Publika data som riskfaktor

En förstudie om påverkan på informations-säkerhet och säkerhetsskydd

Daniel Eidenskog, Christian Vestlund

FOI-R--5931--SE

Mars 2026

FOI

Daniel Eidenskog, Christian Vestlund

Publika data som riskfaktor

En förstudie om påverkan på informationssäkerhet och säkerhetsskydd

Titel	Publika data som riskfaktor – En förstudie om påverkan på informationssäkerhet och säkerhetsskydd
Title	Public data as a risk factor – A prestudy on impacts on information security and protective security
Rapportnr/Report no	FOI-R--5931--SE
Månad/Month	Mars
Utgivningsår/Year	2026
Antal sidor/Pages	47
ISSN	1650-1942
Uppdragsgivare/Client	Trafikverket
Forskningsområde	Cyberförsvar och cybersäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	B34208
Godkänd av/Approved by	Foteini Papiri
Ansvarig avdelning	Cyberförsvar och ledningsteknik

Bild/Cover	Trinity college library, Dublin. Marouh från Pixabay.

Sammanfattning

Med ökad generell hotbild mot Sverige blir även underrättelsehotet mer påtagligt. Den stora mängden publikt tillgängliga data kan om de kombineras potentiellt leda till information som påverkar skyddet av säkerhetskänslig verksamhet. Genom moderna analysmetoder kan stora mängder data av olika typ kombineras för att dra slutsatser som inte explicit uttrycks i ursprungliga data. Detta ger problem med exempelvis sekretess- och riskbedömningar inför publicering av öppna data eller offentliga handlingar.

Denna rapport presenterar en förstudie med ett första steg mot att förstå vilka risker för sekretess och säkerhetsskydd som kan uppstå ur antagonisters möjligheter att nyttja publika data i underrättelsesammanhang. Det långsiktiga målet är att bidra med kunskap som behövs för att kunna göra genomarbetade och välförankrade sekretess- och riskbedömningar, som även hanterar de problem som uppstår genom publika data.

Förstudien är av explorativ natur och ger en översikt över underrättelsearbete, källor till publika data samt metoder för bearbetning och analys av insamlade data. Rapporten diskuterar även ett antal ytterligare områden och perspektiv som behöver hanteras i framtida forskning, såsom datamängdernas omfattning, tekniker för komplexa analyser, riskbedömningsmetodik, kompetensbehov, etik och juridik.

Nyckelord: Publika data, sekretess, riskbedömning, OSINT

Summary

With an increased general threat level affecting Sweden, the intelligence threat is becoming more pronounced. The large volume of publicly available data can potentially reveal information that compromises the protection of security-sensitive activities when combined. Through modern analytical methods, large volumes of heterogeneous data can be co-analyzed to infer information not explicitly stated in the original data. This creates challenges for secrecy and risk assessments prior to the publication of open data or public records.

This report presents a study that takes an initial step toward understanding the risks to secrecy and protective security arising from adversaries' potential to exploit public data in an intelligence context. The long-term goal is to contribute the knowledge needed to conduct thorough and well-grounded secrecy and risk assessments that also address problems arising from public data.

This preliminary study is exploratory in nature and provides an overview of intelligence operations, sources of public data, and methods for processing and analyzing collected data. The report also discusses additional areas and perspectives that must be addressed in future research, such as the extents of the data sets, techniques for advanced analyses, risk assessment methodology, competence needs, ethics, and law.

Keywords: Public data, confidentiality, risk assessment, OSINT

Innehåll

1 Inledning

Beredskaps- och säkerhetsfrågor har aktualiserats genom den ökade hotbild som det oroliga världsläget medför. Sverige och Europa utsätts inte bara för militära hot utan även fortlöpande antagonistiska aktiviteter i form av underrättelseverksamhet, påverkansoperationer och cyberangrepp (Trafikverket, 2025b, s. 13). En viktig fråga för skyddet av transportinfrastruktur och annan samhällsviktig verksamhet är vilken information svenska myndigheter och företag oavsiktligt eller omedvetet delar med sig av, trots att den borde omfattas av säkerhetsskydd eller näraliggande sekretessbestämmelser. Samtidigt finns det en stark trend mot att alltmer så kallade öppna data ska tillgängliggöras av offentliga aktörer, såsom myndigheter och offentliga bolag. Denna trend har också understöd i EU-lag (Direktiv 2019/1024, 2019) och nationell lag (SFS 2022:818, 2022). Öppna data från offentliga aktörer utgör dock endast en delmängd av den sammanlagda mängd allmänt tillgängliga data – i denna rapport benämnda som *publika data* – där även exempelvis offentliga handlingar, kommersiella aktörer och öppet tillgängliga projekt (eng. open-source projects) återfinns bland källorna.

Idag finns det en mycket omfattande tillgång till publika data samt stora möjligheter till avancerade IT-baserade analys- och beslutsstöd. Detta innebär en utmaning för verksamheter och information som behöver skyddas enligt säkerhetsskyddslagen eller sekretesslagstiftning. För omfattande infrastruktursystem såsom järnvägen accentueras detta ytterligare genom de permanenta och ofta mycket synliga installationer som finns spridda över landet. Det försämrade säkerhetsläget innebär att underrättelsetrycket från främmande makt stiger samtidigt som skyddet av infrastrukturen mot sabotage och angrepp blir allt viktigare för att upprätthålla Sveriges totalförsvarsförmåga.

Den ökande mängden publika data kan illustreras genom exempelvis kartdata, där underlag kan samlas in i form av (1) öppna data och allmänna handlingar från publika aktörer såsom Lantmäteriet och kommunerna, (2) kommersiellt tillgängliga data från tjänster som Google Maps[1] och Maxar Intelligence[2] samt (3)

[1] https://www.google.com/maps (besökt 2026-03-24).
[2] https://maxarenergysource.com/maxar-intelligence/about.html (besökt 2026-03-24).

öppna källor såsom OpenStreetMap[3].

Säkerhetsskydd är ett komplicerat ämne med många svåra frågeställningar för verksamhetsutövaren. En svårighet är bedöma vilka verksamheter och uppgifter som omfattas av säkerhetsskydd, speciellt när verksamheten eller uppgifterna inte nödvändigtvis är säkerhetskänsliga i den egna verksamheten men däremot har potential att påverka säkerheten på det nationella planet. Det är också svårt att förstå vilka uppgifter och vilka data som har potential att röja information om säkerhetskänsliga verksamheter eller kan avslöja uppgifter som omfattas av säkerhetsskydd. Här finns det ett stort behov av att förenkla för organisationerna att genomföra sitt säkerhetsarbete, bland annat genom att förstå antagonisternas möjligheter till slutledningar utifrån publika data.

Under perioden 2024–2025 genomförde FOI ett projekt tillsammans med Lantmäteriet för att ta fram en metod för riskbedömning vid tillgängliggörande av geodata som öppna data (Davidsson m. fl., 2025b). De konstaterade att riskbedömningar av denna typ är komplicerade där exempelvis avancerade analystekniker såsom AI kan användas vid aggregering av geodata för att potentiellt avslöja känslig information. Riskbedömningen kan inte heller begränsas till den information som finns eller tillgängliggörs inom den egna organisationen, utan måste även ta hänsyn till hur informationen kan aggregeras med den övriga informationsmängd som en antagonist kan ha tillgång till (Davidsson m. fl., 2025a, s. 15).

Denna rapport utforskar antagonisternas arbete med att få tag på och analysera data för att ta reda på information som denne sedan kan använda för sina ändamål. Tanken är att förståelse för antagonisternas arbetssätt och datakällor ger insikt i hur publika data kan användas för antagonistiska ändamål och vilken effekt som publicering av ytterligare data kan få. Efter en bakgrund (i kapitel 2) som beskriver den övergripande problembilden går den utforskande resan via underrättelsearbete (i kapitel 3), publika datakällor (i kapitel 4) och underrättelseanalys (i kapitel 5). Därefter följer en diskussion (i kapitel 6) om ytterligare aspekter som är relevanta för ämnet och för fortsatta forskningsstudier. Avslutningsvis presenteras slutsatserna från arbetet (i kapitel 7).

[3] https://www.openstreetmap.org (besökt 2026-03-24).

1.1 Syfte och mål

Denna rapport utgör rapporteringen från projektet *Risker för informationssäkerhet och säkerhetsskydd från publika data (RISP) – Förstudie* som har finansierats genom Trafikverkets forskningsmedel. Projektet har genomförts på Totalförsvarets forskningsinstitut (FOI) under vintern 2025–2026. Projektet har genomförts som ett tillagt arbetspaket i projektet *Beredskapshänsyn i utveckling och långsiktsplanering av transportsystem (BULT)* som också finansieras av Trafikverket.

Det långsiktiga syftet med projektet är att bidra till förståelsen för hur publika data kan påverka aspekter av informationssäkerhet och säkerhetsskydd för den svenska järnvägen. Målet med denna förstudie är att sammanställa bakgrundsinformation inom området och att undersöka hur en större forskningsstudie kan utformas. I detta ingår att undersöka möjligheter och metoder för att förbättra förståelsen för gränslandet för vilken information som behöver omfattas av sekretess eller säkerhetsskydd. Förstudien utgår från järnvägssystemet för att ha ett konkret, tydligt och avgränsat område med hög relevans för samhällets beredskap.

Avsikten med förstudien är att undersöka förutsättningarna för ett större forskningsprojekt med målet att förbättra möjligheterna att identifiera och förstå skyddsvärden för olika data. Studier i ett fortsättningsprojekt kan exempelvis utgå från scenarier såsom (1) att identifiera data som indirekt kan röja känslig information som skulle kunna användas av antagonister samt (2) förstå balansen mellan potentiellt omfattande nytta med att publicera data och låggradiga sekretess- och säkerhetsskyddsbehov.

Det eventuella framtida fortsättningsprojektet förväntas ge viktig kunskap om hur publika data (inklusive öppna data) kan påverka information och verksamheter som omfattas av sekretess och säkerhetsskydd, ur såväl angriparens som försvararens perspektiv. Dessa resultat är av värde för många offentliga aktörer inom såväl transportsektorn som andra samhällssektorer. Metoder och kunskap kring insamling och kartläggning från publika källor stärker aktörernas möjligheter att upprätthålla säkerhetsskyddet och skydda information som omfattas av sekretess. Metoder och kunskap i form av exempelvis riktlinjer eller bedömningsgrunder inför publicering av öppna data är värdefulla för att

aktörerna ska kunna fullgöra de åtaganden som följer av exempelvis EU:s regelverk kring öppna data.

De övergripande målen för denna rapport är att på ett övergripande plan

- undersöka vilka metoder och publika källor som kan användas för att studera hur kartläggning av järnvägen (inklusive stödjande infrastruktur och digitala system) kan göras
- undersöka vilka metoder som kan användas för att studera hur insamlad information relaterar till och påverkar information som omfattas av säkerhetsskydd.

Tanken är endast att ge övergripande guidning till potentiella metoder och källor inför ett framtida forskningsarbete. Detaljerad genomgång och val av metoder behöver göras utifrån det framtida arbetets faktiska inriktning.

1.2 Metod

Då projektet utgör en förstudie har metoderna huvudsakligen varit av explorativ natur. Explorativa metoder har fördelen av att snabbt kunna ge en bred förståelse för ett problemområde, vilket är nödvändigt för att kunna förfina frågeställningar och metodval inför ett fortsättningsprojekt. Samtidigt ger explorativa metoder inga garantier för att det undersöka området täcks in tillräckligt väl då metoderna saknar tillräcklig systematik för detta.

Informationsinsamlingen består av explorativa litteratursökningar inom såväl forskningslitteratur som annan litteratur. Litteraturen inkluderar bland annat juridiska aspekter, processnära aspekter (såsom regelverk och styrningar), underrättelseinhämtning samt beskrivningar av öppna och publika datamängder

1.3 Terminologi

Detta avsnitt definierar några centrala begrepp som används i denna rapport.

- **Publika data** utgör data som på något sätt är tillgänglig för allmänheten. Publika data kan exempelvis komma från offentliga källor, kommersiella källor eller öppna källor. Publika data behöver inte vara tillgängliga gratis, utan kan även vara avgiftsbelagda. Publika data inkluderar bland annat *öppna data*.
- **Öppna data** utgör ”information som samlats in, producerats eller betalats för av statliga organ [...] och som kostnadsfritt görs tillgänglig för återanvändning för alla typer av ändamål.”[4]

Begreppen *data* och *information* är svårdefinierade och det finns många olika definitioner av dem (Rowley, 2007). Inom informationsteorin ingår begreppen i den så kallade DIKW-hierarkin, namngiven efter de engelska orden för data, information, kunskap och vishet. Följande exempel på definitioner är hämtade ur Rowleys (2007) sammanställning:

- **Data** utgör diskreta, objektiva faktum eller observationer, som är oorganiserade och obearbetade, och som inte bär någon specifik mening”(Rowley, 2007, s. 170, förf. övers.).
- **Information** utgörs av data som har försetts med betydelse, relevans och mening”(Rowley, 2007, s. 171, förf. övers.).

Begreppen används relativt utbytbart i denna rapport på grund av svårigheten i att definiera dem samt det såväl praktiska som subjektiva problemet med att särskilja vad som utgör data respektive information.

[4]https://data.europa.eu/sv/dataeuropa-academy/what-open-data (besökt 2026-03-24).

2 Bakgrund

Att järnvägen spelar en viktig roll i totalförsvaret står utom tvekan och fick extra mycket fokus i samband med Natomedlemskapet.[5] Vikten av transporter i allmänhet och av järnvägen i synnerhet återkommer i rapporter och yttranden från myndigheter och andra organisationer. Regeringen framhåller transportinfrastrukturen, inklusive järnvägen, som en viktig förutsättning för att det militära försvaret ska fungera (Prop. 2024/25:34, 2024, s. 106):

> En väl fungerande och underhållen transportinfrastruktur, såsom vägar, järnvägar, hamnar och infrastruktur för luftfart, är en viktig förutsättning för att det militära försvaret ska kunna lösa sina uppgifter.

Järnvägens roll i det militära försvaret understryks även av Försvarsmakten (Försvarsmakten, 2025b, s. 5). Järnvägen är också viktig för det civila försvaret. Militära underrättelse- och säkerhetstjänsten (Must) lyfter fram järnvägstransporter som ett exempel på samhällsviktig infrastruktur som krävs för att civilsamhället ska kunna fortsätta fungera i en konflikt (Försvarsmakten, 2025a, s. 30):

> Sverige behöver säkerställa att bland annat elförsörjning, väg- och järnvägstransporter och sjukvård kan fortsätta fungera oavsett konfliktnivå.

Därtill är järnvägen en viktig kugge i samhällets funktion i normalläge. Sammantaget innebär det att det övergripande skyddsvärdet hos järnvägssystemet är högt. En aspekt av att upprätthålla detta skyddsvärde är att säkerställa att veta vilken information som omfattas av sekretess eller säkerhetsskydd och att hantera denna information korrekt.

[5] Se exempelvis https://www.infrastrukturnyheter.se/20241011/30614/rapport-111-miljarder-kravs-att-mota-natos-krav-pa-svensk-transportinfrastruktur (besökt 2026-03-24).

2.1 Järnvägssystemet

Det svenska järnvägssystemet är komplext och omfattande med över 15 700 km trafikerade spår där transporterna under 2024 summerades till över 13 miljarder personkilometer plus 21 miljarder tonkilometer godstransporter (Trafikanalys, 2024). Samma år hade trafiken knappt 50 huvudmän, huvudsakligen offentliga organisationer, och utfördes av drygt 30 olika operatörer som sammantaget hade över 3 200 dragfordon.[6]

Järnvägssystemet består av många delar som samtliga behöver fungera för att upprätthålla en fungerande infrastruktur. Spåranläggning, trafikplatser, kraftförsörjning, signalsystem, trafikeringssystem, kommunikationssystem och tågskyddssystem är några av dessa delar (Trafikverket, 2025a). Därtill finns en omfattande digital infrastruktur med landsomfattande IT-infrastruktur och olika tjänster som används av bland annat resenärer, operatörer och entreprenörer.

2.2 Hotbilden mot järnvägen

Denna studie fokuserar på ett övergripande plan på hur en antagonist kan nyttja publika data vid underrättelsearbete eller angrepp på den svenska järnvägen. Hotbilden mot kritisk infrastruktur i Sverige är bred. Både Säpos och Musts årsrapporter beskriver ett försämrat säkerhetsläge och att främmande makt riktar in underrättelse- och sabotageverksamhet även mot civila mål (Försvarsmakten, 2025a; Säkerhetspolisen, 2025).

En övergripande beskrivning av hotbilden återfinns i Trafikverkets rapport *Öppen antagonistisk hotbild mot transportsektorn* (Trafikverket, 2025b). Rapporten tar upp en komplex hotbild med ett brett spektrum av hot och antagonister, där främmande makt agerar allt mer offensivt (Trafikverket, 2025b, s. 5). Med transportsystemets komplexitet (järnvägen inräknad) behövs ett starkt skydd med en bred motståndskraft för att hantera den komplexa hotbilden (Trafikverket, 2025b, s. 6).

[6] Uppgifterna är hämtade från Trafikanalys (2024) och det underliggande statistiska underlaget som återfinns på https://www.trafa.se/bantrafik/bantrafik/ (besökt 2026-03-24).

Antagonistisk underrättelseverksamhet utgör en viktig komponent i hotbilden i gråzonsläge. Främmande makts olagliga underrättelseinhämtning kombineras även med lagliga, öppna källor (så kallad open source intelligence, OSINT) vilket ställer stora krav på korrekt hantering av verksamheternas information (Trafikverket, 2025b, s. 13). Inhämtning av information i cyberdomänen utgör en av byggstenarna i främmande makts underrättelseverksamhet, exempelvis när det gäller Kinas underrättelseinhämtning mot Sverige (Trafikverket, 2025b, s. 27). Underrättelseaktiviteter mot transportsektorn kan exempelvis handla om påverka beslutsfattande, inhämta information om säkerhetskyddsklassificerade tjänster, inhämta finansiell information och kartlägga rutiner (Trafikverket, 2025b, s. 33, 34, 39, 43).

Järnvägen är idag mycket beroende av avancerade IT-system för sin funktion. Kvalificerade cyberangrepp är ett område där avvägningen mellan angreppets effekt och angriparens risk ofta är fördelaktig för angriparen. Många gånger kan angreppen genomföras på stort avstånd, vanligen över internet, vilket gör att attribuering[7] och lagföring blir mycket svårt eller omöjligt. Kombinerat med den centrala funktion som IT-systemen numera har för olika verksamheter kan effekten bli kännbar för den drabbade. Säpos årsrapport beskriver att svenska IT-system och IT-infrastrukturer är tydliga mål för kvalificerade hotaktörer (Säkerhetspolisen, 2025, s. 36):

> Idag är tröskeln för att genomföra cyberangrepp mot mål i Sverige låg då det finns betydande sårbarheter att utnyttja. Omfattande sårbarheter i infrastruktur och IT-system kombinerat med främmande makts höga cyberförmåga och stora informationsbehov utgör ett allvarligt hot mot Sveriges säkerhet.

2.3 Antagonistens informationsbehov

Angrepp varierar betydligt i genomförande och mål beroende på angreppsdomän men kan grovt kategoriseras i kategorierna obehörigt tillträde och skadlig inverkan. Målet med ett angrepp varierar beroende på hotaktör och eventuell

[7] Attribuering innebär att peka ut gärningspersonerna eller den bakomliggande organisation eller nation som står bakom ett cyberangrepp.

konfliktnivå. För fysiska angrepp kan det exempelvis handla om stöld och sabotage av fysiska tillgångar och för cyberangrepp kan det handla om överbelastningsattacker, ransomware, informationsstöld och sabotage.

Ett begrepp som brukar användas för att beskriva strukturen eller faserna i en attack i sammanhanget är *attackkedjor* (eng. kill chain). Attackkedjor är ursprungligen ett militärt begrepp för genomförandet av målstyrd bekämpning. Ett exempel på militär attackkedja är F2T2EA som består av sex faser (U.S. Department of the Air Force, 2021):

1. Hitta (eng. find) – Identifiera potentiella mål.
2. Fixera (eng. fix) – Identifiera specifika mål som är värda att agera mot.
3. Spåra (eng. track) – Övervaka målet tills beslut tas om agerande.
4. Uppdragsplanera (eng. target) – Val av metod för att agera mot målet. I militära sammanhang beskrivs detta steg ofta som val av vapen.
5. Agera (eng. engage) – Genomförande av attack mot målet.
6. Utvärdera (eng. assess) – Utvärdera effekten av attacken.

Inom cyberdomänen beskrivs cyberangrepp ofta i termer av *cyberattackkedjor* (eng. cyber kill chains). Begreppet är en vidareutveckling av det militära begreppet och togs fram av företaget Lockheed Martin och består av sju faser (Hutchins m. fl., 2011):

1. Kartläggning (eng. reconnaissance) – Samla information om system som ska attackeras, exempelvis informationssystem, organisationen, personal, m.m.
2. Beväpning (eng. weaponization) – Anskaffa eller utveckla skadlig kod eller verktyg för att genomföra en attack.
3. Leverans (eng. delivery) – Initiala angrepp genom att exempelvis skicka länkar till skadlig kod i phishingmejl.
4. Exploatering (eng. exploitation) – Utnyttjande av sårbarheter för att skapa ett fotfäste i IT-system.
5. Installation (eng. installation) – Installation av skadlig kod eller verktyg i målmiljön.

6. Ledning och kontroll (eng. command and control) – Fjärrstyrning av installerade verktyg.
7. Åtgärder i målmiljö (eng. actions on objective) – Åtgärder i målmiljön för att uppnå målet med attacken, exempelvis identifiera specifika tillgångar, förflytta sig i målmiljön, kryptera data med ransomware och exfiltrera data.

Varken militära attackkedjor eller cyberattackkedjor är tillämpbara för att beskriva alla typer av angrepp då tillvägagångssätt varierar stort mellan olika aktörer och angreppsdomäner. Även om tillvägagångssätten varierar har de generellt ett tillvägagångssätt som inkluderar kartläggning, förberedelser och verkställande av angrepp. Första steget för en antagonist, oavsett typ av angrepp, är att inhämta information för att därefter planera och genomföra angreppet. All information som kan underlätta planering och genomförande är av intresse för en antagonist. För att angripa järnvägen kan det exempelvis handla om var IT-system finns, vilka underleverantörer som används, vilka transporter som genomförs, när transporter genomförs, var ett angrepp får störst konsekvenser och var konsekvenserna av ett angrepp är svåra att åtgärda.

3 Underrättelsearbete

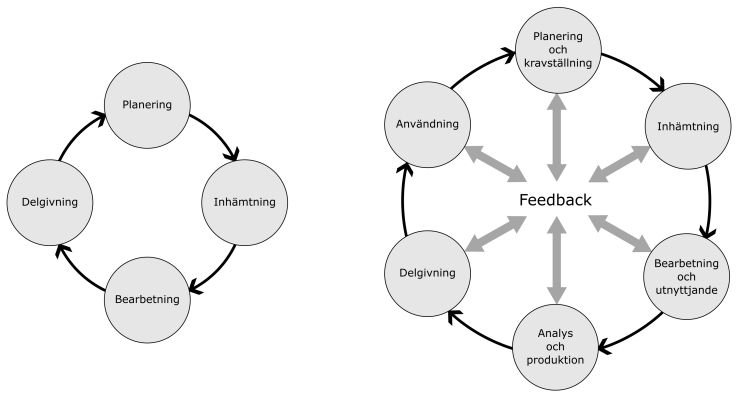
Underrättelsearbete är ett samlingsbegrepp som rymmer ett antal olika principer, metoder och tekniker för att samla in och bearbeta information samt dra slutsatser utifrån den bearbetade informationen. Begreppen underrättelser, underrättelsearbete och underrättelsetjänst förknippas ofta med militära och civila säkerhetstjänster, såsom Militära underrättelse- och säkerhetstjänsten (Must) samt Säkerhetspolisen (Säpo). Begreppen är dock lika applicerbara i andra sammanhang med liknande behov kring informationsinsamling och bearbetning inför beslut, vid såväl defensiva aktiviteter (såsom bedömning av hotbilder och förebyggande av angrepp) som vid offensiva aktiviteter (såsom rekognosering av infrastruktur och planering av angrepp).

I denna rapports kontext blir underrättelsearbetet relevant som en spegling av antagonisters underrättelsearbete. Målet blir då att organisationen ska kunna förbättra skyddet av sin egen verksamhet och information genom att förstå vilken information antagonisterna kan samla in och vilka slutsatser de kan dra ur den insamlade informationen.

Underrättelseinhämtning kan ske på flera olika sätt. I Försvarsmaktens *Reglemente Underrättelsetjänst* definieras sex inhämtningsdiscipliner (Försvarsmakten, 2022):

- akustiska underrättelser (acoustic intelligence, ACINT)
- bildunderrättelser (image intelligence, IMINT)
- personbaserad inhämtning (human intelligence, HUMINT)
- signalunderrättelser (signal intelligence, SIGINT)
- signaturunderrättelser (measurement and signature intelligence, MASINT)
- underrättelser från öppna källor (open source intelligence, OSINT).

I både svenska och amerikanska militära publikationer förekommer också flera tematiska begrepp som utgår från de områden som underrättelserna berör (Chairman of the Joint Chiefs of Staff, 2013; Försvarsmakten, 2022; U.S. Army,



a) Försvarsmaktens underrättelsecykel. b) Underrättelsecykeln enligt Lowenthal (2026).

Figur 1: Två variationer av underrättelsecykeln (Försvarsmakten, 2022; Lowenthal, 2026).

2023). *Reglemente Underrättelsetjänst* tar upp följande exempel på tematiska områden (Försvarsmakten, 2022, s. 60):

- ekonomiska underrättelser (economic intelligence, ECOINT)
- geospatiala underrättelser (geospatial intelligence, GEOINT)
- medicinska underrättelser (medical intelligence, MEDINT)
- tekniska underrättelser (technical intelligence, TECHINT).

Då denna studie utgår från underrättelseinhämtning från publikt tillgängliga källor ligger fokus på OSINT med tillhörande metoder för inhämtning av publika data.

3.1 Underrättelsearbetets faser

Figur 1a visar Försvarsmaktens underrättelsecykel enligt *Reglemente Underrättelsetjänst* (Försvarsmakten, 2022, s. 21–22). En utökad version som bygger på Lowenthals (2026) förtydligande av respektive steg återfinns i figur 1b. Lowenthal delar upp bearbetningssteget i separata steg för bearbetning och analys,

lägger till ett steg för användning av resultaten samt lägger in feedback som en övergripande aktivitet för alla steg i cykeln. Följande avsnitt beskriver kortfattat de olika stegen i Lowenthals (2026) modell.

3.1.1 Planering och kravställning

Planering och kravställning (eng. planning and requirements) handlar om att fastställa strategin för att uppnå en lyckad underrättelseprodukt i det aktuella fallet. För att göra detta behöver kraven på resultaten ställas upp utifrån indata från underrättelsearbetets intressenter och mottagare. Här bestäms även vilka metoder som väljs ut för det aktuella underrättelsearbetet.

Tidshorisonten för hur resultaten ska användas utgör en faktor som påverkar planeringen. Kortsiktigt underrättelsearbete fokuserar mer mot dagsaktuella frågor, ofta med relativt strikta tidsgränser för när resultaten behöver vara tillgängliga. Långsiktigt underrättelsearbete antar en mer strategisk karaktär, med fokus på trender och frågeställningar som kan bli aktuella i framtiden.[8] De olika tidsperspektiven innebär bland annat att olika metoder, kompetenser och risknivåer blir relevanta i respektive fall (Lowenthal, 2026, s. 83).

3.1.2 Inhämtning

Inhämtning (eng. collection) innebär att samla in data genom de källor och metoder som identifierats i planeringen. Här kan en stor bredd av källor och metoder användas, beroende på kravställningen för den aktuella insamlingen. Här kommer också faktorer såsom resursutnyttjande och risktagande in för att anpassa de olika insamlingsaktiviteterna till den uppsatta målbilden (Lowenthal, 2026, s. 81–82).

Styrningen av exakt vad inhämtningen behöver fokusera på kan ske direkt utifrån planering och kravställning, men även mer reaktivt utifrån underrättelseanalytikernas behov. Det senare fallet, så kallad analysdriven inhämtning (eng. analytically driven collection), utgör en integrerad

[8] Lowenthal (2026, s. 83) kallar tidsperspektiven för *current intelligence* respektive *long-term intelligence*.

underrättelseverksamhet där analytikerna får ett betydande inflytande över vilken data och information som ska inhämtas (Lowenthal, 2026, s. 84).

3.1.3 Bearbetning och utnyttjande

Bearbetning och utnyttjande (eng. processing and exploitation) innebär att den data som samlats in bearbetas för att bli användbar i den efterföljande analysen. Det kan exempelvis handla om bilder där innehållet behöver identifieras, infångade radiosignaler som behöver avkodas eller texter som behöver översättas (Lowenthal, 2026, s. 82).

3.1.4 Analys och produktion

Analys och produktion (eng. analysis and production) utgör det steg där analytiker bearbetar den insamlade underrättelseinformationen för att dra slutsatser för de frågor som ställts upp i planeringssteget. Produkten av analysen är någon form av underrättelserapport som sedan kan delges till berörda parter, vanligtvis någon form av beslutsfattare, för vidare hantering och styrning i verksamheten. Analyssteget innebär ofta en samlad värdering av många olika underrättelser som sinsemellan kan vara motsägande (Lowenthal, 2026, s. 84).

3.1.5 Delgivning

Delgivning (eng. dissemination) utgör det steg där analytikerna överlämnar eller presenterar resultaten till mottagarna.

3.1.6 Användning

Användning (eng. consumption) är det steg där resultaten nyttjas i beslutsfattande eller andra aspekter av avnämarens verksamhet. Användningen ligger därmed huvudsakligen utanför underrättelsearbetet.

3.1.7 Feedback

Feedback utgör en viktig aspekt av underrättelsecykeln där de olika intressenterna och deltagarna i och kring underrättelsearbetet har möjlighet att utbyta erfarenheter och återkoppla exempelvis på vilka sätt resultaten varit användbara och vilka perspektiv som saknats (Lowenthal, 2026, s. 86–87).

3.2 Direkt och indirekt information

Vid OSINT fokuserar inhämtningssteget helt på information som går att få från källor som är tillgängliga utan att ta till tveksamma eller kriminella metoder. Det innebär att data som samlas in på ett eller annat sätt alltid är att betrakta som publikt tillgänglig, oavsett om den kommer från helt öppna källor eller exempelvis hämtas mot betalning från kommersiella källor. Denna typ av data är vanligtvis att betrakta som *direkt*, det vill säga att dess innehåll avslöjar på ett direkt sätt något av värde. Men data kan även avslöja sådant som inte direkt framgår. Det kan exempelvis ske genom att undersöka vad som är utelämnat eller genom att väga samman olika datamängder. Sådan deriverad information är att betrakta som *indirekt*.

Indirekt information uppkommer primärt i underrättelsecykelns analyssteg. I vissa fall kan den indirekta informationen vara relativt lätt att extrapolera fram, exempelvis att en fastighet invid järnvägen kan vara extra intressant för en angripare om den saknar publik information i fastighetsregistret. Om inte annat kan avsaknaden av publik information vara ett tecken på att det finns relevanta skäl för att den har sekretessbelagts. När det gäller mer subtil eller komplex indirekt information kan det behövas betydligt mer omfattande och komplicerade analyser. Att information fås fram indirekt betyder inte att den är (eller borde vara) sekretessbelagd, då det lika gärna kan handla om information som helt enkelt inte fanns dokumenterad eller sammanställd innan analysen genomfördes.

4 Publika datakällor

I detta kapitel beskrivs publika källor med exempel på data som kan inhämtas från respektive källa. Gränserna mellan olika typer av källor är emellanåt otydliga, men har i praktiken ingen större betydelse för informationsinhämtning. Exempelvis kan öppna data publiceras på webbsidor och öppna källkodsprojekt är ofta tillgängliga via webbsidor som GitHub. Vilken data som är användbar för en antagonist beror till stor del på antagonistens mål och förmågor. I denna studie antas antagonister ha stora förmågor och långsiktiga mål. Vidare antas att sådana antagonister har intresse av att samla in alla möjliga typer av data från alla tillgängliga källor.

Allmänna och offentliga handlingar I princip kan alla typer av data som förvaras eller upprättas hos en myndighet blir *allmänna handlingar*. Vissa undantag finns, såsom säkerhetskopior och minnesanteckningar. Offentlighetsprincipen innebär att vem som helst får läsa *offentliga handlingar*, det vill säga allmänna handlingar som inte omfattas av sekretess. Regleringen av vilka uppgifter som ska beläggas med sekretess görs främst genom offentlighets- och sekretesslagen (SFS 2009:400, 2009). Information som är sekretessbelagd ska inte vara publikt tillgänglig men kan i vissa fall publiceras av tredje part, exempelvis i samband med en dataläcka (se beskrivning längre ner i denna förteckning).

Handlingar som begärs ut kan exempelvis innehålla data om upphandlingar med tekniska kravställningar och leverantörer av olika system. De kan också innehålla direkt användbara data såsom ritningar, kartmaterial, personallistor och tågrörelser. Därtill kan de avslöja information om ägarförhållanden, avsedd användning, externa beroenden, fysiska skyddsåtgärder, banors användning, kontaktuppgifter och mycket mer. Bredden på data som kan återfinnas i offentliga handlingar är mycket stor.

Öppna data Öppna data regleras i den så kallade öppna datalagen.[9] Öppna datalagen reglerar dock inte vilken data som måste tillgängliggöras. *Myndigheten för digital förvaltning* (DIGG) har publicerat vägledningar

[9] Lag (2022:818) om den offentliga sektorns tillgängliggörande av data.

för hantering av öppna och delade data där de bland annat beskriver datamängder som är internationellt prioriterade då de har ett stort värde för vidareutnyttjande. Prioriterade datamängder inkluderar exempelvis:[10]

- Företagsinformation
- Geospatial information
- Transport och infrastruktur, inklusive bredband
- Upphandling och inköp.

Nyhetsartiklar och intervjuer Nyhetsmedia innehåller flera olika typer av data men sällan med någon särskild detaljnivå. Rapporter om incidenter kan ge viss insikt i konsekvenser som inte alltid är triviala att inse. Ett exempel från hösten 2025 är rapporterna om effekterna av att både stambanan och Botniabanan var avstängda vilket medförde att transporter blev fördröjda då de behövde ske via E4:an istället.[11] Ett annat exempel är diskussionen kring Malmbanans vikt för såväl svensk gruvindustri som för Nato och försvaret av Sverige efter en urspårning i december 2023.[12]

Poddar, video och streaming Mycket data kan hämtas från olika plattformar som publicerar video- och ljudinspelningar, såsom YouTube och Spotify. Det kan vara allt från professionella produktioner till korta videosnuttar inspelade av privatpersoner med mobiltelefoner. En svårighet med denna typ av datakälla är att hitta intressanta data då det ofta krävs mer arbete för att identifiera relevant data i en video- eller ljudinspelning.

Många svenska organisationer publicerar eget material på olika plattformar. Trafikverket är ett exempel där Järnvägspodden[13] publiceras på YouTube, Spotify, Apple Podcasts och libsyn.

[10] https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/prioriterade-informationsmangder (besökt 2026-03-24).
[11] https://www.svt.se/nyheter/lokalt/vasterbotten/avskurna-jarnvagar-slar-hart-mot-transportforetag-i-umea (besökt 2026-01-26).
[12] https://www.sverigesradio.se/avsnitt/jarnvagen-ar-sveriges-svaga-lank-i-forsvaret-grans (besökt 2026-03-24).
[13] https://www.trafikverket.se/om-oss/nyheter/trafikverkets-podcasts/jarnvagspodden/ (besökt 2026-01-21).

Akademiska publikationer Akademiska publikationer innehåller ett brett spektrum av ämnen och detaljnivåer. Inom cybersäkerhet har det under lång tid varit populärt att publicera artiklar om kritiska cybersårbarheter med exempel som Heartbleed,[14] Meltdown,[15] och KRACK[16]. Vissa publikationer om sårbarheter och attacker får stor spridning i media och olika forum medan andra kan gå obemärkt förbi då de rapporterar om sårbarheter som på ytan inte verkar vara kritiska.

Webbsidor, webbtjänster och webbarkiv Organisationers webbsidor och webbtjänster kan innehålla användbara data om projekt, produkter, infrastruktur, personal m.m. Program som webcrawlers och liknande kan användas för att extrahera data och identifiera ytterligare webbsidor som kanske inte är medvetet publikt exponerade. Även om webbsidor uppdateras och innehåll försvinner kan det gå att hitta historiskt innehåll via webbarkiv[17] som sparar äldre versioner av webbsidor. Webbtjänster såsom Google Maps kan användas för att skapa sig en uppfattning om exempelvis platser och goegrafiska förhållanden utan behovet av fysiska besök.

Exempel på data från webbsidor kan vara Trafikverkets Järnvägsnätbeskrivning (JNB)[18] och Trafikverkets publicerade information om ett nytt digitalt signalsystem för järnvägen där både det befintliga och det tilltänkta systemet beskrivs[19].

Exponerade gränssnitt och tjänster Ett normalt tillvägagångssätt vid cyberangrepp för att kartlägga system är att skanna exponerade gränssnitt och tjänster. Detta kräver dock interaktion med angriparens mål och kan upptäckas av de som försvarar organisationens nätverk. Inhämtning genom denna typ av gränsytor ligger således i gränslandet mellan OSINT och andra typer av underrättelseinhämtning.

[14] https://www.heartbleed.com/ (besökt 2026-03-12).
[15] https://meltdownattack.com/ (besökt 2026-03-12).
[16] https://www.krackattacks.com (besökt 2026-03-12).
[17] Ett exempel på webbarkiv är https://archive.org (besökt 2026-03-24).
[18] https://bransch.trafikverket.se/for-dig-i-branschen/jarnvag/jarnvagsnatsbeskrivningen-jnb/ (besökt 2026-03-24).
[19] https://bransch.trafikverket.se/for-dig-i-branschen/teknik/ett-nytt-digitalt-signalsystem-for-jarnvagen/sa-fungerar-det-nya-signalsystemet/ (besökt 2026-01-26).

Praktiska exempel på hur angrepp genomförts och hur exponerade gränssnitt nyttjas är incidentrapporter. En aktör som publicerar incidentrapporter är Amerikanska CISA som även publicerar vägledningar (eng. advisories) där de behandlar specifika hot och hotaktörer. I vägledningarna går det bland annat att hitta exempel på kartläggningar som gjorts för att söka efter angreppsvägar (Cybersecurity and Infrastructure Security Agency, 2024).

Djupa och mörka näten Det *djupa nätet* (eng. deep web) och det *mörka nätet* (eng. dark web, darknet) är begrepp som beskriver typer av innehåll på internet. Det djupa nätet kan beskrivas som innehåll som inte är indexerat av sökmotorer och som kan kräva inloggning för att komma åt. Det mörka nätet är typiskt sett krypterat och kräver speciella mjukvaror såsom en TOR-webbläsare för att komma åt. Företaget Crowdstrike har estimerat att cirka 90 % av internet utgörs av de djupa näten medan cirka 6 % utgörs av de mörka näten (Baker, 2025).

Ett exempel som relaterar till svensk infrastruktur är dataintrånget hos Svenska Kraftnät där stulna data publicerades på det mörka nätet.[20] Publicerade data inkluderade bland annat systemuppdateringar, supportfiler och drivrutiner,[21] typer av information som kan användas för att kartlägga informationssystem.

Digitala plattformar med användargenererat innehåll Olika typer av digitala plattformar där användare skapar och delar innehåll, exempelvis sociala medier, bloggar, forum och maillistor, har stor potential att innehålla användbara data för en angripare. Modereringen på digitala plattformar varierar stort och det är ofta upp till användare att själva välja vad de vill publicera och att bedöma trovärdigheten på innehåll de läser.

Digitala plattformar med användargenererat innehåll kan användas för att kartlägga de personer som skriver där, såväl genom vad och hur de skriver som genom att kunna länka en individ till olika konton eller olika sajter. Ett

[20] https://www.svt.se/nyheter/inrikes/hackergruppen-svenska-kraftnats-data-lackt-pa-darknet (besökt 2026-01-21).

[21] https://www.svk.se/sakerhet-och-beredskap/cybersakerhet/samlad-information-om-dataintranget/ (besökt 2026-01-21).

exempel är hur Ross Ulbricht, skaparen av handelsplatsen Silk Road på det mörka nätet, kunde identifieras av FBI.[22]

Ett exempel på potentiellt användbara data är en analys som gjordes av inlägg på forumet StackOverflow där tusentals nycklar och tokens för autentisering mot webbtjänster hittades.[23] Majoriteten av datamängden beskrivs vara oanvändbar för angrepp men det är inte omöjligt att vissa data är användbara i kombination med annan data. Ett annat exempel är användare på datorspelsforum som publicerat militära hemligheter om stridsflygplanet Eurofighter.[24]

Specialiserade databaser och sökmotorer Det finns många typer av specialiserade databaser och sökmotorer där data kan hittas om exempelvis sårbarheter, IP-allokeringar och publikt exponerade enheter. Några exempel på denna typ av tjänster är CVE[25], DB-IP[26] och Shodan[27]. CVE är en databas som publicerar information om kända mjukvarusårbarheter, DB-IP är en sökmotor för att geolokalisera IP-adresser och Shodan är en sökmotor för att hitta internetanslutna enheter. Shodan indexerar många typer av enheter, från vanliga servrar till webbkameror, och används ofta inom akademisk forskning om säkerhet i kritisk infrastruktur. Exempelvis publicerade Kant m. fl. (2020) en artikel om riskerna med att kritisk infrastruktur exponeras på internet där Shodan använts för att hitta exponerade gränssnitt.

Öppna källkodsprojekt Mjukvaror baserade på öppen källkod har en mycket utbredd användning och i flera fall är företag med i utvecklingen av projekten. Öppna källkodsprojekt kan ge flera olika typer av information till en antagonist. Sårbarheter i öppen källkod kan vara en potentiell ingång för antagonister att kartlägga eller påverka IT-system där mjukvaran används. Det förekommer även läckage av exempelvis lösenord och

[22] Fallet med Ulbricht beskrivs i två delar på https://www.wired.com/2015/04/silk-road-1/ och https://www.wired.com/2015/05/silk-road-2/ (besökta 2026-03-24).
[23] https://matan-h.com/analyze-stackoverflow (besökt 2026-03-24).
[24] https://www.ndtv.com/world-news/eurofighter-typhoon-another-military-secret-leaked-on-online-gaming-hub-how-it-was-handled-7330695 (besökt 2026-01-26).
[25] https://www.cve.org/ (besökt 2026-03-24).
[26] https://db-ip.com (besökt 2026-03-24).
[27] https://www.shodan.io (besökt 2026-03-24).

krypteringsnycklar när utvecklare av misstag inkluderar dessa i bidrag till projekten.

Dataläckor Dataläckor kan uppstå genom intrång eller oavsiktlig exponering. Exempelvis kan datadumpar från intrång innehålla en bred mängd data såsom personlig information och lösenord. Datadumpar går att hitta på vanliga internet, exempelvis på webbplatser som pastebin.com och justpaste.com, såväl som på de djupa och mörka näten. Det finns även företag som säljer lösningar för att övervaka sidor där datadumpar publiceras.[28]

Oavsiktliga dataläckor uppstår ofta på grund av säkerhetsbrister. Ett exempel är 1177-läckan där inspelade samtal låg fritt tillgängliga på en server.[29] Fallet involverade flera underleverantörer och berodde på brister i både regelefterlevnad och teknisk implementation.

Grålitteratur Det produceras mängder med rapporter, böcker och andra publikationer från exempelvis tankesmedjor, ideella organisationer, icke-akademiska konferenser och enskilda personer. Dessa publikationer kan innehålla data som är användbara för angripare. Ett bra exempel på grålitteratur är examensarbeten som inhämtar, sammanställer och analyserar information för att besvara en forskningsfråga och dessutom är granskade. Exempelvis publicerades under 2025 ett examensarbete om järnvägens roll för totalförsvaret vid Kungliga Tekniska Högskolan (Kindlund, 2025).

Kommersiella tjänster Det finns otaliga kommersiella tjänster som erbjuder olika typer av data. I vissa fall är det offentliga uppgifter som sammanställs[30] medan det i andra fall är kommersiellt inhämtad data som tillhandhålls. Exempel på kommersiella tjänster är Google Maps[31] och Maxar Intelligence[32].

[28] https://darknetsearch.com/pastebin-leaks (besökt 2026-03-24).
[29] https://www.imy.se/nyheter/granskning-klar-av-1177-incident/ (besökt 2026-01-21).
[30] Till exempel från bolagsregistret (såsom https://www.bolagsfakta.se), inkomstuppgifter (såsom https://ratsit.se), fordonsregistret (såsom https://car.info) och aktuella tågpositioner (såsom https://mobility.portal.geops.io/world.geops.transit). Webbplatserna besöktes 2026-03-26.
[31] https://www.google.com/maps (besökt 2026-03-26).
[32] https://maxarenergysource.com/maxar-intelligence/about.html (besökt 2026-03-26).

> Kommersiella aktörer kan avslöja olämpliga data genom sina tjänster. Ett exempel är fitnessappen Strava som registrerar användarnas motionsrundor och publicerar dem på en så kallad heatmap. Genom denna funktion visade Strava tydligt lokalisering och utformning av USA:s militärbaser i exempelvis Syrien och Afghanistan.[33] Detta verkar ha upprepats igen när positionen för ett franskt hangarfartyg avslöjades genom Strava i mars 2026.[34]

Källorna som tagits upp i detta kapitel tillåter oftast inhämtning över internet. I de flesta fall behöver en antagonist inte besöka specifika fysiska platser eller ange sin identitet för att komma åt data. I fallet med offentliga handlingar bryter det i de flesta fall mot grundlagen om myndigheten som ska lämna ut handlingen efterforskar vem som begärt ut den (SFS 1949:105, 1949, kap 2, 18 §). I många fall är det också möjligt att inhämta publikt tillgängliga data genom att fysiskt besöka platser eller prata med personer utan att det är illegalt eller att beteendet kan anses tveksamt eller misstänkt.

[33] https://www.mapulus.com/blog/strava-fitness-tracker-military-secrets-location-data (besökt 2026-03-24).

[34] https://www.msn.com/en-us/technology/software/this-strava-privacy-setting-just-reportedly-exposed-the-location-of-a-french-warship-here-s-how-to-turn-it-off/ar-AA1Zfzzz (besökt 2026-03-25).

5 Bearbetning och analys

Inhämtning av data från publika informationskällor kan snabbt resultera i stora mängder data av olika typ och i olika format. Efterföljande bearbetning och analys av informationen är en komplex och tidskrävande uppgift som ställer stora krav på personalen. I en forskningsartikel beskriver Keliris m. fl. (2019) ett exempel på manuell modellering av ett kraftförsörjningssystem baserat på publika data där ett moment med geografisk kartläggning tog 40 mantimmar. Bedömningar medför också en risk att påverkas av kognitiv bias, vilket kan leda till inkonsekventa bedömningar när flera personer är inblandade.

Detta kapitel beskriver tekniker och metoder som kan användas för att automatisera och systematisera analys av publika data. Kapitlet är inte uttömmande utan ska ses som en startpunkt för vidare utforskning.

5.1 Teknik och verktygsstöd

Det finns många moment i OSINT-processen som är möjliga att automatisera på olika sätt. Automatiserad inhämtning över internet har förekommit under lång tid genom användning av exempelvis spindlar (eng. web crawlers) och exponerade gränssnitt. I ett FOI-memo om datadriven analys av webbdata delas nödvändiga förutsättningar in i tre kategorier: infrastruktur, stödverktyg och kompetens (Rosell, 2019). Infrastruktur handlar framförallt om resurser för lagring och beräkningar, men också sätt att strukturera data. Stödverktyg berör stöd till analytiker för att analysera inhämtade data medan kompetens handlar om personalens förmåga att kunna nyttja verktyg och teknik. Dessa förutsättningar är rimligen också relevanta för analys av andra typer av publika data än webbdata. Teknikutvecklingen håller högt tempo och mängder med tekniker och lösningar är tillämpbara för att hantera och analysera publika data. Två exempel är så kallad big data och artificiell intelligens (AI).

Big data och relaterade tekniker för hantering av storskaliga, komplexa och heterogena datamängder (Rao m. fl., 2019) är i många fall en förutsättning för att automatisera analyssteget. Ett exempel på relaterade tekniker är datasjöar (eng.

data lakes) som introducerats för att hantera strukturerade och ostrukturerade data samt bemöta problem som uppstår med big data (Hai m. fl., 2023). Andra närliggande tekniker inkluderar stora datasjöar (Cuzzocrea, 2021), datadammar (Sawadogo & Darmont, 2021), ETL[35] (Simitsis m. fl., 2023) och datavirtualisering (Bogdanov m. fl., 2020).

Användningen av AI inom OSINT har utforskats under längre tid. Browne m. fl. (2024) presenterar en genomgång av forskning om AI i OSINT-applikationer mellan 2011 och 2021. I artikeln ger de exempel på forskning om AI och maskininlärning inom de olika OSINT-faserna. Det förekommer mycket forskning och utveckling av verktyg som nyttjar AI, men det fanns också tydliga begränsningar i forskningen som undersöktes. Exempelvis är forskningen begränsad i hur många informationskällor som används och hur praktiskt användbara forskningsresultaten är. Precis som för hanteringen av stora datamängder finns det ett stort antal tekniker och verktyg som kan användas för att analysera data. Baserat på utvecklingen inom AI under senaste åren (Raza m. fl., 2025) är det troligt att AI fortsätter att utvecklas och tillämpas inom flera användningsområden. Akademiska litteraturgenomgångar tyder dock på att det finns outforskade områden i överlappet mellan OSINT och AI (Browne m. fl., 2024; Evangelista m. fl., 2021).

5.2 Metoder för informationsbedömning

Informationsbedömning är en aktivitet som ställer stora krav på de individer som genomför analys och värdering av information. Klassificering av tillgångar och information är vanligt förekommande inom informationssäkerhetsområdet och väletablerade metoder existerar (Andersson, 2023). När data indirekt relaterar till identifierade tillgångar blir det svårare att bedöma betydelsen och i förlängningen klassificeringen av specifika data. Bergström m. fl. (2021) beskriver en metod för generell informationsklassificering utifrån krav på bland annat granularitet och anpassningsbarhet. Metoden baseras bland annat på information inhämtade från representanter för svenska myndigheter och får således med perspektivet med offentlighets- och sekretesslagen.

[35] ETL är akronym för Extration-Transformation-Loading och omfattar metoder och teknik för hur data extraheras, transformeras och laddas in i en lagringslösning, exempelvis en datasjö.

Inom underrättelseområdet förekommer mycket forskning om hur information analyseras och bedöms. Ett vanligt begrepp för metoder som används är strukturerade analystekniker (eng. structured analytic techniques). Teknikerna handlar huvudsakligen om tankesätt för att externalisera, organisera och evaluera analytisk tänkande (Chang m. fl., 2018). Det finns flera typer av strukturerade analystekniker och de kan grupperas på flera olika sätt. Grunt (2019) beskriver flera olika taxonomier för strukturerade analystekniker, där tekniker grupperas i kategorier såsom visualiserande och konträra. Ett av målen med teknikerna är att antaganden och kognitiv bias inte automatiskt accepteras utan explicit utvärderas som en del av analysprocessen.

I ett forskningsprojekt med FOI och Lantmäteriet utforskades riskerna med öppna geodata (Davidsson m. fl., 2025b). Syftet med projektet var att ”utveckla en metod för att kunna bedöma vilka risker för Sveriges säkerhet som kan uppstå vid tillgängliggörande av geodata som öppna data”. Ett resultat från projektet var ett utkast på metod för riskbedömning som bestod av sex steg:

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

Metoden i sig är relativt lik andra riskbedömningsmetoder, men en nytänkande ansats i projektet var användningen av begreppet relevans i riskbedömningarna. Relevans är tänkt att användas istället för sannolikhet för att förstå varför en viss information bidrar till att en konsekvens kan realiseras.

6 Diskussion

Det är en mycket komplex uppgift att undersöka hur tillgången till publika data kan påverka skyddet av information som omfattas av sekretess eller säkerhetsskydd. Förenklat går problemet som ska besvaras att uttrycka med tre frågor: ”Är den samlade informationen farlig?”, På vilket sätt är informationen farlig?öch ”Vad är det som gör informationen farlig?Frågorna har dock en bedräglig enkelhet, då den samlade mängden information som bedömaren behöver ta hänsyn till kan vara extremt stor och spretig samtidigt som de potentiella riskerna kan vara mycket svåra att inse.

Detta kapitel tar upp en diskussion kring några ytterligare perspektiv på problembilden och hur arbetet i denna rapport kan tas vidare i ett framtida forskningsprojekt.

6.1 Riskbedömning

I praktiken är det inte alltid uppenbart för en försvarare vilken information som kan vara användbar för en antagonist. Det är uppenbart att viss information kan nyttjas av antagonister och därmed omfattas av sekretess på grund av dess innehåll, exempelvis när den berör kritiska detaljer kring säkerhets- och bevakningsåtgärder[36]. Annan information kan vara mycket mer subtil i sin relation till sekretessbelagda uppgifter när den inte uppenbart avslöjar något som kan användas av en antagonist.

Om hänsyn tas till övrig information som redan finns tillgänglig blir en riskbedömning desto mer komplicerad. Öppna datalagen är tydlig i att tillgängliggörande av data ska ta hänsyn till krav på informationssäkerhet och risker för Sveriges säkerhet,[37] men beskriver inte hur det bör gå till i praktiken. Exempelvis framgår inte i vilken utsträckning som hänsyn behöver tas till andra publikt tillgängliga data eller hur långt analysen behöver tas för att eliminera allt

[36] Säkerhets- och bevakningsåtgärder omfattas av sekretess enligt 18 kap. 8 § offentlighets och sekretesslagen (2009:400) om det kan antas att syftet med åtgärden motverkas om uppgiften röjs.
[37] Lag (2022:818) om den offentliga sektorns tillgängliggörande av data, 2 kap. 1 §.

mer obskyra eller subtila risker för Sveriges säkerhet. Det finns rimligen en gräns för när riskanalysarbetet inte längre ger tillräcklig mereffekt för att motivera fortsatt arbete. Ytterligare en aspekt att ta hänsyn till är att riskbedömningar kan påverkas av kognitiv bias, vilket påverkar kvaliteten på arbetet.

Vägledningen om tillgängliggörande av data från Myndigheten för digital förvaltning belyser specifikt att särskilda risker med att information kombineras eller samlas ihop", så kallad aggregering, ska beaktas.[38] Problemet med aggregering är framförallt att kombinering av olika data kan leda till att ny information uppstår som inte är möjlig att härleda utifrån data från enbart en datakälla. Dessutom tillkommer och föråldras information ständigt, vilket gör att tidsperspektivet är en försvårande faktor när risker ska bedömas. Antagonister med långa tidsperspektiv kan samla på sig stora mängder data över längre tid, vilket möjliggör djup kartläggning av en verksamhet. Aggregering av datamängder har beskrivits som ett särskilt allvarligt problem för öppna geodata (Winterdahl m. fl., 2023).

Sammantaget ställs stora krav på analysförmåga och kunskap hos de som gör riskbedömningar. Det är osannolikt att en enskild individ kan inhämta, analysera och bedöma alla tillgängliga data som en antagonist har tillgång till och systematiskt härleda risker från insamlade data. Högst sannolikt behövs metoder, processer och verktyg som är anpassade för bedömning av publika data för att effektivt och systematiskt kunna bearbeta data och genomföra riskbedömningar.

6.2 Andra underrättelsemetoder

Främmande makt – speciellt de mer resursstarka staterna – förväntas använda mer långtgående underrättelsemetoder utöver OSINT i sina operationer. Ett första, icke-offensivt lager av underrättelseinhämtning utgörs av inhämtning via egna eller allierades kanaler. Det kan exempelvis handla om bilddata från egna satelliter eller kommunikation som fångats upp genom passiv signalspaning. Därutöver finns de mer långtgående metoderna såsom dataintrång, rekrytering av nyckelpersoner och fysiskt spioneri.

[38] https://www.digg.se/kunskap-och-stod/oppna-och-delade-data/vagledning-for-att-tillgangliggora-information (besökt 2026-12-16).

Även om kvalificerade hotaktörer kan förväntas använda mer långtgående underrättelsemetoder behöver sekretessen kring data bedömas och hanteras korrekt. Mer riktade eller offensiva metoder har naturligtvis potential att ge underrättelser med högre värde, exempelvis genom att de ger direkt tillgång till sekretessklassificerat material eller andra uppgifter som inte vanligtvis sprids publikt. Sådana metoder för dock i regel med sig ökad kostnad och ökad risk för upptäckt, vilket innebär att det är fördelaktigt för antagonisten om denne kan uppnå sina underrättelsemål genom OSINT. Mindre kvalificerade hotaktörer har inte heller möjlighet att genomföra komplex och offensiv underrättelseverksamhet i samma skala, vilket gör att det relativa värdet av OSINT kan vara högre för dem. Därtill finns andra hotaktörer, såsom kriminella och aktivister, som till stor del saknar förutsättningar för mer långtgående underrättelseinhämtning.

6.3 Etiska perspektiv

En viktig skillnad mellan främmande makts underrättelseverksamhet och ett eget förebyggande arbete är hanteringen av etiska hänsyn. En underrättelsetjänst hindras knappast av etiska hänsyn i ett skarpt läge.

Insamling av data från publika källor innebär rimligtvis inte några större etiska problem i de flesta fall. Problem kan dock uppstå när det gäller insamling och hantering av persondata eller när inhämtningen sker på ett sådant sätt att enskilda individer eller sårbara grupper kan utsättas för olämplig behandling.

6.3.1 Verksamheternas arbete

I en verksamhets egna analysarbete kring att förstå påverkan från publika data kan det uppstå etiska dilemman, exempelvis om arbetsscheman för personal eller hur en person med speciell behörighet förflyttar sig kan bidra till information om säkerhetskänslig verksamhet. Det finns lagar som begränsar en organisations rätt att behandla information om enskilda personer, exempelvis GDPR (Direktiv 2019/1024, 2016) och dataskyddslagen (SFS 2018:218, 2018). Därtill kan bearbetning av data exempelvis innebära att personalen känner sig övervakade eller att de upplever att deras frihet begränsas, även om datainsamlingen ändå skulle

skett av andra skäl. Det finns således anledning för verksamheterna att kritiskt reflektera över vilka effekter insamling, bearbetning och analys kan få.

6.3.2 Forskningsetik

Ur ett forskningsetiskt perspektiv gäller *lag (2003:460) om etikprövning av forskning som avser människor*, där 3–4 § anger när den är applicerbar. Här återges de delar av paragraferna som är mest relevanta i denna kontext:

> 3 § Denna lag ska tillämpas på forskning som innefattar behandling av
>
> 1. personuppgifter som avses i artikel 9.1 i EU:s dataskyddsförordning (känsliga personuppgifter) [...]
>
> 4 § Utöver vad som följer av 3 § ska lagen tillämpas på forskning som
>
> 1. innebär ett fysiskt ingrepp på en forskningsperson,
>
> 2. utförs enligt en metod som syftar till att påverka forskningspersonen fysiskt eller psykiskt eller som innebär en uppenbar risk att skada forskningspersonen fysiskt eller psykiskt [...] (SFS 2003:460, 2003)

I ett framtida forskningsprojekt bör denna aspekt vara relativt lätt att hantera, exempelvis genom att helt enkelt avgränsa bort den typen av inhämtning och data som skulle falla under lagens definition vid eventuella fallstudier. Den typen av data kan istället tas med genom fingerade men representativa data för fiktiva personer.

6.4 Juridiska perspektiv

Lagstiftningen är komplex kring bland annat sekretess, säkerhetsskydd, dataskydd och offentlighet. Det finns dessutom många lagar och regleringar som i åtskilliga fall är motstridiga eller åtminstone drar åt olika håll. Ett exempel är öppna datalagen som säger att data ska tillgängliggöras ”under förutsättning att krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och att det inte innebär risker för Sveriges säkerhet”(SFS 2022:818, 2022, 2 kap. 1§).

Samtidigt är det långt ifrån säkert att det finns en tillämplig sekretessparagraf i offentlighets- och sekretesslagen (SFS 2009:400, 2009) som är applicerbar för att kunna sekretessbelägga data. Om data är att betrakta som en offentlig handling enligt tryckfrihetsförordningen SFS 1949:105 (1949) ska den därmed vara offentlig.

I vissa fall finns det en klar rangordning mellan lagarna, men så är inte alltid fallet. Därtill är det ibland oklart hur avvägningar mellan olika intressen ska göras, till exempel när det gäller publicering som öppna data kontra att säkerställa olika skyddsperspektiv. Citatet från öppna datalagen som återges ovan är ett exempel där en sådan avvägning behöver göras.

Det framgår inte hur långt en berörd organisation måste gå för att säkerställa att skyddet upprätthålls. Hur ska låggradiga säkerhetsrisker vägas mot en alltför restriktiv hållning till publicering av öppna data eller att allmänna handlingar sekretessbeläggs i onödan? Avvägningen mellan säkerhet och öppenhet är så pass svår att en uttömmande utredning av varje fall skulle ta mycket stora resurser i anspråk. Avvägningen om var gränsen går för när öppna data innebär risker för Sveriges säkerhet är inte prövad juridiskt när denna text skrivs, vilket innebär att det saknas prejudikat för detta. Här behöver troligtvis domstolarna eller lagstiftarna komma med någon slags riktlinje för hur avvägningen ska genomföras och dokumenteras för att den juridiskt sett ska kunna anses vara korrekt utförd. Även om riskbedömningarna huvudsakligen är ett informationssäkerhetsproblem så är de juridiska perspektiven högst relevanta för att kunna göra en korrekt bedömning som även tar rimlig hänsyn till andra intressen och behov.

6.5 Framtida forskning

Som rapporten har visat så finns ett stort antal områden som behöver undersökas vidare för att åstadkomma god kunskap och välfungerande metoder för att bedöma hur publika data påverkar sekretess och säkerhetsskydd. Det finns redan genomförd forskning inom vissa av områdena, men den är långt ifrån heltäckande och behöver därmed kompletteras med ny forskning. Detta avsnitt tar upp några av de forskningsområden som bör vara aktuella för ett fortsättningsprojekt.

6.5.1 Datamängdernas omfattning

Ett högst relevant forskningsområde är att undersöka vilka data som faktiskt går att hitta i publika datamängder samt vilken omfattning dessa data har. Denna fråga är viktig för att kunna ge förståelse för bredden och djupet i befintlig och potentiellt tillkommande publika data. En djupare förståelse för publika data innebär möjlighet att gå vidare för att undersöka hur denna kan bearbetas och analyseras för att i förlängningen även kunna förstå vilken typ och nivå av påverkan som publika data kan ge.

Ett lämpligt tillvägagångssätt för denna forskningsfråga är genom litteraturstudier och systematisk kartläggning av datakällor för att ta fram en slags karta över möjliga datamängder. Därefter genomförs en eller flera fallstudier där specifikt avgränsade fall undersöks på djupet för att få konkreta exempel på omfattningen av tillgängliga publika data och deras innehåll.

6.5.2 Tekniker för komplexa analyser

De senaste åren har inneburit en enorm utveckling av tekniker för att sammanställa, analysera och dra slutsatser ur stora, komplexa och heterogena datamängder. Big data och AI innebär helt nya sätt att hantera dessa datamängder. Samtidigt är teknikerna inte uppenbara när det gäller vad de kan åstadkomma eller i vissa fall ens hur de åstadkommer de resultat de ger. Teknikutvecklingen går fortsatt framåt med hög hastighet vilket innebär att forskning på teknikens följdverkningar behöver hänga med i utvecklingen. Detta område innebär sannolikt ett fokus på kontinuerlig omvärldsbevakning för att förstå nya eller förbättrade analystekniker, automationer och beslutsstöd. Att ta fram egna tekniker vore troligtvis en alltför omfattande och komplex väg att gå.

Lämpliga tillvägagångssätt är kontinuerliga eller återkommande litteraturstudier och marknadsöversikter för att fånga upp och förstå nya eller vidareutvecklade tekniker samt deras möjligheter. Lovande tekniker kan – om praktiskt möjligt – användas för att analysera data från fallstudierna som nämns i avsnitt 6.5.1.

6.5.3 Riskbedömningsmetodik

Riskbedömningar som genomförs i samband med exempelvis publicering av öppna data eller sekretessbedömning av offentliga handlingar kan i vissa fall bli mycket svåra, speciellt när den berörda informationen potentiellt kan påverka säkerheten långt bortom verksamhetens eller organisationens egna gränser. För att göra sådana riskbedömningar på ett effektivt och konsekvent sätt och samtidigt ta hänsyn till påverkan från publika data behövs en välgrundad metodik. Det finns många tidigare arbeten inom riskbedömningsmetodik, men de flesta tycks endast omhänderta relativt enkla eller lokalt bedömningsbara faktorer. Metoden som togs fram av Davidsson m. fl. (2025a) är ett exempel där metoden utvecklats för att ta hänsyn till komplicerade och svåröverblickade relationer mellan stora datamängder. Den metoden är dock fokuserad på risker som kan uppstå för Sveriges säkerhet vid publicering av öppna geodata, vilket innebär att den inte nödvändigtvis är applicerbar för andra områden.

Tillvägagångssättet för att vidareutveckla riskbedömningsmetodiken bör sannolikt bestå av flera steg: Först en litteraturstudie för att undersöka och sammanställa befintliga metoder, med fokus på de som hanterar komplexa relationer mellan olika potentiella riskfaktorer. Därefter kan en utveckling av en uppdaterad metod genomföras centrerat kring exempelvis workshoppar och fallstudier.

6.5.4 Kompetensbehov inför riskbedömningar

Att riskbedömningar som berörs av påverkan från publika data kan bli komplexa står utom tvivel, exempelvis genom det arbete som Davidsson m. fl. (2025a) har genomfört. Personer som deltar i sådana riskbedömningar behöver kompetens inom flera områden, men det är inte uppenbart exakt vilka kompetensbehov som föreligger. Ett forskningsområde är således att undersöka kunskaps- och kompetensbehovet för att kunna genomföra väl förankrade och realistiska riskbedömningar.

Det är i regel komplicerat att undersöka kompetensbehov då de inblandade i många fall inte själva är helt medvetna om vilka kunskaper och kompetenser de saknar. Det kommer därför troligtvis att krävas en kombination av flera forskningsmetoder för att nå bra resultat inom området. Det kan exempelvis

handla om litteraturstudier och översikter för att sammanställa vilka kompetensområden som verkar relevanta, enkäter för att kartlägga befintliga kompetenser samt workshoppar för att fånga upp nya eller okända kompetensområden.

6.5.5 Juridiska perspektiv

Det finns flera områden där de juridiska aspekterna kan få en signifikant praktisk inverkan. Ett sådant område är riskbedömningar och avvägningar vid exempelvis publicering av öppna data eller sekretessbedömning för offentliga handlingar. Det finns omfattande, komplexa och bitvis motstridiga lagar och intressen som behöver hanteras i samband med både egen datainsamling och vid riskbedömningar. De juridiska perspektiven behöver en genomlysning genom forskningen för att bättre kunna förstå och tillämpa regelverken i processer och praktik. Det kan exempelvis handla om att bättre förstå praxis och lagstiftarens intentioner bakom lagarna samt relationerna mellan olika regelverk.

7 Slutsats

Mängden publika data som har potential att tillsammans avslöja sårbarheter är i praktiken oöverskådlig. Bedömningen av om det medför risk att publicera data – oavsett om det sker som öppna data eller på andra sätt – kan därför vara mycket svår att göra med hög grad av säkerhet. För myndigheter ska bedömningen också ta hänsyn till offentlighetsprincipen, vilket kan innebära att risker med att publicera data behöver accepteras om det inte tydligt går att motivera varför de bör omfattas av sekretess.

Kartläggning av samhällskritiska infrastrukturer, såsom järnvägssystemet, är i praktiken en form av underrättelsearbete oavsett om den görs av en underrättelsetjänst eller av en annan organisation. Förståelse för underrättelsearbete och de metoder som används där är därmed relevanta när en organisation som Trafikverket vill ta reda på vilka publika data som finns tillgängliga och vilken information data kan ge.

Fortsatta studier inom området behöver täcka in ett brett spektrum av forskningsfrågor och kräver en kombination av olika forskningsmetoder för att täcka in den omfattande problembild som området innebär. Litteraturstudier, fallstudier och workshops är några av de metoder som kan vara aktuella i ett framtida forskningsprojekt för att bygga vidare på det arbete som presenteras i denna rapport.

Referenser

Andersson, S. (2023). Problems in information classification: insights from practice. *Information & Computer Security*, *31*(4), 449–462. https://doi.org/10.1108/ICS-10-2022-0163

Baker, K. (2025). The dark web explained. *Crowdstrike*. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web/

Bergström, E., Karlsson, F., & Åhlfeldt, R.-M. (2021). Developing an information classification method. *Information & Computer Security*, *29*(2), 209–239. https://doi.org/10.1108/ICS-07-2020-0110

Bogdanov, A., Degtyarev, A., Shchegoleva, N., Korkhov, V., & Khvatov, V. (2020). Big data virtualization: Why and how. *CEUR Workshop Proceedings (2679)*, 11–21.

Browne, T. O., Abedin, M., & Chowdhury, M. J. M. (2024). A systematic review on research utilising artificial intelligence for open source intelligence (OSINT) applications. *International Journal of Information Security*, *23*(4), 2911–2938. https://doi.org/10.1007/s10207-024-00868-2

Chairman of the Joint Chiefs of Staff. (2013). Joint Publication 2-0, Joint Intelligence.

Chang, W., Berdini, E., Mandel, D. R., & Tetlock, P. E. (2018). Restructuring structured analytic techniques in intelligence. *Intelligence and National Security*, *33*(3), 337–356. https://doi.org/10.1080/02684527.2017.1400230

Cuzzocrea, A. (2021). Big data lakes: models, frameworks, and techniques. *2021 IEEE International Conference on Big Data and Smart Computing (BigComp)*, 1–4. https://doi.org/10.1109/BigComp51126.2021.00010

Cybersecurity and Infrastructure Security Agency. (2024). Enhancing Cyber Resilience: Insights from CISA Red Team Assessment of a U.S. Critical Infrastructure Sector Organization.

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

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

Direktiv 2019/1024. (2016). Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32016R0679

Direktiv 2019/1024. (2019). Europaparlamentets och rådets direktiv (EU) 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn (omarbetning). https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX:32019L1024

Evangelista, J. R. G., Sassi, R. J., Romero, M., & Napolitano, D. (2021). Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. *Journal of Applied Security Research*, *16*(3), 345–369. https://doi.org/10.1080/19361610.2020.1761737

Försvarsmakten. (2022). *Reglemente Underrättelsetjänst* (Nr M7739-352152). Försvarsmakten.

Försvarsmakten. (2025a). Must årsöversikt 2024.

Försvarsmakten. (2025b). Yttrande över Trafikverkets förslag till nationell plan för transportinfrastrukturen 2026–2037.

Grunt, P. (2019). Structured Analytic Techniques: Taxonomy and Technique Selection for Information and Intelligence Analysis Practitioners. *Journal of Management and Financial Sciences*, (30), 115–136. https://doi.org/10.33119/jmfs.2017.30.7

Hai, R., Koutras, C., Quix, C., & Jarke, M. (2023). Data lakes: A survey of functions and systems. *IEEE Transactions on Knowledge and Data Engineering*, *35*(12), 12571–12590. https://doi.org/10.1109/TKDE.2023.3270101

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*(1), 80.

Kant, D., Creutzburg, R., & Johannsen, A. (2020). Investigation of risks for critical infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan. *Electronic Imaging*, *32*, 1–16.

Keliris, A., Konstantinou, C., Sazos, M., & Maniatakos, M. (2019). Open source intelligence for energy sector cyberattacks. I *Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies* (s. 261–281). Springer.

Kindlund, A. (2025). *Järnvägens betydelse för totalförsvaret i kris och krig: Så blir norra Sveriges järnväg mer robust och motståndskraftig* [examensuppsats, Kungliga Tekniska Högskolan].

Lowenthal, M. M. (2026). *Intelligence – From secrets to policy, 10th edition*. Sage & CQ Press.

Prop. 2024/25:34. (2024). Totalförsvaret 2025–-2030. https://www.regeringen.se/rattsliga-dokument/proposition/2024/10/prop.-20242534

Rao, T. R., Mitra, P., Bhatt, R., & Goswami, A. (2019). The big data system, components, tools, and technologies: a survey. *Knowledge and Information Systems*, *60*(3), 1165–1245. https://doi.org/10.1007/s10115-018-1248-0

Raza, M., Jahangir, Z., Riaz, M. B., Saeed, M. J., & Sattar, M. A. (2025). Industrial applications of large language models. *Scientific Reports*, *15*(1), 13755. https://doi.org/10.1038/s41598-025-98483-1

Rosell, M. (2019). *Förutsättningar för datadriven underrättelseanalys baserad på webbdata* (FOI Memo 6955). Totalförsvarets forskningsinstitut.

Rowley, J. (2007). The wisdom hierarchy: representations of the DIKW hierarchy. *Journal of Information Science*, *33*(2), 163–180. https://doi.org/10.1177/0165551506070706

Sawadogo, P., & Darmont, J. (2021). On data lake architectures and metadata management. *Journal of Intelligent Information Systems*, *56*(1), 97–120. https://doi.org/10.1007/s10844-020-00608-7

SFS 1949:105. (1949). Tryckfrihetsförordning. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/tryckfrihetsforordning-1949105_sfs-1949-105/

SFS 2003:460. (2003). Lag om etikprövning av forskning som avser människor. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-

forfattningssamling/lag-2003460-om-etikprovning-av-forskning-som_sfs-2003-460/
SFS 2009:400. (2009). Offentlighets- och sekretesslag. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/offentlighets-och-sekretesslag-2009400_sfs-2009-400/
SFS 2018:218. (2018). Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218/
SFS 2022:818. (2022). Lag om den offentliga sektorns tillgängliggörande av data. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-2022818-om-den-offentliga-sektorns_sfs-2022-818/
Simitsis, A., Skiadopoulos, S., & Vassiliadis, P. (2023). The history, present, and future of ETL technology. *DOLAP*, 3–12.
Säkerhetspolisen. (2025). Säkerhetspolisen 2024 – 2025.
Trafikanalys. (2024). Bantrafik 2024. https://www.trafa.se/globalassets/statistik/bantrafik/bantrafik/2024/bantrafik-2024.pdf
Trafikverket. (2025a). Järnvägsnätsbeskrivning 2027. https://bransch.trafikverket.se/for-dig-i-branschen/jarnvag/jarnvagsnatsbeskrivningen-jnb/jarnvagsnatsbeskrivning-2027/
Trafikverket. (2025b). Öppen antagonistisk hotbild mot transportsektorn – November 2025. https://trafikverket.diva-portal.org/smash/get/diva2:2017307/FULLTEXT02.pdf
U.S. Army. (2023). Intelligence (FM 2-0).
U.S. Department of the Air Force. (2021). Air Force doctrine publication 3-60: Targeting.
Winterdahl, M., Mittermaier, E., Severin, M., During, C., & Gunnarson, C. (2023). *Möjliga hot och risker rörande öppna geodata – Redovisning av arbete i en förstudie* (FOI Memo 8296). Totalförsvarets forskningsinstitut.

ISSN 1650-1942