationssäkerhetsarbete, där MSB på sin hemsida ger stöd för användare avseende vilka steg som behöver tas.

Under våren 2024 prövades och utvärderades det första utkastet vid den första i en serie av workshoppar. De därpå följande workshopparnas upplägg och inriktning påverkades av utfallet av föregående workshop (i tillämpliga fall).

3.3 Planering och genomförande av workshoppar

Sammanlagt har FOI anordnat tre workshoppar och Lantmäteriet har anordnat två workshoppar under 2024. Målsättningen med de tre workshoppar som FOI anordnade har varit att testa det utkast till metod som hade tagits fram under våren 2024 och få synpunkter på upplägget och ytterligare kunskap från experter som dagligen arbetar med dessa problemställningar. Målsättningen med de två workshoppar som Lantmäteriet anordnade var att samla synpunkter och erfarenheter inför konkreta underlag till beslut hos Lantmäteriet rörande tillgängliggörande av specifika geodatamängder.

I tabell 1 nedan återfinns en sammanställning av de workshoppar som har genomförts. Antal deltagare nedan inkluderar inte projektmedlemmar från FOI eller Lantmäteriet. Däremot inkluderas andra representanter från FOI och Lantmäteriet som har deltagit på workshopparna som experter.

Tabell 1. Sammanställning av genomförda workshoppar.

Workshop	Syfte	Deltagare	Utvärdering
Workshop 1 – anordnad av FOI	Testa ett utkast till metod för offentliga aktörer att i samverkan göra riskbedömningar av geodata vilka tillgängliggörs som öppna data.	15 representanter från statliga myndigheter	Skriftlig och muntlig
Workshop 2 – anordnad av FOI	Dokumentera offentliga aktörers behov för att kunna göra riskbedömningar av geodata med avseende på Sveriges säkerhet.	8 personer från kommuner och myndigheter som tillgängliggör geodata	Muntlig
Workshop 3 – anordnad av FOI	Identifiera och värdera vilka konsekvenserna för Sveriges säkerhet kan bli om geodata tillgängliggörs som öppna data.	14 personer från statliga myndigheter, kommuner och länsstyrelser	Skriftlig och muntlig
Workshop 4 – anordnad av Lantmäteriet	Genomföra bedömning av möjliga risker med att tillgängliggöra värdefulla datamängder som öppna geodata, inklusive att föreslå lämpliga åtgärder för skyddsvärda geodata och på detta sätt förse Lantmäteriet med argument till kommande beslutsunderlag rörande specifika datamängder.	18 representanter från statliga myndigheter	Skriftlig och muntlig
Workshop 5 – anordnad av Lantmäteriet	Genomföra bedömning av möjliga risker med att tillgängliggöra värdefulla datamängder som öppna geodata, inklusive att föreslå lämpliga åtgärder för skyddsvärda geodata och på detta sätt förse Lantmäteriet med argument till kommande beslutsunderlag rörande specifika datamängder.	19 representanter från statliga myndigheter	Skriftlig och muntlig

74 Winehav, M., & Nevhage, B., (2011).

3.3.1 Workshop 1

Den första workshoppen fokuserade på att testa det utkast till metod som inledningsvis hade tagits fram. Målet med workshoppen var att få deltagarnas utvärdering av de olika stegen i metoden samt deras syn på arbetssättets lämplighet för att åstadkomma en riskbedömning. Deltagarna utgjordes av representanter från olika statliga myndigheter som tillgängliggör eller hanterar geodata. Denna workshop utgick från enbart en hotaktör i form av en antagonistisk främmande makt. Inför workshoppen fick deltagarna ta del av agenda och scenarion samt ett memo om risker med tillgängliggörande av öppna geodata.[75]

3.3.2 Workshop 2

Syftet med workshop 2 var att undersöka de offentliga aktörernas behov av metod för att kunna göra riskbedömningar vid tillgängliggörande av geodata som öppna data. Målen med workshoppen var att:

- lista vilka behov deltagarna själva uttrycker att de har för att kunna genomföra riskbedömningar av geodata med avseende på Sveriges säkerhet på ett ändamålsenligt sätt
- dokumentera de hot och risker som deltagarna identifierar
- få ökad kunskap av hur deltagarna arbetar med aggregeringsproblematiken
- representanter från kommunala verksamheter och statliga myndigheter som tillgängliggör eller hanterar geodata hade fördjupade diskussioner, delvis i helgrupp och delvis i mindre grupper, rörande dessa frågor.

3.3.3 Workshop 3

Den tredje och sista workshoppen som FOI anordnade bestod av en fördjupning avseende det moment i metoden som handlar om att identifiera och värdera konsekvenser. Denna workshop innehöll även en diskussion om innebörden av begreppet Sveriges säkerhet. Då tidigare tester inte hade lett till ett identifierande och värderande av konsekvenser för Sveriges säkerhet på ett tillfredsställande sätt önskade projektgruppen att fokusera på just dessa teman under workshop 3. Mot bakgrund av detta valde projektgruppen att söka arbetssätt för att på ett bra sätt illustrera vad konsekvenserna kan bestå av. Syftet med denna workshop var därför att identifiera och värdera konsekvenserna för Sveriges säkerhet om geodata tillgängliggörs som öppna data. Målet med den tredje workshoppen var att utvärdera två olika arbetssätt för att identifiera och värdera konsekvenser för Sveriges säkerhet genom identifikation och värdering med hjälp av:

- scenarier och bedömningskriterier
- bedömningskriterier, men utan användning av scenarier.

För att få tid till utvärderingen valde projektgruppen att enbart utgå från en antagonist. Före workshoppen fick deltagarna ta del av agenda, scenarion samt ett memo om risker med öppna geodata.[76]

3.3.4 Workshop 4 och 5

Lantmäteriet anordnade under 2024 två workshoppar med stöd av det utkast till metod som hade tagits fram och de genomfördes under ledning av Lantmäteriets medarbetare i projektgruppen. FOI-representanter från projektgruppen deltog vid dessa workshoppar. Dessa workshoppar syftade till att myndigheter i samverkan skulle genomföra en bedömning av möjliga risker med att tillgängliggöra värdefulla datamängder som öppna geodata. I arbetet under workshopparna ingick uppgiften att föreslå lämpliga åtgärder för skyddsvärda geodata. Målet med workshopparna var att förse Lantmäteriet med synpunkter och erfarenheter inför kommande beslutsunderlag rörande specifika datamängder, avseende tillgängliggörande eller inte, eller med förbehåll och krav på användare.

Deltagarna utgjordes av representanter från statliga myndigheter som tillgängliggör mycket geodata samt myndigheter från försvars- och säkerhetsområdet. De fick inledningsvis en redovisning rörande analysobjekten och deras tillämpningar samt en föredragning om vilka förändringar öppna datalagen medför. Deltagarna fick därefter tillämpa metoden samt diskutera hotbilder och gemensamma risker med kombinerade geodata.

75 Winterdahl, M. m.fl. (2023).

76 Winterdahl, M. m.fl. (2023).

3.3.5 Kunskap om geodata och säkerhetsfrågor vid workshopparna

Deltagarna vid workshopparna har varit representanter från myndighet, länsstyrelse och kommun. Vissa deltagare har haft kunskap om geodata och stor erfarenhet av att informationsklassificera data inom detta område. Andra deltagare har istället erfarenhet av säkerhetsfrågor. Exempel på roller som har deltagit är informationsägare, informationshandläggare, säkerhetschefer och strateger. Deltagarna har huvudsakligen representerat statliga myndigheter med ansvar för geografisk information, exempelvis sådana myndigheter som deltar inom det så kallade Geodatarådet[77] och som har kunskaper om exempelvis land, vägar och vattendrag.

3.3.6 Beslut om analysobjekt

Analysobjekten, det vill säga de datamängder som behandlades vid workshopparna valdes ut av projektgruppen på grundval av tidigare diskussioner rörande eventuell känslighet och risker för Sveriges säkerhet i de fall dessa datamängder tillgängliggörs. Lantmäteriet fick ta det slutgiltiga beslutet kring val av analysobjekt. Vid workshopparna valdes även tematiska områden, exempelvis Sveriges vattendrag och omgivande hav eller Sveriges marktäcke. Beroende på tema har ett visst urval gjorts kring vilka myndigheter som har bjudits in.

3.4 Nytt problem kräver ny hantering

MEGS som presenteras i kapitel 4 är ett resultat av både litteraturstudier och utvärderingar efter ovan redovisade workshoppar. Samarbetet mellan FOI och Lantmäteriet har varit av avgörande betydelse. Lantmäteriets kunskap om de olika datamängderna och förståelsen för hanteringen av dessa har varit central, liksom det engagemang och den tid som har avsatts för att få metoden så användbar som möjligt. Tanken med MEGS är att den ska bidra till att uppnå mer enhetliga och konsekventa bedömningar genom en föreslagen struktur. En grundpelare i metoden är att involvera olika sorters kompetens och representanter från flera offentliga aktörer vid bedömning av riskerna. På grund av detta ingår i metoden ett omfattande förberedande arbete samt ett arbete som sker i samverkan med andra offentliga aktörer och internt vid den initierande aktören.

Litteraturstudier har gett förutsättning för att identifiera vilka aspekter som har varit väsentliga att ta med i förslaget till processtöd. Metoden är även utvecklad efter litteratur om hur riskbedömning kan göras, vilka hinder som finns för att göra noggranna och träffsäkra bedömningar samt hur man kan använda olika sorters svarsalternativ vid frågeställningar som ges till deltagarna. Workshoppar har gett inspel till om föreslaget arbetssätt utifrån dessa aspekter har fungerat samt vad som har behövt förändras.

Riskbedömningar görs ofta utifrån bedömning av sannolikhet och konsekvens. Eftersom det inte finns någon definition av Sveriges säkerhet är det även oklart hur allvarlig en konsekvens är för Sveriges säkerhet och det är i allmänhet inte möjligt att kvantifiera konsekvenserna. Som konstaterats ovan, är det dessutom olämpligt att ta hänsyn till sannolikheten vid bedömningar med avseende på Sveriges säkerhet. För att hantera dessa väsentliga hinder i en riskbedömningsmetod har projektgruppen infört begreppet *relevans* istället för sannolikhet. För konsekvenserna har projektet testat att göra en ansats att utveckla konsekvensnivåer utifrån en möjlig innebörd av Sveriges säkerhet. Relevans, konsekvensnivåer och dess kriterier för Sveriges säkerhet används i den föreslagna riskbedömningsmetoden MEGS.

3.4.1 Konsekvensnivåer och kriterier för Sveriges säkerhet

I kapitel 2 redogjordes det för att Sveriges säkerhet kan definieras utifrån yttre säkerhet (politisk självständighet och territoriell suveränitet) och inre säkerhet (landets demokratiska statsskick och samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå). Sveriges säkerhet kan alltså anses utgöras av fyra dimensioner.

Utifrån de fyra dimensionerna har åtta kriterier som beskriver olika grad av påverkan på Sveriges säkerhet utvecklats i projektet. Detta för att kunna bedöma konsekvenserna för Sveriges säkerhet. Kriterierna överensstämmer med dimensionerna, förutom kriteriet landets demokratiska statsskick som utvecklas till att istället bestå av fem kriterier: *grundläggande fri- och rättigheter, fria och rättvisa val, offentlighet och transparens, rättsstatens principer* samt *befolkningens förtroende för offentliga institutioner och det demokratiska beslutsfattandet* (tabell 2). Beslutet att utveckla dimensionen landets demokratiska statsskick till fyra separata kriterier föregicks av diskussioner inom projektgruppen. Den specifika utformningen gjordes efter diskussioner med juridiska experter på FOI. För att kunna avgöra hur allvarlig konsekvensen kan bli för Sveriges säkerhet utifrån de åtta kriterierna konstruerades,

77 Lantmäteriet. (u.å.). *Geodatarådet*. *https://www.lantmateriet.se/geodataradet*

utifrån lagstiftning, effektnivåer för respektive kriterium. Effektnivåerna består av fyra nivåer, *a-d*, där effektnivå a är den allvarligaste.

Kriteriets effektnivåer används för att bestämma hur allvarlig konsekvensen är. Det finns *fem konsekvens nivåer*: existentiell skada, allvarlig skada, begränsad skada, obetydlig skada eller okänd/oklar skada.

Tabell 2. Översikt av hur de åtta kriterierna konstruerats utifrån fyra dimensioner. De fyra effektnivåerna används för att förstå kriteriet och därmed vilken som blir den högsta konsekvensnivån, av fem, för Sveriges säkerhet. Kriterierna ska endast betraktas som exempel på sådana kriterier och inte uppfattas som en tillräcklig eller uttömmande lista som täcker alla aspekter av de fyra dimensionerna av Sveriges säkerhet.

Inre eller yttre säkerhet	Dimension	Kriterium	Effektnivå	Konsekvensnivå av skada på Sveriges säkerhet
Yttre säkerhet	Politisk självständighet	Politisk självständighet	a-d	Existentiell skada Allvarlig skada Begränsad skada Obetydlig skada Okänd/oklar skada
Yttre säkerhet	Territoriell suveränitet	Territoriell suveränitet	a-d	
Inre säkerhet	Landets demokratiska statsskick	Grundläggande fri- och rättigheter	a-d	
Inre säkerhet	Landets demokratiska statsskick	Fria och rättvisa val	a-d	
Inre säkerhet	Landets demokratiska statsskick	Offentlighet och transparens	a-d	
Inre säkerhet	Landets demokratiska statsskick	Rättsstatens principer	a-d	
Inre säkerhet	Landets demokratiska statsskick	Befolkningens förtroende för offentliga institutioner och det demokratiska beslutsfattandet	a-d	
Inre säkerhet	Samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå	Samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå	a-d	

Kriterierna ska endast betraktas som exempel på sådana kriterier och inte uppfattas som en tillräcklig eller uttömmande lista som täcker alla aspekter av de fyra dimensionerna av Sveriges säkerhet. Kriterierna, effektnivåerna och konsekvensnivåerna gäller endast konsekvenser av antagonistiskt ursprung och berör följaktligen endast hotaktörers agerande.

3.4.2 Relevans

För den typ av komplexa risker som ska beaktas här har ett alternativt angreppsätt utvecklats. Istället för att bedöma hur sannolikt det är att en konsekvens blir realiserad, används *relevans* för att bedöma i vilken omfattning som själva tillgängliggörandet av geodata bidrar till att konsekvensen realiseras.

Ett alternativ att tillgå när det inte är möjligt att bedöma sannolikhet är att inte inkludera detta steg, vilket är det alternativ som SÄPO använder gällande säkerhetsskydd.[78] I MEGS används relevans för att utveckla förståelsen för den risk som kan föreligga om geodata tillgängliggörs. Det är möjligt att identifiera konsekvenser, men om de inte kan härledas till tillgängliggjorda geodata är det inte geodata som är orsaken till risken. Om man bortsåg från relevansen, och alltså bara grundar sin bedömning på konsekvens, skulle det kunna innebära att geodata som egentligen inte innebär en risk för Sveriges säkerhet (för att relevansen är låg) ändå inte tillgängliggörs.

Ett annat alternativ för att hantera avsaknaden av sannolikhet är att inkludera sårbarhet i riskbedömningen. MSB lyfter i sin vägledning Säkerhetsåtgärder i informationssystem[79] att sårbarheter inom organisationen ska undersökas för att undvika otillbörlig spridning av information. Förutsättningen här är att någon utomstående kan ta sig in, fysiskt eller digitalt, i de system som innehåller information. Gällande geodata är det den initierande aktören som tillgängliggör informationen. Om informationen därefter används för antagonistiskt bruk har då inte med en sårbarhet hos initierande aktör att göra. Öppna datadirektivet skulle kanske kunna anses innebära

78 Säkerhetspolisen. (2023c). *Vägledning i säkerhetsskydd. Introduktion.*

79 MSB (2023). *Vägledning, Säkerhetsåtgärder i informationssystem*. MSB2032.

en juridisk sårbarhet[80], men då riskbedömningen avser att bedöma geodata inför ett tillgängliggörande är det inte den juridiska aspekten som här ska bedömas.

Relevans införs därmed för att skapa en bredare förståelse för potentiella risker som ett tillgängliggörande av geodata kan innebära. Det innebär möjligtvis att konsekvenserna kan förstås på ett annat sätt och att en rimlig riskbedömning av geodata avseende Sveriges säkerhet kan göras.

3.5 Metodens steg

Metoden för att genomföra riskbedömningar består av följande sex steg, där steg 5 kan utföras som en serie av workshoppar:

1. Inled processen
2. Skapa underlag
3. Förbered gemensam bedömning av risker
4. Individuell bedömning av risker
5. Genomför gemensam bedömning av risker
6. Besluta

3.6 Metodens utveckling

En del av projektets mål var att testa metoden och få synpunkter från workshopparnas deltagare. Av särskilt intresse har vid alla utom en workshop, varit att testa och erhålla respons på den utvecklade metodens workshop-format. Anledningen till detta är att samverkan mellan olika kompetenser och myndigheter via workshop är en väsentlig del i metoden. Varje workshop avslutades med att deltagarna genomförde skriftliga eller muntliga utvärderingar och reflektioner. Utvärderingarna i workshoppar 1 och 3 genomfördes via förberedda frågor baserade på respektive workshops syfte. Som exempel på hur resultat från en workshop har omsatts i metoden kan nämnas hotbildsbeskrivning. I och med att metoden har testats och delar av den reviderats har metoden inte testats i sin helhet. Dock bygger metoden på delar som har framkommit i litteratur och workshoppar. En översikt av metodens prövade och oprövade delar finns i tabell 3 nedan.

Inom projektet har fråge- och svarsmallar samt ett exempelscenario utformats. Flera scenarier har arbetats fram och använts under workshopparna, dock publiceras dessa inte här utifrån säkerhetshänsyn. Scenarierna användes under workshoppar som stöd i att belysa hur tillgängliggörande av informationsmängder och exempel på hur teknisk utveckling kan medföra potentiella risker för samhället.[81] Ett exempel på scenario som användes finns i Bilaga A.

Tabell 3: Översikt över metoddelar och om de har testats under en workshop i projektet.

Del av metod	Steg i metod	Metodförslag från deltagare vid workshop	Metodförslag baserat på projektgruppens erfarenheter	Metodförslag från litteraturen	Testad empiriskt i projektet
Beskrivning av analysobjekt och nyttjandeanalys	Steg 2		x		x (delvis)
Hotbildsbeskrivning	Steg 2	x	x		
Relevant lagstiftning	Steg 2		x		
Andra geodatamängder	Steg 2		x	x	
Individuell bedömning	Steg 4	x	x		
Riskidentifiering utifrån obestämd hotaktör	Steg 5		x		x
Riskidentifiering utifrån hotaktörer i hotbildsbeskrivning	Steg 5		x		x
Scenarier	Steg 5			x	x

80 Croon, A., Longworth, S., Refors Legge, M., & Winther, P. (2023). *Vägar till juridisk motståndskraft. Att identifiera och motverka användning av juridiska sårbarheter i rättssystem.* FOI-R--5501--SE. Totalförsvarets forskningsinstitut, Stockholm.

81 Se exempelvis Jonsson, D., Eriksson, C., Ingemarsdotter, J., Rossbach, N. & Wedebrand, C. (2023). *Gråzonslägen i krig och fred*. FOI-R--5447--SE. Stockholm, Totalförsvarets forskningsinstitut; Ingemarsdotter, I., Eidenskog, D. & Hedtjärn Swaling, V. (2020), *Vilse i lasagnen? - En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur.* FOI--R--4814--SE.Stockholm Totalförsvarets forskningsinstitut.

Kriterier Sveriges säkerhet	Steg 5		x		x
Konsekvensnivåer	Steg 5		x	x	x
Relevans	Steg 5		x		
Konsekvens-relevansmatris	Steg 5		x	x	
Rekommendation	Steg 5		x		x
Beslut	Steg 6		x		
Kungöra beslutet	Steg 6		x		

Säkerhetshänsyn

För att ge möjlighet till utbyte av information och dialog om faktiska hot har projektgruppen under projekttiden haft kontinuerlig diskussion rörande sekretesshänsyn. Arbetsformer har valts utifrån lämplig säkerhetsnivå. Detta har skett för att avgöra på vilket sätt projektarbetet bör bedrivas för att garantera säkerheten i informationsspridningen dels inom projektet, dels som resultat från projektet. Exempelvis har workshopparna genomförts i för ändamålet lämpliga lokaler.

Diskussion om säkerhetsfrågor har skett inom projektgruppen men även med andra representanter hos uppdragsgivaren Lantmäteriet samt med representanter för säkerhetsmyndigheter och säkerhetsenheter på deltagande myndigheter. I några fall saknade personer hos kommuner nödvändig säkerhetsklassning varför relevanta tjänstepersoner inte kunde delta vid workshoppen. För projektet innebar det minskad representation från kommunerna än vad projektet från början hade planerat. Projektgruppen har beslutat att i denna rapport inte redogöra närmare för vilka myndigheter som varit representerade vid workshopparna och att inte heller närmare redogöra för vilka analysobjekt som har använts vid workshopparna.

4. Metod för riskbedömning vid tillgängliggörande av öppna geodata

Resultatet presenteras i denna rapport i två kapitel. I detta kapitel redogörs för projektets resultat i form av en metod för riskbedömning av öppna geodata inför ett eventuellt tillgängliggörande, MEGS. Till MEGS har begreppet relevans införts. Relevans och konsekvensnivåer presenteras som en del av steg 5 i MEGS. I nästkommande kapitel 5, redovisas identifierade hinder när det gäller att använda MEGS och behov av nationellt stöd som skulle underlätta för dess användning.

Syfte med MEGS är att möjliggöra för offentliga aktörer att i samverkan genomföra bedömningar av riskerna med att tillgängliggöra öppna geodata för Sveriges säkerhet, med särskilt beaktande av aggregeringsproblematiken. MEGS består av sex steg (figur 4). Stegen har en struktur som bygger på varandra. Metoden beskrivs i korthet i efterföljande avsnitt 4.1–4.6. En detaljerad instruktion av hur metoden används i praktiken presenteras i *Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data*.

Figur 4: Figuren visar övergripande bedömningsmetodens sex steg som bör utföras sekventiellt.

4.1 Steg 1: Inled processen

Steg 1 innefattar på ett övergripande plan (*Inled processen* i figur 4) att initierande aktör *initierar* bedömningsarbetet, *utser* de som ansvarar för riskbedömningen (och tillsätter resurser) samt *planerar* riskbedömningens genomförande.

4.2 Steg 2: Skapa underlag

Steg 2 (*Skapa underlag* i figur 4) innebär kartläggning av den kontext inom vilken riskbedömningen ska göras och en sammanställning av underlag som behövs för det vidare arbetet. Underlagen består av:

1. En ändamålsenlig beskrivning av analysobjektet i analyserat format och en nyttjandeanalys.
    - Beskrivningen av analysobjektet bör exempelvis omfatta filformat, informationsinnehåll, upplösning och attribut.
    - Nyttjandeanalysen bör beskriva exempelvis vilka aktörer som använder analysobjektet idag och vilka potentiella negativa konsekvenser som kan uppstå om analysobjektet inte tillgängliggörs i analyserat format som öppna data.
2. En aktuell hotbildsbeskrivning om hotaktörer och ny teknik.
    - En hotbildsbeskrivning bör innehålla en detaljerad genomgång av åtminstone de hotaktörer som Säkerhetspolisen (Säpo) och den militära underrättelse- och säkerhetstjänsten (Must) behandlar i sina årsrapporter då de aktörer som tas upp anses utgöra de allvarligaste hoten mot Sveriges

säkerhet. För respektive hotaktör kan bland annat frågor om aktörens världsbild, motiv och mål vara användbara i det fortsatta arbetet med att identifiera risker.

- Hotbildsbeskrivningen bör även innehålla beskrivning av teknik som kan vara av betydelse för produktion, behandling och användning av geodata.

3. En sammanställning av relevant lagstiftning som har betydelse för riskbedömningen.
4. En sammanfattning av andra öppna och kommersiella geodatamängder. Detta inkluderar andra geodatamängder som kan kombineras med analysobjektet (aggregering eller ackumulering) eller som motsvarar analysobjektet vad gäller exempelvis täckningsgrad, aktualitet, precision och upplösning och som därmed skulle kunna utgöra alternativ till analysobjektet.
5. Ett antal aktuella och relevanta scenarier för användning i steg 5.
    - Mellan tre och fem scenarier som tillsammans spänner upp ett så stort utfallsrum som möjligt. Scenarierna bör utgå från olika hotaktörer, situationer och händelser. De bör även representera olika verksamheter och angreppsmål. För att scenarierna ska vara relevanta bör de dessutom vara konstruerade så att de förutsätter eller öppnar för användning av geodata i någon del av det beskrivna händelseförloppet.

4.3 Steg 3: Förbered gemensam bedömning

Steg 3 innefattar på ett övergripande plan (*Förbered gemensam bedömning av risker* i figur 4) att det förberedande arbetet, utöver steg 2, också innebär förberedelser inför den kommande workshoppen. Steg 3 består av det förberedelsearbete som behöver göras för att genomföra workshopen och utgörs av att i) identifiera vilka aktörer som ska delta i riskbedömningen, ii) planera för workshoppens genomförande, iii) distribuera inbjudningar och iv) skicka underlag till de aktörer som har accepterat att delta i workshoppen.

4.4 Steg 4: Gör individuell bedömning

Steg 4 innefattar på ett övergripande plan (*Gör individuell bedömning av risker* i figur 4) att workshoppens deltagare förbereder sig inför workshoppen genom att bekanta sig med analysobjektet och det underlag från steg 2 som initierande aktör har skickat ut. De ska även enskilt försöka identifiera vilka risker tillgängliggörande av analysobjektet som öppna data kan leda till.

4.5 Steg 5: Genomför gemensam bedömning

Steg 5 innefattar på ett övergripande plan (*Genomför gemensam bedömning av risker* i figur 4) att workshoppen genomförs där risker identifieras, värderas och en rekommendation om tillgängliggörande utifrån en samlad bedömning görs. Det huvudsakliga arbetet med att identifiera och värdera potentiella risker sker under workshoppen. Workshoppen består av fyra moment beskrivna nedan. Genomgående gäller att det arbete som genomförs under workshoppen ska dokumenteras noggrant.

Moment 1 – Identifiera risker

I moment 1 ska deltagarna i grupp identifiera och beskriva potentiella risker som ett tillgängliggörande av analysobjektet kan innebära för Sveriges säkerhet. Deltagarna har innan workshoppen arbetat individuellt (steg 4) med att identifiera konsekvenser som ett tillgängliggörande av analysobjektet kan leda till. Dessa utgör en bra utgångspunkt för att i gruppen identifiera ytterligare risker. Till stöd för detta arbete finns tre olika tillvägagångssätt för att identifiera risker:

1. **Riskidentifiering utifrån obestämd hotaktör.** Deltagarna utgår från en icke-identifierad, obestämd hotaktör. Deltagarna behöver då föreställa sig hur en hotaktör skulle kunna använda analysobjektet för exempelvis underrättelseinhämtning eller planering och genomförande av operationer som leder till skada på Sveriges säkerhet.
    - När gruppen har enats om en uppsättning potentiella risker ska de konsekvenser som risken kan leda till identifieras.

2. **Riskidentifiering utifrån hotaktörer i hotbildsbeskrivning.** Deltagarna utgår från de olika hotaktörer som har identifierats i underlagsarbetet (steg 2). Utifrån hotaktörens världsbild, motiv och mål undersöks hur analysobjektet skulle kunna användas. Exempelvis kan deltagarna utforska om analysobjektet kan underlätta för de olika identifierade hotaktörerna att nå sina mål.
    - När gruppen har enats om en uppsättning potentiella risker ska de konsekvenser som risken kan leda till identifieras.
3. **Använda scenarier.** Deltagarna använder scenarier (från steg 2) som verktyg för att sporra kreativitet och utgöra utgångspunkter för vidare diskussioner.
    - När gruppen har enats om en uppsättning potentiella risker ska de konsekvenser som risken kan leda till identifieras.

För att de tre tillvägagångssätten ska vara givande bör det i steg 2 ha förberetts ett väl utarbetat underlag att använda sig av i form av hotbildsbeskrivning och scenarier.

Moment 2 – Värdera risker

I MEGS konkretiseras risk genom att de konsekvenser som identifierats i moment 1 värderas utefter i) hur allvarlig skada på Sveriges säkerhet de kan leda till (konsekvensnivå) samt ii) hur relevant analysobjektet är för riskernas realiserande (relevans). För att värdera risken ska därför först konsekvensnivån bedömas, och därefter relevansnivån.

Konsekvensernas allvarlighetsgrad

I kapitel 3 beskrevs översiktligt det framtagna tillvägagångssättet för att bedöma hur allvarlig en konsekvens kan bli för Sveriges säkerhet. Det beskrevs att Sveriges säkerhet kan bedömas utifrån åtta kriterier: politisk självständighet, territoriell suveränitet, grundläggande fri- och rättigheter, fria och rättvisa val, offentlighet och transparens, rättsstatens principer, befolkningens förtroende för offentliga institutioner och det demokratiska beslutsfattandet samt samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå. Kriterierna består av fyra effektnivåer, a-d, där effektnivå a är den allvarligaste. I tabell 4 ges en heltäckande beskrivning av kriterium, kriteriernas effektnivåer samt den lagstiftning som ligger till grund för effektnivåerna.

Tabell 4. Översikt av de åtta kriterierna och kriteriernas fyra effektnivåer. Effektnivå *a* är den allvarligaste.

Kriterium	Beskrivning	Effektnivåer
I. Politisk självständighet	Enligt 1§ regeringsformen (1974:152) utgår all offentlig makt från folket, och styret av landet ”förverkligas genom ett representativt och parlamentariskt statsskick”. Det ska alltså vara upp till folket att genom sina representanter besluta om landets öde och styre. Detta kriterium representerar därför den svenska politiska ledningens, och i förlängningen det svenska folkets, förmåga och möjlighet att själv besluta i frågor som rör landets öde och styre, inklusive utrikes-, säkerhets- och försvarspolitik.	a. Den politiska ledningen och det svenska folket saknar makt att besluta i alla frågor som rör landets öde och styre. b. Den politiska ledningen och det svenska folket saknar makt att besluta i många frågor som rör landets öde och styre. c. Den politiska ledningen och det svenska folket saknar makt att besluta i enstaka frågor som rör landets öde och styre. d. Den politiska ledningen och det svenska folket har full makt att besluta i alla frågor som rör landets öde och styre.
II. Territoriell suveränitet	Detta kriterium representerar den svenska statens (inklusive den politiska ledningen och Försvarsmakten) kontroll över det svenska territoriet på land, till sjöss och i luften.	a. Den svenska staten saknar kontroll över hela landets territorium. b. Den svenska staten saknar kontroll över betydande delar av landets territorium. c. Den svenska staten saknar kontroll över delar av landets territorium. d. Den svenska staten har full kontroll över hela landets territorium.

III. Grundläggande fri- och rättigheter	Detta kriterium rör det demokratiska statsskickets funktion och fortlevnad. Enligt prop. 1995/96:129 ska påverkan på detta kriterium vara resultat av kriminella aktiviteter för att utgöra skada på Sveriges säkerhet.	a. De civila och politiska fri- och rättigheterna har avskaffats eller kan av annan anledning inte upprätthållas. b. Flera civila och politiska fri- och rättigheter kan inte upprätthållas. c. Enstaka civila och politiska fri- och rättigheter kan inte upprätthållas. d. De civila och politiska fri- och rättigheterna upprätthålls.
IV. Fria och rättvisa val	Detta kriterium rör det demokratiska statsskickets funktion och fortlevnad. Enligt prop. 1995/96:129 ska påverkan på detta kriterium vara resultat av kriminella aktiviteter för att utgöra skada på Sveriges säkerhet.	a. Val kan förekomma men de är varken fria eller rättvisa. b. Val förekommer men de är till stor del inte fria eller rättvisa. c. Val förekommer men de är delvis inte fria eller rättvisa. d. Val är fria och rättvisa.
V. Offentlighet och transparens (offentlighetsprincipen)	Detta kriterium rör det demokratiska statsskickets funktion och fortlevnad. Enligt prop. 1995/96:129 ska påverkan på detta kriterium vara resultat av kriminella aktiviteter för att utgöra skada på Sveriges säkerhet.	a. Inga beslut inom politiska församlingar eller förvaltning är sakliga, offentliga eller transparenta. b. En stor del av besluten inom politiska församlingar eller förvaltning är inte sakliga, offentliga eller transparenta. c. Enstaka beslut inom politiska församlingar eller förvaltning är inte sakliga, offentliga eller transparenta. d. Beslut inom politiska församlingar eller förvaltning är sakliga, offentliga och transparenta.
VI. Rättsstatens principer	Detta kriterium rör det demokratiska statsskickets funktion och fortlevnad. Enligt prop. 1995/96:129 ska påverkan på detta kriterium vara resultat av kriminella aktiviteter för att utgöra skada på Sveriges säkerhet.	a. Inga beslut inom politiska församlingar, förvaltning eller domstolar fattas på laglig grund eller är opartiska. b. En stor del av besluten inom politiska församlingar, förvaltning eller domstolar fattas inte på laglig grund eller är inte opartiska. c. Enstaka beslut inom politiska församlingar, förvaltning eller domstolar fattas inte på laglig grund eller är inte opartiska. d. Beslut inom politiska församlingar, förvaltning och domstolar fattas på laglig grund och är opartiska.

VII. Befolkningens förtroende för offentliga institutioner och det demokratiska beslutsfattandet	Detta kriterium rör befolkningens förtroende för förvaltning och politisk ledning. Enligt prop. 1995/96:129 ska påverkan på detta kriterium vara resultat av kriminella aktiviteter för att utgöra skada på Sveriges säkerhet.	a. Befolkningen har förlorat förtroende för offentliga institutioner eller det demokratiska beslutsfattandet. b. Befolkningen har lågt förtroende för offentliga institutioner eller det demokratiska beslutsfattandet. c. Befolkningen saknar till viss del förtroende för offentliga institutioner eller det demokratiska beslutsfattandet. d. Befolkningen har förtroende för såväl offentliga institutioner som det demokratiska beslutsfattandet.
VIII. Samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå	Detta kriterium syftar på nödvändigheten att all sådan verksamhet som behövs för samhällets löpande funktion på nationell nivå fungerar tillfredsställande. Notera att även lokal verksamhet, som kommunal vattenförsörjning, kan ha betydelse för samhällets funktion på nationell nivå om till exempel personer eller organisationer med nationell betydelse påverkas om verksamheten inte fungerar tillfredsställande.	a. Samhällsviktig verksamhet utsätts för störningar av sådan omfattning att samhällets funktionalitet på nationell nivå slås ut. b. Samhällsviktig verksamhet utsätts för störningar så att de har omfattande påverkan på samhällets funktionalitet på nationell nivå. c. Samhällsviktig verksamhet utsätts för störningar så att de har viss påverkan på samhällets funktionalitet på nationell nivå. d. Samhällsviktig verksamhet kan utsättas för störningar men dessa är av sådan art att de inte påverkar samhällets funktionalitet på nationell nivå.

De fyra effektnivåerna (tabell 4) används för att möjliggöra en bedömning om den högsta konsekvensnivån. Det finns fem konsekvensnivåer: existentiell skada, allvarlig skada, begränsad skada, obetydlig skada eller okänd/oklar skada. Existentiell skada är den allvarligaste konsekvensnivån medan obetydlig skada inte medför skada på Sveriges säkerhet. Konsekvensnivån okänd/oklar skada används när inget av kriterierna anses relevanta eller då deltagarna av annan orsak inte lyckas bestämma konsekvensnivå. I tabell 5 ges en översikt samt beskrivning av vilken konsekvensnivå som ska väljas utifrån effektnivåerna.

Tabell 5: Konsekvensnivåer för uppskattning av skada på Sveriges säkerhet vid riskbedömningar av geodata vid tillgängliggörande som öppna data.

Konsekvensnivå16	Definition/beskrivning
Existensiell skada (a)	Sveriges I) politiska självständighet, II) territoriella suveränitet, eller III) demokratiska statsskick förloras, eller IV) samhällsviktig verk- samhet utsätts för störningar av sådan omfattning att samhällets funktionalitet på nationell nivå slås ut.
Allvarlig skada (b)	Sveriges I) politiska självständighet, II) territoriella suveränitet, eller III) demokratiska statsskick utsätts för allvarlig påverkan, eller IV) samhällsviktig verksamhet utsätts för störningar så att de har omfat- tande påverkan på samhällets funktionalitet på nationell nivå.
Begränsad skada (c)	Sveriges I) politiska självständighet, II) territoriella suveränitet, eller III) demokratiska statsskick utsätts för påverkan i begränsad omfatt- ning, eller IV) samhällsviktig verksamhet utsätts för störningar så att de har viss påverkan på samhällets funktionalitet på nationell nivå.
Obetydlig skada (d)	Sveriges I) politiska självständighet, II) territoriella suveränitet; eller III) demokratiska statsskick påverkas ej, eller IV) samhällsviktig verk- samhet kan utsättas för störningar men dessa är av sådan art att de inte påverkar samhällets funktionalitet på nationell nivå.
Okänd/oklar skada	Det är oklart om någon av de fyra dimensionerna av Sveriges säker- het påverkas eller det är okänt hur Sveriges säkerhet kan påverkas, exempelvis på grund av brist på information.

Ett alternativ till ovanstående förfarande gällande konsekvenser är att använda Säpos konsekvensnivåer enligt *Vägledning i säkerhetskydd.*[82] Förfarandet i MEGS behöver då justeras efter Säpos indelning.

Analysobjektets relevans

För att tillgängliggörande av analysobjektet ska utgöra en risk för Sveriges säkerhet är det inte tillräckligt att kunna identifiera situationer, händelser och skeenden som leder till skada på Sveriges säkerhet, utan analysobjektet måste dessutom på ett avgörande sätt orsaka eller underlätta att de negativa konsekvenserna uppstår.

Att bestämma relevansen syftar till att bedöma hur beroende de identifierade konsekvenserna är av tillgång till analysobjektet som öppna data. Relevans varierar beroende på hotaktör. Exempelvis kan hotaktörerna ha varierande grad av resurser eller vara mer eller mindre beroende av öppna data. Därför bör bedömningen av relevans ta hänsyn till hotaktörens resurser. För en resursstark hotaktör med tillgång till alternativa datakällor eller metoder för datainhämtning kan analysobjektet vara relativt oviktigt. För en annan hotaktör kan emellertid samma analysobjekt vara helt centralt för att hotaktören ska nå sina mål. När deltagarna besvarar frågorna bör de därför också beakta om relevansen förändras om hotaktören i det identifierade händelseförloppet eller skeendet vore någon av de andra hotaktörer som beskrivs i hotbildsbeskrivningen.

För att bestämma relevansen ska deltagarna besvara ett antal frågor gällande exempelvis hur användbart och unikt analysobjektet är för diverse hotaktörer, om hotaktörerna har förmåga att utnyttja det och hur stor resursbesparing tillgång till analysobjektet som öppna data leder till. Frågorna är konstruerade med ett numeriskt värde. Efter att frågorna besvarats omräknas svaren till ett medelvärde som representerar en av fem relevansnivåer: mycket liten, liten, inte obetydlig, stor och mycket stor.

Moment 3 – Samlad bedömning

I det tredje momentet av workshoppen görs en samlad bedömning av de risker som har identifierats. I MEGS operationaliseras risk som en kombination av hur allvarliga konsekvensernas effekter är utifrån fem konsekvensnivåer, samt analysobjektets relevans för hotaktören. En hög risk föreligger följaktligen om konsekvenserna av ett tillgängliggörande kan medföra skada på Sveriges säkerhet och analysobjektet är relevant för att en hotaktör ska kunna realisera hotet.

För att göra en samlad bedömning förs varje identifierad konsekvens in i en konsekvens-relevansmatris (figur 5). Matrisen fylls i baserat på konsekvensnivå (obetydlig, begränsad, allvarlig eller existentiell) och relevansnivå (mycket liten, liten, inte obetydlig, stor och mycket stor) som har angivits i moment 2. Okänd/oklar konsekvens fylls inte i matrisen utan behandlas separat. Syftet med matrisen är att skapa en överblick över resultatet och att visualisera riskernas allvarlighetsgrad. Ju närmre det högra övre hörnet en konsekvens markeras, desto högre är risken. Om Säpos konsekvensnivåer har använts i moment 2 behöver matrisens konsekvensnivåer anpassas för att avspegla detta.

Moment 4 – Rekommendation

Slutprodukten från workshoppen är deltagarnas rekommendation om lämpligheten i att tillgängliggöra analysobjektet som öppna data. Baserat på identifierade konsekvenser och relevans markerade i konsekvens-relevansmatrisen (moment 3) ska rekommendationen utgå från den risk som har ansetts allvarligast, det vill säga som har den högsta konsekvensnivån och relevansen i matrisen. Om deltagarna anser att det krävs åtgärder innan analysobjektet tillgängliggörs bör de även ge förslag på vilka åtgärder som är lämpliga. Det är tillräckligt att deltagarna har identifierat en risk för Sveriges säkerhet för att anse att analysobjektet inte kan tillgängliggöras i analyserat format.

82 Säkerhetspolisen (2023c).

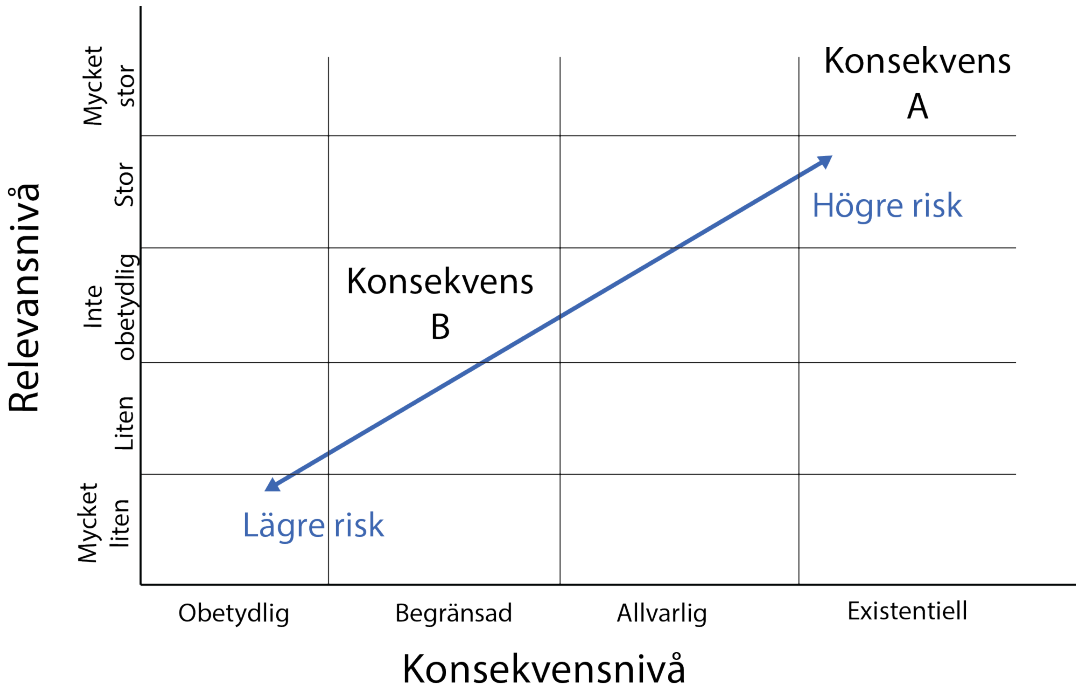
Detta innebär något av alternativen:

- Analysobjektet kan tillgängliggöras som öppna data.
- Analysobjektet kan tillgängliggöras som öppna data efter att någon form av åtgärd vidtagits. Detta ska även inkludera vilka dessa åtgärder är.
- Analysobjektet kan inte tillgängliggöras som öppna data. Men det är ändå möjligt att på annat sätt distribuera där den initierande aktören kan kontrollera användningen av analysobjektet. Detta ska inkludera en beskrivning av det tänkta sättet att distribuera.
- Analysobjektet bör inte tillgängliggöras. Hänvisning sker till sekretess och tillämpligt lagrum.

I deltagarnas rekommendation bör det tydligt framkomma vilka risker som har identifierats, vilka konsekvensnivåer och vilken relevans man har tilldelat varje risk samt vilken rekommendation, inklusive eventuella åtgärder, som deltagarna har lämnat. Dessutom bör centrala resonemang och argument, eventuellt identifierade osäkerheter i bedömningsunderlag och beslut, nyckelantaganden som har gjorts samt avvikande åsikter dokumenteras för att en utvärdering av bedömningen ska kunna göras. Om säkerhetsskyddsklassificerad information har dokumenterats under workshoppen måste dokumentationen också säkerhetsskyddsklassificeras, men även i frånvaron av sådan information ska den initierande aktören göra en bedömning av om dokumentationen behöver säkerhetsskyddsklassificeras.[83]

4.6 Steg 6: Besluta

Det är den initierande aktören som tar det slutgiltiga beslutet om huruvida analysobjektet ska tillgängliggöras som öppna data eller inte och vilka eventuella åtgärder som behöver vidtas. Som beslutsunderlag har aktören under processens gång fått rekommendationen från workshoppen som naturligtvis ska beaktas innan beslut tas. Beslut ska tillsammans med motivering och beslutsunderlag dokumenteras noggrant. Efter att ett beslut har fattats om analysobjektet och dess eventuella tillgängliggörande kungörs beslutet och, om det inte är olämpligt på grund av sekretess eller säkerhetsskydd, med motivering till berörda aktörer i informationssyfte och för att bidra till konsekventa bedömningar.



Figur 5: Konsekvens-relevansmatris för användning vid den samlade bedömningen. Figuren kommer från *Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data.*

83 Säkerhetspolisen, (2023a). *Vägledning i säkerhetsskydd. Informationssäkerhet.*

5. Hinder och behov av stöd på nationell nivå

Baserat på både workshopdeltagarnas kommentarer och projektgruppens erfarenheter har såväl möjliga hinder och svårigheter som offentliga aktörers behov för att kunna göra riskbedömningar identifierats under utvecklingen av MEGS. Här presenteras dessa hinder och behov.

5.1 Hinder och svårigheter att genomföra MEGS

Under arbetets gång har projektgruppen identifierat ett antal hinder och svårigheter som begränsar de offentliga aktörernas möjligheter att göra riskbedömningar av geodata. Dessa hinder och svårigheter har sammanfattats i kategorierna kompetens och kunskap hos deltagare och tankefällor nedan.

5.1.1 Kompetens och kunskap

Resultatet av riskbedömningarna avgörs av deltagarnas kompetens om hot och geodata samt möjligheten till samverkan. Användning av MEGS syftar till att avgöra om en geodatamängd kan medföra risk för Sveriges säkerhet. Det är dock sällan geodata i sig som utgör en risk, utan det är snarare de analyser som geodata tillåter som kan orsaka eller underlätta risker. Det har därför blivit uppenbart under projektets gång att deltagarna i riskbedömningen behöver goda kunskaper om såväl geodata, geografiska informationssystem (GIS) och rumsliga analyser som antagonistiska hot mot Sverige. Det innebär att deltagarna som ska genomföra riskbedömningen behöver förstå både den samlade antagonistiska hotbilden mot Sverige samt hur analysobjektet kan användas av en antagonist. Det var emellertid få av deltagarna på projektets workshoppar som hade kunskap och erfarenhet om både hotbilden och hantering och användning av geodata. Deltagarna hade snarare bakgrund inom antingen säkerhetsfrågor eller användning och hantering av geodata och GIS. De förra hade därmed god förståelse för hotbilden men saknade kunskap om geografiska analyser. De senare förstod däremot hur analysobjekten kan användas, vilka analyser som man kan göra med dem och hur man kan aggregera eller ackumulera data, men ansåg vanligtvis att de saknar förståelse för hotbilden.

MEGS är utformad för att deltagare med olika kompetenser ska arbeta tillsammans och bidra med sina respektive erfarenheter och kunskap för att på så sätt kunna bedöma riskerna med analysobjektet. I och med att två sorters kompetens tillsammans ska identifiera och analysera risker, är följden att riskbedömningen beror på deltagarnas samlade kompetens och aktiva ansvarstagande att samarbeta med varandra. Om samarbetet uteblir, eller om kompetens saknas, medför det att riskbedömningen kommer att bli bristande. En försvårande omständighet är att de offentliga aktörerna kan ha en organisationsindelning som innebär fördelning av arbetsuppgifter som gör det komplicerat att identifiera vilka personer som är relevanta att inkludera.

Eftersom riskbedömningarna kräver en viss nivå av kompetens om vad för slags analyser som är möjliga att genomföra med hjälp av analysobjektet, har redovisningar om analysobjekten genomförts vid workshopparna. Redovisningarna underlättade till viss del för icke geodata-kunniga personer att bidra till att identifiera risker. Detta kompenserar dock inte för behovet att geodatakunniga deltagare medverkar, då redovisningen enbart visar delar av kunskapen om geodata.

5.1.2 Tankefällor

Vid workshopparna och vid dialog inom projektgruppen har vad som skulle kunna kallas för ”tankefällor” framkommit. Utmärkande för en tankefälla är att den utgör ett hinder eller avleder uppmärksamheten från huvuduppgiften, samtidigt som den egentligen inte är relevant för riskbedömningen. Istället för att lita på processen och de steg som den består av, så fastnar deltagarna i ett tankesätt och har svårt att komma vidare.

Exempel på en återkommande tankefälla är att ”det spelar ingen roll vad vi beslutar om för det finns redan kartor och bilder i tillgängliga kartor på internet”. Det stämmer att det finns ett omfattande material i tillgängliga digitala karttjänster. Men det innebär inte nödvändigtvis att det överensstämmer med den geodata som eventuellt ska tillgängliggöras. Ett exempel är tidpunkten vid vilken data skapades. Om tidpunkten för produktionen av analysobjektet respektive karttjänstens material skiljer sig, kan skillnaderna i sig avslöja information som

är intressant för en antagonist, till exempel om det finns förändringar i markytan. Detta är även ett exempel på aggregeringsproblematik. Andra exempel på skillnader som kan finnas mellan en karttjänst och ett analysobjekt är retuscheringar, datas kvalitet eller geografisk omfattning och om informationen är nedladdnings- och/eller bearbetningsbar.[84] Speciellt möjligheterna att analysera vidare med data i ett GIS gör att skillnaderna kan vara större än vad man vid första anblicken tänker sig.

Genom att uppmärksamma och vara medveten om dessa tankefällor kan det hjälpa utövarna, samt en facilitator vid workshop, att undvika dem under riskbedömningen och går att läsa om i punktlistan nedan. Några av dessa tankefällor utvecklas i *Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna geodata*[85]:

- ”Alternativa data finns redan tillgängliga.”
  - Alternativa data kan ha annan upplösning, kvalitet, geografisk täckning, ålder etc. som gör att de inte överensstämmer med analysobjektet. Om det finns likvärdiga data tillgängliga kan det istället finnas fog för att undersöka potentiell aggregering mellan dessa och analysobjektet.

- ”Den stora onda nationella aktören har ändå allt och vet allt/den onda nationen tar allt, därför spelar det ingen roll om åtgärd vidtas eller ej.”
  - Bara för att en del av den *stora onda nationen* har data betyder det inte att alla delar av organisationen har det och använder det. De operativa organen behöver inte ha tillgång till samma data.

- ”Analysobjektet ska antingen tillgängliggöras eller inte alls vara tillgängligt för det offentliga.”
  - Att ett analysobjekt bedöms innebära en risk för Sveriges säkerhet innebär inte automatiskt att det är oåtkomligt för det offentliga. Åtgärder kan vidtas på flera sätt så att analysobjektet ändå blir tillgängligt. T.ex. kan analysobjektet behandlas genom maskning eller avskalning. Det kan göras tillgängligt via licens. I de fall där åtgärd inte finns eller inte räcker till kan dock analysobjektet bli otillgängligt för det offentliga.

- ”Konsekvens/risk beror på vem som är hotaktör.”
  - I vissa fall kan det vara så. Därför innehåller metoden ett arbetssätt där hotbeskrivning används för att identifiera konsekvenser. Men det är även viktigt att komma ihåg att hotbeskrivningen förändras över tid, liksom hotaktörens resurser. Metoden innehåller även ett arbetssätt där det är fritt för deltagarna att identifiera potentiella konsekvenser. Ett sätt att ta sig an denna uppgift är att utgå från deltagarens kunskap eller expertområde. Exempelvis genom att identifiera möjliga risker för dricksvatten.

- ”Analysobjektet är redan tillgängliggjort.”
  - Ny bedömning kan göras och data dras tillbaka vid behov. Data är ej statiskt.

- ”Fastnar i scenario.”
  - Metoden innehåller scenario som arbetssätt för att identifiera konsekvenser. Scenario ska ses som tankehjälp och ett sätt för gruppen att ha en gemensam bild av vad som kan ske, för att underlätta för dialog och det fortsatt arbetet. Det är inte ett facit eller enda möjliga alternativ. Behov av struktur för nationell samordning.

84 Nikander, J., Jama, T., & Tenkanen, H. (2024).

85 Davidsson m.fl. (2025).

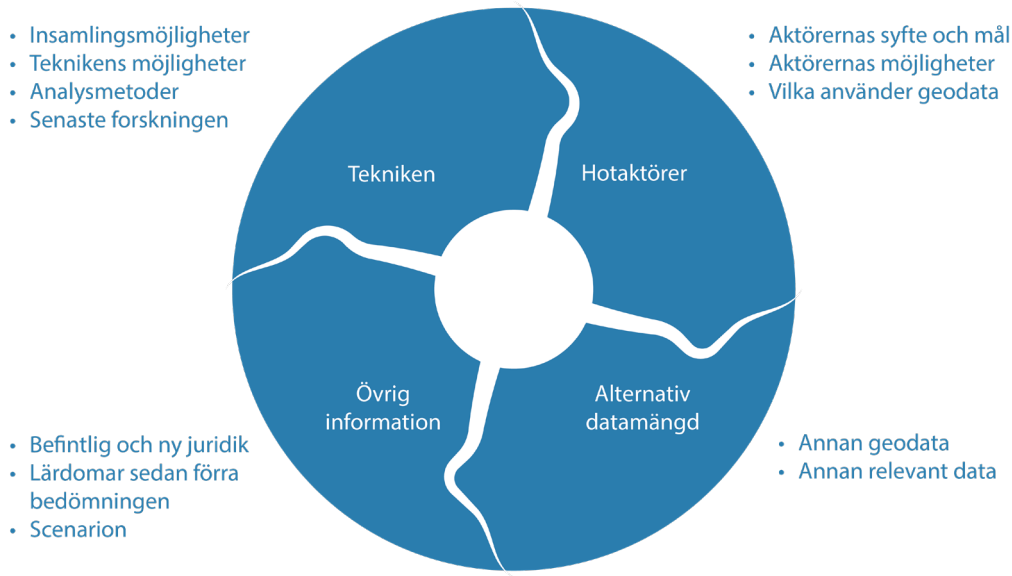
5.2 Struktur för nationell samordning

Riskbedömning av geodata avseende Sveriges säkerhet kräver tid och resurser och innebär behov av samverkan mellan flertalet aktörer, men det saknas nationell samordning och stöttning för aktörerna som ska genomföra riskbedömningen. De uppgifter som ingår i det förberedande arbetet (steg 2) inför workshopen är resurskrävande och innebär att sammanställa stora mängder information. Relevant lagstiftning ska sammanfattas och information om andra öppna och kommersiella data sammanställas. Vidare ska den aktuella hotbilden sammanställas utifrån hotaktörer och teknik samt ett antal scenarier skapas. Detta är ett arbete som kräver stora resurser men som är angeläget för att kunna göra ändamålsenliga riskbedömningar.

Deltagarna vid workshopparna lyfte den insats i form av arbetstid som riskbedömning av geodata innebär, samtidigt som den tid som finns att tillgå är begränsad. Det framkom därmed en rad förslag för hur en nationell samordnande funktion behövs för att både stötta vid riskbedömning och för att underlätta arbetsbördan. Eftersom varje aktör som ska genomföra en riskbedömning behöver upprepa arbetet i det förberedande steget finns det sannolikt såväl ekonomiska som personella fördelar med att samordna dessa uppgifter nationellt. Därför bör både relevant lagstiftning och information om öppna och kommersiella data samordnas som en regelbunden nationell sammanställning som berörda aktörer kan ta del av när riskbedömningar ska genomföras.

Det bör inte vara varje enskild offentlig aktörs ansvar att sammanställa en ny hotbildsbeskrivning varje gång en riskbedömning ska genomföras utan en sådan bör kunna sammanställas och kommuniceras från en nationell samordningsfunktion. Förutom att en sådan nationell samordning förmodligen skulle leda till en hotbildsbeskrivning av högre kvalitet skulle den även kunna minska riskerna för att säkerhetsskyddsklassificerat material som ligger till grund för beskrivningen röjs. Deltagarna framhäver att riskbedömningen går ut på att hitta den ”svarta svanen” – det vill säga ett hot som troligen inte har skett tidigare.

Vid workshopparna uppkom att deltagarna har ganska skilda uppfattning om vilka hot som Sveriges står inför. Hotbilden är dynamisk vilket innebär att varje enskild bedömning gäller en begränsad tid och för det specifika fallet. Exempelvis använder sig stater av organiserad brottslighet och kriminella nätverk, vilket innebär att det inte går att skilja dem åt. Ett förslag som kom upp är att en myndighet får i nationellt uppdrag att ta fram anpassad hotbeskrivning till den aktör som efterfrågar. De öppna beskrivningar som finns att tillgå via exempelvis Säpo och Must är inte nog detaljerade att använda som bedömningsunderlag. Hotbildsbeskrivningen behöver därför omfatta såväl hotaktörer som påverkar Sveriges säkerhet som ny teknik som påverkar hur geodata kan samlas in, bearbetas och utnyttjas (figur 6). Ytterligare studier kring vad en hotbildsbeskrivning behöver innehålla för att stödja vid riskbedömningen av geodata behöver genomföras. Hotbildsbeskrivningen behöver även vara föränderlig över tid.



Figur 6. Figuren visar på exempel, ej fullständigt, på delar som bör beaktas vid en hotbildsanalys. Här bör ytterligare studier genomföras för att ta fram vad en hotbildsbeskrivning behöver innehålla för att stödja vid genomförandet av riskbedömningen av geodata.

Dessutom bör ett nationellt bibliotek av lämpliga scenarier som kan användas i riskbedömningarna utvecklas och administreras. Idealt bör dessa scenarier spänna upp ett så stort utfallsrum som möjligt för att deltagarna ska ha möjlighet att utforska en stor mängd möjliga hot och framtida utvecklingar. Om inga lämpliga scenarier finns kan existerande scenarier uppdateras för att bättre passa analysobjektet och initierande aktörs behov eller så kan nya scenarier utvecklas. Uppdaterade och nya scenarier bör sedan adderas till det redan existerande scenariobiblioteket så att andra aktörer kan återanvända dem.

En nationell samordningsfunktion kan även ha funktionen att beslut om analysobjekt ska tillgängliggöras eller åtgärdas, kan delas till andra. I steg 6 ska beslut kungöras. Här finns möjlighet att en nationell samordning kan underlätta när beslut om liknande analysobjekt ska tas. Eftersom vissa typer av geodata, exempelvis ortofoton, produceras och tillhandahålls av flera olika aktörer är det önskvärt att dessa aktörer tar konsekventa beslut gällande tillgängliggörande. Om olika aktörer tar olika beslut kan det leda till såväl risker för Sveriges säkerhet som försämrat förtroende för de offentliga aktörerna bland allmänheten.

För att underlätta riskbedömningen lyfte deltagarna att det skulle underlätta med någon form av sammanställning över vad det är om ska skyddas. En sådan sammanställning kan underlätta vid riskbedömningen i och med att det då blir tydligare vad för slags information som inte ska framkomma vid ett tillgängliggörande. Här har MSB, Myndigheten för samhällsskydd och beredskap bra listor med vad som är samhällsviktig information men än mer detaljerad kunskap än dessa efterfrågades. Det framkom förslag kring en sammanställning som besvarar följande frågor:

1. Vad ska skyddas?
2. Mot vad ska det skyddas?
3. Hur ska det riskbedömas?
4. Vad är mest känsligt för den civila delen av totalförsvaret?

En försvårande omständighet med en sådan sammanställning, förutom att den i sig blir hemlig, är att omvärldsläget förändras och därmed ändras också det som ska skyddas.

Det lyftes även önskemål om rekommendationer för hur ofta riskbedömningar bör ske. Till exempel utifrån hur data ändras eller i vilken omfattning ny data tillkommer hos andra aktörer.

6. Diskussion

Kapitel 6 diskuterar både utvecklingen av MEGS och förutsättningarna för att tillämpa metoden idag. Diskussion förs också om förutsättningarna att arbeta med tillgängliggörande av geodata på det sätt som öppna datalagen föreskriver.

Att riskbedöma geodata avseende potentiell risk för Sveriges säkerhet är ett komplicerat och inte helt utrett område. Det kräver omfattande juridiska utredningar, förståelse för att berörda aktörer uppfattar frågan som svår och behov av myndighetssamverkan, något som det idag kan saknas struktur för. Därför lyfts områden som kräver fortsatta studier, både för utvecklingen av MEGS men också för att utreda vad det innebär för statliga aktörer att efterleva öppna datalagen.

6.1 MEGS som ett utkast till metod för att göra riskbedömning

Att bedöma risker, oavsett källan till riskerna, kan vara en komplicerad uppgift. Svårigheter i riskbedömningen uppstår framför allt då bedömningen är osäker och det inte finns tillräcklig information att bygga bedömningen på. För att bemöta detta har MEGS utvecklats som ett stöd för riskbedömning av geodata och för att se om ett tillgängliggörande kan innebära risk för Sveriges säkerhet.

För riskbedömning avseende Sveriges säkerhet inför ett eventuellt tillgängliggörande av geodata är det inte möjligt att bedöma sannolikheten för att en konsekvens ska realiseras. Ett alternativ är att bortse från sannolikhet och endast bedöma konsekvens. Men då det i praktiken går att identifiera konsekvenser från all typ av geodata, presenteras i denna rapport ett alternativt sätt för att nyansera konsekvensbedömningen genom att begreppet *relevans* införts. Relevansen gör det möjligt att förstå om tillgängliggörandet av geodata bidrar till att konsekvensen kan realiseras, eller om konsekvensen kan ske även om geodata inte tillgängliggörs och att geodata därmed är irrelevant. Relevansen har även utvecklats för att hantera det faktum att en risk kan inträffa på grund av att information tillgängliggörs, inte för att informationen tillskansas på illegalt tillvägagångssätt. En fördel med bedömning av relevans är att geodata kan tillgängliggöras om det inte är relevant för konsekvensens realiserande. Det förhindrar att mer geodata än nödvändigt inte tillgängliggörs på grund av identifierade konsekvenser.

Eftersom relevans är ett nytt begrepp inom riskfältet innebär det en hel del utmaningar. Relevans ska exempelvis inte ses på samma sätt som en sannolikhet. Det innebär att en låg relevans inte automatiskt innebär en låg risk. Detta skiljer sig från det mer klassiska sättet att se på risk som summan av konsekvens och sannolikhet där risken påverkas om sannolikheten är låg (även om konsekvensen är hög). Relevansens nyanserande av konsekvensen ska ses som ett stöd för den som genomför riskbedömningen att förstå konsekvensen och om geodata är en avgörande länk för att konsekvensen kan inträffa. Det innebär samtidigt att det här inte varit möjligt att sätta exakta avgränsningar för relevansens nivåer (mycket liten – mycket stor).

Eftersom relevans är ett nytt begrepp kräver det fortsatt arbete för att både specificera dess definition och för hur relevansen kan bedömas med hjälp av frågor eller andra stödverktyg i riskbedömningen. Relevans och hur det presenteras i denna rapport ska ses som ett första steg för att på ett alternativt sätt angripa bedömningen av de komplexa risker som tillgängliggörandet av geodata utgör.

Utmaningar med att göra bedömningar

Det finns flera utmaningar med att göra bedömningar. I vissa fall skulle man kanske vilja att bedömningen hade sin grund på kvantitativa data eftersom klassiska och standardiserade sannolikhetsbedömningar i många fall då kan användas. Det alternativ som står till buds när det saknas kvantitativa data är mänskliga bedömningar. Eftersom det saknas kvantitativa data för risker som kan uppstå när geodata tillgängliggörs som öppna data baseras MEGS på mänskliga bedömningar. Forskning har emellertid visat att sådana bedömningar ofta brister när det gäller både noggrannhet och precision. Mänskliga bedömningar lider nämligen ofta av såväl snedvridningar, det vill säga psykologiska mekanismer som minskar bedömningarnas precision, som brus som leder till stora variationer i resultat.[86] MEGS är utformad för att, åtminstone delvis, minska bias genom att man exempelvis arbeta med

86 Kahneman, D., Sibony, O., & Sunstein, C. R. (2021).

experter. Det finns dock behov av att arbeta vidare och justera metoden för att ytterligare minska effekterna av bland annat bias.

Ett ytterligare exempel på behov av utveckling av metoden är att deltagarna i MEGS nuvarande utformning behöver göra absoluta bedömningar vad gäller konsekvens och relevansnivå. Detta behöver utvecklas då det inte finns tydliga avgränsningar för konsekvenser eller relevansnivåer. Ett exempel är att forskning har visat att det är lättare och leder till mindre variation om bedömningar istället görs relativt en fallskala bestående av exempel som illustrerar de olika konsekvensnivåerna.[87]

Den uppgift som de offentliga aktörerna är satta att göra är alltså att uppskatta risker som kan uppstå vid ett framtida tillfälle när en viss geodatamängd tillgängliggörs som öppna data. En tolkning av lagtexten är därför att det är själva tillgängliggörandet som fritt tillgängliga data i digital form som kan medföra risker för Sveriges säkerhet, och det är just dessa risker som riskbedömningen ska identifiera och värdera. En aspekt som dock har orsakat viss tvetydighet under projektets gång är begreppet Sveriges säkerhet som inte är helt tydlig definierat. Inom utvecklingsarbetet av MEGS har projektgruppen därför försökt operationalisera Sveriges säkerhet utifrån förarbeten till säkerhetsskyddslagen där begreppet diskuteras. Den operationalisering som används i MEGS har dock ingen juridisk giltighet utan ska betraktas som ett stöd vid värdering av konsekvensnivå.

Samverkan

Ett antagande som gjordes i början av det här projektet var att riskbedömningar vid tillgängliggörande av geodata som öppna data bör göras i samverkan. Det är visserligen alltid upp till den initierande aktören att ta det slutgiltiga beslutet att tillgängliggöra sina geodatamängder, men en etablerad struktur för regelbunden samverkan medför flera fördelar. Exempelvis är det möjligt att offentliga aktörer utarbetar olika rutiner och gör sinsemellan inkonsekventa riskbedömningar utan samverkan. Genom att samverka kan sådan inkonsekvens förmodligen undvikas i högre utsträckning. Troligen kan samverkan även förbättra bedömningarnas kvalitet då det erbjuder de offentliga aktörerna en bredare kompetens inom riskarbete och kunskap om geodata, framförallt om flera aktörer från olika beredskapssektorer involveras. Forskning har dessutom visat att människor som samverkar kan lösa uppgifter bättre än enskilda personer om samverkan utformas på lämpligt vis.[88] Samverkan kan möjligen även minska risken för vissa snedvridningar som är vanliga vid mänskliga bedömningar. I metodens nuvarande utförande utförs själva riskbedömningen i huvudsak i samverkan i workshop-format. För att motverka eventuellt förstärkningsbias (groupthinking) har MEGS därför också utformats med ett individuellt värderingsteg.

En tänkbar konsekvens av att tillgängliggöra geodata är att information om exempelvis säkerhetskänslig verksamhet röjs, vilket medför att verksamheters belägenhet, funktion, förmåga, beredskap eller annan information som anses skyddsvärd avslöjas. De aktörer som bedriver sådan verksamhet sitter troligen på relevant kunskap gällande om säkerhetskänslig verksamhet kan röjas vid tillgängliggörande av en viss geodatamängd. Det vore därför eftersträvansvärt att de aktörer som bedriver säkerhetskänslig verksamhet får möjlighet att vara med och analysera om tillgång till geodata som öppna data kan bidra till att röja säkerhetskänslig information. Ett sådant förfarande ställer dock vissa krav på de aktörer som bedriver säkerhetskänslig verksamhet. För att de ska kunna göra en ordentlig analys och besvara frågor från initierande aktör på ett erforderligt sätt behöver aktören som bedriver säkerhetskänslig verksamhet personal med kompetens inom geodata, rumsliga analyser och GIS. Hur arbetet med att involvera aktörer som arbetar med säkerhetskänslig verksamhet kan inkluderas bättre i MEGS är något som författarna också ser bör utvecklas vidare. Eftersom antalet aktörer som bedriver säkerhetskänslig verksamhet kan vara stort skulle ett alternativ sätt att arbeta vara att några utpekade aktörer, såsom exempelvis sektorsansvariga myndigheter eller tillsynsmyndigheter, istället får ett annat ansvar för att bidra till att göra denna analys.

När ska riskbedömning av geodata göras?

Riskbedömning av geodata med avseende på Sveriges säkerhet kan göras vid olika tillfällen. Det skulle exempelvis kunna göras vid insamling av data, vid utlämnande av data eller löpande vid den offentliga aktör som producerar och tillgängliggör data. För de offentliga aktörer som ämnar tillgängliggöra geodata finns alltså ett antal olika situationer då en riskbedömning behöver genomföras. Analysobjektet kan exempelvis redan finnas tillgängligt för användare men vara avgiftsbelagt så att endast de aktörer som har tillräckliga finansiella resurser

87 Kahneman, D., Sibony, O., & Sunstein, C. R. (2021).

88 Kerr, N. L., & Tindale, R. S. (2004). Group Performance and Decision Making. *Annual Review of Psychology,* 55, 623–655. https://doi.org/10.1146/annurev.psych.55.090902.142009

har tillgång till det. Den offentliga aktören kan i detta fall också utföra mer eller mindre avancerade kontroller av datamängdernas användare för att försöka förhindra att hotaktörer får tillgång till geodatamängden. En annan situation då riskbedömning är aktuell är då den offentliga aktören har utvecklat en ny eller förbättrad geodatamängd. I detta fall har alltså ingen annan aktör tillgång till dessa geodata än. En tredje situation då riskbedömningen skulle kunna utföras är innan den tänkta geodatamängden har producerats. Det kan alltså vara en fördel att redan på ett tidigt stadium bedöma om en planerad geodatamängd kan medföra risker för Sveriges säkerhet för att avgöra om kostnaden för att producera geodatamängden är godtagbar även om den inte kan tillgängliggöras som öppna data. Det är dock viktigt att notera att riskbedömningar behöver göras återkommande, exempelvis när viktiga omständigheter, såsom en förändrad hotbild, förändras.

MEGS som lärandeprocess

Att bedöma risker vid tillgängliggörande av geodata som öppna data bör uppfattas som en kontinuerlig lärandeprocess. Eftersom det är omöjligt att helt förutse alla risker som kan uppstå när geodata tillgängliggörs, då riskerna är under ständig förändring och de offentliga aktörerna skaffar sig ny kunskap och erfarenhet är det troligt att såväl riskbedömningar som metoder och processer behöver ändras över tid. Förhoppningen är att MEGS kan utgöra en grund för en myndighetsgemensam metod. Det krävs dock ytterligare arbete för att utveckla och testa metoden. Metoden bör därför utvecklas efter hand av de offentliga aktörerna själva, eller av en för uppgiften ansvarig myndighet.

När en metod för riskbedömningar ska utvecklas är ett tänkbart alternativ att återanvända redan existerande metoder. Projektgruppen har inte gjort en grundlig analys av hur andra EU-länder har implementerat öppna datadirektivet och om det i dessa länders lagstiftning krävs motsvarande riskbedömningar när geodata ska tillgängliggöras. Den svenska förvaltningsmodellen och juridiska förutsättningar med bland annat offentlighetsprincipen, självständiga myndigheter och det kommunala självstyret erbjuder dock specifika utmaningar varför det inte är säkert att andra länders lösningar är tillämpbara i Sverige. Därför kan det vara svårt att jämföra Sverige med andra länder ifråga om hanteringen av öppna geodata. Trots det bör framtida undersökningar göra en noggrannare kartläggning av hur andra länder har implementerat öppna datadirektivet och hur man hanterar de risker som kan uppstå.

MEGS är utformad för att göra riskbedömningar av geodata. Öppna datadirektivet och öppna datalagen gäller emellertid alla typer av data som produceras av offentliga aktörer. Det behövs alltså motsvarande metoder för att göra riskbedömningar även för andra typer av data. Även om MEGS är utformad för riskbedömningar av geodata är det tänkbart att delar av metoden kan återanvändas vid bedömningar av andra data.

6.2 Erfarenheter från workshoppar under projektets gång

Erfarenheter från projektet visar att deltagarna i riskbedömningen behöver särskild kompetens för att kunna göra ändamålsenliga och grundliga riskbedömningar. Exempelvis behöver deltagarna god förståelse för geodata, rumsliga analyser och GIS för att över huvud taget förstå hur geodata utgör en risk. Dessutom behöver de förstå hotbilden mot Sverige, både vad gäller hotaktörer och de tekniska möjligheter som finns att nyttja geodata för antagonistiska ändamål. Under de workshoppar som genomfördes under projektet var det dock tydligt att många deltagare saknade en tillräcklig förståelse för hotbilden. De deltagare som hade bakgrund inom säkerhetsavdelningar eller liknande, och följaktligen hade en god förståelse för hotbilden, saknade ofta förståelse för geodata och hur de kan användas av en hotaktör. Deltagare som hade arbetat ingående med geodata, GIS och rumsliga analyser förstod däremot hur geodata skulle kunna användas men uttryckte i allmänhet en önskan om bättre förståelse för hotbilden.

Facilitatorns roll är central för att workshopparna i riskbedömningen ska bli framgångsrika och produktiva. En facilitatorns roll är att skapa förutsättningar för att genomföra en bra workshop. Det krävs exempelvis tydlig och fast styrning för att deltagarna ska fokusera på den avsedda uppgiften och för att styra bort uppmärksamheten från irrelevanta diskussioner. En facilitator som är kunnig på geodata och säkerhetsfrågor i allmänhet kan dessutom med relevanta frågor leda deltagarna vidare för att lösa givna uppgifter. Vidare kan facilitatorn förklara och förtydliga specifika begrepp som används i MEGS. Exempelvis kan begreppet analyserat format vara svårt att ta till sig under workshoppen. Analyserat format avser i MEGS det format i vilket man avser att tillgängliggöra analysobjektet. Begreppet används därmed som en samlingsbeteckning för analysobjektets egenskaper såsom filformat, datastruktur, upplösning, attributuppsättning, metadata med mera. Det är emellertid vanligt att

deltagarna glömmer detta och istället beaktar en generell typ av geodata än det specifika analysobjektet i analyserat format. Om detta händer behöver facilitatorn påminna deltagarna om att det är analysobjektet som ska bedömas.

Konsekvenserna av ett tillgängliggörande av analysobjektet kan vara svåra att visualisera. Under projektets gång har det ibland varit en svårighet att få alla deltagare att utgå från liknande världsbild på workshoppen, även om scenarier används för att hjälpa gruppen på traven. Det är dock viktigt att notera att dessa scenarier är en tankehjälp och en uppstart, inte en prognos eller det mest sannolika alternativet. Därför behöver facilitatorn återigen förtydliga hur scenarierna ska användas för att identifiera risker. Man måste låta scenarierna bli en smältdegel för hotförståelse och inte något dimensionerande. Även exempel på redan inträffade incidenter kan bistå i att visualisera konsekvenser.

Vissa deltagare påpekade under workshopparna att tänkbara hotaktörer redan kan ha tillgång till analysobjektet genom inköp via bulvaner eller genom att få tillgång till den offentliga aktörens IT-system via cyberangrepp. Dessutom var man medveten om att det kan finnas alternativa data som kan användas istället för analysobjektet. För vissa typer av geodata kan det nämligen existera andra öppna eller kommersiella geodata som motsvarar analysobjektet. Vad som kan anses motsvara analysobjektet varierar dock från situation till situation och mellan olika hotaktörer beroende på deras motiv och mål. Faktorer som informationsinnehåll, täckningsgrad, aktualitet, precision och upplösning kan troligen påverka huruvida andra data kan anses motsvara analysobjektet. Under dessa diskussioner kunde deltagarna dock glömma att beakta att bedömningen skulle göras för analysobjektet i analyserat format vilket i allmänhet är viktigt att beakta när man jämför med potentiellt alternativa data (exempelvis kan upplösningen skilja sig åt vilket kan ha betydelse för en hotaktör).

6.3 Riskerna med öppna geodata och Sveriges säkerhet är ett nationellt problem

MEGS är ett stöd för offentliga aktörer att i samverkan genomföra riskbedömningar av öppna geodata med avseende på Sveriges säkerhet. Dessa riskbedömningar är såväl komplexa som svåra att genomföra då hot och risker är svåröverblickbara och föränderliga samtidigt som deras sannolikheter i allmänhet inte låter sig uppskattas. Möjligheter att aggregera och ackumulera data och information medför särskilt oöverskådliga konsekvenser. Aggregering och samkörning av stora datamängder pågår redan nu av en lång rad aktörer i dagens digitaliserade samhälle, bland annat för att genom datadrivna innovationer bidra till effektiviseringar. Det är omöjligt att göra en aggregeringsbedömning som är heltäckande för Sveriges säkerhet. Detta orsakas dels av den ofantliga mängden data som potentiellt kan aggregeras och de oändliga antal kombinationsmöjligheter som kan utföras, dels av att det rör något så komplext och delvis svårgripbart som Sveriges säkerhet. Aggregeringsproblemet nämns i förarbetena till öppna datalagen och Myndigheten för digital förvaltnings vägledning för att tillgängliggöra information,[89] men det saknas för närvarande en tillfredsställande hanteringsmetod.

Lagstiftningen efterfrågar riskbedömning för Sveriges säkerhet inför tillgängliggörande av geodata som öppna data. Därför behöver de offentliga aktörerna bedöma hur tillgängliggörande av deras geodata påverkar alla aktörer som har betydelse för Sveriges säkerhet. Det betyder att istället för att utgå från enbart sin egen verksamhet måste nu alla andra potentiellt relevanta verksamheter inkluderas i bedömningen. På det viset påminner riskbedömningar vid tillgängliggörande av öppna geodata om andra säkerhetsanalyser som informationssäkerhetsanalyser och säkerhetsskyddsanalyser. Men riskbedömningar av geodata medför även andra svårigheter som möjligtvis är unika för denna typ av bedömningar. Exempelvis kan geodata användas för att göra rumsliga analyser och nyttjas i modern teknik för såväl navigering som automatiserad identifiering av potentiellt intressanta mål.

Riskbedömningarna förväntas genomföras av tjänstepersoner på flera nivåer i samhället, inklusive bland annat kommuner och regioner, men ska avse risker på nationell nivå. Det är en bedömning med en långt bredare omfattning än vad dessa tjänstepersoner vanligtvis arbetar med, det vill säga främst den egna verksamheten. Det är oklart om dessa tjänstepersoner idag har rätt förutsättningar för att göra riskbedömningar med avseende på Sveriges säkerhet när geodata ska tillgängliggöras som öppna data. Erfarenheter från det här projektet antyder dessutom att förståelsen för hotbilden i dagsläget är ofullständig. Det finns alltså behov av såväl utbildning som träning för att tjänstepersoner vid de offentliga aktörerna på ett grundligt och ändamålsenligt sätt ska kunna bedöma risker för Sveriges säkerhet när geodata tillgängliggörs som öppna data. Det är troligt att såväl utbildning och träning som

89 Se SOU 2020:55, *Innovation genom information* och Myndigheten för digital förvaltning, (2025). *Vägledning för att tillgängliggöra information*. [Hämtad: 2025-01-27] https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/vagledning-for-att-tillgangliggora-information

framtagande av underlag som behövs för att kunna göra riskbedömningar bör samordnas nationellt. Dessutom saknas idag en aktör som har nationellt ansvar för genomförande och samordning av riskbedömningar av data.

Sammanfattningsvis medför ovanstående att sådana riskbedömningar som efterfrågas i öppna datalagen utgör en grannlaga uppgift för den enskilda tjänstepersonen inom offentlig förvaltning. Om medarbetare (inklusive beslutsfattare) själva upplever bristande kompetens inför bedömningarna kan det leda till flera olika typer av problem. Exempelvis kan onödig stress uppstå när medarbetarna upplever att de saknar kompetens. Dessutom finns en risk att medarbetare ignorerar arbetsuppgiften och ansvaret då uppgifterna upplevs för komplexa och svåra för att därmed försöka undvika det ansvar som det medför.[90] Detta kan möjligtvis avhjälpas med ett nationellt samordnat stöd.

Nationell samordning

Flera av de uppgifter som den initierande aktören behöver utföra i MEGS innebär att sammanställa stora mängder information. Exempelvis ska relevant lagstiftning sammanfattas och information om andra öppna och kommersiella data sammanställas. Detta är ett omfattande arbete som kräver resurser men som är angeläget för att kunna göra ändamålsenliga riskbedömningar. Eftersom varje aktör som ska genomföra en riskbedömning behöver upprepa detta arbete finns det sannolikt såväl ekonomiska som personella fördelar med att samordna dessa uppgifter nationellt. Det vore lämpligt om det arbetet samordnas som en regelbunden nationell sammanställning som berörda aktörer kan ta del av när riskbedömningar ska genomföras. Troligen behöver sådana sammanställningar uppdateras regelbundet för att återspegla de förändringar som sker.

Det bör troligen heller inte vara varje enskild offentlig aktörs ansvar att sammanställa en ny hotbildsbeskrivning varje gång en riskbedömning ska genomföras. För att underlätta de offentliga aktörernas riskbedömningar och minska de samhällsekonomiska kostnaderna och eventuellt få en högre kvalitet föreslår därför författarna till denna rapport att en ändamålsenlig och aktuell hotbildsbeskrivning sammanställs löpande på nationell nivå.

Inom MEGS ser vi också att det potentiellt kan framkomma ytterligare okända hot vid de myndighetsgemensamma riskbedömningarna. För att säkerställa ett lärande och kunskapshöjande inom dessa områden ser projektgruppen att det därför borde finnas en utpekad mottagare av eventuellt nya risker. Troligen bör detta vara samma aktör som ansvarar för de återkommande hotbildsbeskrivningarna för att säkerställa ett lärande, återkoppling och kunskapshöjning inom området.

Sammanfattningsvis finns det alltså stora behov av en nationell samordning för att offentliga aktörer ska kunna göra ändamålsenliga och noggranna riskbedömningar för att inte tillgängliggörande av geodata ska medföra risker för Sveriges säkerhet. Denna samordning bör bestå av såväl stöd i form av informationssammanställning, hotbildsbeskrivning och utbildning som teknisk och organisatorisk infrastruktur som kan underlätta samverkan och informationsutbyte.

90 Alvesson, M., Einola, K., & Schaefer, S. M. (2022). Dynamics of wilful ignorance in organizations. *The British Journal of Sociology,* 73(4), 839–858, doi: 10.1111/1468-4446.12963.e

7. Slutsatser

FOI och Lantmäteriet har under 2024 och 2025 arbetat tillsammans med att ta fram ett utkast till metod för riskbedömning vid tillgängliggörande av geodata avseende Sveriges säkerhet. Utkastet till denna metod benämns för läsbarhetens skull MEGS. MEGS presenteras i kapitel 4 samt i separat rapport, *Förslag till processtöd för riskbedömning av geodata avseende vid tillgängliggörande av geodata*.[91]

Nedan sammanställs några resultat från projektet:

- ett utkast till metod för att genomföra en riskbedömning av geodata, som redovisas i kapitel 4 och i en separat rapport[92]
- en dokumentationsmall för genomförande av samverkansmöten mellan myndigheter
- en operationalisering av Sveriges säkerhet i olika nivåer för att försöka underlätta för handläggare i offentlig verksamhet
- en operationalisering av risk som en kombination av relevans och konsekvens
- det redovisade arbetet kan utgöra en utgångspunkt även för ansvariga för andra datamängder än geodata
- ett förslag om utveckling av gemensamt stöd på nationell nivå.

Förståelsen för avigsidorna av digitalisering och tillgängliggörande av geodata i samhället behöver fortsatt utvecklas. Det handlar om hotbilder, metoder för att förstå risker, utvecklingsarbete och samarbete hos myndigheter som har ansvar för dataproduktion och tillgängliggörande. Förhoppningen är att MEGS kan utgöra en grund för en myndighetsgemensam metod. Metoden kan dock på intet sätt ses som optimal eller slutgiltig. Snarare ska den betraktas som inledningen på ett arbete och en process där myndigheter tillsammans arbetar vidare med riskbedömningar med avseende på geodata och aggregering där dessa kan förfinas stegvis. Baserat på erfarenheter från genomförda riskbedömningar och framtida forskning kan metodens validitet och reliabilitet förbättras och utkastet till metod kan på det sättet bidra till att stödja den lärandeprocess som behövs.

Utöver att denna rapport presenterar en metod för riskbedömning gällande Sveriges säkerhet vid tillgängliggörande av geodata, belyser den även den gråzon, eller snarare det vita fält, inom vilket detta riskbedömningsarbete ska genomföras. Här åskådliggörs även de krav som ställs på enskilda aktörer att genomföra denna typ av riskbedömning. I detta fall påbjuder lagstiftningen tillgängliggörande av data och riskbedömning av denna utifrån Sveriges säkerhet när det samtidigt saknas tillräckliga förutsättningar för att genomföra sådana bedömningar.

För att fortsätta detta arbete bör vidare dialoger mellan relevanta offentliga aktörer fortsatt föras. Framförallt bör någon aktör få huvudansvar för sådana riskbedömningar som MEGS har utvecklats för. Det behöver även ske fortsatt arbete med att förstå vilken geodata och information som är skyddsvärd utifrån aspekter såsom säkerhetsskyddsklassificering och samhällsviktig verksamhet, samt andra data som kan komma att påverka Sveriges säkerhet.

7.1 Identifierade behov och förslag på framtida arbete

I arbetet med att ta fram ett utkast till metod för riskbedömning av geodata för att uppfylla öppna datalagen har behov av fortsatt arbete identifierats. Behoven som identifierats består, förutom av fortsatt arbete och utveckling av MEGS, av förslag på åtgärder som behövs för att underlätta för de aktörer som ska utföra riskbedömningar av tillgängliggörande av geodata. Förslagen som presenteras har i vissa fall beskrivits tidigare i rapporten och har ingen inbördes ordning.

Flera av förslagen kan innebära att arbetet behöver genomföras under sekretess:

- Utse en aktör som får ansvar för MEGS nationellt och som utvecklar, förvaltar och sprider den till berörda aktörer.
- Utse ansvarig/-a myndighet/-er som återkommande tar fram hotbildsbeskrivningar med fokus på risker med geodata i syfte att stödja de civila myndigheter som producerar och tillhandahåller geodata.

91 Davidsson m.fl. (2025).

92 Davidsson m.fl. (2025).

- Utred möjligheten att skapa ny struktur för ansvarsfördelning av riskbedömning av geodata. Undersök om det skulle vara möjligt att exempelvis utse ansvariga myndigheter utifrån olika tematiska indelningar på geodata. Ett sätt kan vara att låta en specialiserad myndighet ansvara för en viss mängd geodata och vara initierande aktör som genomför bedömningen, som de andra myndigheterna sedan ska förhålla sig till.
- Uppdra till lämplig aktör att ta fram gemensamma riktlinjer och rutiner för hur offentliga aktörer som tillhandahåller geodata bör följa upp och ha uppsikt över nedladdning/nyttjande av tillgängliggjord geodata.
- Fortsätt arbetet med möjliga åtgärder såsom utveckling av inhämtning och retuschering. Det arbetet behöver ske i dialog med fler myndigheter än Försvarsmakten. Särskilt myndigheter med skyddsvärd verksamhet eller tillsynsmyndigheter, såsom länsstyrelser och Fortifikationsverket, behöver fortsätta utreda och utbildas inom de åtgärdsmetoder som finns idag och som utvecklas hela tiden. Exempelvis finns det nya metoder som kan försvåra automatiserad analys av stora mängder data med nya AI-metoder, till exempel objektigenkänning. Ett sätt kanske kan vara att addera svagt brus till data som inte påverkar en mänsklig användare men som AI-metoderna inte har tränats för och som påverkar analysen.
- Gör en utredning där geodata såsom den beskrivs i denna rapport och satellitdata jämförs. Det finns både likheter och skillnader mellan dessa data vilket behöver undersökas ytterligare för att avgöra vilka data som kan anses motsvara geodata som tillgängliggörs av offentliga aktörer.
- Gör en kartläggning över alternativa geodata. Vilken geodata finns redan idag? Skulle exempelvis viss satellitdata kunna motsvara geodata?
- Fördjupa kunskapen om riskområden för riskbedömningar av geodata. Ett exempel är nutida och framtida teknikrisker, t.ex. möjligheterna att göra objektidentifiering med hjälp av AI. Ett annat exempel är risker med satellitdata och hur den bör beaktas vid riskbedömningar av geodata. Det behövs mer utbildning och kunskap och handledning rörande området med tillgängliggörande av öppna geodata. Inom totalförsvaret betonas vikten av att öva, träna och testa. Det gäller även i detta sammanhang. Här behövs utbildning i aggregering och varför det är relevant – här behövs flera fallstudier med olika inriktning och varierande konsekvenser.
- Sist i listan, men absolut inte minst handlar om behovet av att utreda vidare problematiken med aggregering och ackumulering av geodata. Tillgång till geodata kan tillåta en stor mängd analyser vilket innebär en betydande utmaning. För att svenska myndigheter ska lära sig mer om detta problem skulle ett sätt att angripa aggregeringsproblematiken vara att organisera ett gemensamt så kallat hackaton. Det innebär ett tillfälle att samla experter med lämplig kompetens (exempelvis geodata, teknik, digitalisering, IT och säkerhet) som testar att utföra och undersöka hur analysobjekt, enskilt eller kombinerat med andra data, kan användas för att planera och genomföra operationer som kan skada Sveriges säkerhet. Hackaton är inom IT-branschen en välkänd metod för att exempelvis utveckla mjukvara och testa cybersäkerhet. Ett hackaton skulle troligen öka förståelsen för många aktörer kring hot och risker med tillgängliggörandet av geodata och det skulle samtidigt kunna vara ett sätt öka samverkan mellan försvars- och säkerhetsexperter med civila myndigheter och geodataexperter.

Referenser

Alvesson, M., Einola, K., & Schaefer, S. M. (2022). Dynamics of wilful ignorance in organizations. *The British Journal of Sociology*, *73*(4), 839–858, doi:10.1111/1468-4446.12963.

Aven, T., (2016). Risk assessment and risk management: Review of recent advances on their foundation, *European Journal of Operational Research* 253:1, 1–13, doi:10.1016/j.ejor.2015.12.023.

Aven, T., Ben-Haim, Y., Boje Andersen, H., Cox, T., Droguett, E. L., Greenberg, M., Guikema, S., Kröger, W., Renn, O., Thompson, K. M. & Zio, E., (2018). *Society for Risk Analysis Glossary*, https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf [Hämtad 2024-03-06].

Aven, T., Renn, O. & Rosa, E. A., (2011). On the ontological status of the concept of risk, *Safety Science* 49:8, 1074–1079, doi:10.1016/j.ssci.2011.04.015.

Bannigan, K., & Watson, R. (2009). Reliability and validity in a nutshell. *Journal of Clinical Nursing*, *18*(23), 3237–3243, doi:10.1111/j.1365-2702.2009.02939.x.

Baum, S. D. (2020). Quantifying the probability of existential catastrophe: A reply to Beard et al. *Futures*, *123*, 102608, doi: 10.1016/j.futures.2020.102608.

Beard, S., Rowe, T. & Fox, J., (2020). An analysis and evaluation of methods currently used to quantify the likelihood of existential hazards, *Futures* vol. 115, 102469, doi:10.1016/j.futures.2019.102469.

Breakwell, G. M. (2007). *The psychology of risk*. Cambridge University Press, Cambridge.

Carlbom, O., Douglas, D., Larsson, P. & Lindgren, R. (2001). *Civil och militär regional ledning och samverkan vid samordning av samhällets resurser i extraordinära situationer*. FOI-R--0064--SE. Totalförsvarets forskningsinstitut, Stockholm.

Clardy, A. (2022). What can we know about the future? Epistemology and the credibility of claims about the world ahead. *Foresight*, *24*(1), 1–18, doi:10.1108/FS-01-2021-0020.

Coppedge, M., Gerring, J., Altman, D., Bernhard, M., Fish, S., Hicken, A., et al. (2011). Conceptualizing and Measuring Democracy: A New Approach. *Perspectives on Politics*, *9*(2), 247–267, doi:10.1017/S1537592711000880.

Croon, A., Longworth, S., Refors Legge, M., & Winther, P. (2023). *Vägar till juridisk motståndskraft. Att identifiera och motverka användning av juridiska sårbarheter i rättssystem.* FOI-R--5501--SE. Totalförsvarets forskningsinstitut, Stockholm.

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

Eriksson, C., Denward, C., Hedtjärn Swaling, V., & Mickelsson, L. (2020). *Kunskap för beredskap: Vad har risk- och sårbarhetsanalys gett för effekt hittills och hur kan nyttan öka?* FOI-R—4804--SE. Totalförsvarets forskningsinstitut, Stockholm.

Försvarsmakten & MSB (2021). *Handlingskraft. Handlingsplan för att främja och utveckla en sammanhängande planering för totalförsvaret 2021-2025*. FM2021-17683:2, MSB2020-16261-3.

Hahmann, S., & Burghardt, D. (2013). How much information is geospatially referenced? Networks and cognition. *International Journal of Geographical Information Science*, *27*(6), 1171–1189, doi:10.1080/13658816.2012.743664.

Hansson, S. O. (2004). Philosophical Perspectives on Risk. *Techné*, *8*(1), 10–35.

Hansson, S. O. (2022). Can Uncertainty Be Quantified? *Perspectives on Science*, *30*(2), 210–236, doi:10.1162/posc_a_00412.

Ingemarsdotter, I., Eidenskog, D. & Hedtjärn Swaling, V. (2020), *Vilse i lasagnen? En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*. FOI-R--4814--SE. Totalförsvarets forskningsinstitut, Stockholm.

Integritetsskyddsmyndigheten (2021). *Vad är personuppgifter?* https://www.imy.se/privatperson/dataskydd/introduktion-till-gdpr/vad-ar-personuppgifter/ [Hämtad 2025-05-13].

James, P. (2015). *Urban Sustainability in Theory and Practice*. Routledge, Abingdon.

Jonsson, D., Eriksson, C., Ingemarsdotter, J., Rossbach, N. & Wedebrand, C. (2023). *Gråzonslägen i krig och fred*. FOI-R--5447--SE. Totalförsvarets forskningsinstitut, Stockholm.

Kahneman, D., Sibony, O. & Sunstein, C. R., (2021). *Noise: A Flaw in Human Judgment*. Little Brown & Co, New York.

Kerr, N. L., & Tindale, R. S. (2004). Group Performance and Decision Making. *Annual Review of Psychology*, *55*, 623–655, doi:10.1146/annurev.psych.55.090902.142009.

Kommissionens genomförandeförordning (EU) av den 21.12.2022 om fastställande av en förteckning över särskilda värdefulla dataset och arrangemangen för offentliggörande och vidareutnyttjande av dessa, Pub. L. No. C(2022) 9562.

Lantmäteriet. (u.å.). *Geodatarådet*. https://www.lantmateriet.se/geodataradet [Hämtad 2025-05-13].

Lantmäteriet. (u.å.). Öppna data. https://www.lantmateriet.se/sv/geodata/vara-produkter/oppna-data/ [Hämtad 2025-05-13].

Lantmäteriverket. (u.å.). *Så här skaffar du laserskannat material*. https://www.maanmittauslaitos.fi/sv/laserskannat-material [Hämtad 2024-11-22].

Mousavi, S., & Gigerenzer, G. (2014). Risk, uncertainty, and heuristics. *Journal of Business Research*. 67(8), 1671-1678, doi:10.1016/j.jbusres.2014.02.013.

MSB (2018). *Gemensamma grunder för samverkan och ledning vid samhällsstörningar*. MSB777.

MSB (2023). *Vägledning, Säkerhetsåtgärder i informationssystem*. MSB2032.

MSB (2024). *Riskhantering*. https://metodstod-informationssakerhet.msb.se/sv/utforma/riskhantering/ [Hämtad 2025-05-13].

MSB (2025). *Metodstöd för informationssäkerhetsarbete*. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/arbeta-systematiskt-informationssakerhet-och-cybersakerhet/metodstod-for-informationssakerhetsarbete/ [Hämtad 2025-05-13].

Myndigheten för digital förvaltning, (2025). *Vägledning för att tillgängliggöra information*, https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/vagledning-for-att-tillgangliggora-information [Hämtad 2025-01-27].

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, doi:10.5194/isprs-archives-XLVIII-4-W12-2024-121-2024.

Prop. 2017/18:89. *Ett modernt och stärkt skydd för Sveriges säkerhet – ny säkerhetsskyddslag*.

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

Prop. 2024/25:34. *Totalförsvaret 2025–2030*.

SFS 2006:544. *Lag om kommuners och regioners åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap.*

SFS 2018:585. *Säkerhetsskyddslag*.

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

Slovic, P., Peters, E., Finucane, M. L. & MacGregor, D. G. (2005). Affect, risk, and decision making. *Health Psychology* 24(4), 35-40, doi:10.1037/0278-6133.24.4.S35.

Sonnsjö, H. & Mobjörk, M,. (2013). *Om indirekta, komplexa och oönskade händelser. Att analysera risker med stor osäkerhet*. FOI-R--3649--SE. Totalförsvarets forskningsinstitut, Stockholm.

SOU 2020:55. *Innovation genom information (Öppna data-utredningen)*.

SOU 2024:64 *Motståndskraft i samhällsviktiga tjänster*.

Svahn, M., Jarlsbro, M., Michélsen Forsgren M. & Lindahl, D. (2024). *Delat ansvar är ingens ansvar? En analys av den svenska statsförvaltningens ansvar och styrning vad gäller svenskt informations- och cybersäkerhetsarbete*. FOI-R--5546--SE. Totalförsvarets forskningsinstitut, Stockholm.

Svenska institutet för standarder (2018). *Riskhantering – Vägledning*. ISO 31000:2018, IDT.

Svenska institutet för standarder (2022). *Informationssäkerhet, cybersäkerhet och integritetsskydd – Vägledning om riskhantering inom informationssäkerhet*. ISO/IEC 27005:2022, IDT.

Säkerhetspolisen, (2023a). *Vägledning i säkerhetsskydd. Informationssäkerhet*.

Säkerhetspolisen, (2023b). *Vägledning i säkerhetsskydd. Säkerhetsskyddsanalys*.

Säkerhetspolisen, (2023c). *Vägledning i säkerhetsskydd. Introduktion*.

Taleb, N. N. (2010). *The Black Swan. The Impact of the Highly Improbable* (2:a utg.). Random House, New York.

Winehav, M. & Nevhage, B. (red.), (2011). *FOI:s modell för risk- och sårbarhetsanalys (FORSA)*. FOI-R--3288--SE. Totalförsvarets forskningsinstitut, Stockholm.

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

www.regeringen.se [hämtad 2025-03-18]

Bilaga A: Scenario

Scenario autonom navigering

AI-tekniken skapar idag nya förutsättningar för kvalificerad automatisk bildanalys, till exempel parvis jämförelse av bilder från luftfarkoster för att avgöra om de visar samma geografiska plats. Bilderna visar samma landskap men kan ha olika upplösning, olika vyer, och vara från olika årstider. Om den ena bilden är georefererad kan positioner hos detaljer i den andra bilden bestämmas och som en följd också kamerans position och orientering.

En tillämpning för den här tekniken är autonom navigering av drönare. Bildanalysen kombineras med tröghetsnavigering för kontinuerlig och robust skattning av drönarens position och flygriktning. Bildtekniken stöder positionering och motverkar feltillväxten över tid som är vanlig i ett system med bara tröghetsnavigering. Systemet fungerar som ett komplement till traditionell navigering med GNSS och är särskilt användbart i situationer där GNSS-systemen är utsatta för störning eller drönaren flyger så att satelliterna är skymda, till exempel i stadsmiljö med höga byggnader eller i skogsmiljö. Det är också då som detaljerade bilder med god georeferering som relativt nya ortofoton fungerar mycket bättre än satellitbilder som underlag.

Autonomi och flygning i skydd har många tillämpningar, inte minst militärt men också civilt då det tar bort behovet att ha en pilot i närheten samt gör det svårare att upptäcka och hindra drönaren. Det finns exempelvis ingen kommunikation mellan pilot och drönare att detektera, pejla och störa. Den här tekniken utvecklas för närvarande i första hand för speciella tillämpningar men på sikt kommer den med stor sannolikhet också dyka upp hos kommersiella drönare som komplement till traditionell navigering med GNSS.

Exempel - Terrorattack med autonoma drönare

En terroristgrupp planerar att attackera ett större evenemang i Sverige. Man planerar använda nya snabba kommersiella drönare som kan navigera autonomt med kamerabilder. De ska placeras ut på lämpliga platser flera veckor i förväg, exempelvis på taket på en öde byggnad eller i en mindre lastbil med öppningsbart tak som sedan ställs på en långtidsparkering. Drönarna ska förses med sprängladdningar med avsikt att sprida skräck och skada.

Terroristerna planerar att i lugn och ro ha lämnat landet efter utplaceringen av drönarna och befinna sig på sin hemmabas där de slutplanerar och programmerar in flygrutt, laddar upp navigeringsunderlag och slutmål via mobilnätet. Både planering och programmering sker med stöd av tillgängliga öppna geodata som enkelt kan laddas ned från nätet. Data som används är nya ortofoton och höjddata. Genom att använda VPN och olika proxys döljer man sin egen IP-adress. Terroristernas mål är en större demonstration som går emot de uppfattningar man står för.

Drönarna är visserligen små och kan inte bära stora sprängladdningar men de är också svåra att upptäcka och om de skulle bli upptäckta är de besvärliga att följa och hindra. Eftersom drönarna opererar helt autonomt finns ingen radiokommunikation med en pilot som kan pejlas in och/eller störas. En tillfällig störning eller avsiktlig avstängning av GNSS-signalerna i syfte att försvåra angrepp hjälper inte heller.

Flygrutten programmeras för att dra nytta av terrängen och använda maximalt skydd av träd och hus. Med flygning nära bostadshus försvåras också möjligheterna till verkanseld från eventuella skyddssystem. Korta och snabba uppstigningar genomförs vid behov för större yttäckning med kameran och kalibrering av position och orientering. Allt detta ökar möjligheterna att angreppet lyckas.

Terroristerna följer upptakten till demonstrationen via nyheter på internet och vid lämplig tidpunkt aktiveras drönarna. Någon drönare upptäcks men kan ändå inte hindras. Attacken lyckas. Alla drönare når sina mål vilket resulterar i flera dödsoffer och ett stort antal skadade.

Attacken får stort genomslag i media. Upprördheten är stor i många läger. Den blir inte mindre när det står klart att attacken fjärrstyrts av terrorister utanför landet och att drönarna opererat autonomt med kameradata och inte kunnat hejdas av existerande skyddssystem då dessa i huvudsak baseras på detektion och störning av kommunikationen med en pilot.

Efterspel och potentiella konsekvenser – stöd för diskussion

- En ökad misstro mot myndigheter och politiker och möjligheterna att skydda befolkningen och demokratiska värden.
- Rädsla för drönare så fort man ser eller hör någon. Drönartekniken och företag som använder drönare hamnar i onåd och misstänks. Hårdare reglering kan bli nödvändig, ska vem som helt kunna skaffa och använda autonoma drönare? Detta hotar hämma innovation och nyttiggörande för annars goda ändamål, såsom snabb leverans av läkemedel till otillgängliga platser.
- Journalister ställer frågor och spekulerar i behov av reglering av tillgång till underlag för autonom navigering.
- Om attacker kan genomföras utan att en angripare är fysiskt närvarande sänks sannolikt tröskeln för olika angrepp. En person behöver inte vara starkt radikaliserad och acceptera martyrskap för att genomföra angrepp. I ett värsta scenario kan det räcka att någon känner sig tillräckligt förfördelad eller orättvist behandlad, och exempelvis vilja störta en drönare rakt in i gruppen anställda hos kronofogden när de fikar på bakgården. En plats som kan vara lokaliserad genom studier av detaljerade öppna flygbilder.
- Om främmande makt ges tillgång till underlag för navigering ökar deras förmåga och försvårar vårt eget försvar.

FOI

LANTMÄTERIET

ISSN 1650-1942

www.foi.se