



Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data

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

Maria Ciepielewska, Sofia Stjernlöf

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

Maria Ciepielewska, Sofia Stjernlöf.

Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data

Titel: Förslag till processtöd för riskbedömning av geodata vid tillgängliggörande som öppna data

Rapportnummer FOI-R--5768--SE

Månad Maj

År 2025

Antal sidor 58

ISSN 1650-1942

Uppdragsgivare Lantmäteriet

Forskningsområde Övrigt

Projektnummer E13927

Godkänd av Malek Finn Khan

Ansvarig avdelning Försvarsanalys

Omslagsbild: Shutterstock

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

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett annat sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Totalförsvarets Forskningsinstitut (FOI) och Lantmäteriet har i samarbete tagit fram ett utkast till Metod för riskbedömning vid tillgängliggörande av Geodata som öppna data avseende Sveriges säkerhet – MEGS. Metoden utarbetades som ett resultat av öppna datalagen där tillgängliggörande av data ska föregås av en riskbedömning. I lagens förarbete uttrycks det även att riskbedömningen ska ta hänsyn till aggregering, vilket MEGS gör.

Riskbedömningar baseras ofta på sannolikhet och konsekvens, men för komplexa risker, som de som rör Sveriges säkerhet, är detta tillvägagångssätt inte tillämpligt. Här har *relevans* introducerats i stället för sannolikhet, och en ansats med konsekvensnivåer testas utifrån en möjlig innebörd av Sveriges säkerhet. I den föreslagna riskbedömningsmetoden används relevans, konsekvensnivåer och förslag på kriterier för dessa nivåer.

MEGS består av sex steg som leder fram till ett underlag inför ett beslut om en specifik uppsättning geodata kan utgöra en risk för Sveriges säkerhet eller ej, och om denna geodata därmed kan tillgängliggöras. De sex stegen, som bland annat inkluderar framtagande av förberedande material och genomförande av en workshop i samverkan med andra aktörer, beskrivs utförligt i processtödet. Till hjälp vid riskbedömningens genomförande vid workshoppen finns även en dokumentationsmall.

Framtagandet av MEGS samt de avväganden som ligger bakom metodens utformning beskrivs i en separat rapport *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, for making geodata open data related to Sweden's security. The method, *Proposed Process Support for Risk Assessment of Geodata when Making them Available as Open Data – A Collaborative Effort by Government Agencies* was created in response to the Open Data Act, which mandates a risk assessment prior to data release and requires consideration of aggregation, addressed by MEGS.

Risk assessments are often based on probability and consequence, but for complex risks, such as those related to Sweden's national security, this approach is not applicable. Instead, relevance has been introduced for and is replacing probability, and an approach using consequence levels is tested based on potential implications for Sweden's national security. In the proposed risk assessment method, relevance, consequence levels, and proposed criteria for these levels are used.

MEGS consists of six steps that lead to a decision basis for whether a specific set of geodata poses a risk to Sweden's security and therefore can, or cannot be made available. The six steps, which include preparatory materials and the implementation of a workshop in collaboration with other stakeholders, are described in detail in the process support guide. A documentation template is also available to assist in conducting the risk assessment during the workshop.

The development of MEGS and the considerations behind the method's design are described in a separate report *Method for Risk Assessment of Geodata when Making them Available as Open Data*.

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

Förord

Detta processtöd är ett resultat av ett myndighetsgemensamt arbete som är tänkt att ge ett praktiskt stöd för myndigheter i att gemensamt bedöma riskerna för Sveriges säkerhet, när de ska tillgängliggöra öppna geodata.

Arbetet, som pågått 2024 - 2025, har finansierats med 2:4-medel från Myndigheten för samhällsskydd och beredskap. Projektet har utförts av Lantmäteriet och Totalförsvarets forskningsinstitut, med stöd av flertalet statliga myndigheter och två kommuner.

Det finns idag flera metoder för olika typer av riskbedömningar men det saknas en vedertagen metod och praktiskt stöd för denna nya typ av riskbedömning. Processtödet syftar till att underlätta korrekta, enhetliga och myndighetsgemensamma bedömningar.

Det finns flera utmaningar som processtödet syftar till att underlätta. En av utmaningarna är att bedömningen ska beakta riskerna med aggregering av annan data. Ett annat exempel på utmaning är att bedömningen bör ske i samverkan med experter på bland annat geodata. Med utmaningarna som utgångspunkt har vi försökt skapa ett stöd för att möjliggöra dessa komplexa bedömningar i offentliga verksamheter som tillgängliggör geodata.

Vi vill rikta ett stort tack till de myndigheter och kommuner som har deltagit i arbetet. Den kunskap och de erfarenheter som vi fått del av har varit av stort värde för slutresultatet.

Lantmäteriet kommer att använda processtödet i sin verksamhet för att riskbedöma geodata fortlöpande. Myndigheten har också i sin samordnande roll på geodataområdet för avsikt att fortsätta att utveckla processtödet tillsammans med bland annat Geodatarådet.

Lantmäteriet och FOI ser ett fortsatt behov av att arbeta vidare med dessa frågor med berörda aktörer och hoppas därför på en fortsatt god myndighetssamverkan.

Sofia Stjernlöf
Projektledare Lantmäteriet

Minna Severin
Projektledare FOI

Innehållsförteckning

Begreppslista	7
1. Inledning	9
1.1 Syfte med processtödet	9
1.2 Avgränsningar	10
1.3 Processtödet målgrupp	10
1.4 Utveckling av processtödet	10
1.5 Läsanvisningar	10
2. Centrala begrepp	11
2.1 Roller och befattningar i riskbedömningen	11
2.2 Analysobjekt och analyserat format	12
2.3 Skillnaden mellan information och data	12
3. Översikt av innehållet i MEGS och metodens tillämpning	13
3.1 MEGS övergripande process	13
3.2 Grundläggande metodavvägningar i MEGS	14
3.3 När ska riskbedömning göras?	16
3.4 Resultatet är beroende av deltagarnas kompetens och samverkan	16
3.5 Dokumentera löpande	17
3.6 Beakta säkerhetsskydd	17
4. Beskrivning av MEGS	19
4.1 Steg 1: Inled processen	19
4.2 Steg 2: Skapa underlag	20
4.3 Steg 3: Förbered gemensam bedömning av risker	23
4.4 Steg 4: Gör individuell bedömning av risker	24
4.5 Steg 5: Genomför gemensam bedömning av risker	24
4.6 Steg 6: Besluta	35
5. Tankefällor och motargument	37
Referenser	41
Bilaga 1: Dokumentationsmall: riskbedömning workshop	45
Bilaga 2: Kriterier Sveriges säkerhet	53
Bilaga 3: Konsekvensnivåer	57

Begreppslista¹

Akkumulering

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

Aggregering

Sammanställning av flera data- eller informationsmängder.

Analysobjekt

Den geodatomängd 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.

Geodatomängd

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 riskbedömnings- processen.

Offentlig aktör

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

¹ Listan är tagen från Davidsson, Åsa, Mittermaier, Eva, Severin, Minna, Söderman, Ulf, Winterdahl, Mathias, Ciepielewska, Maria & Stjernlöf, Sofia, *Riskbedömning av geodata vid tillgängliggörande som öppna data*. FOI-R--5745--SE. Totalförsvarets forskningsinstitut, Stockholm (2025)..

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

Offentliga aktörer ska tillgängliggöra sina digitala data som öppna data enligt lagen (2022:818) om den offentliga sektorns tillgängliggörande av data (hädanefter benämnd öppna datalagen). Sådant tillgängliggörande ska dock endast göras så länge det inte leder till risker för Sveriges säkerhet. Bland de data som är särskilt prioriterade för tillgängliggörande, så kallade värdefulla datamängder, dominerar olika typer av geografiska data (geodata) som ortofoton, markhöjddata och landtäckedata. I Sverige produceras geodata av många olika offentliga aktörer; en del av dessa data finns redan idag tillgängliga som öppna data medan andra erbjuds mot exempelvis licensavgift. Förutom särskilt värdefulla data producerar många offentliga aktörer även andra typer av geodata som kan vara föremål för tillgängliggörande som öppna data, exempelvis markfuktighet och vägtrumms position.

Att göra riskbedömningar med avseende på Sveriges säkerhet är långt ifrån en trivial uppgift. Det ställer stora krav på såväl resurser som kompetens. Öppna datalagen med tillhörande förarbeten ger begränsad vägledning för hur en sådan riskbedömning ska göras. Dessutom saknas nationella riktlinjer eller prejudicerande domar som offentliga aktörer kan lita sig mot när de ska göra riskbedömningar. Brist på vägledning kan leda till att varje aktör gör egna tolkningar av lagen och skapar olika interna rutiner för riskbedömningar vid tillgängliggörande av geodata. Det kan i sin tur resultera i att offentliga aktörer gör olika bedömningar av samma typ av geodata vilket kan leda till skada för Sveriges säkerhet. Det finns behov av översyn av lagstiftningar som berör problematiken med tillgängliggörande av data i förhållande till skydd av data. Här beskrivs ett förslag till metod för att göra riskbedömningar vid tillgängliggörande av geodata som öppna data med avseende på Sveriges säkerhet. För läsbarhetens skull används hädanefter förkortningen MEGS, som står för "Metod för riskbedömningar av öppna Geodata med avseende på Sveriges säkerhet". Syftet med denna metod är att möjliggöra för offentliga aktörer att i samverkan genomföra regelbundna riskbedömningar av geodata med avseende på Sveriges säkerhet, med särskilt beaktande av den så kallade aggregeringsproblematiken. MEGS är tänkt att användas av offentliga aktörer i samverkan för att bidra till att uppnå enhetliga och konsekventa bedömningar och för att involvera bredast möjliga kompetens i riskbedömningen.

1.1 Syfte med processtödet

MEGS är utvecklad för att vara ett stöd till de offentliga aktörer som berörs av öppna datalagen. Syftet med detta processtöd är att beskriva hur metoden kan användas i avsikt att uppnå kraven i öppna datalagen. Processtödet beskriver hur en riskbedömning av en geodatamängd kan genomföras för att undersöka vilka risker för Sveriges säkerhet som ett tillgängliggörande av den specifika geodatamängden kan medföra. Författarnas förhoppning är att stödet ska fungera både som övergripande beskrivning av MEGS och som handbok att vända sig till under det praktiska arbetet med riskbedömningar. För bakgrundsbeskrivning, information om metodutveckling och motivering hänvisas läsaren till rapporten *Riskbedömning av geodata vid tillgängliggörande som öppna data*.¹

¹ Davidsson, Å., Mittermaier, E., Severin, M., Söderman, U., Winterdahl, M., Ciepielewska, M. & Stjernlöf, S., *Riskbedömning av geodata vid tillgängliggörande som öppna data*. FOI-R--5745--SE, Totalförsvarets forskningsinstitut, Stockholm (2025).

1.2 Avgränsningar

MEGS är utformad utifrån öppna datalagen och inte annan lagstiftning såsom säkerhetsskyddslagen eller offentlighets- och sekretesslagen där det också finns krav på riskbedömning. Det är upp till respektive aktör att säkerställa att berörd lagstiftning följs.

1.3 Processtödet målgrupp

Detta processtöd riktar sig främst till anställda vid myndigheter och andra offentliga aktörer som ska tillgängliggöra data enligt öppna datalagen, exempelvis informationsägare och handläggare. Tillämpningen av metoden förutsätter vissa förkunskaper om exempelvis geodata, riskbedömning och säkerhetsskydd.

1.4 Utveckling av metoden

MEGS är utvecklat utifrån ett verksamhetsnära perspektiv i nära samarbete mellan FOI och Lantmäteriet. Det har utvecklats med inspiration från riskvärderingsmodeller som FORSA² genom en iterativ process där metoden har testats vid workshoppar med offentliga aktörer och därefter reviderats. Metoden har inte prövats i sin helhet. Den ska därför ses som ett utkast och underlag för fortsatt utveckling. För mer utförlig beskrivning av projektets genomförande och hur metoden arbetats fram, se kapitel 3 i Riskbedömning av geodata vid tillgängliggörande som öppna data.³

1.5 Läsanvisningar

Processtödet består av fem kapitel och tre bilagor. Efter det inledande kapitlet följer kapitel 2 som utgörs av en beskrivning av hur ett antal centrala begrepp som används i den fortsatta texten ska förstås. Kapitel 3 består av en allmän översikt av MEGS och dess generella struktur samt utgångspunkter, kommentarer om vilka personer som är lämpliga deltagare i riskbedömningen och säkerhetsskyddsaspekter. I kapitel 4 beskrivs de sex stegen i MEGS i detalj med råd för ett framgångsrikt genomförande. Kapitel 5 redogör för ett antal tankefall som har visat sig vara vanliga under framtagandet av metoden. Bilagorna består av 1) ett förslag till dokumentationsmall som kan användas under workshop, 2) en detaljerad tabell med de kriterier för Sveriges säkerhet som används vid värdering av risker och 3) en tabell med de konsekvensnivåer som används i MEGS.

² Winehav, M. & Nevhage, B.,. *FOI:s modell för risk- och sårbarhetsanalys (FORSA)*. FOI-R--3288--SE. Totalförsvarets forskningsinstitut, Stockholm, Sverige (2011).

³ Davidsson, m.fl. 2025.

2. Centrala begrepp

I processtödet med tillhörande bilagor används en uppsättning begrepp med specifika betydelser. Definitioner av de flesta begrepp finns i begreppslistan i början av denna skrift. Här preciserar vi mer i detalj hur ett antal centrala begrepp ska förstås och hur de används.

2.1 Roller och befattningar i riskbedömningen

Riskbedömningen involverar en stor mängd aktörer och befattningshavare. Här förtydligas hur de mest centrala aktörerna och befattningshavarna benämns i detta processtöd.

Med begreppet offentlig aktör avser vi här alla de aktörer som omfattas av öppna datalagen och som alltså ska göra en riskbedömning av digitala data innan de tillgängliggörs som öppna data. Begreppet omfattar alla de myndigheter samt regioner och kommuner som producerar och tillgängliggör geodata. Öppna datalagen gäller emellertid även andra aktörer, exempelvis vissa offentligt ägda bolag; även dessa omfattas därför av begreppet ”offentlig aktör”.⁴

I denna skrift används termen initierande aktör för att benämna den offentliga aktör som har för avsikt att tillgängliggöra en viss geodatamängd eller ser behov av att genomföra en riskbedömning, och följaktligen inleder riskbedömningsprocessen. Övriga offentliga aktörer som involveras i riskbedömningen kallas deltagande aktörer. Eftersom flera olika offentliga aktörer kan genomföra riskbedömningsprocesser parallellt kan en aktör inta olika roller beroende på vems process de för närvarande deltar i.

Hos de offentliga aktörer som producerar digitala data finns vanligen informationsägare, det vill säga befattningshavare som ”har ansvaret för den information som skapas och hanteras inom den egna organisationen”.⁵ Det är troligen informationsägaren som ansvarar för tillgängliggörande av geodata och som därför har huvudansvaret för att en riskbedömning genomförs.⁶

Vi föreslår att varje offentlig aktör dessutom utser en processledare som leder riskbedömningsprocessen och ansvarar för dess genomförande. Det är även processledaren som agerar som kontaktperson för och är deltagare vid andra offentliga aktörers riskbedömningar. I sin *Vägledning för att tillgängliggöra information* föreslår Myndigheten för digital förvaltning att varje offentlig aktör under ledning av en samordnare etablerar en arbetsgrupp för tillgängliggörande av data.⁷ För att riskbedömningen ska bli en integrerad del av tillgängliggörandeprocessen bör processledaren ingå i denna arbetsgrupp.

Utvecklingen av MEGS har tydligt visat att processledaren behöver en för ändamålet lämplig kompetens.⁸ För att realistiskt och uttömmande kunna bedöma risker med geodata behöver processledaren ha en gedigen förståelse för exempelvis geodata i allmänhet, rumsliga analyser och geografiska informationssystem (GIS). Det är vidare fördelaktigt om processledaren även har god förståelse för rådande hotbild och säkerhetsskyddsarbete. Eftersom riskbedömningsprocessen sannolikt involverar sekretessbelagd eller säkerhetsskyddsklassificerad information behöver processledaren vara behörig att hantera sådant material.

4 1 kap. 5-7 §§ öppna datalagen (2022:818) preciseras vilka aktörer som omfattas av lagen.

5 Sveriges Kommuner och Regioner, *Termer och begrepp*, (2025), <https://klassa.skr.se/sidor/stodmaterial/Begrepp> [hämtad 2025-01-27].

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

7 Myndigheten för digital förvaltning 2025.

8 Davidsson, m.fl. 2025.

2.2 Analysobjekt och analyserat format

Den geodatomängd för vilken riskbedömningen ska göras benämns här analysobjekt. Analysobjektet är alltid en enskild och specifik geodataprodukt såsom det definieras av den initierande aktören. En offentlig aktör kan producera flera olika geodatomängder och kan finna det lämpligt att utföra riskbedömning för alla dessa samlat. I så fall är varje geodatomängd ett separat analysobjekt.

I processtödet syftar analyserat format på det format i vilket initierande aktör avser att tillgängliggöra analysobjektet. Eftersom en viss typ av geodata kan förekomma i olika format – exempelvis kan ortofoton produceras i olika upplösning, och en specifik vektorprodukt kan tillgängliggöras med varierande uppsättning attribut – behöver man i riskbedömningen precisera vilket format som avses. Begreppet analyserat format används därmed som en samlingsbeteckning för analysobjektets egenskaper såsom filformat, datastruktur, upplösning, attributuppsättning, metadata med mera. I riskbedömningen ska alla deltagare beakta analysobjektet i just det analyserade formatet snarare än som en generisk typ av geodata på vilket analysobjektet är ett exempel. Det går till exempel att tänka sig en offentlig aktör som under tjugo års tid har producerat ortofoton med en upplösning på tio centimeter över ett visst geografiskt område, och som har för avsikt att tillgängliggöra dessa som öppna data. Då är det denna geodatomängd (analysobjektet) i detta specifika format (analyserat format) som ska beaktas i riskbedömningen och inte ortofoton i allmänhet. Om den initierande aktören fattar beslutet att inte tillgängliggöra analysobjektet i analyserat format betyder det alltså inte nödvändigtvis att ortofoton över det aktuella området inte kommer att tillgängliggöras som öppna data. Aktören kan nämligen vidta åtgärder – till exempel att minska upplösningen till en meter eller välja att inte publicera sitt arkiv med historiska foton – för att göra analysobjektet publicerbart i annat format och därmed reducera riskerna för Sveriges säkerhet.

2.3 Skillnaden mellan information och data

Termerna ”data” och ”information” används i allmänhet ofta synonymt. Exempelvis definieras data som ”information i digitalt format oberoende av medium” i 1 kap. 4 § öppna datalagen.⁹ Det finns en fördel med att skilja på data och information då de relaterar till olika kognitiva processer. Inom informationsvetenskap har man under lång tid därför använt sig av den konceptuella begreppshierarkin DIKW (från engelskans Data-Information-Knowledge-Wisdom) för att illustrera hur olika nivåer av allt mer avancerad kognitiv bearbetning är beroende av varandra.¹⁰

I detta processtöd definieras data som representation av bland annat fakta och idéer i en form lämpad för överföring och bearbetning av människor eller av automatiska hjälpmedel.¹¹ De data som avses här är framförallt digitala data i form av siffror eller text lagrade i standardiserade datastrukturer och datafiler på ett digitalt medium. Information definieras som det budskap eller den innebörd, andemening eller tolkning som bland annat data förmedlar till en människa. Data kan bli information först om det presenteras på ett för mottagaren lämpligt sätt. Exempelvis brukar geodata bli förstäligt först då det presenteras genom mjukvara såsom GIS.

Vad som utgör information skiljer sig åt beroende på mottagarens förförståelse. De som inte har en gedigen förståelse för geodata i allmänhet, rumsliga analyser och GIS uppfattar kanske endast det primära informationsinnehållet i de geodata som behandlas, exempelvis höjd över havet när markhöjddata utgör analysobjekt. De med större erfarenhet av att arbeta med geodata och GIS har bättre förutsättningar att beakta de tillämpningar som denna geodatomängd tillåter, exempelvis hur markhöjddata kan användas för att beräkna vattenflöden och följaktligen position och riktning för vattendrag.

På grund av informationens kontextberoende väljer vi att, till skillnad från öppna datalagen men i överensstämmelse med tradition inom informationsvetenskap,¹² definiera data och information så att begreppen förmedlar olika nivåer av kognitiv förståelse. I processtödet ska därför begreppen data och information uppfattas enligt ovanstående definitioner. Denna distinktion är förmodligen även central för att förstå olika hotaktörers inställning till en viss geodatomängd. Det är nämligen inte nödvändigtvis data i sig som är hotaktörens primära mål utan kunskap om exempelvis tänkta angreppsmål eller Sveriges intentioner och förmåga.

9 Ambitionen i EU:s så kallade öppna datadirektiv är bredare då man istället för ”data” använder begreppet ”handling” som definieras som ”allt innehåll, oberoende av medium (papper eller elektronisk form eller i form av ljudinspelningar, bildinspelningar eller audiovisuella inspelningar) eller [...] varje del av sådant innehåll” (Artikel 2.6).

10 Ackoff, R. L. ”From Data to Wisdom”, *Journal of Applied Systems Analysis* vol. 16 (1989); Jennifer Rowley, ”The wisdom hierarchy: representations of the DIKW hierarchy”, *Journal of Information Science* 33:2 (2007), doi:10.1177/0165551506070706.

11 Definitionen är modifierad från MSB:s definition av data, se MSB, *Termbanken för informationssäkerhet*, 2025, <https://termbank-informationssakerhet.msb.se/> [hämtad 2025-03-10].

12 Ackoff 1989; Rowley 2007.

3. Översikt av innehållet i MEGS och metodens tillämpning

Syftet med MEGS är alltså att bedöma vilka risker för Sveriges säkerhet som tillgängliggörande av en viss geodatamängd kan medföra. En sådan uppgift är krävande då den dels fokuserar på Sveriges säkerhet snarare än den egna verksamheten, dels rör risker som är svåra att både identifiera och värdera. I de riskbedömningar som öppna datalagen kräver befinner sig de objekt som kan påverkas vid ett tillgängliggörande vanligen utanför den egna verksamheten. Det är alltså fullt möjligt att den offentliga aktör som tillgängliggör en viss geodatamängd inte utsätts för några risker vid ett tillgängliggörande medan andra aktörer som exempelvis bedriver säkerhets-känslig verksamhet kan påverkas i betydande omfattning.¹³ De risker som ska beaktas i riskbedömningen är dessutom av antagonistisk karaktär vilket medför ett stort mått av informationsunderskott då vi inte har tillräcklig kunskap om hotaktörerna, som dessutom vanligtvis försöker dölja sin verksamhet. För vissa risker kan det till och med vara svårt att avgöra om den egna verksamheten har blivit drabbad eller vem som är antagonisten. Sammantaget medför dessa komplikationer att de riskbedömningar som ska göras enligt öppna datalagen är behäftade med omfattande osäkerheter. Därför är det en rekommendation att göra riskbedömningar återkommande då omständigheterna eller de offentliga aktörernas kunskap och erfarenhet förändras.

3.1 MEGS övergripande process

MEGS består av nedanstående steg, (figur 1). Hur de olika stegen genomförs i praktiken beskrivs i detalj i kapitel 4.

- Steg 1. Inled processen: Processledaren inleder riskbedömningsprocessen, utser arbetsgrupp om det finns behov av en sådan samt planerar processen.
- Steg 2. Skapa underlag: Processledaren, eller arbetsgruppen som denne har utsett, tar fram de underlag som behövs för riskbedömningen. I underlagen ingår i) en beskrivning av analysobjektet och hur det för närvarande används, ii) en hotbildsbeskrivning, iii) en sammanställning av lagstiftning som är relevant för riskbedömningen, iv) en sammanställning av andra relevanta geodata samt v) lämpliga scenarier för användning i workshopen.
- Steg 3. Förbered gemensam bedömning av risker: Innan workshopen behöver den initierande aktören bestämma vilka andra aktörer som ska inkluderas i processen. Workshoppens genomförande planeras, inbjudan skickas till andra aktörer och underlag skickas till de aktörer som har för avsikt att delta i workshopen.
- Steg 4. Gör individuell bedömning av risker: Innan workshopen gör deltagarna individuella bedömningar genom att med hjälp av analysobjektet, dokumentationsmallen och de underlag som den initierande aktören har skickat ut identifiera möjliga risker som tillgängliggörande av analysobjektet som öppna data kan leda till. Det är särskilt viktigt att analysera hur aggregering och ackumulering kan bidra till risker då analysobjektet tillgängliggörs som öppna data.
- Steg 5. Genomför gemensam bedömning av risker: Under workshopen ska de offentliga aktörerna i samverkan identifiera och värdera möjliga risker som ett tillgängliggörande av analysobjektet kan leda till, samt ge en rekommendation om huruvida analysobjektet kan tillgängliggöras i analyserat format. Workshopen består av fyra moment.

13 Davidsson, m.fl. 2025.

- Moment 1: Deltagarna inleder med att identifiera eventuella risker som kan uppstå om analysobjektet tillgängliggörs som öppna data. Detta görs genom att kartlägga vilka konsekvenser som kan uppstå vid ett tillgängliggörande.
- Moment 2: De identifierade konsekvenserna graderas baserat på hur stor skada på Sveriges säkerhet de kan medföra. Dessutom bedömer deltagarna hur relevant analysobjektets är för att konsekvenserna ska uppstå.
- Moment 3: I det tredje momentet markeras varje identifierad konsekvens i en konsekvens- relevansmatris baserat på bedömd konsekvens- och relevansnivå. Konsekvenser som medför skada på Sveriges säkerhet och där analysobjektet är av relevans för konsekvensernas realiserande utmärker risker för Sveriges säkerhet.
- Moment 4: Slutligen lämnar deltagarna en rekommendation om huruvida analysobjektet kan tillgängliggöras som öppna data i analyserat format, om åtgärder behövs innan analysobjektet kan tillgängliggöras eller om analysobjektet inte bör tillgängliggöras.
- Steg 6. Besluta: Baserat på rekommendationen från workshopen ska initierande aktör fatta något av följande beslut: i) analysobjektet ska tillgängliggöras som öppna data i analyserat format, ii) åtgärder krävs innan analysobjektet kan tillgängliggöras som öppna data inklusive en beskrivning av dessa åtgärder, iii) analysobjektet ska inte tillgängliggöras som öppna data men kan tillgängliggöras på annat sätt eller iv) analysobjektet ska sekretessbeläggas. Beslut och motivering ska dokumenteras noga och kungöras till andra offentliga aktörer som berörs eller kan tänkas bli berörda av beslutet.



Figur 1: Riskbedömningens översiktliga struktur består av sex olika steg.

3.2 Grundläggande metodavvägningar i MEGS

Risk kan definieras på många olika sätt beroende på syfte och kontext.¹⁴ Här definieras risk som en situation, händelse eller ett skeende med möjlig negativ konsekvens för Sveriges säkerhet vilken kan bli resultatet av tillgängliggörande av öppna geodata. De potentiella riskerna som kan uppstå vid ett tillgängliggörande kan alltså medföra negativa, men möjligtvis oklara, konsekvenser för Sveriges säkerhet. Ordet ”kan” signalera dessutom att tillgängliggörande av en viss geodatamängd möjligtvis orsakar eller på annat sätt bidrar till riskerna. Det finns alltså åtminstone två källor till osäkerhet när potentiella risker ska bedömas: osäkerhet gällande konsekvensernas beskaffenhet samt

14 Se t.ex. Hansson, S. O., “Philosophical Perspectives on Risk”, *Techné* 8:1 (2004); Aven, T., Renn, O. & Rosa, E. A., “On the ontological status of the concept of risk”, *Safety Science* 49:8 (2011), doi:10.1016/j.ssci.2011.04.015; 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., *Society for Risk Analysis Glossary*, 2018, <https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf> [hämtad 2024-03-06]; Aven, T., “Risk assessment and risk management: Review of recent advances on their foundation”, *European Journal of Operational Research* 253:1 (2016), doi:10.1016/j.ejor.2015.12.023.

osäkerhet angående den kausala kopplingen mellan tillgängliggörande av en geodatamängd och de situationer, händelser och skeenden som kan leda till negativa konsekvenser.¹⁵

I MEGS operationaliseras risk som en kombination av hur allvarliga konsekvensernas effekter är och analysobjektets relevans för hotaktörer. En hög risk föreligger följaktligen om i) konsekvenserna av ett tillgängliggörande kan medföra skada på Sveriges säkerhet och ii) analysobjektet är relevant för minst en hotaktör. Genom detta förfarande syftar användning av MEGS till att angripa de två osäkerheter som nämndes ovan.¹⁶

Relevans införs i MEGS som ett alternativ till sannolikhet. För en komplex risk är det ibland inte möjligt att uppskatta hur sannolikt det är att risken realiserar. Begreppet relevans används för att bedöma den omfattning som tillgängliggörandet av geodata bidrar till att realisera konsekvensen. Relevans används för att skapa en bredare förståelse för risker som ett tillgängliggörande kan innebära. Om inte relevansen nyanserar konsekvensen skulle egentligen all geodata kunna innebära konsekvens. Men relevansen innebär att man kan förstå om geodata är relevant för att konsekvensen ska inträffa. Det innebär dock inte att konsekvensen är beroende av att det finns en relevans. Relevansen kan vara låg medans konsekvensen fortfarande är hög. På samma sätt kan relevansen vara hög men konsekvensen låg.¹⁷

Risker för Sveriges säkerhet är nästan uteslutande av antagonistisk karaktär. Därför är det främst antagonistiska risker som är tänkta att identifieras och värderas i MEGS; andra risker som exempelvis naturolyckor beaktas alltså i regel inte. I 2 kap. 1 § öppna datalagen konstateras dessutom att de offentliga aktörerna ska tillgängliggöra data ”i den utsträckning som krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas”. I MEGS bedöms bara risker för Sveriges säkerhet varför varken informationssäkerhet eller skydd av personuppgifter beaktas. Innan riskbedömningen behöver deltagande aktörer informationsklassa och vidta lämpliga dataskyddsåtgärder för att säkerställa informationssäkerhet och skydd av personuppgifter.

Den aktör som genomför riskbedömningarna enligt öppna datalagen är inte nödvändigtvis den som utsätts för risken. Ibland finns den aktör som utsätts för risken utanför organisationen som tillgängliggör geodata. Den som utsätts för risk behöver heller inte vara en avgränsad verksamhet utan kan vara nationalstaten Sverige. Till detta ska läggas möjligheterna att aggregera och ackumulera, det vill säga att kombinera, datamängder för att därigenom erhålla ny information. Aggregering och ackumulering underlättas betydligt genom användning av digitala system. För att kunna bedöma riskerna med att tillgängliggöra en viss geodatamängd behöver de offentliga aktörerna därför analysera hur en geodatamängd kan aggregeras med andra data, och om sådana kombinationer medför att information om säkerhetskänslig verksamhet kan röjas eller innebär andra risker. En riskbedömning med avseende på Sveriges säkerhet kan således inte vara begränsad till enbart den egna verksamheten då aktörens beslut påverkar och påverkas av andra aktörers beslut. Sammantaget antyder dessa komplikationer att aktörernas normala arbete med informationssäkerhet, exempelvis klassning av information, vanligtvis är otillräckligt för att beakta risker för Sveriges säkerhet när geodata tillgängliggörs som öppna data.¹⁸

De avvägningar och komplikationer som har beskrivits ovan medför att riskbedömningen oundvikligen präglas av stora osäkerheter. Det finns olika metoder för att försöka hantera sådana osäkerheter; de flesta baseras på mänskliga bedömningar. Då det i allmänhet saknas tillförlitliga data för att kvantitativt kunna uppskatta risker för Sveriges säkerhet utgår även MEGS från mänskliga bedömningar.¹⁹

MEGS ska uppfattas som en sammanhängande helhet baserat på tidigare forskning och de erfarenheter som har inhämtats under utvecklingen av metoden. Processtödet är skrivet utifrån antagandet att metoden används i sin helhet. Dessutom har många av de steg som ingår i metoden visat sig vara nödvändiga för att överhuvudtaget kunna göra en ändamålsenlig bedömning av de risker som ett tillgängliggörande kan leda till. Trots det ska MEGS inte ses som optimal eller slutgiltig. Snarare ska den betraktas som inledningen på en process där metoden stegvis förfinas så att dess ändamålsenlighet (validitet) och tillförlitlighet (reliabilitet) förbättras baserat på erfarenheter från genomförda riskbedömningar med metoden och framtida forskning. Över tid är det därför möjligt att användare ser ett behov av förändring och utveckling av metoden. Eftersom den kontext i vilken riskbedömningar av geodata utförs är under konstant förändring ska detta ses som en naturlig del av metoden. Det är emellertid

15 Se vidare Davidsson, m.fl. 2025.

16 Se vidare Davidsson, m.fl. 2025.

17 Se vidare Davidsson, m.fl. 2025.

18 Se vidare Davidsson, m.fl. 2025.

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

troligt att centrala moment i metoden behöver bibehållas, och det är viktigt att de förändringar som man inför förankras i dokumenterade empiriska data, erfarenheter eller etablerad vetenskaplig kunskap. Metoden ska därför i sin helhet betraktas som en kontinuerlig lärandeprocess (figur 1). En ambition bör vara 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.

3.3 När ska riskbedömning göras?

En riskbedömning ska göras när en offentlig aktör har för avsikt att tillgängliggöra en viss geodatamängd som öppna data. Myndigheten för digital förvaltning konstaterar exempelvis att återkommande "informationsklassning och riskbedömning ska ligga till grund för beslut om publicering och lämpliga säkerhetsåtgärder under publicerandet".²⁰ När det gäller risker för Sveriges säkerhet är återkommande riskbedömningar nödvändiga då hoten förändras över tid vilket kan leda till nya risker som tidigare inte har beaktats. Dessutom är geodata vanligen inte konstanta utan påverkas av exempelvis förändringar i samhälle och miljö, justeringar i existerande data, ny inhämtning eller uppdatering av attribut innehåll. Det är alltså inte tillräckligt att göra endast en riskbedömning vid det initiala tillgängliggörandet och sedan anta att inget vidare riskarbete behövs. Snarare bör riskbedömningarna ses som en återkommande uppgift så snart relevanta omständigheter förändras. Offentliga aktörer som löpande samlar in nya geodata kan tjäna på att göra en riskbedömning redan innan inhämtningen, speciellt om det innebär att data med högre upplösning eller förändrat informationsinnehåll produceras. Då kan aktörerna på ett tidigt stadium undersöka om dessa geodata kan innebära risker för Sveriges säkerhet.

3.4 Resultatet är beroende av deltagarnas kompetens och samverkan

För att riskbedömningen ska bli så ändamålsenlig och tillförlitlig som möjligt är det viktigt att de deltagare som involveras i processen har relevant kompetens.²¹ Det är särskilt angeläget att deltagarna i den gemensamma bedömningen har goda kunskaper om geodata, rumsliga analyser och GIS för att kunna identifiera och bedöma risker om analysobjektet förekommer som öppna data. Exempelvis är det sällan data i sig som utgör en risk, utan risken kan finnas i resultaten av de rumsliga analyser som geodata tillåter eller aggregering och ackumulering av data. För att kunna identifiera dessa risker behöver deltagarna ha kunskap om vilka rumsliga analyser som kan göras med olika typer av geodata eller hur dessa kan kombineras.

Den gemensamma bedömningen i MEGS genomförs i form av en workshop. Syftet med workshoppen är att underlätta samverkan genom att samla relevanta aktörer med olika bakgrund. Att de offentliga aktörerna samverkar vid riskbedömningar av geodata har flera fördelar. För det första ger det den initierande aktören tillgång till en bredare kompetens och andra aktörer som producerar geodata. Det bör bidra till att deltagarna kan anlägga ett så brett perspektiv som möjligt när risker identifieras, och att grupp tänkande i största möjliga mån undviks.²² För det andra kan samverkan medföra utbyte av erfarenheter när det gäller exempelvis riskbedömningar och konkreta exempel på hot mot säkerhetskänsliga verksamheter, vilket i sin tur leder till kompetensutveckling och ömsesidigt lärande. En fördel med att involvera representanter från flera olika offentliga aktörer i riskbedömningen är de skilda sektorsspecifika kunskaper som dessa besitter. Ju fler olika branscher och beredskapssektorer som är representerade i riskbedömningen, desto fler risker och möjligheter till aggregering beaktas förmodligen i processen. Till skillnad från de individuella bedömningarna underlättar workshopformatet dessutom diskussion mellan de offentliga aktörerna då det finns möjlighet att exempelvis identifiera möjlig aggregering och ackumulering, ställa följdfrågor, ifrågasätta antaganden och efterfråga fördjupade beskrivningar eller förtydliganden av resonemang. Slutligen kan samverkan leda till att offentliga aktörer tar mer konsekventa beslut om att tillgängliggöra, eller inte tillgängliggöra, geodata. Sammantaget leder detta troligen till bättre underbyggda riskbedömningar.

20 Myndigheten för digital förvaltning 2025.

21 Davidsson, m.fl. 2025.

22 Montibeller, G. & von Winterfeldt, D., "Cognitive and Motivational Biases in Decision and Risk Analysis", *Risk Analysis* 35:7 (2015), doi:10.1111/risa.12360; Elna Schirrmeister, E., Göhring, A.-L. & Warnke, P., "Psychological biases and heuristics in the context of foresight and scenario processes", *Futures & Foresight Science* 2:2 (2020), doi:10.1002/ffo2.31.

3.5 Dokumentera löpande

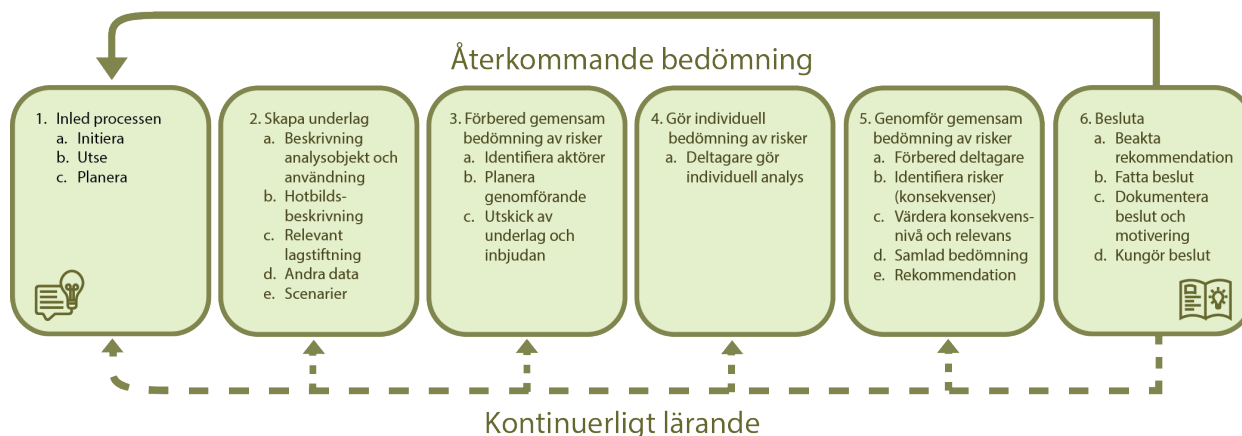
Alla de steg som utgör underlag till det slutliga beslutet ska dokumenteras. För att underlätta en återkommande analys och upprätthålla transparens i processen ska dokumentationen beskriva vad som har gjorts och innehålla motiveringar till de rekommendationer och beslut som tas. Slutsatser, rekommendationer och beslut som framkommer i riskbedömningen behöver dokumenteras och grundligt motiveras utifrån de underlag och analyser som görs under processens gång. Det är särskilt viktigt att också dokumentera eventuellt avvikande åsikter som vidhålls under workshoppen.

3.6 Beakta säkerhetsskydd

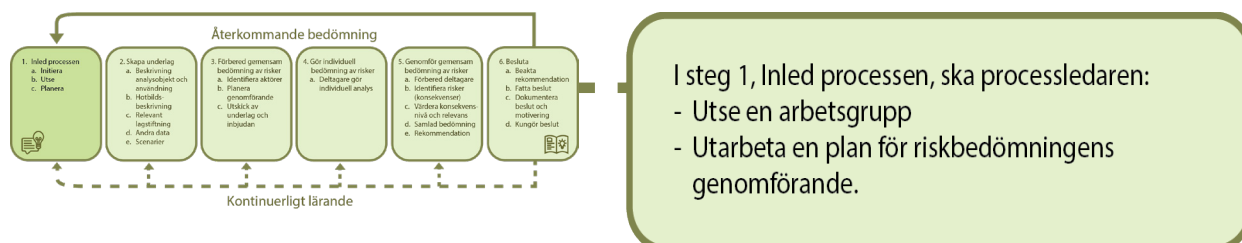
Vid bedömning av risker med geodata är det troligt att säkerhetsskyddsklassificerad eller annan sekretessbelagd information behandlas i processen. Även dokumentationen från riskbedömningen, dess olika steg liksom hotbilsbeskrivningen kan komma att omfattas av sekretess. Säkerhetsskyddet behöver därför löpande beaktas under arbetet med riskbedömningen, och alla som deltar i riskbedömningen behöver vara behöriga att delta i processen. I riskbedömningsprocessen kan därmed säkerhetsskyddsanalyser, relevanta säkerhetsskyddsavtal (när så är nödvändigt), säkerhetsprövning av deltagande personal, hanteringsregler med mera behövas.

4. Beskrivning av MEGS

Det här avsnittet är en steg-för-steg-beskrivning av hur riskbedömningen av geodata ska utföras i praktiken. MEGS består av sex steg som utförs sekventiellt. Varje steg beskrivs utförligt nedan.



4.1 Steg 1: Inled processen



När den initierande aktören avser att tillgängliggöra en viss geodatamängd som öppna data eller av annat skäl anser att en riskbedömning krävs, ska processledaren hos denna aktör inleda riskbedömningsprocessen. Då arbetet med att genomföra en riskbedömning är omfattande kan det vara nödvändigt att utse en arbetsgrupp som får arbeta med olika delar av processen, som att sammanställa information om andra geodatamängder, göra en utförlig beskrivning av analysobjektet med dess användning eller förbereda workshoppen. Processledaren har det primära ansvaret för riskbedömningens genomförande varför det är lämpligt att denne leder arbetsgruppen.

I det inledande arbetet ska en plan för riskbedömningens genomförande utarbetas. Förutom en tidsplan inbegriper detta även att tilldela medlemmar i arbetsgruppen uppgifter och tidsramar.

4.2 Steg 2: Skapa underlag



I steg 2, Skapa underlag, bör följande underlag sammanställas inför fortsatt arbete:

- En ändamålsenlig beskrivning av analysobjektet i analyserat format och en nyttjandeanalys (4.2.1).
- En aktuell hotbildsbeskrivning om hotbildaaktörer och ny teknik (4.2.2).
- En sammanställning av relevant lagstiftning som har betydelse för riskbedömningen (4.2.3).
- En sammanfattning av andra öppna och kommersiella geodatamängder (4.2.4).
- Ett antal relevanta och aktuella scenarier för användning i steg 5 (4.2.5).

För att kunna genomföra riskbedömningen krävs betydande förberedelser såsom beskrivning av analysobjekt, hotbild, lagstiftning, andra datamängder samt utveckling av scenarier. Dessa underlag bör kunna delas med de aktörer som ska delta i den gemensamma bedömningen. Resultatet av underlagsarbetet ska dokumenteras för vidare förmedling till deltagare som medverkar i riskbedömningens senare steg och för att bedömningar i efterhand ska kunna utvärderas. Dessutom kan underlagen användas för att uppdatera eventuellt nationella sammanställningar av hotbildsbeskrivning, beskrivningar av relevant lagstiftning, information om andra geodatamängder och lämpliga scenarier.

4.2.1 Beskriv analysobjekt och hur det används

Eftersom representanter från flera olika aktörer involveras i riskbedömningen är det nödvändigt att noggrant beskriva analysobjektet i analyserat format, exempelvis vad gäller:

- datastruktur
- filformat
- geografisk täckning
- aktualitet
- produktionssätt
- informationsinnehåll
- precision
- upplösning
- attribut
- nuvarande och planerad metod för distribution och tillgängliggörande.

Den sista punkten ovan bör också inkludera en beskrivning av vilken grad av kontroll den initierande aktören för tillfället har på användares tillgång till analysobjektet, exempelvis i form av krav på avgifter, registrering och ID-kontroller samt vilka licenser som används. Denna information behövs för att i senare steg kunna analysera hur tillgängliggörande av analysobjektet som öppna data kan underlätta hotaktörers tillgång till denna geodatamängd. Även om deltagarna i riskbedömningen bör vara kunniga i användningen av geodata, rumsliga analyser och GIS är det lämpligt att ge dem en utförlig beskrivning av hur analysobjektet kan användas. Det kan göras genom att kort presentera exempel på vilka rumsliga analyser som kan utföras med analysobjektet. Det är särskilt viktigt när komplexa produkter ska bedömas, som exempelvis punktmoln från laseravbildning av landskap eller produkter från hyperspektral fjärranalys. Förutom en beskrivning av analysobjektet är det lämpligt att kartlägga hur spritt analysobjektet är i dagsläget och hur det används i samhället. För att utföra denna uppgift kan man utgå från följande frågor:

- Vem/vilka använder analysobjektet idag?
- Vilka är de potentiella negativa konsekvenserna med att inte tillgängliggöra analysobjektet i analyserat format som öppna data?

4.2.2 Beskriv hoten

En uppdaterad och relevant hotbilda-beskrivning är viktig för att kunna bedöma vilka risker tillgängliggörande av en viss geodatamängd kan medföra. Hotbilda-beskrivningen bör bestå av två delar, dels en beskrivning av relevanta hotaktörer som bör beaktas i riskbedömningen, dels en genomgång av ny teknik som kan ha betydelse för att kunna bedöma risker.

4.2.2.1 Hotaktörer

Det finns ett flertal tänkbara hotaktörer som kan hota Sveriges säkerhet. I sina årsrapporter behandlar Säkerhetspolisen (Säpo) och den Militära underrättelse- och säkerhetstjänsten (Must) de aktörer som anses utgöra de allvarligaste hoten; dessa kan användas som utgångspunkt för att identifiera vilka antagonister som kan tänkas nyttja analysobjektet. För varje identifierad hotaktör kan nedanstående frågor beaktas i hotbilda-beskrivningen:

- Hur ser hotaktörens världsbild ut?
- Vilka är hotaktörens motiv?
- Vilka är hotaktörens mål?
- Vilka behov har hotaktören för att nå sina mål?
- Vilka tillvägagångssätt använder sig hotaktören av för att nå sina mål? Hur har aktörens beteende förändrats sedan senaste hotbilda-beskrivningen?
- Vilka är hotaktörens prioriterade angrepps-/påverkansmål? Det vill säga vilka befattningshavare, organisationer, befolkningsgrupper eller andra angrepps-/påverkansmål brukar aktören fokusera på?
- Vilken är hotaktörens förmåga (resurser, kunskap och färdigheter)?

Även om expertisen inom området antagonistiska hot kan sakna adekvata svar på alla dessa frågor bör de i möjligaste mån, och utifrån dagens kunskapsläge, besvaras för att underlätta riskbedömningen.

4.2.2.2 Ny teknik

Teknikutvecklingen är snabb, och många nya teknologier har direkt påverkan på såväl hotbild som riskbedömningar. Exempelvis har utveckling inom artificiell intelligens lett till att det idag går att utföra automatiserad igenkänning av mönster eller avvikelser i data, automatiserad identifiering av intressanta platser och objekt samt att identifiera retuscherade områden.²³ Ett annat exempel är data mining som gör det möjligt att hantera stora datamängder för att hitta mönster och trender. För närvarande utvecklas även obemannade plattformar som utan mänsklig styrning kan använda geodata för navigering.²⁴ Den tekniska utvecklingen ökar potentiellt olika hotaktörers förmåga att nyttja geodata för informationsinhämtning och planering, och öppna nya möjligheter att utföra underrättelseinhämtning och sabotage på avstånd. Därför bör hotbilda-beskrivningen behandla ny teknik som har betydelse för produktion, behandling och användning av geodata och som kan nyttjas av hotaktörer eller som på annat sätt påverkar riskbedömningen. Förutom att illustrera hur ny teknik kan använda geodata, bör denna kartläggning även inkludera information om teknik som tillåter hotaktören att själv samla in data som motsvarar analysobjektet eller som för antagonisten på ett positivt sätt kan komplettera analysobjektet. Idealt bör hotbilda-beskrivningen innehålla en kort beskrivning av tekniken och på vilket sätt den kan påverka risker vid tillgängliggörande av geodata.

23 Zhang, J., Pan, B., Zhang, Y., Liu, Z. & Zheng, X., "Building Change Detection in Remote Sensing Images Based on Dual Multi-Scale Attention", *Remote Sensing* 14:21 (2022), doi:10.3390/rs14215405; Zhang, G., Lu, S. & Zhang, W., "CAD-Net: A Context-Aware Detection Network for Objects in Remote Sensing Imagery", *IEEE Transactions on Geoscience and Remote Sensing* 57:12 (2019), doi:10.1109/TGRS.2019.2930982; Horváth, J., Baireddy, S., Hao, H., Montserrat, D. M. & Delp, E. J., "Manipulation Detection in Satellite Images Using Vision Transformer", , 2021 *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* (2021), doi:10.1109/CVPRW53098.2021.00114; Nie Yuchen, Ding Xiangling, Zhu Wenyi & Zhao Yulin, "A Systematic Review on Detection of Manipulated Satellite Images", 2023 *IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (2023), doi:10.1109/CSCloud-EdgeCom58631.2023.00011

24 Li, J., Qin, H., Wang, J. & Li, J., "OpenStreetMap-Based Autonomous Navigation for the Four Wheel-Legged Robot Via 3D-Lidar and CCD Camera", *IEEE Transactions on Industrial Electronics* 69:3 (2022), doi:10.1109/TIE.2021.3070508; Włodarczyk-Sielicka, M., Polap, D., Prokop, K., Polap, K. & Stateczny, A., "Spatial Visualization Based on Geodata Fusion Using an Autonomous Unmanned Vessel", *Remote Sensing* 15:7 (2023), doi:10.3390/rs15071763

4.2.3 Sammanfatta relevant lagstiftning

För att alla deltagare ska vara medvetna om den lagstiftning som påverkar tillgängliggörande av öppna data och riskbedömningen bör gällande författningar sammanställas. Lagstiftningen är under ständig förändring varför det är särskilt viktigt att upplysa de som deltar i riskbedömningen om eventuellt nya författningar eller justeringar i redan gällande författningar.

4.2.4 Sammanställ information om andra geodatamängder

För att kunna bedöma vilka risker tillgängliggörande av analysobjektet kan leda till är det viktigt att veta vilka andra data som redan finns eller som inom kort kommer att finnas tillgängliga. Det är exempelvis svårt att analysera aggregeringsproblematiken utan att ha en uppfattning om vilka andra datamängder som analysobjektet kan kombineras med. Dessutom kan det vara relevant att kartlägga om det finns några alternativa öppna eller kommersiella data som motsvarar analysobjektet när det gäller exempelvis täckningsgrad, aktualitet, precision och upplösning.

4.2.5 Skapa scenarier

Med hjälp av scenarier kan man skapa en gemensam föreställning om omvärlden eller en kontext för en händelseutveckling. Att ha gemensamma föreställningar om omvärlden och dess aktörer är ett sätt att underlätta för en grupp människor att föra en relevant diskussion. Scenarier kan bidra till att skapa stämning bland mottagarna.²⁵ Scenarier används ofta som ett första steg för att beslutsfattare ska kunna utforma strategier och åtgärder.²⁶ Det finns olika former av scenarier. De kan vara explorativa som beskriver en oviss framtid. De kan vara prediktiva scenarier som exempelvis prognoser, eller normativa scenarier där man ger en bild av en önskad framtid. I den riskbedömning som det här är fråga om är scenarierna av explorativ karaktär. Att använda scenarier är ett sätt att ställa deltagarna i riskbedömningen inför dittills okända eller obeaktade hot eller alternativa framtidsbilder.²⁷

För att kunna använda scenarier behöver lämpliga sådana samlas in eller utvecklas i underlagsarbetet. Scenarier är alltså, om de konstrueras på lämpligt sätt, användbara verktyg för att utforska möjliga risker som kan uppstå när analysobjektet tillgängliggörs som öppna data. För att det ska vara möjligt bör deltagarna ta del av och analysera flera olika scenarier som spänner upp ett så stort utfallsrum som möjligt. Enligt tidigare forskning på området bör antalet scenarier vara tre till fem.²⁸ Med ett stort utfallsrum menas att scenarierna bland annat utgår från olika hotaktörer och motiv; beskriver skilda typer av situationer, händelser eller skeenden; förutsätter eller beskriver användning av olika typer av utrustning och tillvägagångssätt samt representerar olika typer av verksamheter och påverkans- eller angreppsmål. För att scenarierna ska vara relevanta är det dessutom en fördel om de är konstruerade så att de förutsätter eller öppnar för användning av geodata i någon del av det beskrivna händelseförloppet. Scenarier bör vara såväl trovärdiga och realistiska som logiskt konsistenta men de ska inte förmedla en bild av en värld alltför lik den nuvarande och därigenom bekräfta deltagarnas förutfattade åsikter och övertygelser. Scenarierna ska på ett övertygande sätt illustrera en värld som är tillräckligt lik den nuvarande för att vara realistisk samtidigt som de ska vidga deltagarnas medvetande för till synes osannolika, men likväl trovärdiga och möjliga, situationer, händelser och skeenden.²⁹

Ett sätt att sträva efter logisk konsistens, realism och trovärdighet när scenarier skapas är att olika aktörers handlingar framstår som såväl realistiska som logiska utifrån aktörernas mål och motiv. Som exempel kan scenariokonstruktörerna utgå från hotaktörernas världsbild och motiv enligt hotbildsbeskrivningen. Beskrivningen av hur andra aktörer – som politiker, myndigheter, företag, media och allmänhet – beter sig och handlar ska också vara logiskt konsistent utifrån dessa aktörers normala beteende och bevekelsegrunder. För att kunna utveckla scenarier som utmanar gängse föreställningar samtidigt som de framstår som rimliga och realistiska behöver scenariokonstruktörerna bemöda sig om att, så gott det går, medvetandegöra sig om och utmana sina egna övertygelser, förutfattade meningar och fördomar.

25 Bennessved, P & Olsson, M., (2023) *Centrala begrepp och metoder inom scenariometodiken*. FOI Memo 8178. Totalförsvarets forskningsinstitut, Stockholm, Sverige.

26 Jonsson, D., (2017) *Att använda scenarier i planering för civilt försvar*. FOI-R--4434--SE. Totalförsvarets forskningsinstitut, Stockholm, Sverige.

27 Schoemaker, P. J. H., "Scenario Planning: A Tool for Strategic Thinking", *MIT Sloan Management Review* vol. 36 (1995); Riel Miller, "Futures literacy: A hybrid strategic scenario method", *Futures* 39:4 (2007), doi:10.1016/j.futures.2006.12.001

28 Amer, M., Daim, T. U., & Jetter, A., A review of scenario planning., *Futures*, 46, 23–40. <https://doi.org/10.1016/j.futures.2012.10.003>

29 Schoemaker 1995; Miller 2007.

God praxis är att explicit formulera och teckna ned sina nuvarande antaganden om centrala trender, aktörer och variabler – exempelvis om politiska, ekonomiska och sociala förhållanden i världen och Sverige, hotaktörer eller möjliga tillvägagångssätt – för att sedan kritiskt ifrågasätta dem.³⁰

4.3 Steg 3: Förbered gemensam bedömning av risker



Huvuddelen av riskbedömningen genomförs under en workshop. För att den ska bli ändamålsenlig och fungera smidigt krävs dock förberedelser. Bland förberedelserna ingår att identifiera och bjuda in lämpliga deltagare planera workshoppens genomförande och skicka ut underlag.

I steg 3, Förbered gemensam bedömning av risker bör ingå följande arbete:

- Identifiera potentiellt deltagande aktörer (4.3.1). Eftersträva att aktörer inom så många olika beredskapssektorer som möjligt deltar i workshopen för att få bredast möjliga perspektiv.
- Planera för genomförande av workshop (4.3.2).
- Skicka ut inbjudan till potentiellt deltagande aktörer (4.3.3).
- Skicka ut underlag från steg 2 till de deltagare som har svarat att de tänker delta på workshopen (4.3.4).

4.3.1 Identifiera deltagande aktörer

Vanligtvis bör alla offentliga aktörer som producerar geodata bjudas in till workshopen. Även om det i normalfallet inte är praktiskt möjligt eller troligt att alla har möjlighet att delta bör initierande aktör bemöda sig om att inkludera flera olika offentliga aktörer i riskbedömningen. Den initierande aktören bör åtminstone i största möjliga mån garantera att aktörer inom så många olika beredskapssektorer som möjligt deltar i workshopen för att få bredast möjliga perspektiv.

4.3.2 Planera för genomförande av workshop

Workshopen behöver förberedas genom att bland annat bestämma tid och plats, utarbeta agenda och tidsplan samt ordna praktiska arrangemang som förtäring och pauser. Eftersom säkerhetsskyddsklassificerad information kan behandlas under workshopen bör platsen vara anpassad för detta, exempelvis genom att genomföra den i avlyssningsskyddade utrymmen.³¹

Dessutom behöver de roller som är nödvändiga för workshoppens genomförande tillsättas. De funktioner som vanligtvis behöver skötas under en workshop är facilitering, dokumentation och hantering av praktiska arrangemang som mat och dryck samt tidtagning. Man kan räkna med att det behövs åtminstone en person per sådan funktion under workshopen. Om man tänker genomföra delar av workshopen i smågrupper är det en fördel att vara flera facilitatorer för att säkerställa att alla gruppers arbete är produktivt. Tänk också på att om säkerhetsskyddsklassificerad information kommer att behandlas behöver detta förberedas i god tid genom att säkerställa att närvarande personer är säkerhetsprövade och att eventuella säkerhetsskyddsavtal finns på plats i tid för workshopen.

I förberedelserna bör även ingå att ta fram en plan för hur resultaten från workshopen ska hanteras. Planen behöver bland annat beskriva hur deltagarnas åsikter, idéer, resonemang och argument ska samlas in och dokumenteras. Därtill behöver den beskriva om initierande aktör ska genomföra en enkät i slutet av workshopen, och vad enkäten i så fall har för syfte och utformning.

30 Schirrmeyer, Göhring & Warnke 2020.

31 Säkerhetspolisen, *Vägledning i säkerhetsskydd. Avlyssningsskyddade utrymmen* (2023a).

4.3.3 Skicka ut underlag och inbjudan

När underlagsarbetet är utfört och det finns en preliminär plan för workshoppen ska en inbjudan skickas till tilltänkta deltagande aktörer. De aktörer som accepterar inbjudan att delta i workshoppen bör i god tid få tillgång till underlagen – det vill säga beskrivning av analysobjekt och dess användning, en hotbildsbeskrivning, scenarier samt sammanställningar av relevant lagstiftning och andra geodatamängder – och analysobjektet för att kunna göra en individuell förberedande analys. Underlagen kan även innehålla information om tankefallor (se kapitel 5) som är vanligt förekommande vid riskbedömningar och hur dessa kan bemötas.

4.4 Steg 4: Gör individuell bedömning av risker



I steg 4, Gör individuell bedömning av risker:

- Respektive deltagare ska innan workshoppen göra en separat bedömning. Förutom egen kunskap bör deltagarna ta stöd av dokumentationsmall och underlagen från steg 2 (4.4).

För att den gemensamma bedömningen ska bli framgångsrik och effektiv behöver deltagarna förbereda sig. Den individuella bedömningen syftar till att alla deltagare ska vara väl förberedda inför workshoppen, att de bekantar sig med analysobjektet och gör en preliminär analys av vilka risker ett tillgängliggörande kan leda till, med särskilt beaktande av aggregeringsproblematiken. Innan workshoppen bör varje deltagare därför studera dokumentation av analysobjektet, nyttjandeanalysen och hotbildsbeskrivningen, skaffa sig en överblick av andra relevanta geodata och läsa igenom föreslagna scenarier. Dessutom bör de bekanta sig med upplägget för workshoppen och studera den dokumentationsmall (se bilaga 1) som används.

Det kan också vara en fördel att redan under detta steg börja identifiera risker som kan uppstå om analysobjektet tillgängliggörs som öppna data. Genom att i lugn och ro studera analysobjektet, andra tillgängliga data, hotbildsbeskrivningen och scenarier kan deltagarna börja notera möjliga risker i dokumentationsmallen (bilaga 1) och beskriva vilka konsekvenser som kan uppstå.

4.5 Steg 5: Genomför gemensam bedömning av risker



I steg 5, Genomför gemensam bedömning av risker finns fyra moment:

- Identifiering av vilka potentiella risker som kan finnas om analysobjektet tillgängliggörs som öppna data och vilka konsekvenserna kan bli om dessa risker realiserar.
- Uppskattning av konsekvensernas allvarlighetsgrad och analysobjektets relevans för riskerna.
- Samlad bedömning av riskerna.
- Rekommendation till den initierande aktören om lämpligheten i att tillgängliggöra analysobjektet som öppna data.

Den gemensamma bedömningen genomförs i form av en workshop som består av fyra moment. Målet med workshoppen är att nå en gemensam bedömning av om (i) analysobjektet kan tillgängliggöras som öppna data i analyserat format, (ii) om åtgärder bör vidtas innan analysobjektet tillgängliggörs som öppna data, (iii) om analysobjektet är olämpligt att tillgängliggöra som öppna data men kan tillgängliggöras på annat vis eller (iv) om analysobjektet över huvud taget inte bör tillgängliggöras. Detta ska göras för varje hotaktor.

4.5.1 Förbered deltagare

Workshoppen inleds med standardaktiviteter som presentation av syftet med workshoppen och agendan för dagen samt att deltagarna presenterar sig för varandra.³² Eftersom större delen av arbetet under workshoppen utförs i mindre grupper behöver deltagarna delas in i grupper av lämplig storlek (4–5 personer per grupp brukar vara lagom) och sammansättning. Det är en fördel om varje grupp består av deltagare från olika offentliga aktörer och med skilda bakgrunder. Arbetets kvalitet kommer troligen att öka, och eventuella missuppfattningar och snedvridningar/bias minskas, om varje grupp har löpande tillgång till en facilitator. Denne kan driva på gruppens arbete genom att exempelvis ställa öppna frågor när gruppen har kört fast eller hjälpa gruppen att komma vidare när dess medlemmar fokuserar för mycket på detaljer eller ovidkommande faktorer.³³

Även om deltagarna ska ha fått nödvändig information via underlagen som den initierande aktören har skickat ut i steg 3 kan det ibland vara en fördel med ett fåtal korta inledande presentationer av relevant information. Exempelvis kan förevisningar av analysobjektet och exempel på analyser som kan utföras med analysobjektet öka deltagarnas förståelse för vilka risker ett tillgängliggörande kan medföra.

4.5.2 Moment 1: Identifiera risker

Första momentet i workshoppen är att identifiera möjliga händelser och skeenden samt konsekvenser av dessa, som ett tillgängliggörande av analysobjektet kan leda till. Detta arbete utförs med fördel i mindre grupper där varje grupp ska identifiera potentiella risker och konsekvenser. De individuella bedömningarna har förhoppningsvis resulterat i konkreta förslag på risker som man kan utgå ifrån under workshoppen genom att deltagarna presenterar dessa för varandra i smågrupper och sedan försöker identifiera andra risker. Man kan även inleda med att deltagarna tillsammans försöker identifiera risker genom att använda de tillvägagångssätt som beskrivs nedan.

Det går att identifiera risker på olika sätt, exempelvis genom att i) utgå från en obestämd eller generisk hotaktör, ii) utgå från de hotaktörer som identifierats i hotbildsbeskrivningen eller iii) använda scenarier. De tre tillvägagångssätten presenteras här nedan i ordning av ökande grad av detaljrikedom. Beroende på detaljrikedom ställs olika stora krav på deltagarnas kreativitet för att identifiera risker. Exempelvis kräver riskidentifiering utifrån obestämd hotaktör vanligtvis större påhittighet från deltagarnas sida än användning av scenarier. Ett tillvägagångssätt med högre detaljrikedom kan däremot vara alltför styrande så att deltagarna endast beaktar den information som ges i uppgiften istället för att använda sin kreativitet eller utgå från egna erfarenheter. Samtidigt kan en högre grad av detaljrikedom medföra att de konsekvenser som identifieras av deltagarna blir konkretare än vid användning av tillvägagångssätt med lägre detaljrikedom. Tillvägagångssätten kräver dessutom olika mycket förberedelser från den initierande aktörens sida. Att utveckla lämpliga scenarier eller anpassa redan existerande scenarier medför en större arbetsinsats från den initierande aktörens sida än att låta deltagarna utgå från en obestämd hotaktör. De olika tillvägagångssätten medför alltså olika för- och nackdelar som processledaren bör vara medveten om när workshoppen förbereds och genomförs.

Beroende på vilka tillvägagångssätt som används, identifieras troligen olika risker, varför det är en fördel att kombinera flera olika tillvägagångssätt under en och samma workshop. Tillvägagångssätten kan nyttjas sekventiellt så att deltagarna först använder ett sätt och när facilitatorn anser att man har uttömt dess potential byter gruppen till nästa sätt. En annan ansats är att låta grupperna använda olika tillvägagångssätt parallellt. Det kan ske genom att de fördelas mellan grupperna så att varje enskild grupp endast använder ett tillvägagångssätt samtidigt som facilitatorn garanterar att alla sätt kommer till användning i åtminstone en grupp. När grupparbetena är färdiga får varje grupp presentera vilka tillvägagångssätt de har använt och vilka risker som har identifierats för övriga deltagare. Därmed går det att nyttja fördelarna med alla tillvägagångssätten men sannolikt med något mindre tidsåtgång än om alla grupper använder flera sätt sekventiellt.

De olika för- och nackdelarna som orsakas av graden av detaljrikedom har även betydelse för i vilken ordning tillvägagångssätten bör användas om man använder dem sekventiellt i workshoppen. Exempelvis kan psykologiska mekanismer som förankring och tillgänglighetsbias³⁴ påverka deltagarnas kreativitet i högre utsträckning vid användning av scenarier än när andra metoder används. Det kan därför vara en fördel att inleda med metoder med lägre detaljrikedom för att sedan övergå till mer detaljerade tillvägagångssätt. Detta måste också observeras om flera

32 Se t.ex. Eliasson, M. & Villför Larsson, P., *Sätt fart på arbetsmötet. En handbok i facilitering*, 3 utg. Meetings International Publishing AB, Ystad (2017); Mattsson, E. & Jöborn, A., *Möteskokboken*, 2 utg. Ordrum AB, Göteborg (2017).

33 Montibeller & von Winterfeldt 2015; Schirmeister, Göhring & Warnke 2020.

34 Montibeller & von Winterfeldt 2015.

arbetssätt används parallellt. Deltagarna som då ska arbeta utifrån en generisk hotaktör kommer att bli påverkade i sin bedömning om de redan har tagit del av andra deltagares identifierade konsekvenser. När identifieringen i grupper är klar ska varje grupp presentera de risker och konsekvenser som har identifierats för övriga grupper så att alla deltagare kan utgå från samtliga identifierade risker i moment 2, värdera risker.

4.5.2.1 Riskidentifiering utifrån obestämd hotaktör

Den metod som troligen kräver minst förberedelser är att låta deltagarna utgå från en icke-identifierad, obestämd hotaktör. I ett första steg innebär det att deltagarna behöver 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. Denna uppgift bör i ett inledande skede präglas av kreativitet, exempelvis genom att deltagarna enskilt skriver ned alla tänkbara situationer, händelser och skeenden för att grupperna sedan ska ha ett så stort urval som möjligt att välja från. Uppgiften till deltagarna kan alltså sägas vara:

- Identifiera vad en hotaktör skulle kunna göra med tillgång till analysobjektet i analyserat format.

På detta stadium i processen får ingen kritik eller ifrågasättande förekomma då det vanligen hämmar kreativiteten varför denna inledande uppgift med fördel utförs enskilt. Självklart kan deltagarna utgå från de risker som de har identifierat i de individuella bedömningarna innan workshopen. När deltagarna inte lyckas identifiera fler potentiella risker kan man inom grupperna börja diskutera förslagen. Till en början bör gruppen fokusera på att – om så behövs – föreslå justeringar, förändringar eller utvidgningar som kan göra de identifierade situationerna, händelserna eller skeendena mer realistiska. Uppgiften är alltså att med utgångspunkt i de inledande enskilda förslagen utarbeta så många relevanta exempel på risker som möjligt. Här är det ofta värdefullt att grupperna har tillgång till en facilitator som kan utmana, ställa frågor och sporra gruppen. När gruppen har enats om en uppsättning potentiella risker är det dags att identifiera vilka konsekvenser de kan leda till. För detta kan deltagarna exempelvis diskutera följande frågor:

1. Vilka direkta och indirekta negativa konsekvenser för Sveriges säkerhet kan de identifierade situationerna, händelserna eller skeendena leda till? Beakta exempelvis personella, materiella, politiska, sociala, informationsmässiga, ekonomiska, miljömässiga och kognitiva effekter som kan ha påverkan på Sveriges säkerhet?
2. I vilken utsträckning kan information om säkerhetskänslig verksamhet röjas om analysobjektet tillgängliggörs som öppna data?
3. I vilken utsträckning kan en hotaktör genom aggregering, ackumulering eller annan bearbetning av analysobjektet erhålla information som kan skada Sveriges säkerhet?

Deltagarna bör eftersträva att vara så konkreta som möjligt och i detalj beskriva de konsekvenser som kan bli resultatet av ett tillgängliggörande av analysobjektet som öppna data. Återigen kan resultat från de individuella bedömningarna innan workshopen vara användbara.

4.5.2.2 Riskidentifiering utifrån hotaktörer i hotbilsbeskrivning

Ett annat tillvägagångssätt är att utgå från de olika hotaktörer som har identifierats i underlagsarbetet och utifrån deras världsbild, motiv och mål undersöka hur analysobjektet skulle kunna användas. Detta tillvägagångssätt har många likheter med föregående tillvägagångssätt men deltagarna har här hjälp av informationen i hotbilsbeskrivningen för att identifiera risker. Exempelvis kan de utforska hur analysobjektet kan underlätta för de olika identifierade hotaktörerna att nå sina mål.

Liksom när deltagarna utgår från en obestämd hotaktör bör det inledande skedet präglas av kreativitet, exempelvis genom att deltagarna enskilt antecknar alla möjliga situationer, händelser eller skeenden som kan uppstå om hotaktörerna får tillgång till analysobjektet. Om de har lämpliga exempel kan deltagarna utgå från de risker som de har identifierat i de individuella bedömningarna innan workshopen.

Deltagarna kan uppmanas att göra följande uppgift:

- Identifiera vad varje identifierad hotaktör skulle kunna göra med tillgång till analysobjektet i analyserat format.

Dessutom kan följande frågor underlätta vid identifiering av möjliga risker:

1. Vilka av hotaktörens mål kan underlättas med tillgång till analysobjektet?
2. Hur kan analysobjektet bidra till att hotaktören når sina mål?

Liksom när man utgår från obestämd hotaktör får på detta stadium i processen varken kritik eller ifrågasättande förekomma för att inte hämma kreativiteten. När deltagarna inte lyckas identifiera fler potentiella risker kan grupperna inbördes börja diskutera förslagen. Även här bör grupperna fokusera på konstruktiv utveckling och föreslå förändringar som kan göra de identifierade situationerna, händelserna eller skeendena mer realistiska och relevanta. När gruppen har enats om en uppsättning potentiella risker är det dags att identifiera vilka konsekvenser de kan leda till. För detta kan deltagarna exempelvis diskutera följande frågor:

1. Vilka kan konsekvenserna bli om hotaktören når sina mål?
2. Om gruppen har identifierat konkreta situationer, händelser eller skeenden, vilka direkta och indirekta negativa konsekvenser för Sveriges säkerhet kan de leda till? Beakta exempelvis personella, materiella, politiska, sociala, informationsmässiga, ekonomiska, miljömässiga och kognitiva effekter som kan ha påverkan på Sveriges säkerhet.
3. I vilken utsträckning kan information om säkerhetskänslig verksamhet röjas om analysobjektet tillgängliggörs som öppna data?
4. I vilken utsträckning kan en hotaktör genom aggregering, ackumulering eller annan bearbetning av analysobjektet erhålla information som kan skada Sveriges säkerhet?

Precis som när man utgår från en obestämd hotaktör bör deltagarna eftersträva att vara så konkreta som möjligt och i detalj beskriva konsekvenserna. Det är även viktigt att så många hotaktörer som möjligt beaktas i analysen då olika hotaktörer kan ha olika behov, resurser, motiv och mål. Exempelvis kan ett visst analysobjekt vara ointressant för en statlig underrättelsetjänst men mycket relevant och eftertraktat för en inhemsk extremistisk organisation.

4.5.2.3 Använda scenarier

Ovan beskrivs vad ett scenario är och vad man bör tänka på när man tar fram scenarier. Om scenarier ska användas i den gemensamma riskbedömningen vid workshop bör man betrakta dem som ett medel för att utforska det möjliga snarare än det sannolika.³⁵ De är därmed verktyg för att sporra deltagarnas kreativitet och utgör utgångspunkter för diskussionen. För facilitatorn är det, enligt våra erfarenheter av genomförda workshoppar, viktigt att bemöda sig om att deltagarna inte bara betraktar de använda scenarierna som en slutprodukt som så snabbt som möjligt ska klaras av – exempelvis genom en hastig utvärdering som mynnar ut i ett konstaterande att scenariot är orealistiskt – för att sedan gå vidare till nästa moment i arbetet. Istället är scenarierna det första steget i en process som ska leda fram till att gruppen kan svara på frågor som exempelvis:

1. Vilka direkta och indirekta negativa konsekvenser för Sveriges säkerhet kan de situationer, händelser eller skeenden som illustreras i scenarierna leda till? Beakta exempelvis personella, materiella, politiska, sociala, informationsmässiga, ekonomiska, miljömässiga och kognitiva effekter som kan ha påverkan på Sveriges säkerhet.
2. Innebär den situation, händelse eller skeende som beskrivs i scenariot en risk för Sveriges säkerhet? Om inte, kan man tänka sig liknande eller närliggande situationer, händelser eller skeenden (dvs. ett nytt scenario) som medför exempel på risk för Sveriges säkerhet? I så fall, vad krävs, det vill säga vilka villkor ska vara uppfyllda, för att det ska utgöra risk för Sveriges säkerhet? Vilka direkta och indirekta konsekvenser kan dessa situationer, händelser eller skeenden leda till?

³⁵ Schoemaker 1995; Miller 2007; Piirainen, K. A., Gonzalez, R. A. & Bragge, J., "A systemic evaluation framework for futures research", *Futures* 44:5 (2012), doi:10.1016/j.futures.2012.03.008

3. Är analysobjektet en viktig eller nödvändig komponent för att hotaktören ska kunna uppnå sina mål i scenariot (både det ursprungliga scenariot och de nya scenarier som blir resultatet av föregående punkt)? Om analysobjektet inte är en nödvändig komponent, finns det liknande situationer, händelser eller skeenden där analysobjektet är en förutsättning för hotaktören att uppnå sina mål? Om analysobjektet underlättar, snarare än är en förutsättning för, hotaktören att nå sina mål, hur mycket "underlättande" krävs för att det ska medföra en risk för Sveriges säkerhet?
4. Om det finns en utpekad hotaktör i scenariot, hur skulle risken förändras om det var en annan hotaktör? Utvärdera hur risken för Sveriges säkerhet förändras beroende på vilken av de hotaktörer som pekas ut i hotbilsbeskrivningen som är antagonist i scenarierna.

Det ligger ett stort ansvar på såväl facilitatorer som deltagare att säkerställa att grupperna arbetar aktivt med scenarierna för att i så hög grad som möjligt utforska utfallsrummet och därmed eventuella risker som tillgängliggörande av analysobjektet som öppna data kan leda till. Facilitatorn bör vid behov ställa mot- eller följdfrågor och agera djävulens advokat för att driva gruppen framåt i arbetet.

En del av ovanstående frågor snuddar vid nästa moment, det vill säga värdering, men syftet med frågorna är på detta stadium främst att tvinga deltagarna att identifiera så många potentiella risker som möjligt. Genom att fundera på, och möjligen besvara, frågorna förbereds deltagarna även för moment 2.

4.5.3 Moment 2: Värdera risker

När risker har identifierats är nästa moment i workshopen att värdera dessa risker (figur 1). I moment 2 konkretiseras riskerna genom att de konsekvenser som har identifierats i moment 1 värderas utefter (i) hur allvarlig skada på Sveriges säkerhet de kan leda till samt (ii) hur relevant analysobjektet är för riskernas realiserande.

4.5.3.1 Konsekvensernas allvarlighetsgrad

Utifrån de potentiella risker och konsekvenser som har identifierats i moment 1 ska deltagarna för varje identifierad konsekvens undersöka i vilken grad Sveriges säkerhet kan påverkas. I metoden operationaliseras Sveriges säkerhet genom åtta kriterier som representerar värden som anses viktiga för Sveriges säkerhet och som därmed är skyddsvärda:³⁶

- 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
- samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå.

För varje identifierad konsekvens från moment 1 ska effekten på Sveriges säkerhet bedömas genom att deltagarna får gradera hur mycket varje kriterium påverkas. Fyra nivåer används för att beskriva olika grader av påverkan på kriterierna där *a* indikerar störst påverkan och *d* indikerar att konsekvensen inte leder till någon påverkan. Nivåerna och dess olika kriterier beskrivs i bilaga 2. För att kunna bestämma nivå (bilaga 2) är det följderna av en handling, händelse, skeende, aktivitet eller företeelse som ska beaktas. Om exempelvis endast en kommun drabbas av en händelse kan skadan anses vara lokal. Men det kan inte uteslutas att det också skadar Sveriges säkerhet. Följderna kan nämligen ha nationell betydelse, till exempel om den drabbar personer eller verksamheter som har en nyckelroll i totalförsvaret.

Bedömning av konsekvensernas allvarlighetsgrad kan göras i smågrupper där medlemmarna i varje grupp enas om vilken nivå som är lämplig för varje kriterium (bilaga 2) och konsekvens (tabell 1). Denna uppgift kan emellertid med fördel också göras enskilt där varje deltagare gör en egen uppskattning. De enskilda uppskattningarna vägs sedan samman till en gemensam bedömning, exempelvis genom att omvandla effektnivåerna till numeriska värden och sedan beräkna medelvärdet av alla deltagares uppskattningar.

³⁶ Davidsson, m.fl. 2025.

Notera att kriterierna i bilaga 2 inte bör uppfattas som en tillräcklig eller uttömmande lista som täcker alla aspekter av Sveriges säkerhet utan snarare är preliminära utkast. Därför kan kriterierna omformuleras och kompletteras med fler kriterier när de offentliga aktörerna finner det lämpligt. Det finns fem konsekvensnivåer som beskrivs i tabell 1: *existentiell*, *allvarlig*, *begränsad*, *obetydlig* och *okänd/oklar skada*, där *existentiell skada* innebär den allvarligaste skadan medan *obetydlig skada* innebär att Sveriges säkerhet inte skadas. *Okänd/oklar skada* används i de fall då deltagarna inte anser att något av kriterierna (bilaga 2) är lämpliga eller då de av annan anledning inte kan bestämma konsekvensnivå.

Tabell 1: Konsekvensnivåer för uppskattning av skada på Sveriges säkerhet vid riskbedömningar av geodata vid tillgängliggörande som öppna data.³⁷

Konsekvensnivå ³⁸	Definition/beskrivning
Existentiell skada (a)	Sveriges I) politiska självständighet, II) territoriella suveränitet, eller III) demokratiska statsskick förloras, eller IV) samhällsviktig verksamhet 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 omfattande 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 omfattning, 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 verksamhet 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 säkerhet påverkas eller det är okänt hur Sveriges säkerhet kan påverkas, exempelvis på grund av brist på information.

Det kriterium som anses påverkas i störst omfattning (där *a* innebär störst och *d* minst påverkan) bestämmer vilken den totala konsekvensnivån blir för respektive konsekvens. Om deltagarna exempelvis anser att en konsekvens påverkar den territoriella suveräniteten på nivå *b* medan övriga dimensioner påverkas på lägre nivåer blir den totala konsekvensnivån *b*, det vill säga *allvarlig skada*.

Om inga kriterier verkar relevanta för en viss konsekvens, det vill säga deltagarna har använt konsekvensnivån *okänd/oklar skada*, är det möjligt att de identifierade riskerna inte medför skada på Sveriges säkerhet. Det kan dock även vara så att detta indikerar att de befintliga kriterierna är otillräckliga och att det behövs fler kriterier. Samma situation kan uppstå om deltagarna har graderat alla kriterium för en specifik konsekvens på lägsta nivån (*d*), men av någon anledning tycker att detta känns otillfredsställande eller ologiskt. I dessa fall bör deltagarna diskutera konsekvensen i helgrupp för att avgöra om det behövs nya kriterier eller om alla kan enas om att konsekvensen inte medför skada på Sveriges säkerhet. Om deltagarna anser att det verkligen behövs nya kriterier bör de föreslå sådana inklusive lämpliga nivåer, för att därefter på nytt bestämma konsekvensnivå för konsekvensen i fråga. Notera att bedömningen av konsekvensnivå även för de andra konsekvenserna som har identifierats under workshopen behöver uppdateras när ett nytt kriterium adderas. Det kan nämligen visa sig att konsekvensnivåerna för dessa konsekvenser ändras vid tillförsel av ett nytt kriterium. Ett alternativ till ovanstående förfarande är att använda Säpos konsekvensnivåer.³⁹ Då ska inte kriterierna (bilaga 2) användas eftersom de inte är anpassade efter Säpos konsekvensnivåer.

³⁷ Tabell från Davidsson, Mittermaier, Severin, Söderman, Winterdahl, Ciepielewska & Stjernlöf 2025.

³⁸ Bokstäver inom parentes syftar på den högsta identifierade effektnivån för respektive identifierad konsekvens, se bilaga 2.

³⁹ Säkerhetspolisen, *Vägledning i säkerhetsskydd. Introduktion* (2023c).

4.5.3.2 Är analysobjektet relevant?

I metoden representerar relevans hur viktigt analysobjektet är för konsekvensernas realiserande.⁴⁰ Det går att identifiera situationer, händelser och skeenden som leder till allvarliga konsekvenser för Sveriges säkerhet men där det är betydelselöst om hotaktören i fråga har tillgång till analysobjektet eller inte. I metoden bestäms relevans genom att besvara ett antal frågor där svaren vägs samman till ett samlat mått. Nedan finns förslag på frågor som kan vara lämpliga att använda under workshoppen. Frågorna ger troligen inte en uttömmande bild av analysobjektets relevans för en hotaktör, varför de kan justeras och nya frågor inkluderas efter behov. Det är utifrån de konsekvenser som har identifierats i moment 1 som nedanstående frågor ska besvaras.

Relevans varierar emellertid beroende på hotaktör. När deltagarna besvarar frågorna nedan 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. Exempelvis kan analysobjektet vara relativt oviktigt för en resursstark hotaktör som har tillgång till alternativa datakällor eller metoder för datainhämtning (analysobjektet kan visserligen vara relevant även i detta fall då det kan komplettera eller bekräfta information från de alternativa datakällorna). För en annan hotaktör som saknar dessa alternativ kan emellertid samma analysobjekt vara helt centralt för att hotaktören ska kunna nå sina mål. Hotaktörernas förmåga i stort – det vill säga deras resurser, kunskap och färdigheter – är en annan faktor som kan inverka på hur relevant analysobjektet är då det kan påverka i vilken utsträckning hotaktören kan utnyttja och tillgodogöra sig geodata. Vad som räknas som ”motsvarande information”, eller alternativ, varierar också beroende på vilken hotaktör som betraktas. För vissa antagonister är lokal information tillräckligt för att kunna uppnå sina mål medan andra söker data med nationell täckning.

En faktor som påverkar relevansen är om analysobjektet är användbart för hotaktörerna. För att ett analysobjekt ska anses användbart ska det på något sätt bidra till eller underlätta att hotaktören når sina mål i de konsekvenser som har identifierats. För att beakta denna aspekt av relevansen kan följande frågor besvaras:

1. I vilken utsträckning orsakar eller underlättar analysobjektet i analyserat format hotaktören att nå sina mål (så som de beskrivs i de identifierade konsekvenserna)?
2. Hur betydelsefullt är hotaktörens tillgång till analysobjektet i analyserat format för de identifierade konsekvenserna?
3. I vilken utsträckning är hotaktören beroende av analysobjektet i analyserat format för att kunna planera och genomföra de aktiviteter som identifierats?

Ett alternativ till fråga 3 är: ”I vilken utsträckning kan hotaktören planera och genomföra de aktiviteter som identifierats utan analysobjektet i analyserat format?” Observera dock att svaret på denna fråga innebär omvänd skala – det vill säga svaret ”i hög utsträckning” implicerar en låg relevans till skillnad från fråga 3 där samma svar implicerar hög relevans – vilket gör det mer komplicerat att kombinera svaren på samtliga frågor till en sammanvägd relevans (se beskrivning nedan). Om en hotaktör saknar alternativa informationskällor är naturligtvis relevansen högre än om det finns andra tillgängliga data som motsvarar analysobjektet. För att beakta huruvida analysobjektet kan anses vara unikt för hotaktören, och därmed potentiellt eftersträvänsvärt, kan följande fråga besvaras:

4. I vilken utsträckning saknas andra data som motsvarar analysobjektet (i analyserat format) och som hotaktören skulle kunna använda för att uppnå samma resultat?

Med data som ”motsvarar” analysobjektet avses här sådana data som för hotaktörens syften överensstämmer med analysobjektet med avseende på exempelvis typ av data, täckningsgrad, aktualitet, precision och upplösning. Syftet med fråga 4 är att undersöka om det för hotaktörens syften finns alternativ som denne kan använda istället för analysobjektet. Här kan det vara bra att utgå från nuvarande situation; hur skulle hotaktören gå till väga idag för att åstadkomma de effekter som det identifierade händelseförloppet eller skeendet resulterar i? För att hitta ett svar på denna fråga kan det dessutom underlätta att beakta om det finns andra öppna eller kommersiella data som motsvarar analysobjektet i analyserat format, om hotaktören kan inhämta motsvarande information själv eller via aggregering, ackumulering eller annan bearbetning av öppna eller kommersiella data. Underlagsarbetet i steg 2 inkluderar att ta fram en sammanställning av andra data som kan vara till hjälp när fråga 4 besvaras. När det finns en utpekad hotaktör är det även lämpligt att försöka analysera hur väl denne kan tillgodogöra sig

40 Davidsson, m.fl. 2025.

analysobjektet och de möjligheter som det ger, möjligtvis tillsammans med andra data. Denna aspekt kan beaktas med följande fråga:

5. I vilken utsträckning har hotaktören förmåga (det vill säga resurser, kunskap och färdigheter) att använda analysobjektet för att uppnå sina mål?

För att kunna besvara ovanstående frågor krävs naturligtvis att man i underlagsarbetet har gjort en grundlig dokumentation av relevanta hotaktörer, vilka andra öppna data som finns tillgängliga samt vilken ny teknik och vilka alternativa datamängder som kan användas av en hotaktör (se avsnitt 4.2.2 och 4.2.4).

En annan faktor som påverkar relevansen är hur mycket tillgängliggörande av analysobjektet som öppna data i analyserat format underlättar för hotaktören att nå sina mål. Om ovanstående frågor syftar till att avslöja om analysobjektet alls är användbart, är syftet här alltså främst att beakta hur mycket resurser fri tillgång till analysobjektet kan frigöra för hotaktören eller hur mycket risktagandet kan minskas. Om hotaktören måste ta stora risker eller om det krävs stora resurser för att samla in information som motsvarar analysobjektet är dess relevans rimligtvis högre än i det omvända fallet. För att beakta denna aspekt av relevansen kan följande två frågor besvaras under workshopen:

6. Hur stora tidsmässiga, ekonomiska och personella resurser skulle hotaktören behöva använda för att införskaffa motsvarande data själv om analysobjektet inte finns tillgängligt som öppna data?
7. Hur stora risker skulle hotaktören behöva ta för att införskaffa motsvarande data själv om analysobjektet inte finns tillgängligt som öppna data?

Frågorna implicerar att en hotaktör i de flesta fall kan få åtkomst till data som motsvarar analysobjektet, exempelvis från kommersiella leverantörer eller genom att stjäla motsvarande geodata via cyberintrång, men att detta medför tidsmässiga, ekonomiska och personella kostnader. Dessutom kan alternativa sätt att införskaffa motsvarande data innebära att hotaktören tvingas ta stora risker vilka kan medföra upptäckt eller att angreppsmålet (i det här fallet Sveriges) underrättelsetjänst, kontraspionage eller brottsbekämpande myndigheter får värdefull information om hotaktörens intentioner och verksamhet. Liksom vid uppskattning av konsekvensnivå (avsnitt 4.5.3.1) kan deltagarna besvara frågorna i grupp eller enskilt. Fördelen med att låta deltagarna besvara frågorna enskilt är att initierande aktör kan utnyttja massans vishet vilket vanligtvis leder till mer precisa resultat.⁴¹

Tabell 2: Exempel på omvandling av svar till numeriska värden vid uppskattning av relevans. Notera att det här förutsätts att svaret i mycket hög utsträckning innebär hög relevans.

I mycket hög utsträckning			I mycket låg utsträckning	
☐	☐	☐	☐	☐
↓	↓	↓	↓	↓
4	3	2	1	0

För att få ett samlat värde på relevansen för en specifik konsekvens ska svaren på frågorna kombineras till en samlad uppskattning. Den samlade uppskattningen utgörs av medelvärdet av respektive svars numeriska värde tilldelade enligt tabell 2. Detta medelvärde avrundas till närmsta heltal och omvandlas därefter till en relevansnivå enligt tabell 3.

⁴¹ Kahneman, D., Sibony, O. & Sunstein, C. R., *Noise: A Flaw in Human Judgment* Little Brown & Co, New York (2021).

Tabell 3: Omvandling av det beräknade medelvärde av svar (tabell 2) till uppskattad relevans. Notera att det här, liksom i tabell 2, förutsätts att hög siffra innebär hög relevans medan låg siffra innebär låg relevans.

4	3	2	1	0
↓	↓	↓	↓	↓
Mycket stor relevans	Stor relevans	Inte obetydlig relevans	Liten relevans	Mycket liten relevans

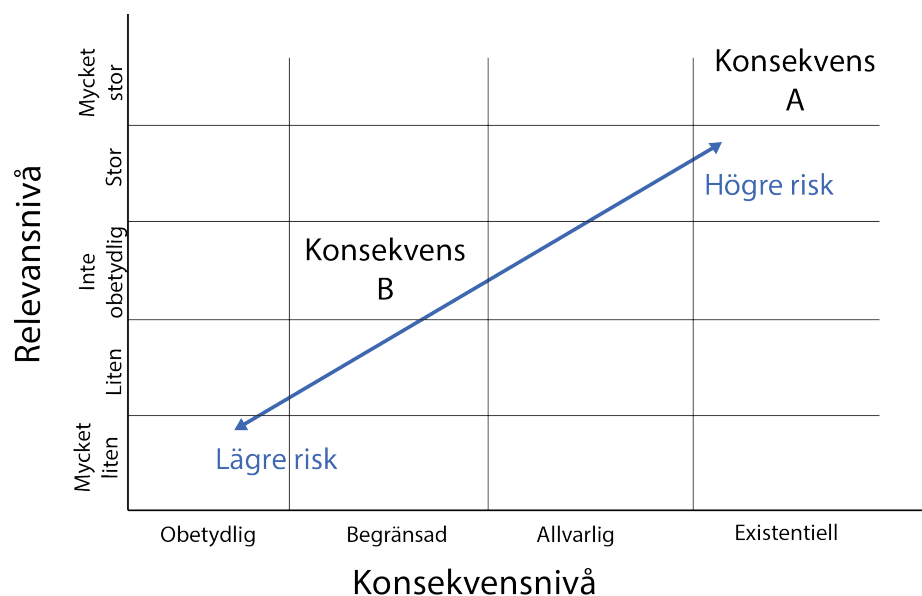
Det är viktigt att vissa aspekter av relevansen inte ges större tyngd i sammanvägningen, exempelvis genom att inkludera flera frågor som egentligen syftar på samma eller liknande aspekter. Därför bör de frågor som deltagarna får svara på med lika vikt reflektera olika aspekter av relevansen. Om deltagarna till exempel ombeds svara på frågorna 1 (analysobjektets användbarhet), 4 (analysobjektets unicitet), 5 (hotaktörens förmåga) och 6 (hotaktörens resursbesparing om analysobjektet förekommer som öppna data) ovan berörs fyra olika aspekter som då kan ges lika vikt vid beräkning av relevansen. Omvänt skulle svar på endast frågorna 1, 2, 3 och 4 resultera i att analysobjektets användbarhet ges högre vikt än dess unicitet samtidigt som andra aspekter (såsom hotaktörens förmåga) inte ges någon vikt alls i den sammanvägda relevansen.

För att deltagarna ska kunna uttrycka nyanser i sina svar bör svarsalternativen för alla frågor ovan vara enligt en bedömningsskala. Svarsalternativen kan exempelvis vara en femgradig skala från *i mycket hög utsträckning* till *i mycket låg utsträckning*, från *mycket betydelsefullt* till *inte alls betydelsefullt* eller från *mycket stora* till *obetydliga* beroende på frågans utformning (se dokumentationsmallen, bilaga 1). Eftersom svaren på frågorna ska kombineras till en samlad uppskattning på relevans betyder det också att frågorna bör utformas på enhetligt sätt så att ett motsvarande svarsalternativ utmed skalan alltid innebär samma nivå av relevans. Exempelvis är frågorna och svarsalternativen i dokumentationsmallen (bilaga 1) utformade så att svaren *i mycket hög utsträckning*/*mycket betydelsefullt*/*mycket stora* alltid innebär hög relevans.

4.5.4 Moment 3: Samlad bedömning

I workshoppens tredje moment görs en samlad bedömning av de risker som har identifierats. Detta åstadkoms genom att varje identifierad konsekvens markeras i en konsekvens-relevansmatris enligt figur 2 utifrån de konsekvens- och relevansnivåer som har bestämts i moment 2. Ju närmare det övre högra hörnet i matrisen en konsekvens markeras, desto större bedöms risken vara. Syftet med matrisen är dels att skapa en överblick av resultatet, dels att snabbt visualisera riskernas allvarlighetsgrad.

Ett exempel på hur det kan se ut visas i figur 2. Syftet med figuren är att visa de relativa bedömningarna av konsekvens och relevans och hur de förhåller sig till varandra. Där utgör konsekvens A en betydande risk då den bedöms kunna medföra existentiell skada på Sveriges säkerhet samtidigt som analysobjektet bedöms ha mycket stor relevans för konsekvensens realiserande. Konsekvens B däremot utgör en lägre risk då den anses medföra endast begränsad skada på Sveriges säkerhet samtidigt som analysobjektet har en inte obetydlig relevans för konsekvensen. Med en uppsättning konsekvenser som i figur 2 representerar konsekvens A alltså den högsta risken eftersom den är närmast det övre högra hörnet i matrisen. Notera också att det utan ytterligare metodutveckling inte går att bestämma en skarp gräns mellan relevansnivåer eller konsekvenser som innebär risk för Sveriges säkerhet och konsekvenser som inte gör det. I nuläget är det därför upp till deltagarna att bestämma var dessa gränser går. Konsekvenser som getts konsekvensnivån *okänd/oklar skada* och för vilka deltagarna inte har lyckats identifiera nya lämpliga kriterier eller på annat sätt enats om hur de ska hanteras i moment 2 ska dokumenteras noga. Om Sāpos konsekvensnivåer har använts i moment 2 behöver matrisen anpassas för att avspegla detta.



Figur 2. Exempel på konsekvens-relevansmatris där två olika konsekvenser har markerats.

4.5.5 Moment 4: Deltagarnas rekommendation

Workshoppen ska utmynna i en rekommendation som baseras på den samlade bedömning som deltagarna har utfört. Rekommendationen ska vara välmotiverad utifrån det arbete som har genomförts och med hänvisning till den dokumentation som har utförts under workshoppen. Det ställs därför stora krav på att centrala resonemang, exempel och annat material som framkommer under workshoppen dokumenteras.

4.5.5.1 Förslag på åtgärder

Innan deltagarna i workshoppen lämnar en rekommendation ska de undersöka om åtgärder bör vidtas innan analysobjektet tillgängliggörs samt vilka åtgärder som kan vara lämpliga. Beroende på typ av data finns flera möjliga åtgärder,⁴² exempelvis att:

- ta bort attribut som anses kunna bidra till riskerna
- generalisera data
- förändra upplösningen
- editera data
- retuschera data
- använda olika åtkomstmetoder för olika varianter av samma typ av geodata (exempelvis begränsad tillgång till data med högre upplösning medan data med lägre upplösning tillgängliggörs som öppna data)
- inte publicera historiska data utan bara data från senaste inhämtningen
- endast tillåta åtkomst till en begränsad yta istället för hela Sverige.

Som exempel har det finska Lantmäteriverket valt att tillgängliggöra data från laserskanning och flygfotografering i en lägre upplösning som öppna data medan mer detaljerade data kräver användningstillstånd.⁴³ Det kan också vara klokt att undvika att tillgängliggöra fritextfält då dessa kan innehålla text som avslöjar känslig information. Det är vanligtvis en fördel att redan vid produktionen och insamling ha kontroll över dataformat och inmatningsmöjligheter för att minska risken för att känslig information publiceras. De olika åtgärderna är olika effektiva då vissa är relativt lätta att kringgå för en motiverad hotaktör medan andra kräver mer ansträngning eller resurser för att motverka.

⁴² Se även Myndigheten för digital förvaltning 2025.

⁴³ Se <https://www.maanmittauslaitos.fi/sv/laserskanning-och-fotograferingsflygningar> [hämtad 2024-11-22].

4.5.5.2 Rekommendation

Baserat på den samlade analysen ska deltagarna på workshopen enas om en rekommendation till den initierande aktören. I praktiken innebär det att föreslå en av ett fåtal möjligheter: i) analysobjektet kan tillgängliggöras som öppna data i analyserat format, ii) analysobjektet kan tillgängliggöras som öppna data först efter att åtgärder vidtagits, iii) analysobjektet kan inte tillgängliggöras som öppna data men kan förmedlas på annat sätt så att den initierande aktören kan kontrollera användningen eller iv) analysobjektet bör inte tillgängliggöras alls. Punkt iv) blir förmodligen främst aktuell om man anser att analysobjektet bör omfattas av sekretess. Initierande aktör har troligen redan genomfört informationsklassning och sekretessbedömning av analysobjektet men under riskbedömningens gång kan ny kunskap uppkomma som föranleder en omvärdering. I sådant fall krävs även en hänvisning till tillämpligt lagrum. Deltagarna kan bestämma vilken rekommendation som är lämpligast genom att beakta nedanstående sekvens av frågor:

1. Kan analysobjektet tillgängliggöras som öppna data i analyserat format?
2. Om nej, finns det lämpliga åtgärder som kan vidtas för att analysobjektet ska kunna tillgängliggöras som öppna data?
3. Om det saknas ändamålsenliga åtgärder för att kunna tillgängliggöra analysobjektet som öppna data, kan analysobjektet tillgängliggöras på annat sätt? I så fall, hur kan analysobjektet tillgängliggöras?
4. Om analysobjektet inte kan tillgängliggöras bör det omfattas av sekretess. Vilket lagrum åberopas i så fall för denna rekommendation?
5. Oavsett svar krävs en tydlig motivering av rekommendationen med hänvisning till de slutsatser som har dragits i arbetet.

Det är utifrån den risk som medför högst konsekvens- och relevansnivå i moment 3 som rekommendationen ska utgå då det är den allvarligaste risken som bestämmer hur analysobjektet bör behandlas. Det är även tillräckligt att deltagarna har identifierat en risk för Sveriges säkerhet för att anse att analysobjektet inte kan tillgängliggöras i analyserat format. Då krävs alltså att man vidtar åtgärder innan analysobjektet tillgängliggörs eller, om riskerna anses alltför stora eller lämpliga åtgärder saknas, att man begränsar tillgången till analysobjektet. Det är naturligtvis möjligt att deltagarna inte kan enas om en rekommendation. Då bör rekommendationen bestämmas genom ett majoritetsförfarande som åtföljs av noggrann dokumentation av eventuella avvikande åsikter med tillhörande argument och resonemang.

4.5.6 Dokumentera resultaten från workshopen

Eftersom spårbarhet och transparens bör prägla riskbedömningsprocessen är det viktigt att resultatet från workshopen dokumenteras noggrant. I synnerhet identifierade konsekvenser, uppskattade konsekvens- och relevansnivåer, rekommendationen och föreslagna åtgärder, centrala resonemang och argument samt avvikande åsikter. Det är särskilt viktigt att rekommendationen, inklusive eventuella åtgärdsförslag, dokumenteras tillsammans med en utförlig motivering till varför denna rekommendation anses mest lämplig. Observera att MEGS inte innehåller en del om att identifiera åtgärder eller värdera dessa åtgärder. Metoden innebär endast att deltagarna kan föreslå åtgärder, men dessa ska inte ses som uttömmande eller enda alternativet.

Riskbedömningen ska även präglas av kontinuerligt lärande, exempelvis genom att metoden löpande uppdateras (figur 1). För att samla in empiriska data till stöd för metodutveckling är det därför fördelaktigt att ytterligare material samlas in. Om exempelvis workshoppens moment 2 görs enskilt är värdena på de enskilda svaren på varje fråga intressanta data för att studera variationen i bedömningarna. För att underlätta detta arbete är det en fördel att låta deltagarna använda standardiserade dokumentationsmallar som samlas in i slutet av workshopen (se bilaga 1). Det kan även vara lämpligt att genomföra en enkät i slutet av workshopen för att samla in data om deltagarnas uppfattning om exempelvis metoden, dokumentationsmallarna samt workshoppens genomförande och resultat. Initierande aktör kan dessutom sammanfatta erfarenheter från delmoment som var särskilt produktiva eller som gav otillfredsställande resultat.

4.6 Steg 6: Besluta



I steg 6, Beslut, ska den initierande aktören:

- Med stöd av rekommendation från workshoppen fatta beslut om analysobjektet ska tillgängliggöras och i så fall hur (4.6.2).
- Besluta, motivera och dokumentera grund till beslut (4.6.3).
- Beslut och, om det inte hindras av säkerhetsskydd eller annan sekretess, motivering kungörs till berörda aktörer (4.6.4).

I det sista steget i riskbedömningen ska den initierande aktören ta ett beslut om huruvida analysobjektet ska tillgängliggöras som öppna data i analyserat format eller om åtgärder behöver vidtas. Dessutom ska beslutet kungöras till övriga offentliga aktörer och dokumenteras på erforderligt vis.

4.6.1 Beakta rekommendation och åtgärder

Initierande aktör ska noga beakta identifierade risker, de konsekvenser som de medför, deltagarnas värdering av riskerna samt de motiveringar och resonemang som deltagarna har framfört under workshoppen. Om inte mycket goda skäl finns bör rekommendationen följas. Rekommendationen från workshoppen kan föreslå att åtgärder krävs innan analysobjektet tillgängliggörs. Då behöver initierande aktör beakta de förslag som finns och anpassa dessa så att identifierade risker elimineras. Initierande aktör kan emellertid vanligen analysobjektet bättre än någon annan och känner förmodligen till användningen väl varför denne är bäst lämpad att i detalj utforma åtgärderna.

När åtgärder utformas bör användningen av geodatamängden beaktas så att aktörer inom samhällsviktig verksamhet som har behov av analysobjektet i tillräcklig utsträckning garanteras tillgång till det så att dessa aktörer fortsatt kan lösa sina uppgifter. Om deltagarna på workshoppen exempelvis har föreslagit att analysobjektet inte ska tillgängliggöras som öppna data kan det ändå finnas skäl för initierande aktör att garantera att vissa särskilt prioriterade aktörer, exempelvis räddningstjänst och Polisen, har tillgång till data när sådana behov finns.

4.6.2 Fatta beslut

När rekommendationen har behandlats och initierande aktör har utformat lämpliga åtgärder kan ett beslut fattas om huruvida analysobjektet kan tillgängliggöras som öppna data eller inte. Notera att ett beslut som innebär att analysobjektet inte tillgängliggörs som öppna data inte hindrar att aktörer som har adekvata behov av det får tillgång till dessa data. Ett beslut att inte tillgängliggöra analysobjektet som öppna data är inte heller detsamma som att analysobjektet omfattas av sekretess. Den initierande aktören kan vidta många olika åtgärder för att säkra att exempelvis aktörer med samhällsviktig verksamhet har tillgång till analysobjektet samtidigt som riskerna för Sveriges säkerhet minimeras.

4.6.3 Dokumentera beslut och motivering

Beslutet tillsammans med motivering och beslutsunderlag ska noga dokumenteras för att kunna utvärderas i efterhand, som stöd i eventuella rättsliga processer och som del i den kontinuerliga lärandeprocess som metoden är avsedd att vara. Dokumentation kan även användas för att vidareutveckla metoden.

4.6.4 Kungör beslutet

När den initierande aktören har tagit ett beslut angående tillgängliggörande av analysobjektet bör detta beslut kungöras till övriga offentliga aktörer. Såvida inte säkerhetsskyddshänsyn hindrar det bör även en motivering förmedlas. Ett kungörande är ett sätt att underlätta ett konsekvent beslutsfattande bland de offentliga aktörerna.

5. Tankefällor och motargument

Under utvecklingsarbetet av den metod som här beskrivs framkom ett antal vanliga missuppfattningar eller tankefällor.⁴⁴ Utmärkande för en tankefälla är att den utgör ett hinder för en ändamålsenlig och konstruktiv riskbedömning då den vanligtvis avleder uppmärksamheten från uppgiften. Det är troligt att dessa uppkommer även i framtida riskbedömningar av geodata. För att användare av metoden ska vara medvetna om dessa tankefällor och veta hur man kan bemöta dem följer här en kort beskrivning av var och en.



Resultatet av riskbedömningen innebär ett val mellan att tillgängliggöra analysobjektet som öppna data eller att inte tillgängliggöra det alls.

Vissa deltagare kan befara att riskbedömningarna kommer att leda till att analysobjektet sekretessbeläggs och att aktörer som har behov av dessa geodata därmed kommer att förvägras tillgång till dem. En sådan inställning kan leda till en uttrycklig misstänksamhet mot riskbedömningen och en farhåga att metoden är en förevändning för att hemlighålla geodata från legitim användning.

Syftet med riskbedömningen är att, i enlighet med öppna datalagen (2022:818), utvärdera om tillgängliggörandet av geodata kan leda till risker för Sveriges säkerhet. Det faktum att man har identifierat sådana risker behöver emellertid inte föranleda att geodatamängden i fråga måste sekretessbeläggas, och därmed förvägra medborgare och organisationer legitim tillgång till det. Det finns nämligen en rad åtgärder som kan införas för att i största möjliga mån eliminera dessa risker samtidigt som data, i ett eller annat format, tillgängliggörs för samhällelig användning. Valet för de offentliga aktörerna är alltså inte enbart mellan att tillgängliggöra analysobjektet i analyserat format som öppna data eller att sekretessbelägga det.



Man kan inte bedöma riskerna om man inte vet nyttan med geodatamängden

Ett vanligt argument under utvecklingsarbetet av metoden var att man behöver väga riskerna mot nyttan, och att det därför inte går att bedöma riskerna om man inte känner till (samhälls)nyttan med analysobjektet. Det går emellertid inte att väga nyttor mot risker. Om man exempelvis gör en riskbedömning för ett analysobjekt som både bidrar med stor samhällsnytta och medför stora risker för Sveriges säkerhet om det tillgängliggörs blir inte riskerna lägre bara för att samhällsnyttan är stor. Riskerna för Sveriges säkerhet kommer fortsatt vara höga. Däremot kan alternativrisker uppstå, det vill säga risker som uppstår om analysobjektet inte tillgängliggörs som öppna data. Att bedöma samhällsnytta och risker för Sveriges säkerhet är två olika uppgifter, och båda är behäftade med betydande osäkerhet. Liksom det är svårt att uppskatta alla möjliga risker med ett tillgängliggörande av analysobjektet, är det svårt att bedöma alla möjliga nyttor med analysobjektet.

Initierande aktör och deltagare i riskbedömningen ska visserligen beakta nuvarande användning av analysobjektet (i analyserat format) när man föreslår och utformar åtgärder och när beslut ska fattas. Syftet med denna uppgift är dock att i så stor utsträckning som möjligt säkerställa att aktörer inom samhällsviktig verksamhet garanteras tillgång till geodatamängden så att denna verksamhet kan fungera som avsett.

44 Davidsson, m.fl. 2025.



Det spelar ingen roll vad vi gör för resursstarka statliga aktörer har redan tillgång till alla geodata.

En vanlig kommentar under utvecklingen av MEGS var att det inte spelar någon roll vad vi – det vill säga de offentliga aktörerna – gör eftersom de fientliga statliga aktörerna redan har tillgång till alla våra geodata. Detta är dock en missuppfattning av flera anledningar. För det första är det inte alls säkert att ens de mest resursstarka fientliga statliga aktörerna har tillgång till alla geodata som de offentliga aktörerna producerar. Exempelvis förutsätts ofta att stora statliga aktörer har tillgång till stora mängder satellitdata, och att offentliga aktörers data därmed skulle vara överflödiga. Det finns emellertid tydliga tecken på att så inte alltid är fallet.⁴⁵ Dessutom kan man via satellit bara observera vattenytan och den övre ytan i terrängen. Sverige består av nästan 70% skogsmark så det blir en ansevärd del av landets markyta som inte kan observeras med satelliter.

För det andra är det ibland ett misstag att betrakta en fientligt inställd stat som en enda aktör. För vissa stater är det mer passande att föreställa sig den som bestående av flera olika organ – exempelvis olika underrättelsetjänster, försvarsgrenar och departement – med olika motiv och som genomför olika typer av operationer. Det är heller inte säkert att alla dessa statliga organ utbyter information med varandra varför de kan vara ovetande om vad de andra organen har för information.⁴⁶ Därför kan det vara så att exempelvis en fientlig stats underrättelsetjänst har tillgång till svenska geodata men samma stats försvarsmakt inte har det.

För det tredje är de statliga antagonisterna inte de enda hoten mot Sveriges säkerhet utan det finns andra hotaktörer som troligen inte har lika stora resurser som fientliga stater men som likväl utgör allvarliga hot. Eftersom riskbedömningar behöver ta hänsyn till alla möjliga hot är det alltså inte tillräckligt att bara beakta statliga hotaktörer. Man måste därför bedöma om tillgängliggörande av analysobjektet kan leda till att riskerna för att någon hotaktör, statlig eller icke-statlig, orsakar skada på Sveriges säkerhet ökar. Även om det vore så att alla statliga hotaktörer redan har tillgång till analysobjektet är det alltså en missuppfattning att ett tillgängliggörande av det som öppna data inte leder till några nya risker.



Det finns redan öppna eller kommersiella alternativ - alltså kan vi tillgängliggöra våra data.

När det finns öppna eller kommersiella data som till synes överensstämmer med analysobjektet är det lätt att dra slutsatsen att det är fritt fram att tillgängliggöra geodatamängden. En uppgift i riskbedömningen är ju därför att försöka utröna om det finns alternativa data som motsvarar analysobjektet (se avsnitt 4.5.3). Denna uppgift är emellertid inte trivial. Bara för att det finns andra öppna eller kommersiella alternativ som på vissa sätt tycks motsvara analysobjektet är det nämligen inte nödvändigtvis så att analysobjektet inte tillför ytterligare information. Analysobjektet kan nämligen bidra med information som inte framgår av alternativa data och därmed bekräfta eller utöka den totala informationsmängden som en hotaktör har tillgång till.

Exempelvis skulle man kunna hävda att satellitbilder är lämpliga alternativ till offentliga aktörers ortofoton. Vanligtvis finns dock relevanta skillnader mellan tillgängliga satellitprodukter och de ortofoton som offentliga aktörer producerar. Exempelvis har ortofotona i allmänhet högre upplösning än de flesta satellitbilder vilket bidrar med högre detaljrikedom och att alltså ny information kan inhämtas från ortofotona. Dessutom är satellitbilderna och ortofotona insamlade vid olika tidpunkter så att de kan användas som komplement för att bekräfta redan kända observationer eller bidra med ny information (det vill säga en typ av ackumulation eller aggregering av data). Till exempel kan ortofotona visa på existensen av vissa typer av fordon vid platser som anses intressanta för hotaktörer

45 Zabrodskiy, M, Watling, J, Danylyuk, O V. & Reynolds, N, *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*. Royal United Services Institute for Defence and Security Studies, London, UK (2022).

46 Aaron Bateman, "The Political Influence of the Russian Security Services", *The Journal of Slavic Military Studies* 27:3 (2014), doi:10.1080/13518046.2014.932626; Joss I. Meakins, "Squabbling Siloviki: Factionalism Within Russia's Security Services", *International Journal of Intelligence and Counterintelligence* 31:2 (2018), doi:10.1080/08850607.2018.1417525; Cosimo Melella, Francesco Ferazza & Konstantinos Mersinas, "Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies", *ACIG* 4:2 (2024), doi:10.60097/ACIG/192120

vilket kanske inte framgår av satellitbilderna (och vice versa). Vidare kan satellitbilder sakna fullständig nationell täckning då vissa områden kan ha ansetts ointressanta av satellitbolagens kunder.

Sammantaget kan detta medföra att satellitbilderna inte motsvarar analysobjektet men en sådan slutsats beror även på hotaktör. För vissa hotaktörer kan skillnaderna i upplösning, täckningsgrad, tidpunkt för insamling eller andra kvalitetsskillnader vara irrelevanta varför ett tillgängliggörande av analysobjektet inte ökar riskerna för att dessa hotaktörer ska åstadkomma skada på Sveriges säkerhet. För andra hotaktörer däremot kan dessa kvalitetskillnader vara avgörande. Om den nya, kompletterande eller bekräftande information som tillgång till analysobjektet bidrar med är så pass viktig att det medför risker för Sveriges säkerhet varierar alltså från fall till fall. Det är därför viktigt att alltid göra en rigorös riskbedömning innan geodata tillgängliggörs som öppna data. Om analysobjektet redan finns tillgängligt som kommersiella data ska man även komma ihåg att det i sig utgör ett redan existerande alternativ. Då behöver de offentliga aktörerna beakta hur riskerna kan förändras vid ett tillgängliggörande som öppna data i förhållande till nuvarande situation.

Att det redan finns andra geodata som i vissa aspekter liknar analysobjektet innebär alltså inte att man nödvändigtvis ska dra slutsatsen att det är fritt fram att tillgängliggöra analysobjektet i analyserat format som öppna data. Därför behöver deltagarna i riskbedömningen alltid göra en grundlig analys.



Data har redan tillgängliggjorts - alltså är riskbedömning bortkastat.

Det kan hända att initierande aktör, utan att genomföra en riskbedömning, redan har tillgängliggjort analysobjektet, eller liknande geodata, som öppna data. Då kan det vara lätt att dra slutsatsen att alla hotaktörer redan har tillgång till analysobjektet och att en riskbedömning därför är överflödigt och ett slöseri med både tid och resurser. Att analysobjektet redan existerar som öppna data är naturligtvis olyckligt ur säkerhetshänseende och medför att man måste förutsätta att nuvarande hotaktörer innehar analysobjektet i nuvarande format. Det betyder emellertid inte att en riskbedömning är onödig. Exempelvis är inte de geodata som de offentliga aktörerna producerar statiska utan under kontinuerlig förändring. Landskapet, såsom skog och infrastruktur, och det samhälle som geodata representerar utvecklas kontinuerligt vilket leder till att data blir inaktuella. De offentliga aktörerna kan även av andra orsaker – exempelvis för att öka kvaliteten eller riktigheten eller på grund av ny kunskap – genomföra uppdateringar av geodatomängderna. Det betyder att om en riskbedömning leder till att initierande aktör vidtar åtgärder som i framtiden begränsar tillgången till analysobjektet, eller vissa aspekter av analysobjektet, exempelvis för att inte viss information ska röjas, kan den information som hotaktörer eventuellt redan har tillgång till successivt bli inaktuell.

Referenser

- Ackoff, R. L., "From Data to Wisdom", *Journal of Applied Systems Analysis* vol. 16 (1989), s. 3–9.
- Amer, M., Daim, T. U. & Jetter, A., "A review of scenario planning", *Futures* vol. 46 (2013), s. 23–40, doi:10.1016/j.futures.2012.10.003.
- Aven, T., "Risk assessment and risk management: Review of recent advances on their foundation", *European Journal of Operational Research* 253:1 (2016), s. 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., *Society for Risk Analysis Glossary*, (2018) <https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf> [Hämtad 2024-03-06].
- Aven, T., Renn, O. & Rosa, E. A., "On the ontological status of the concept of risk", *Safety Science* 49:8 (2011), s. 1074–1079, doi:10.1016/j.ssci.2011.04.015.
- Bateman, A., "The Political Influence of the Russian Security Services", *The Journal of Slavic Military Studies* 27:3 (2014), s. 380–403, doi:10.1080/13518046.2014.932626.
- Beard, S., Rowe, T. & Fox, J., "An analysis and evaluation of methods currently used to quantify the likelihood of existential hazards", *Futures* vol. 115 (2020), p. 102469, doi:10.1016/j.futures.2019.102469.
- Bennesved, P. & Olsson, M., *Centrala begrepp och metoder inom scenariometodiken*. FOI Memo 8178. Totalförsvarets forskningsinstitut, Stockholm, Sverige (2023).
- Bishop, P., Hines, A. & Collins, T., "The current state of scenario development: an overview of techniques", *Foresight* 9:1 (2007), s. 5–25, doi:10.1108/14636680710727516.
- Cairns, G., Goodwin, P. & Wright, G., "A decision-analysis-based framework for analysing stakeholder behaviour in scenario planning", *European Journal of Operational Research* 249:3 (2016), s. 1050–1062, doi:10.1016/j.ejor.2015.07.033.
- Carlsen, H., Eriksson, E. A., Dreborg, K. H., Johansson, B. & Bodin, Ö., "Systematic exploration of scenario spaces", *Foresight* 18:1 (2016), s. 59–75, doi:10.1108/FS-02-2015-0011.
- Davidsson, Å., Mittermaier, E., Severin, M., Söderman, U., Winterdahl, M., Ciepielewska, M. & Stjernlöf, S., *Riskbedömning av geodata med avseende på Sveriges säkerhet vid tillgängliggörande som öppna data.*, FOI-R--XXXX--SE. Totalförsvarets forskningsinstitut, Stockholm, Sverige (2025).
- Eliasson, M. & Villför Larsson, P., *Sätt fart på arbetsmötet. En handbok i facilitering*, 3 utg. Meetings International Publishing AB, Ystad (2017).
- Hansson, S. O., "Philosophical Perspectives on Risk", *Techné* 8:1 (2004), s. 10–35.
- Horváth, J., Baireddy, S., Hao, H., Montserrat, D. M. & Delp, E. J., "Manipulation Detection in Satellite Images Using Vision Transformer", *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)* (2021), psp. 1032–1041, doi:10.1109/CVPRW53098.2021.00114.
- Jonsson, D., *Att använda scenarier i planering för civilt försvar*. FOI-R--4434--SE. Totalförsvarets forskningsinstitut, Stockholm, Sverige (2017).

- Kahneman, D., Sibony, O. & Sunstein, C. R., *Noise: A Flaw in Human Judgment*. Little Brown & Co, New York (2021).
- Li, J., Qin, H., Wang, J. & Li, J., "OpenStreetMap-Based Autonomous Navigation for the Four Wheel-Legged Robot Via 3D-Lidar and CCD Camera", *IEEE Transactions on Industrial Electronics* 69:3 (2022), s. 2708–2717, doi:10.1109/TIE.2021.3070508.
- Mattsson, E. & Jöborn, A., *Möteskokboken*, 2 utg. Ordrum AB, Göteborg (2017).
- Meakins, J. I., "Squabbling Siloviki: Factionalism Within Russia's Security Services", *International Journal of Intelligence and CounterIntelligence* 31:2 (2018), s. 235–270, doi:10.1080/08850607.2018.1417525.
- Melella, C., Ferazza, F. & Mersinas, K., "Disjointed Cyber Warfare: Internal Conflicts among Russian Intelligence Agencies", *ACIG* 4:2 (2024), doi:10.60097/ACIG/192120.
- Miller, R., "Futures literacy: A hybrid strategic scenario method", *Futures* 39:4 (2007), s. 341–362, doi:10.1016/j.futures.2006.12.001.
- Montibeller, G. & von Winterfeldt, D., "Cognitive and Motivational Biases in Decision and Risk Analysis", *Risk Analysis* 35:7 (2015), s. 1230–1251, doi:10.1111/risa.12360.
- MSB, *Termbanken för informationssäkerhet*, (2025) <https://termbank-informationssakerhet.msb.se/> [Hämtad 2025-03-10].
- Myndigheten för digital förvaltning, *Vägledning för att tillgängliggöra information*, (2025) <https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/offentliga-aktorer/vagledning-for-att-tillgangliggora-information> [Hämtad 2025-01-27].
- Piirainen, K. A., Gonzalez, R. A. & Bragge, J., "A systemic evaluation framework for futures research", *Futures* 44:5 (2012), s. 464–474, doi:10.1016/j.futures.2012.03.008.
- Rowley, J., "The wisdom hierarchy: representations of the DIKW hierarchy", *Journal of Information Science* 33:2 (2007), s. 163–180, doi:10.1177/0165551506070706.
- Säkerhetspolisen, *Vägledning i säkerhetsskydd. Avlyssningsskyddade utrymmen* (2023a).
- Säkerhetspolisen, *Vägledning i säkerhetsskydd. Introduktion* (2023b).
- Schirrmeister, E., Göhring, A.-L. & Warnke, P., "Psychological biases and heuristics in the context of foresight and scenario processes", *Futures & Foresight Science* 2:2 (2020), p. e31, doi:10.1002/ffo2.31.
- Schoemaker, P. J. H., "Scenario Planning: A Tool for Strategic Thinking", *MIT Sloan Management Review* vol. 36 (1995), s. 25–40.
- Sveriges Kommuner och Regioner, *Termer och begrepp*, (2025) <https://klassa.skr.se/sidor/stodmaterial/Begrepp> [Hämtad 2025-01-27].
- Winehav, M. & Nevhage, B. (Red.), *FOI:s modell för risk- och sårbarhetsanalys (FORSA)*. FOI-R--3288--SE. Totalförsvarets forskningsinstitut, Stockholm, Sverige (2011).
- Włodarczyk-Sielicka, M., Połap, D., Prokop, K., Połap, K. & Stateczny, A., "Spatial Visualization Based on Geodata Fusion Using an Autonomous Unmanned Vessel", *Remote Sensing* 15:7 (2023), doi:10.3390/rs15071763.

- Yuchen, N., Xiangling, D., Wenyi, Z. & Yulin, Z., “A Systematic Review on Detection of Manipulated Satellite Images”, *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)* (2023), s. 6–11, doi:10.1109/CSCloud-EdgeCom58631.2023.00011.
- Zabrodskiy, M., Watling, J., Danylyuk, O. V. & Reynolds, N., *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*. Royal United Services Institute for Defence and Security Studies, London, UK (2022).
- Zhang, G., Lu, S. & Zhang, W., “CAD-Net: A Context-Aware Detection Network for Objects in Remote Sensing Imagery”, *IEEE Transactions on Geoscience and Remote Sensing* 57:12 (2019), s. 10015–10024, doi:10.1109/TGRS.2019.2930982.
- Zhang, J., Pan, B., Zhang, Y., Liu, Z. & Zheng, X., “Building Change Detection in Remote Sensing Images Based on Dual Multi-Scale Attention”, *Remote Sensing* 14:21 (2022), doi:10.3390/rs14215405.

Bilaga 1: Dokumentationsmall: riskbedömning workshop

Moment 1. Identifiera risker

Analysobjekt:

Risk (beskriv situation, händelse, skeende etc.)	Konsekvenser

Moment 2. Värdera risker

Notera att varje risk som identifierats i moment 1 ska dokumenteras på separat blad i moment 2. Konsekvensnivåer och relevans kan värderas enskilt eller i smågrupper enligt instruktion från facilitator.

Analysobjekt:

Risk:

2.1 Konsekvensnivå

Kriterier för att bedöma skada på Sveriges säkerhet och konsekvensnivåer framgår av bilaga 2 och 3.

Kriterium	Effektnivå
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	
Samhällsviktig verksamhet nödvändig för samhällets funktionalitet på nationell nivå	

2.1a Vilken är den högsta identifierade effektnivån?

2.1b Baserat på svaret i 2.1a, markera konsekvensnivå nedan.

Om alternativ *okänd/oklar skada* har valts i 2.1b ska frågor 2.1c – 2.1d diskuteras och besvaras gemensamt av alla deltagare på workshopen.

Existentiell skada	Allvarlig skada	Begränsad skada	Obetydlig skada	Okänd/oklar skada
a	b	c	d	
☐	☐	☐	☐	☐

2.1c Behövs nya kriterier i 2.1?

☐ Ja

☐ Nej, konsekvensen medför ingen skada på Sveriges säkerhet

☐ Nej, men det kan inte uteslutas att konsekvensen medför skada på Sveriges säkerhet

2.1d Benämna och beskriv nytt/nya kriterium/-er och beskriv effektnivåer.

Kriterium	Beskrivning	Effektnivåer

2.2 Relevans

Besvara endast de frågor som facilitator meddelar ska ingå i analysen.

2.2a I vilken utsträckning orsakar eller underlättar analysobjektet i analyserat format hotaktören att nå sina mål (så som de beskrivs i de identifierade konsekvenserna)?

I mycket hög utsträckning				I mycket låg utsträckning
4	3	2	1	0
☐	☐	☐	☐	☐

2.2b Hur betydelsefullt är hotaktörens tillgång till analysobjektet i analyserat format för de identifierade konsekvenserna?

Mycket betydelsefullt				Inte alls betydelsefullt
4	3	2	1	0
☐	☐	☐	☐	☐

2.2c I vilken utsträckning är hotaktören beroende av analysobjektet i analyserat format för att kunna planera och genomföra de aktiviteter som identifierats?

I mycket hög utsträckning				I mycket låg utsträckning
4	3	2	1	0
☐	☐	☐	☐	☐

2.2d I vilken utsträckning saknas andra data som för hotaktörens syften motsvarar analysobjektet (i analyserat format) och som hotaktören skulle kunna använda för att uppnå samma resultat?

I mycket hög utsträckning				I mycket låg utsträckning
4	3	2	1	0
☐	☐	☐	☐	☐

2.2e I vilken utsträckning har hotaktören förmåga (d.v.s. resurser, kunskap och färdigheter) att använda analysobjektet för att uppnå sina mål?

I mycket hög utsträckning				I mycket låg utsträckning
4	3	2	1	0
☐	☐	☐	☐	☐

2.2f Hur stora tidsmässiga, ekonomiska och personella resurser skulle hotaktören behöva använda för att införskaffa motsvarande data själv om analysobjektet inte finns tillgängligt som öppna data?

Mycket stora				Obetydliga
4	3	2	1	0
☐	☐	☐	☐	☐

2.2g Hur stora risker skulle hotaktören behöva ta för att införskaffa motsvarande data själv om analysobjektet inte finns tillgängligt som öppna data?

Mycket stora				Obetydliga
4	3	2	1	0
☐	☐	☐	☐	☐

2.2h Plats för egna frågor: _____

I mycket hög utsträckning				I mycket låg utsträckning
4	3	2	1	0
☐	☐	☐	☐	☐

2.2i Plats för egna frågor: _____

I mycket hög utsträckning				I mycket låg utsträckning
4	3	2	1	0
☐	☐	☐	☐	☐

Beräkna utifrån de numeriska värdena på svaren ovan det aritmetiska medelvärdet av alla svaren.

2.2j Medelvärdet av svaren på ovanstående frågor = _____

2.2k Avrunda svaret i 2.2j till närmaste heltal och markera relevans nedan.

Mycket stor relevans	Stor relevans	Inte obetydlig relevans	Liten relevans	Mycket liten relevans
4	3	2	1	0
☐	☐	☐	☐	☐

2.3 Värdering: Sammanställning

Analysobjekt: _____

2.3a Anteckna konsekvensnivå och relevans för varje identifierad risk i nedanstående tabell.

Risk	Konsekvensnivå	Relevans

2.3b Anteckna de konsekvenser som getts konsekvensnivån okänd/oklar skada i 2.1 och för vilka deltagarna inte har lyckats identifiera nya lämpliga kriterier eller på annat sätt enats om hur de ska hanteras. Motivera varför ingen annan konsekvensnivå än okänd/oklar skada anses lämplig.

Risk	Konsekvens	Motivering

Moment 3. Samlad bedömning*Analysobjekt:* _____

Relevansnivå	Mycket stor				
	Stor				
	Inte obetydlig				
	Liten				
	Mycket liten				
		Obetydlig	Begränsad	Allvarlig	Existentiell
		Konsekvensnivå			

Figur 3. Konsekvens-och relevansmatris**Moment 4. Rekommendation***Analysobjekt:* _____

- ☐ Analysobjektet kan tillgängliggöras i nuvarande format
- ☐ Analysobjektet kan tillgängliggöras först efter att åtgärder har vidtagits
- Föreslagen åtgärd:

- ☐ Analysobjektet bör inte tillgängliggöras som öppna data men kan förmedlas på annat sätt
Föreslaget sätt:

- ☐ Analysobjektet bör omfattas av sekretess. Ange föreslaget lagstöd:

Motivering till rekommendation:

Bilaga 2: Kriterier Sveriges säkerhet¹

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. a. Val förekommer men de är till stor del inte fria eller rättvisa. a. Val förekommer men de är delvis inte fria eller rättvisa. a. 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.
--	--	--

Bilaga 3: Konsekvensnivåer

Konsekvensnivå	Definition/beskrivning
Existentiell skada (a)	Sveriges I) politiska självständighet; II) territoriella suveränitet; eller III) demokratiska statsskick förloras; eller IV) samhällsviktig verksamhet 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 omfattande 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 omfattning; 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 verksamhet 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 säkerhet påverkas eller det är okänt hur Sveriges säkerhet kan påverkas, exempelvis på grund av brist på information.

Det kriterium som anses påverkas i störst omfattning (där *a* innebär störst och *d* minst påverkan) bestämmer vilken den totala konsekvensnivån blir för respektive konsekvens. Om deltagarna exempelvis anser att en konsekvens påverkar den territoriella suveräniteten på nivå *b* medan övriga dimensioner påverkas på lägre nivåer blir den totala konsekvensnivån *b*, det vill säga *allvarlig skada*.

