FOI MEMO

Projekt
Risk- och sårbarhetsfrågor kring öppna geodata – En förstudie

Projektnummer
E13888

Uppdragsgivare
Lantmäteriet

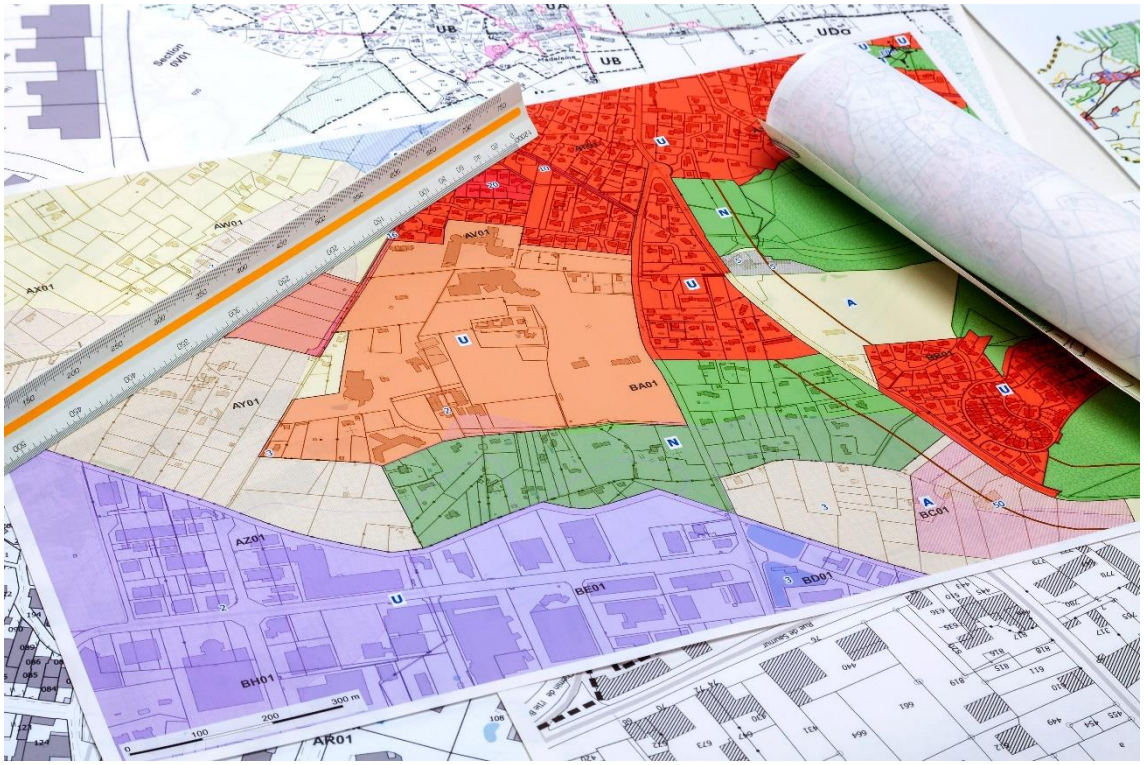
FoT-område
Inget FoT-område

Författare
Mathias Winterdahl, Cecilia During, Eva Mittermaier, Minna Severin och Carina Gunnarson

Datum
2023-11-20

Memo nummer
FOI Memo 8296

Möjliga hot och risker rörande öppna geodata – Redovisning av arbete i en förstudie



Titel
Möjliga hot och risker rörande öppna geodata – Redovisning av arbete i en förstudie

Memo nummer
FOI Memo 8296

Innehållsförteckning

1 Sammanfattning

Med öppna datalagen (2022:818), som genomför EU:s öppna data-direktiv, uppmanas offentliga aktörer att tillgängliggöra sina data, med särskild betoning på geografiska data (geodata), för fritt vidareutnyttjande som så kallade öppna data. Både lagen och direktivet uppmanar aktörerna att beakta säkerhetsmässiga risker innan data tillgängliggörs. Med tanke på de oöverskådliga möjligheterna att aggregera, det vill säga sammanställa och kombinera, olika data är det oklart hur sådana riskbedömningar och identifiering av skyddsvärda data ska göras. Lantmäteriet har därför gett FOI i uppdrag att i en förstudie identifiera potentiella hot och risker som orsakas eller underlättas av en öppen tillgång till offentliga aktörers, med betoning på Lantmäteriets, geodata.

Baserat på en workshop med representanter från Lantmäteriet och FOI har sex typhändelser identifierats vilka sammanfattar ett antal potentiella hot och risker med att fritt tillgängliggöra offentliga aktörers geodata. Det finns tre olika kategorier av orsaker till dessa hot och risker.

- Den stora och lättillgängliga mängden öppna data underlättar för olika hotaktörer att uppnå sina mål vilket kan äventyra allmän och nationell säkerhet.
- Offentliga aktörers öppna geodata tillåter avancerade rumsliga analyser som skulle ha varit mer komplicerade, eller till och med omöjliga, att utföra i frånvaron av dessa geodata.
- Öppna geodata kan aggregeras med andra öppna eller icke-öppna data samt data som inhämtas av hotaktörerna själva.

Aggregeringen av olika datamängder är ett särskilt allvarligt problem då det kan medföra att data som var för sig inte betraktas som skyddsvärda blir en säkerhetsrisk när de kombineras. Varje offentlig aktör gör idag sekretessbedömning och informationsklassning av sina data individuellt. Det är dock oklart om aktörerna har förmåga och resurser att överblicka alla de möjligheter till aggregering av data, och potentiella hot och risker orsakade av sådan aggregering, som möjliggörs genom öppna data-direktivet och den allmänna tekniska utvecklingen. För att kunna hantera de risker som aggregering kan ge upphov till bör offentliga aktörer göra löpande riskbedömningar i samverkan.

2 Introduktion

2.1 Inledning

Idag är geografiska data (geodata) oundgänglig information i både offentliga och privata verksamheter såsom samhällsplanering, trafikplanering, miljöövervakning och planering av nya mobila telefon- och datanät (de Smith m.fl., 2007, 2021). Dessutom har geodata en betydelsefull roll i många innovationer i form av mobila applikationer, självkörande fordon och navigationstjänster. Det finns uppskattningar som tyder på att åtminstone 60 % av all existerande information är knuten till en geografisk position men eftersom positionsbaserad teknik som GPS integreras i allt fler produkter är det troligt att denna andel kommer att öka i framtiden (Hahmann & Burghardt, 2013; UN-GGIM, 2020). Även inom underrättelseverksamheter har man insett värdet av geodata. I USA betraktas inhämtande och analys av geodata till och med som en särskild underrättelsemetod under den engelska beteckningen *geospatial intelligence* (GEOINT) analogt med andra underrättelsemetoder såsom signalspaning (SIGINT) och inhämtning via öppna källor (OSINT) eller mänskliga uppgiftslämnare (HUMINT) (Baber, 2018; Clarke, 2020).

Geodata inbegriper alla data som är knutna till en geografisk position och relaterar därför till specifika punkter, sträckor eller områden på jordens yta. De kan symbolisera både fysiska objekt och administrativa enheter som byggnader, personers eller fordons rörelser, fastigheter, sjöar, vattendrag och kommuner. Vanligen består geodata emellertid av annan information än endast position och utsträckning och kan exempelvis representera jordarter, vegetationstyper och befolkningstäthet för ett geografiskt område eller beskriva den verksamhet som bedrivs i området. Geodata kan även utgöra avbildningar av jordytan i form av bilder eller topografisk representation. Dessutom kan icke-geografiska data ofta knytas till geodata. Till exempel är Statistiska centralbyråns (SCB) befolkningsstatistik sammanställd per regionala och demografiska statistikområden vilka lätt kan kombineras med geodata.

För att främja användningen och spridningen av geodata som produceras av offentliga aktörer har EU:s medlemsländer antagit *Europaparlamentets och rådets direktiv (EU) nr. 2019/1024 av den 20 juni 2019 om öppna data och vidareutnyttjande av information från den offentliga sektorn,* även kallat öppna data-direktivet. Genom direktivet vill man uppmuntra öppet tillgängliggörande av data från offentliga aktörer såvida det inte utgör risk för allmän eller nationell säkerhet eller att skydd för personuppgifter äventyras. För att utreda vilka risker som tillgängliggörandet av myndighetens geodata innebär har Lantmäteriet gett Totalförsvarets forskningsinstitut (FOI) i uppdrag att genomföra en förstudie för att identifiera möjliga hot och risker som kan orsakas eller underlättas av den ökade tillgången på öppna geodata vid införandet av öppna data-direktivet och efterföljande svensk lagstiftning.

2.2 Bakgrund

Den 1 augusti 2022 trädde *lagen* (2022:818) *om den offentliga sektorns tillgängliggörande av data,* hädanefter benämnd öppna datalagen, i kraft och genomför därmed öppna data-direktivet. Lagens syfte är i enlighet med direktivet att ”främja den offentliga sektorns tillgängliggörande av data för vidareutnyttjande” (1 kap. 1 §) så länge det inte medför risker för Sveriges säkerhet, allmän säkerhet och informationssäkerhet eller för att personliga uppgifter röjs.

Öppna data-direktivet är tillämpligt på alla typer av handlingar som framställs av offentliga aktörer och syftar utöver digitala data på exempelvis handlingar i pappersformat, ”ljudinspelningar, bildinspelningar eller audiovisuella inspelningar” (artikel 2.6). Med begreppet öppna data avser EU ”data i öppna format som kan utnyttjas, vidareutnyttjas och delas fritt av vem som helst för valfritt ändamål” (skäl 16) utan licensavgifter (artikel 6.1)[1]. Direktivet kräver dessutom att ”särskilda värdefulla data”, däribland vissa geografiska data, så kallade geodata, som produceras av statliga, regionala eller lokala

[1] Termerna ”artikel” och ”skäl” syftar här på de numrerade artiklarna och skälen som anges i öppna data-direktivet.

myndigheter och andra offentligt finansierade organisationer tillhandahålls som öppna data (artikel 14.1). Vidare ställer direktivet krav på att dessa data ska tillgängliggöras i både ”maskinläsbart format” via API:er[2] och som ”bulknedladdning” (artikel 5). Vilka data som klassificeras som särskilt värdefulla preciseras i *kommissionens genomförandeförordning (EU) av den 21 december 2022 om fastställande av en förteckning över särskilda värdefulla dataset och arrangemangen för offentliggörande och vidareutnyttjande av dessa*. Syftet med öppna data-direktivet är att öka tillgängligheten till offentligt finansierad information och data, dels i demokratihänseende genom att förbättra insyn och öka medborgarnas tillgång till de data som de via offentliga medel bekostar, dels för att stimulera nya lösningar och innovationer exempelvis genom användande av maskininlärning och artificiell intelligens. Samtidigt ska personuppgifter och ”mål av allmänt intresse” (skäl 16) skyddas så att varken personlig integritet eller allmän och nationell säkerhet riskeras (artikel 1).

Öppna data-utredningen (SOU 2020:55), som studerade hur öppna data-direktivet bör införas i svensk lagstiftning, betonar att tryckfrihetsförordningen (TF) redan garanterar att offentliga aktörers handlingar är tillgängliga. Utredningen anser att öppna data-direktivet fokuserar på digitala data varför den föreslår att det begrepp som används i ny svensk lagstiftning bör frikopplas från begreppet ”handling” i den mening som avses i TF. Vidare menar utredningen att innebörden av den nya lagen framförallt ska betraktas som en uppmaning till offentliga aktörer att på eget initiativ tillhandahålla data och information till allmänhet och potentiella användare samt ett förtydligande av *hur* data och information ska tillhandahållas. Utredningen medger att tillgängliggörandet av data kan vara förknippat med risker, framförallt vid aggregering (det vill säga sammanställning och kombination) av data, men anser ändå att införandet av direktivet inte kommer att leda till nämnvärt ökade risker. Flera remissinstanser till öppna data-utredningen uttrycker emellertid farhågor över möjligheterna att aggregera stora mängder av olika data vilkas tillgängliggörande, var för sig, inte anses skadliga men som sammantaget kan utgöra en säkerhetsrisk (Domstolsverket, 2020; FOI, 2020; FRA, 2020; Försvarsmakten, 2020; MSB, 2020; SKR, 2020; Säkerhetspolisen, 2020). Därför efterfrågar de noggrannare utredning av säkerhetsaspekterna av öppna data-direktivet. När regeringen presenterade sin proposition *Den offentliga sektorns tillgängliggörande av data* (prop. 2021/22:225) hade emellertid kommissionen redan inlett ett överträdelseärende mot Sverige varför man inte vidare har utrett konsekvenserna av den nya lagen för Sveriges säkerhet, allmän säkerhet eller skydd av personuppgifter.

Öppna datalagen (2022:818) definierar i 2 kap. 1 § data som ”information i digitalt format oberoende av medium”. I regeringens proposition (prop. 2021/22:225) hävdas att TF redan garanterar öppen tillgång till handlingar i pappersformat, och i överensstämmelse med öppna data-utredningen anser regeringen därför att öppna data-direktivet främst avser tillgängliggörande av digitala data vilket också ska framgå av lagen. Med tanke på att öppna data-direktivet i framtiden kan komma att omfatta nya data (artikel 13.2) är det troligt att mängden öppna data kommer att öka, såväl i Sverige som i övriga stater inom EU, de närmaste åren varför möjligheten till aggregering av olika typer av data och information riskerar att bli oöverskådlig.

Lantmäteriet producerar och förmedlar en betydande mängd särskilda värdefulla datamängder i form av geodata som redan idag används av ett flertal offentliga och privata aktörer inom olika samhällssektorer. Idag är dessa data emellertid licensierade och avgiftsbelagda. För närvarande görs över en miljard överföringar av geodata från Lantmäteriet till myndighetens kunder varje månad, och baserat på erfarenheter från andra länder bedömer myndigheten att användningen på några års sikt kommer att öka tiofalt när data blir öppna. Med tanke på den stora mängd data som tillgängliggörs i samband med implementeringen av öppna data-direktivet öppnas nya möjligheter att aggregera data från olika leverantörer och källor. I dagsläget har Lantmäteriet via licensavtal i huvudsak kontroll på användarna av myndighetens geodata men i och med att data blir öppna och avgiftsfria förlorar myndigheten denna kontroll vilket kan leda till obegränsad spridning av data. Detta kan ge upphov till socioekonomiska

[2] API är förkortning för det engelska begreppet *Application Programming Interface* som är ett gränssnitt för kommunikation mellan olika datorprogram.

vinster men kan även leda till nya och hittills okända säkerhetsrisker (Söderman m.fl., 2017; Ekström & Johannesson, 2020).

2.3 Syfte och problembeskrivning

Enligt 2 kap. 1 § öppna datalagen (2022:818) ska offentliga aktörer tillgängliggöra data för vidareutnyttjande ”i den utsträckning som krav på informationssäkerhet och skydd av personuppgifter kan upprätthållas och under förutsättning att det inte innebär risker för Sveriges säkerhet”. Lagen preciserar dock inte hur en bedömning av eventuella risker för Sveriges säkerhet ska göras. Eftersom informationsklassning, säkerhetsskyddsklassning och riskbedömningar vanligen görs av enskilda aktörer, och då endast för sina egna data, är det vidare oklart om befintlig författning är ändamålsenlig och tillräcklig för bedömning av de risker som orsakas av aggregering av flera olika datamängder från såväl öppna som icke-öppna källor. Syftet med det arbete som redovisas här var därför att identifiera möjliga hot och risker som kan orsakas eller underlättas av den ökade tillgången på öppna geodata som blir resultatet av öppna datalagen (2022:818).

2.4 Tillvägagångssätt

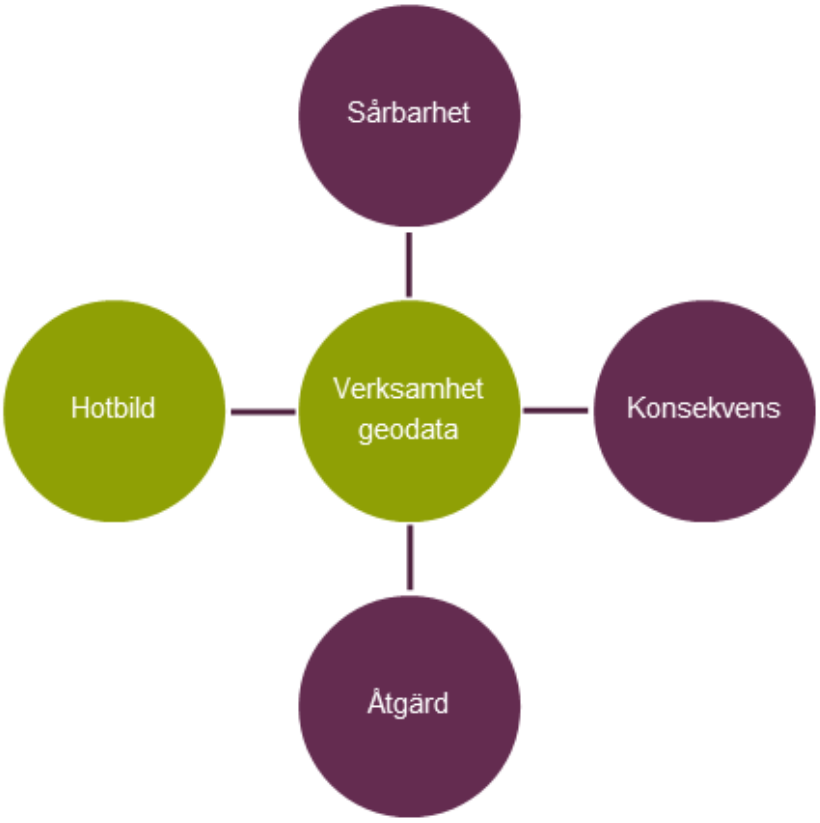
Arbetet som genomfördes inom den förstudie som redovisas i föreliggande Memo bestod (på grundval av en löpande dialog mellan Lantmäteriet och FOI) av:

- studier av Lantmäteriets geodataprodukter och preliminära arbetsmetod för riskbedömning av potentiellt öppna data för att inhämta domänkunskap
- litteraturstudier och genomgång av redan tillgängliga öppna geodata från svenska offentliga aktörer
- genomförande av en workshop i september 2023 med deltagande av representanter från Lantmäteriet samt expertis från FOI avseende såväl tekniska system som olika typer av hot och risker (inom säkerhetspolitik, infrastruktur, m.m.).

Syftet med workshoppen var att identifiera hot och risker som orsakas av eller underlättas av att svenska offentliga aktörer, framförallt Lantmäteriet, tillgängliggör sina geodata som öppna data. I detta arbete besvarade deltagarna frågorna ”Vad?”, ”Vem?” och ”Varför?”, det vill säga de förväntades identifiera och beskriva händelser som orsakas eller underlättas av öppen tillgång till geodata, vilken hotaktör som kan utnyttja dessa data för att uppnå sina syften och motiven till hotaktörens handlingar. Utgångspunkten var relativt ospecifik för att fånga upp så många olika hot och risker samt potentiella hotaktörer som möjligt. Det övergripande syftet med workshoppen var att utveckla ett antal typhändelser som i scenarioform beskriver möjliga händelseförlopp som kan orsakas eller underlättas av tillgång till öppna geodata. Baserat på det arbete som utfördes under workshoppen utvecklades ett antal typhändelser som tillsammans med litteraturstudier användes för att utforska de hot och risker som identifierades.

2.4.1 Typhändelsernas syfte och funktion

FOI har lång erfarenhet av risk- och sårbarhetsanalyser i offentliga verksamheter, och har utvecklat en egen modell för denna typ av analyser (Winehav & Nevhage, 2011; Malmberg Andersson m.fl., 2014). Enligt denna modell kan arbete med hot och risker och de konsekvenser som de kan leda till delas in i fem steg genom 1) kartläggning av verksamheten, 2) analys och bedömning av hur offentliga aktörers verksamhet påverkas av identifierade hot och risker (Hotbild), 3) bedömning av vilka sårbarheter som blottläggs (Sårbarhet), 4) vilka konsekvenser hotens verkställande skulle kunna medföra (Konsekvens) och 5) vilka åtgärder de offentliga aktörerna i ett senare skede kan behöva vidta (Åtgärd; Figur 1). I det arbete som redovisas i föreliggande Memo var syftet med typhändelserna att göra en preliminär analys av hotbilden genom att identifiera möjliga hot och risker med att offentliga aktörer tillgängliggör öppna geodata. Förutom att bekanta oss med verksamheten har vi därmed enbart berört den del av modellen som rör hotbilden.



Figur 1: Schematisk beskrivning av centrala komponenter i föreliggande och framtida arbete med bedömning av säkerhetsrisker med öppna geodata. Komponenter markerade i grönt har berörts i detta arbete (modifierad från Winehav & Nevhage, 2011).

3 Risker med öppna data identifierade i svenskt lagstiftningsarbete

Öppna data-utredningen medger i sitt huvudbetänkande *Innovation genom information* (SOU 2020:55) att ökad tillgänglighet till öppna data kan leda till risker för personlig integritet, allmän säkerhet och Sveriges säkerhet. Utredningen är exempelvis medveten om de risker som aggregering av olika datamängder kan ge upphov till. Därför menar den att ett gediget ”förebyggande och strukturerat säkerhetsarbete” är en nödvändig förutsättning för tillgängliggörande av öppna data (SOU 2020:55, s. 351). Hur detta arbete ska kunna ta hänsyn till alla potentiella risker som underlättas genom tillgången på en stor mängd öppna data klargörs emellertid inte utan utredningen nöjer sig med att betona ”vikten av samverkan mellan aktörerna […] när det gäller att skaffa sig underlag för identifiering och analys av potentiella risker med tillgängliggörande av olika typer av information” (SOU 2020:55, s. 353). Genomgång av säkerhetsarbete ligger förvisso bortom öppna data-utredningens uppdrag men den betonar behovet av fortsatt utredning av hur aktörer kan samverka inom informationssäkerhetsarbetet för att exempelvis kunna hantera de risker som orsakas av aggregering av data.

Flera remissinstanser till öppna data-utredningens betänkande uttrycker oro över hur den nya lagen ökar möjligheterna för en hotaktör att aggregera data från olika källor och därmed underlättar underrättelseinhämtning (FOI, 2020; FRA, 2020; Försvarsmakten, 2020; MSB, 2020; SKR, 2020; Säkerhetspolisen, 2020). Även i regeringens proposition (prop. 2021/22:225) erkänns möjligheten att data som enskilt inte betraktas som känsliga kan, när de kombineras, ge upphov till allvarliga säkerhetsrisker. Flera remissinstanser framhåller dessutom att möjligheten för enstaka myndigheter, eller tjänstemän på dessa myndigheter, att själva överblicka, analysera och bedöma eventuella risker orsakade av tillgängliggörande av sina data i en miljö med stora mängder andra öppna data är begränsad (FRA, 2020; Försvarsmakten, 2020; MSB, 2020; Säkerhetspolisen, 2020). Den myndighet som ansvarar för data kan alltså efter tillbörligt arbete med informationssäkerhet och säkerhetsskydd dra slutsatsen att tillgängliggörande av data inte medför några nämnvärda risker, såvida denna myndighet inte har en fullständig överblick av existerande och framtida öppna data, de kombinationsmöjligheter som dessa data möjliggör, både genom att kombinera olika öppna data och genom att aggregera öppna data med andra typer av data, samt alla tänkbara risker detta medför. Tidigare genomgångar har dock funnit brister i både informationssäkerhets- och säkerhetsskyddsarbete på svenska myndigheter, kommuner och regioner varför Post- och telestyrelsen uppmanar till försiktighet vid tillgängliggörande av öppna data (Post- och telestyrelsen, 2020).

Domstolsverket anser att ansvarsfrågan för bedömning och värdering av risker orsakade av tillgängliggörande av öppna data förblir outredd i öppna data-utredningen och efterfrågar därför förtydliganden på denna punkt (Domstolsverket, 2020; se även Försvarsmakten, 2020). Även andra remissinstanser önskar fortsatt utredning av behoven och möjligheterna till en formaliserad och ”strukturerad samverkan för att överblicka risker när andra aktörer tillgängliggör information” (Skatteverket, 2020; se även SKR, 2020; Säkerhetspolisen, 2020).

Försvarsmakten, som avstyrkte öppna data-utredningen förslag i sin helhet, ställer sig dessutom undrande till hur *lagen* (2016:319) *om skydd för geografisk information* kan kombineras med kraven i den nya lagen om öppna data (Försvarsmakten, 2020).

Vissa remissinstanser vänder sig mot kravet i öppna data-utredningens lagförslag att offentliga aktörer ska lämna ut information i befintligt format (FRA, 2020; Försvarsmakten, 2020). Enligt Försvarets radioanstalt (FRA) kan ett utlämnande av data i befintligt format, när det är i form av digitala data, ge upphov till oavsiktligt läckage av potentiellt säkerhetskänslig information i form av teknisk information knutet till den specifika datafilen och det dataformat som används. Digitala filer innehåller nämligen mer information än endast de siffror eller den text som man avser att förmedla, exempelvis information som avslöjar detaljer om myndighetens digitala infrastruktur.

I regeringens proposition (prop. 2021/22:225) föreslås att offentliga aktörer ska kunna neka tillgängliggörande av data även då andra säkerhetshänsyn än strikt sekretess föreligger. Dessutom kan de skäl som ligger till grund för nekande, åtminstone då risk för Sveriges säkerhet befaras, behöva revideras över tid på grund av exempelvis förändringar i omvärlden. Liksom öppna data-utredningen anser regeringen att bedömningar av risker med tillgängliggörande av data kan kräva samråd med andra myndigheter eller ytterligare vägledning, men nämner inget behov av ytterligare utredning av frågan. Sammantaget gör dock regeringen bedömningen att lagen inte kommer att leda till några särskilda konsekvenser för Sveriges säkerhet, informationssäkerhet eller personlig integritet (prop. 2021/22:225).

4 Typhändelser

De hot och risker som identifierades under workshoppen i det projekt som redovisas i föreliggande Memo samlades i fyra breda scenariokategorier: i) stort aggressivt land i gråzon, ii) politisk extremism, iii) pågående krig och iv) organiserad brottslighet.

4.1 Scenariokategori 1: Stort aggressivt land i gråzon

4.1.1 Crowdsourcing i underrättelsesyfte

Under etiketten ”Det stora folkutbytet” har en mobil applikation lanserats. Applikationen består av tre delar: en animation som visar hur det påstådda folkutbytet, det vill säga den förmodade process då etniska svenskar ersätts med muslimer, har fortskridit under de senaste 20 åren, en karttjänst där ”ansvariga” för denna utveckling pekas ut samt ett diskussionsforum. I färggranna kartanimationer visualiseras hur de röda områdena som domineras av muslimsk befolkning breder ut sig över tid samtidigt som de blå, svenska områdena minskar i omfattning. Karttjänsten visar med hög precision var kontoren för ”ansvariga myndigheter” finns och pekar ut positionen för ”ansvariga personers” bostäder och, i enstaka fall, fritidsboenden. Statistiken och kartmaterialet uppges komma från SCB och Lantmäteriet men då applikationen är knuten till mobilens GPS tillåter den användarna att själva lägga in intressepunkter. Till dessa punkter kan man dessutom bifoga bland annat bilder, filmer och anteckningar. I diskussionsforumet förekommer ofta förfrågningar från användare som vill ha information om specifika byggnader, anläggningar, adresser eller personer. Användare med god lokalkännedom eller annan relevant insikt i frågan brukar snabbt bidra med de efterfrågade uppgifterna varför applikationen har använts för att spåra upp personer med skyddad identitet, flyktingar från auktoritära stater, journalister, politiker, forskare, myndighetstjänstemän och försvarsanställda. I massmedia har också förekommit uppgifter om att applikationen har använts för att sprida nakenbilder, främst på unga kvinnor och HBTQI-personer, samtidigt som deras bostadsadress har pekats ut. Vidare har användare laddat upp omfattande material som dokumenterar känslig information om militära skyddsobjekt och regeringsbyggnader via applikationen.

Från myndighetshåll har man försökt stoppa applikationen men då utvecklaren har sin bas utanför EU har det visat sig svårt. Dessutom har ett flertal snarlika applikationer dykt upp vilket ytterligare har förvärrat situationen. Eftersom de olika applikationernas diskussionsforum uppvisar vissa systematiska skillnader har journalistiska granskningar och politiska utredningar antytt att olika statliga aktörer ligger bakom applikationerna och använder dem för underrättelseinhämtning.

Kommentar: I typhändelsen utnyttjas missnöjda svenska medborgare som omedvetna underrättelseoperatörer då de mobila applikationerna används av främmande makt för att kartlägga personer, fastigheter och anläggningar av intresse för staten i fråga. Eftersom olika stater har skilda motiv bakom sin underrättelseverksamhet används applikationerna på olikartade sätt. Exempelvis kan stater använda dem för att i underrättelsesyfte kartlägga anläggningar och personer som är viktiga för det svenska totalförsvaret, för att kartlägga nyckelpersoner som kan nyttjas för spionage, för att påverka beslutsfattare och journalister eller för att spåra oppositionella inom statens diaspora (Lewis, 2015; Öztürk & Taş, 2020; Jonsson & Gustafsson, 2022; Säkerhetspolisen, 2023).

I applikationerna har Lantmäteriets kart- och fastighetsdata använts som underlag. Som öppna data kan dessa utnyttjas i alla typer av produkter, även sådana med fientligt eller oetiskt innehåll. Alternativ, såsom Google Maps, är vanligtvis avgiftsbelagda och knutna till licensavtal. I denna typhändelse kombineras Lantmäteriets data dessutom med SCB:s data över myndighets- och kommunkontor och befolkningsstatistik. Animationerna utgår från befolkningsdata per demografiskt statistikområde från SCB men dessa manipuleras för att framhäva vissa mönster för att därigenom påverka mottagarna i önskad riktning. Typhändelsen illustrerar dessutom aggregering av öppna data med annan informationsinhämtning, i det här fallet bland annat position för samt bilder och filmer av relevanta objekt.

4.1.2 Riskminimering blir riskmaximering – iscensatta skogsbränder

Efter en osedvanligt varm och torr sommar drabbas flera områden i Sverige av en rad allvarliga skogsbränder som sprider sig ohämmat och hotar både bebyggelse och ett antal avlägsna Sevesoanläggningar[3]. Flera av bränderna tycks ha startat i områden som befinner sig på långt avstånd från närmaste brandstation och släckningsarbetet har i flera fall försenats eller försvårats på grund av hinder längs framryckningsvägar vilket har tvingat räddningstjänsten till onödiga omvägar. Allt från vägarbeten till trafikolyckor har hindrat räddningstjänstens fordon, och trots att man inte har lyckats hitta några tydliga mönster i dessa incidenter förekommer spekulationer i media om hur det kan komma sig att räddningstjänsten har försenats på så många platser.

Kommentar: Bränderna har initierats av en antagonist som har valt ut platserna för bränderna för att åsamka samhället största möjliga skada. Antagonisten har genom att kombinera MSB:s brandbränslekartering och geodata över brandstationer och Sevesoanläggningar med SMHI:s brandriskprognoser, SCB:s befolkningsstatistik per demografiska statistikområden samt Trafikverkets och Lantmäteriets geodata utfört en optimeringsberäkning för att hitta lokaler där sannolikheten för att en skogsbrand ska spridas och drabba så många människor som möjligt är som störst. Därmed har antagonisten kunnat identifiera platser på långt avstånd från närmaste brandstation men där risken för att befolkning och i enstaka fall Sevesoanläggningar kan drabbas av bränderna har maximerats. Lantmäteriets och Trafikverkets geodata över bland annat funktionell vägklass, vägtrafikdata, hastighetsgräns och trafiknätsdata för blåljusverksamhet har använts i nätverksanalyser för att kartlägga de möjliga framryckningsvägar som räddningstjänsten kan tänkas använda. Tillsammans med information från tjänster som Waze har dessa data dessutom använts för att identifiera vägarbeten och lämpliga platser för möjliga hinder längs vägarna.

4.2 Scenariokategori 2: Politisk extremism

4.2.1 Förtroenderaserande verksamhet

Utländsk massmedia rapporterar återigen om det låga förtroendet för offentliga aktörer i Sverige. Vissa reportrar rapporterar med illa dold skadeglädje hur de tidigare så ”självgoda och naiva” svenskarnas förtroende för myndigheter och kommuner succesivt eroderat under flera år, medan andra förbryllat undrar vad som hände med ”det trygga och stabila lilla landet i norr”. Det spekuleras i orsakerna till detta förtroendetapp men de flesta är överens om att de senaste årens synbara infrastrukturella och säkerhetsmässiga sammanbrott förmodligen har varit den viktigaste faktorn. Det började med återkommande strömavbrott vilket resulterade i långvariga problem med tåg- och tunnelbanetrafik samt oförutsägbara möjligheter att handla i butiker eftersom varken betalningar eller kassasystem fungerade under strömavbrotten. Under kalla vintrar rapporterade massmedia från mörka bostäder där de boende i täckjacka och mössa beklagade sig över de ideliga strömavbrotten. Till en början misstänkte man att strömavbrotten orsakades av tjuvar på jakt efter värdefulla metaller då utrustning och vissa installationer stals, men systematiken i dåden medförde att de så småningom rubricerades som medvetna sabotage. Det har emellertid inte uppdagats vem som ligger bakom sabotagen.

Eftersom den spårbundna trafiken har kommit att betraktas som osäker har befolkningen övergått till att åka bil i högre utsträckning vilket i de flesta större orter har lett till omfattande trängsel och missnöje. Efterhand har man dock upptäckt ett flertal sabotage på viadukter och vägtrummor. Lyckligtvis har ingen trafikant råkat ut för någon olycka på grund av dessa sabotage men det har lett till att trafiken har fått ledas om via andra vägar vilket har förvärrat trängseln och missnöjet ytterligare. Dessutom har vissa varuleveranser försenats eftersom de vägar som framförallt har drabbats är de som är viktiga för godstransport.

[3] Sevesoanläggningar är verksamheter som omfattas av *lag* (1999:381) *om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalieolyckor* vilket innebär att de hanterar vissa farliga ämnen i särskild omfattning.

Sedan elbolagen i större utsträckning har börjat anlita vaktbolag har antalet sabotage mot elförsörjningen minskat. Det har dock inte förbättrat situationen för den spårbundna trafiken då den oidentifierade aktören, eller aktörerna, har gått över till att direkt angripa spårinfrastrukturen. En kall januarimorgon saboterades signalsystemet på sträckan Sala-Avesta vilket resulterade i den allvarligaste tågolyckan i Sverige under modern tid. Även dricksvattenförsörjningen har drabbats då flera större vattentäkter har förorenats med dieselolja eller *Cryptosporidium* med initiala behov av omfattande vägbunden transport av dricksvatten som resultat vilket har ökat trafikproblemen ytterligare.

Delar av den svenska förvaltningen har i spåren av sabotagen överbelastats med akuta och oväntade åtgärder. Trots att man från politiskt håll har ökat resurserna till kommuner och regioner samt vissa myndigheter är exempelvis Polisen överhopad med en lång rad utredningar av sabotagen, och Trafikverket har under avsevärd tid blivit tvungen att åtgärda saboterad väg- och järnvägsinfrastruktur. Även sjukvården har, åtminstone lokalt, stundtals varit överbelastad på grund av det förorenade dricksvattnet.

Den kanske största påfrestningen har dock förmodligen varit osäkerheten. På sociala medier har många uttryckt sin frustration över att periodvis inte veta när man kommer anlända till arbetet på morgonen eller om arbetande föräldrar ska hinna till förskolan i tid på eftermiddagen. Ett antal utländska företag med verksamhet i Sverige har öppet dryftat möjligheten att lämna landet på grund av den, som de anser, osäkra situationen. På internet har det dessutom spridits bilder som påstås visa anställda på Trafikverket eller olika elbolag som, under bevakning av poliser, förstör den infrastruktur som de är satta att förvalta. De inledande syrliga kommentarerna till dessa bilder har successivt övergått till upprörda känsloyttringar och bildandet av mer eller mindre organiserade grupper som hävdar att Sverige egentligen styrs av en liten elit av politiker, företagsledare och höga myndighetstjänstemän som önskar krossa ”den riktiga svenskens” livsstil och bygga en ny ekofascistisk diktatur. Denna retorik har dels sporrat hot om våld, dels lett till faktiska våldsdåd riktade mot representanter för olika offentliga aktörer och elbolag.

En ytterligare källa till misstro och misstänksamhet bland det svenska folket blev det senaste valet då en stor mängd vallokaler, i samtliga fall grundskolor, utsattes för bombhot. Vid flera av lokalerna skymtades dessutom drönare i luften varför samtliga hotade lokaler stängdes vilket ledde till att tusentals människor inte fick möjlighet att lägga sin röst. Valet har ogiltigförklarats och trots att regeringen har lovat att valet ska göras om har vissa oppositionspartier antytt att regeringen på ett eller annat sätt är ansvarig för valpåverkan. Indignationen på sociala medier har nått nya nivåer och Sverige har blivit ett land dominerat av misstro, splittring och cynism.

Kommentar: Antagonisten i typhändelsen är okänd men har kartlagt en stor mängd samhällsviktig information för att kunna utföra sabotage och hot mot samhällsviktig infrastruktur och demokratiska val i syfte att på lång sikt minska befolkningens förtroende och tilltro till politiska institutioner och offentlig förvaltning. För att kartlägga lämpliga mål har antagonisten utnyttjat bland annat detaljerade geodata från Svenska kraftnät över transmissionsnätet för elektricitet, inklusive positioner för stationer som ställverk och transformatorstationer; Trafikverkets geodata som visar bland annat positioner för vägtrummor, broar samt ljussignaler och spårväxlar för järnvägstrafik, funktionell vägklass och vägar viktiga för godstransporter; samt Skolverkets geodata för grundskolor. Detta har dessutom kombinerats med manipulation av sociala medier genom att exempelvis upprätta fingerade diskussionsforum, konton och grupper på sociala medier för att öka effekten ytterligare (Thornton, 2017; Linvill & Warren, 2020; Lukito, 2020).

4.2.2 Terroristdåd under falsk flagg

En dimmig höstdag attackeras ett antal förskolor i Täby av maskerade personer, och ett flertal barn och anställda på förskolorna omkommer i vad som snabbt identifieras som ett terrordåd. Gärningspersonerna försvinner snabbt från brottsplatserna samtidigt som polisens jakt försvåras då lämpliga framryckningsvägar har blockerats av bland annat fotanglar och sönderspängda vägtrummor. Inom kort cirkulerar material som påstås komma från krypterade diskussionsforum tillhörande religiöst fundamentalistiska grupper på sociala medier. I dessa forum har man under lång tid diskuterat och planerat dylika terrordåd vilket leder till en hätsk och misstänksam stämning i landet. När så ytterligare attentat sker – den här gången två samtidiga attacker på grundskolor i Jönköpings län – når upprördheten explosiva nivåer. Alternativa medier kräver regeringens avgång samtidigt som rörelser inom extremhögern organiserar upprörda invandringskritiska protester utanför riksdagshuset och Rosenbad. Trots att både statsministern och justitieministern snabbt fördömer terrordåden i starka ordalag och lovar mer resurser till Polisen och Säkerhetspolisen samt tillsätter utredningar för att ”reformera grundlagen”, öka den nationella kameraövervakningen och förbjuda användningen av krypteringstjänster på internet, växer stödet för högerextrema politiska partier explosionsartat.

Kommentar: I syfte att framtvinga politiska förändringar har antagonisten genomfört terrordåd under falsk flagg eftersom dåden ger sken av att ha utförts av militanta islamister. Antagonisten har planerat sina dåd genom att kartlägga lämpliga mål utifrån SCB:s statistik över befolkningssammansättning och ekonomisk status samt SCB:s och Skolverkets geodata över för- och grundskolor. I planeringen har antagonisten även nyttjat Lantmäteriets och Trafikverkets geodata över transportmöjligheter för att identifiera mål där flyktvägarna är mest gynnsamma. Dessa data har tillsammans med information från tjänsten Waze även använts för att kartlägga lämpliga flyktvägar och vilka vägar som måste blockeras för att försvåra polisens efterfölj. De snabbaste flyktvägarna har beräknats med nätverksanalys baserat på geodata över vägnätet. Dåden har kombinerats med manipulation av sociala medier genom upprättandet av fingerade diskussionsforum samt konton och grupper på sociala medier.

4.3 Scenariokategori 3: Pågående krig

4.3.1 Den förlorade hemmaplansfördelen

Ett stort aggressivt land har angripit Sverige militärt. Regeringen har beordrat höjd beredskap och Försvarsmakten har mobiliserat, men försvaret av Sverige går sämre än väntat. Försvarsmakten har i frustration tvingats till ideliga förändringar i planeringen då angriparen alltid verkar ligger steget före. Central infrastruktur bekämpades framgångsrikt genom precisionsbombningar med kryssningsmissiler, ballistiska missiler, drönare eller specialförband redan de första dagarna av invasionen samtidigt som Försvarsmaktens framryckning och gruppering har försvårats då angriparen redan intagit dessa områden eller bekämpar dem med precisionsvapen. Privata militära företag som deltar i angreppet har besatt områden med värdefulla naturresurser som utvinningsbara mineral.

Kommentar: Med en stor mängd detaljerade geodata, bland annat Lantmäteriets kartunderlag, höjddata och ortofoton[4], jordarts- och grundvattenkartor från Sveriges geologiska undersökning (SGU) samt Naturvårdsverkets nationella marktäckedata, har angriparen redan i fredstid lyckats kartlägga nyckelterräng, lämpliga framryckningsvägar och provianteringslokaler, möjliga brohuvuden samt positioner för prioriterade mål för precisionsbekämpning såsom kritisk infrastruktur inom energi-, vatten- och livsmedelsförsörjning, myndighetskontor och räddningstjänst. Detta har lett till att angriparen har lyckats förbereda sig så mycket att Försvarsmakten har förlorat det övertag som dess unika lokalkännedom annars medför. Vissa vapensystem för fjärrbekämpning, som drönare, har dessutom matats med geodata för att de ska ta den lämpligaste (inte nödvändigtvis den kortaste) rutten till sitt mål.

[4] Ortofoton är geometriskt korrigerade flybilder.

4.4 Scenariokategori 4: Organiserad brottslighet

4.4.1 Olaglig avfallshantering

Ett flertal människor har under en tid sökt vård på sjukhus för varierande men allvarliga symptom. Till en början var orsaken till denna ohälsa okänd men det har visat sig att patienterna har utsatts för höga halter av tungmetaller eller organiska föroreningar via dricksvattnet. De flesta patienterna bor på landsbygden och hämtar sitt dricksvatten från egen brunn. Efter vidare utredning har miljöinspektörer och konsulter på flera platser i landet upptäckt onormalt höga halter av olika tungmetaller och organiska föroreningar i såväl yt- som grundvatten. Grundligare undersökningar har lyckats spåra källorna till dessa föroreningar till olagliga samlingar av farligt avfall som dumpats i sjöar, våtmarker och gamla gruvschakt, grävts ned i marken eller blandats med normalt avfall på anläggningar som egentligen inte har tillstånd att hantera farligt avfall. Av mängden att döma har denna dumpning förekommit under lång tid. Platserna för avfallsdumpningen verkar dessutom ha valts ut med omsorg då de är väl dolda och belägna i glest befolkade områden men ändå nära vägar och på relativt kort avstånd från stora centralorter.

Ett antal småföretagare i avfallsbranschen åtalas för grova miljöbrott i spåren av denna avfallshärva, som i massmedia går under beteckningen ”det nya lort-Sverige”, men polisen misstänker att organiserad brottslighet egentligen är ansvarig för verksamheten. Man har emellertid inte lyckats hitta eller lagföra någon huvudman för brotten eftersom avfallskriminalitet är svår att upptäcka och utreda.

Kommentar: I typhändelsen har kriminella organisationer under lång tid dumpat avfall på platser som optimerats för att undgå upptäckt (Massari & Monzini, 2004; Andreatta m.fl., 2023). Förövarna, som har tjänat stora summor pengar på verksamheten, har identifierat gynnsamma platser för dumpning genom att kombinera Lantmäteriets geodata över vägnät, bebyggelse och topografi (markhöjddata) tillsammans med SCB:s befolkningsstatistik, SGU:s jordartskartering och Naturvårdsverkets marktäckedata. Nätverks- och siktanalyser har använts för att optimera transportvägar och minska risken för upptäckt. Lämpliga företag att utnyttja, antingen genom förvärv eller hot, har identifierats genom tillgång till öppna företagsdata medan berörda fastighetsägare, som har tvingats till tystnad, har identifierats via fastighetsdata.

5 Diskussion

Genom ovanstående typhändelser belyser arbetet i detta projekt ett antal möjliga hot och risker som kan orsakas eller underlättas av en fri tillgång till stora mängder öppna geodata. Orsakerna till dessa hot och risker kan delas in i tre övergripande kategorier: 1) hotaktörernas verksamhet förenklas genom att de serveras en stor mängd detaljerade data som annars skulle kräva omfattande resurser för att inhämta, 2) öppna geodata tillåter avancerade rumsliga (geospatiala) analyser som hade varit komplicerade eller omöjliga att utföra med geodata från andra öppna källor och 3) hotaktörerna kan aggregera olika typer av data för att därigenom extrahera information som kan vara säkerhetskänslig.

5.1 Förenkling för antagonist

Gemensamt för de hot och risker som typhändelserna illustrerar är att aktörerna, oavsett om det är resursstarka stater, små terroristceller eller antidemokratiska politiska rörelser, serveras en stor mängd precisa och detaljerade data som underlättar deras verksamhet. Eftersom ingen aktör har obegränsade resurser frigör detta sannolikt resurser som annars hade använts till att samla in, katalogisera och dokumentera liknande data som möjligen har sämre precision. De resurser som aktörerna därmed sparar kan användas för andra aktiviteter i syfte att uppnå sina mål.

Den geografiska positionen för personal, anläggningar och aktiviteter är nyckeluppgifter vid militära operationer och underrättelseinhämtning (Twetman & Bergmanis-Korats, 2021). Även om stora datamängder kan skapa praktiska problem med hantering och analys är inhämtande, delande och användande av data och information därför en nyckelkomponent i underrättelseinhämtning och modern krigföring (Fleming m.fl., 2009; Brunet & Claudon, 2015; Baber, 2018; Clarke, 2020). Som illustreras i typhändelserna kommer den stora mängd detaljerade data som förväntas bli öppna i och med genomförandet av öppna data-direktivet att tillåta en antagonist att med stor noggrannhet kartlägga platser, anläggningar och transportvägar vilket underlättar militärt anfall, terroristdåd, sabotage eller andra brott. Redan idag finns öppna svenska geodata som med hög precision anger position för exempelvis kommun- och myndighetskontor, avloppsreningsverk, vattenkraftdammar (inklusive information om säkerhetsklass) samt det nationella stamnätets ledningar och stationer för elförsörjning. En relativt stor andel av de data som EU-direktivet identifierar som särskilt värdefulla är emellertid fortfarande avgiftsbelagda (Ekström & Johannesson, 2020). Bland dessa finns Lantmäteriets detaljerade avbildningsdata såsom ortofoton som, om och när de blir öppna, tillsammans med bland annat information om jordarter från SGU och marktäcke från Naturvårdsverket exempelvis kan tillåta en militär antagonist att redan i fredstid göra en framkomlighetsanalys med detaljerad kartläggning av nyckelterräng, lämpliga brohuvuden och framryckningsvägar i händelse av ett militärt anfall mot Sverige. Detta kan ge antagonisten så mycket information att Försvarsmakten kan antas förlora en del av det övertag som den unika lokalkännedomen förmodas bidra med i dagsläget (typhändelse ”Den förlorade hemmaplansfördelen”). Även om information i Lantmäteriets kartprodukter tas bort, retuscheras eller på annat sätt förvanskas – vilket i sig kan användas för att identifiera områden av intresse – kan andra data, såsom ortofoton, användas för att bekräfta positioner för till exempel militära anläggningar och kritisk infrastruktur (Zhang m.fl., 2019). Manipulation av ortofoton, eller andra typer av fjärranalysdata, kan också identifieras och indirekt peka ut objekt som kan vara av särskilt intresse (Horváth m.fl., 2021; Yuchen m.fl., 2023). Vidare kan de högupplösta höjddata som Lantmäteriet förfogar över underlätta fredstida signalspaning mot Försvarsmaktens radiokommunikationer, exempelvis under övningar på skjutfält, då dessa data tillsammans med siktanalyser (eng. *viewsheds*) kan användas för att identifiera lämpliga platser för spaning (Komulainen, 2020).

För att kunna avgöra huruvida tillgängliggörandet av offentliga aktörers geodata innebär en risk för allmän eller Sveriges säkerhet behöver man jämföra dessa data med andra, redan tillgängliga data. I det arbete som detta Memo sammanfattar har inte ingått en systematisk inventering av alternativa datakällor till de geodata som svenska offentliga aktörer producerar. Det ingick heller inte i uppdraget att beakta huruvida eventuella alternativa datakällor kan användas av olika hotaktörer för att uppnå

sina syften. Vad gäller avbildningar kan vi dock konstatera att det finns kommersiella satellitbilder och höjddata med en rumslig upplösning i samma storleksordning som Lantmäteriets ortofoton[5]. Dessa data har däremot betydligt sämre precision än Lantmäteriets data; precision för de kommersiella produkterna är i storleksordningen några meter jämfört med en precision på några decimeter för Lantmäteriets data. De avgiftsfria satellitprodukter som finns tillgängliga (t.ex. Landsat, MODIS, SRTM och ASTER) har betydligt lägre horisontell upplösning (30 x 30 meter eller lägre).

Övriga geodata, som exempelvis kartunderlag, befolkningsstatistik och transportrelaterade data, produceras av ansvariga myndigheter varför alternativa källor, i den utsträckning det finns sådana, förmodligen använder myndigheternas data. Vissa gratistjänster, såsom Google Maps och Eniros kartor, verkar dessutom inte uppdateras lika frekvent som Lantmäteriets motsvarigheter. Ett litet, icke-slumpmässigt urval av jämförelser mellan dessa tjänster visar exempelvis att Google Maps och Eniro på vissa svenska orter använder mer än tio år gamla satellit- eller flygbilder.

5.2 Rumsliga analyser

I flera av typhändelserna använder hotaktörerna öppna geodata för att göra rumsliga analyser, till exempel för att hitta mål som är på så långt tidsmässigt avstånd från brandstationer som möjligt, eller för att identifiera de vägtrummor som passeras av flest fordon per dygn. Geodata och geografiska informationssystem (GIS) används rutinmässigt för olika typer av analyser inom offentlig och privat verksamhet för att bland annat optimera lokalisering av butiker eller kommunikationsnoder, för att spåra spridning av sjukdomsfall och i samhällsplanering (de Smith m.fl., 2007, 2021; Franch-Pardo m.fl., 2020). Sådana analyser kräver detaljerade och precisa geodata för användning i exempelvis GIS vilket blir möjligt med öppna geodata men som är betydligt svårare eller omöjligt att göra med gratistjänster som Google Maps. Med geodata och GIS är det exempelvis möjligt att lösa uppgifter som att (de Smith m.fl., 2007, 2021):

- rangordna alla observationspunkter inom en radie av 50 km från punkt C efter hur stor andel av yta D som kan övervakas (typhändelse ”Den förlorade hemmaplansfördelen”)
- välja den vägtrumma som passeras av flest fordon per dygn och som förekommer längs svenska vägar som är viktiga för godstransporter (typhändelse ”Förtroenderaserande verksamhet”)
- avgöra vilket ställverk som omges av minst antal byggnader inom en restid på 30 min (typhändelse ”Förtroenderaserande verksamhet”)
- identifiera alla skogsområden med hög brandrisk inom ett avstånd på minst 30 km från närmaste brandstation (typhändelse ”Riskminimering blir riskmaximering”).

Enligt öppna data-direktivet ska data tillhandahållas både i ”maskinläsbart format” och som ”bulknedladdning”. Detta garanterar möjligheten att utföra sådana rumsliga analyser som nämns ovan. Geodata som kan laddas ned är dessutom vanligtvis möjliga att manipulera vilket en hotaktör skulle kunna göra innan data publiceras eller sprids vidare (typhändelse ”Crowdsourcing i underrättelsesyfte”).

[5] Lantmäteriets moderna ortofoton har en horisontell upplösning på 0,16 eller 0,40 meter medan nuvarande markhöjddata har en upplösning på 1 x 1 meter. Maxar säljer satellitbilder med en horisontell upplösning på 0,3 x 0,3 meter (se https://maxar.com/products/optical-imagery) och kommersiella höjddata med uppgiven horisontell upplösning på 0,5 x 0,5 meter (se https://maxar.com/products/precision3d-data-suite).

5.3 Aggregering av data

De risker som identifierades i öppna data-utredningen och som flera remissinstanser betonade rör möjligheten att aggregera olika datamängder. I alla typhändelserna ingår någon typ av aggregering av data, främst i form av analyser där olika datakällor kombineras för att lösa en uppgift. Dessa analyser vore inte möjliga att utföra om inte de olika datamängderna i en eller annan version fanns tillgängliga. I vissa fall (typhändelse ”Terrordåd under falsk flagg”) har hotaktören dessutom använt öppna användardrivna och mobila tjänster för att samla in information om störningar i vägtrafiken. Det förekommer även aggregering med andra typer av data än geodata, exempelvis befolkningsstatistik och företagsuppgifter (typhändelserna ”Crowdsourcing i underrättelsesyfte”, ”Terrordåd under falsk flagg” och ”Olaglig avfallshantering”). Även om det här arbetet fokuserar på geodata innebär öppna datalagen att också andra typer av data kommer att tillgängliggöras. Europeiska kommissionens genomförandeförordning uppmanar exempelvis offentliga aktörer att tillhandahålla vissa typer av statistik och företagsdata, som tidigare har varit avgiftsbelagda (Ekström & Johannesson, 2020), som öppna data.

En annan säkerhetsaspekt som inte berörs i typhändelserna men som är värd att beakta är att en hotaktör inte bara kan aggregera öppna data med varandra utan kan även kombinera dem med data som aktören själv inhämtar. För resursstarka aktörer kan det innebära avsevärda mängder information men även för privatpersoner finns idag stora möjligheter att själva samla in data vilka kan komplettera tillgängliga öppna data (typhändelse ”Crowdsourcing i underrättelsesyfte”). Det är möjligt att använda teknologi som till exempel mobiltelefoner, drönare, ekolod, åtelkameror och GPS-spårare för att samla in geolokaliserade bland annat positioner eller rörelser, bilder, vattendjup, värmestrålning eller annat ljus i olika våglängder (inklusive infrarött ljus). Det finns ett flertal mobila applikationer med vilka man kan samla in data kopplat till geografisk position och som sedan, bland annat med mobila GIS, kan kombineras med öppna data för att bland annat göra nya rumsliga analyser eller knyta underrättelseuppgifter till en geografisk position (Coetzee m.fl., 2020).

En typ av aggregering som inte uttryckligen illustreras i typhändelserna är då en antagonist genom att kombinera olika typer av data kan härleda säkerhetskänslig information som inte framgår av de enskilda datamängderna. I de fall det finns tidsserier med data, vilket är fallet med exempelvis Lantmäteriets ortofoton, kan en antagonist exempelvis härleda intressanta områden utifrån automatiserade skillnadsanalyser genom vilka förändringar i landskapet kan identifieras och därmed peka ut områden av intresse (Xi & Luo, 2018; Zhang m.fl., 2022). Dylika analyser kan dessutom underlättas med InSAR-data[6], till exempel de som Rymdstyrelsen tillgängliggör, speciellt när den rumsliga upplösningen på dessa data ökar. Teoretiskt kan sådana analyser avslöja även underjordisk verksamhet om denna påverkar jordytan, även om denna förändring är liten.

5.4 Hot och risker i typhändelserna

Fientligt sinnade stater är förmodligen de aktörer som i nuläget har störst intresse av och erforderliga resurser för att kunna hantera stora mängder geodata men det är möjligt att även andra hotaktörer som terroristorganisationer, antidemokratiska rörelser och organiserad brottslighet har behov av dessa data. I en amerikansk studie av eventuella hot och risker kopplade till terrorism och öppna geodata drogs visserligen slutsatsen att terrorister förmodligen främst använder sig av andra informationskällor än publika geodata (Baker m.fl., 2004) men nyhetsrapporter antyder att geografisk information har använts vid vissa terroristdåd (Chassay & Johnson, 2007; Klatell, 2007; Bedi, 2008). Dessutom har tillgängligheten till den kunskap och de data och mjukvaror som krävs för att göra rumsliga analyser ökat betydligt för gemene man under de senaste två decennierna. Idag behöver man inte betala några licensavgifter för att nyttja avancerade GIS som kan användas för att göra de analyser som illustreras i

[6] InSAR är förkortning för *Interferometric Synthetic Aperture Radar* och är en teknik för att mäta små (storleksordningen några millimeter) förändringar i exempelvis jordytans form eller höjd.

typhändelserna. Vidare kan den kunskap som krävs för att använda dessa system lätt inhämtas på internet via instruktioner, lektioner och diskussionsforum (Coetzee m.fl., 2020). Det går därför inte att utesluta att andra aktörer än stater finner behov av geodata i högre utsträckning framgent.

Det verkar finnas få publika studier av eventuella hot och risker med öppna geodata (men se Baker m.fl., 2004 för ett undantag). Vidare är det okänt om, och i så fall hur, olika hotaktörer använder geodata och andra öppna data. Däremot har oron över vilken effekt storskalig insamling av personlig information kan ha på nationell säkerhet ökat under senare år (Twetman & Bergmanis-Korats, 2021). Kartläggning av exempelvis personer med politiska förtroendeuppdrag, beslutsfattare på myndigheter och anställda inom Försvarsmakten i syfte att hota, utpressa, muta eller på annat sätt påverka dem i deras yrkesroll (typhändelse ”Crowdsourcing i underrättelsesyfte”), vilket i längden underminerar demokratin, är ett möjligt hot om stora mängder personliga uppgifter görs öppna, eller när de samlas in och säljs vidare av diverse informationsförmedlare (eng. *data brokers*). Trots att så kallad anonymisering av data vanligtvis används, är det med hög sannolikhet möjligt att identifiera enskilda individer i sådana stora datamängder (Narayanan & Shmatikov, 2009; Rocher m.fl., 2019). Det är inte troligt att de data som förväntas bli öppna när öppna data-direktivet implementeras innehåller personuppgifter men tillgången till många sådana garanteras ändå av TF och finns tillgängliga via olika internettjänster. Sverige har en lång och stolt tradition av öppenhet genom offentlighetsprincipen men den kan möjligtvis också medföra att öppna data-direktivet får andra konsekvenser i Sverige än i andra stater. Därför är det tillrådligt att personuppgifter inte görs tillgängliga som öppna data då det underlättar aggregering med andra data.

Typhändelserna berör främst hot med materiella resultat men det är möjligt att öppna data även kan användas vid påverkansoperationer där exempelvis politiska beslut eller människors förtroende för varandra eller för staten påverkas genom att snedvrida, manipulera eller förfalska öppna data (Geissler m.fl., 2023). Artificiell intelligens kan exempelvis användas för att manipulera satellitbilder (Zhao m.fl., 2021) – en teknik som förmodligen fungerar lika bra för att manipulera ortofoton – vilket skulle kunna användas i påverkanssyfte. Sådana operationer behöver förmodligen kompletteras med manipulation via sociala och alternativa medier (Linvill & Warren, 2020; Lukito, 2020). Gemensamt för kognitivt inriktade påverkansoperationer och vissa av de hot och risker som exemplifieras i typhändelserna är att de är förnekbara. Det innebär att det kan vara svårt att avgöra om det handlar om medvetna operationer och i så fall vem som egentligen är ansvarig för dem (Thornton, 2017). Forskare har föreslagit att den sociala osäkerhet som omskakande händelser kan ge upphov till kan leda till uppkomst och spridning av konspirationsteorier och desinformation (van Prooijen & Douglas, 2017). Att sprida desinformation är dessutom i sig en vanlig metod bland hotaktörer för att skapa splittring i demokratiska samhällen (Thornton, 2017; Hung & Hung, 2022).

I det projekt vars resultat föreliggande Memo sammanfattar har det, av tids- och resursskäl, inte gjorts en noggrann kartering av andra datakällor än svenska statliga myndigheters officiella geodata. Det är ändå troligt att geodata som svenska offentliga aktörer producerar är eftersträvansvärd information, även för en resursstark antagonist, då de skulle kunna utgöra ett viktigt komplement till andra underrättelser såsom personuppgifter och geolokalisering inhämtade via egen insamling av data, diverse öppna källor eller sociala medier. Det är också troligt att geodata får ökad betydelse allt eftersom dess precision och detaljrikedom ökar.

5.5 Behov av samverkan vid bedömning av hot och risker med öppna data

Öppen information utgör en viktig informationskälla när antagonister analyserar operationsmiljöer och samhälleliga svagheter. Typhändelserna i det här arbetet illustrerar ett urval av tänkbara konsekvenser som kan följa av att öppna data tillgängliggörs i högre utsträckning och hur detta kan drabba många olika delar av samhället. Det är därför rimligt att dra slutsatsen att de hot och risker som tillgängliggörande av stora mängder öppna data kan leda till bör beaktas av olika samhällsaktörer såsom myndigheter i de olika beredskapssektorerna.

Resultaten i denna studie tyder, i enlighet med ett flertal av remissyttrandena till öppna data-utredningen, på ett stort behov av samverkan mellan offentliga aktörer vid bedömningar av hot och risker orsakade av tillgängliggörandet av öppna data, med särskilt beaktande av möjligheterna till aggregering av data. Att inkorporera civil-militär samverkan vore ett ändamålsenligt led i uppbyggnaden av en sådan samverkan. Med tanke på den enorma mängd data som kommer att tillgängliggöras genom öppna data-direktivet blir det orimligt att kräva att offentliga aktörer var för sig, och än mindre enskilda tjänstemän eller handläggare vid dessa aktörer, ska ha resurser att kunna överblicka och analysera alla möjliga aggregeringsmöjligheter och de hot och risker som detta kan orsaka. Dessutom är situationen under konstant förändring då tekniker för att producera, sammanställa och analysera digitala data genomgår en snabb och oförutsägbar utveckling. Exempelvis kan man förvänta sig att precision och upplösning för geodata kommer att öka inom de närmaste åren. Idag har Lantmäteriets ortofoton en rumslig upplösning på som bäst 0,16 x 0,16 meter medan markhöjddata har en upplösning på 1 x 1 meter; åtminstone de senare kommer med stor sannolikhet att förbättras framgent vilket resulterar i produkter med ännu större detaljrikedom. Även privatpersoner kommer troligen få ökade möjligheter att med diverse olika sensorer och plattformar kunna samla in olika typer av data som kan leda till nya hot och risker. Det är också oklart vilken påverkan som utvecklingen av maskininlärning och artificiell intelligens kan komma att få för användning, inhämtning och analys av digitala data (Zhang & Lu, 2021; Ghioni m.fl., 2023). Exempelvis finns det på forskningsstadium autonoma och semi-autonoma plattformar, exempelvis så kallade drönare, som kan navigera med hjälp av en kombination av geodata och egeninhämtade data från olika typer av sensorer (Li m.fl., 2022; Włodarczyk-Sielicka m.fl., 2023). Tillgång på stora mängder precisa och detaljerade öppna geodata kommer sannolikt att accelerera denna teknikutveckling. Därför är det troligt att hot- och riskbedömningar regelbundet måste upprepas för att ta hänsyn till teknikutvecklingen. Samtidigt är samhällsnyttan med öppna geodata stor varför tillgängliggörandet av varje ny öppen datamängd bör föregås av att eventuella hot och risker noga vägs mot nyttan med att göra data öppna (Baker m.fl., 2004).

Målet med att identifiera och bedöma potentiella hot och risker med öppna data är inte att alla data ska vara sekretessbelagda. Det finns en stor nytta med och efterfrågan på geodata inom såväl näringsliv som offentliga verksamheter vilket är en av orsakerna till att EU vill göra dessa data mer lättillgängliga. Däremot kan det finnas behov av att undanhålla vissa delar av data från full öppenhet för att minska hot och risker. Man kan till exempel behöva fundera på om det krävs olika nivåer av kontroll på användningen så att vissa attribut eller datamängder fortsättningsvis begränsas till ett fåtal användningsområden eller aktörer. Sådana avväganden och beslut behöver emellertid göras av berörda offentliga aktörer i samverkan.

För att myndigheter i samverkan löpande ska kunna bedöma eventuella hot och risker orsakade av tillgängliggörandet av öppna geodata krävs förutsättningar för ändamålsenligt och säkert informationsutbyte (Ödlund & Olsson, 2019) samt en lämplig metod för riskbedömningar. Typhändelserna beskrivna ovan ska på intet sätt ses som uttömmande, tillräckliga eller som de mest sannolika framtida scenarierna. Syftet är snarare att illustrera exempel på tänkbara hot och risker som på ett eller annat sätt orsakas eller underlättas av en omfattande tillgång på öppna data (Jonsson m.fl., 2017). Även om typhändelserna är fiktiva berör de reella hot och risker (se t.ex. Massari & Monzini, 2004; Thornton,

2017; Linvill & Warren, 2020; Hung & Hung, 2022; Andreatta m.fl., 2023). Det är också vår förhoppning att typhändelserna kan användas i fortsatt arbete med bedömningar av potentiella hot och risker orsakade av tillgängliggörande av öppna data vid svenska myndigheter.

5.6 Framtida arbete

Baserat på föreliggande arbete kan vi konstatera behovet av ytterligare studier. Såväl öppna datalagen (2022:818) som öppna data-direktivet antyder att tillgängliggörandet av öppna data bör föregås av en riskbedömning som beaktar eventuella hot och risker för personlig integritet samt allmän och nationell säkerhet. Det är emellertid oklart hur en sådan bedömning ska kunna göras med tanke på de oändliga kombinationsmöjligheter som aggregering av olika datamängder ger upphov till. Detta Memo antyder ett antal möjliga hot och risker men det finns troligtvis många fler som skulle behöva undersökas genom att ta del av en ännu bredare expertis än den som har deltagit i detta arbete. För att korrekt kunna bedöma hoten och riskerna med att tillgängliggöra öppna data bör även alternativa datamängder och -leverantörer kartläggas och jämföras. Det bör även utredas om och i så fall hur öppna data, framförallt geodata, används av olika hotaktörer. En robust och rättssäker riskbedömning av öppna data kräver dessutom, som vi har argumenterat ovan, med största sannolikhet samverkan mellan olika offentliga aktörer som tillgängliggör öppna data. Fortsatt arbete skulle därför behöva lägga vikt vid utvecklandet av en metod för att göra sådana riskbedömningar i samverkan för att därigenom identifiera skyddsvärda data och föreslå lämpliga skyddsmekanismer.

Vissa av de data som kommissionen pekar ut som särskilt värdefulla skulle i ljuset av en grundlig riskbedömning kunna anses kräva ett mått av skydd. I vilken grad offentliga aktörer har möjlighet att begränsa tillgängliggörandet av sådana data är emellertid än så länge oprövat. Det är vidare oklart hur öppna data-lagen ska tolkas i ljuset av annan författning, exempelvis *lagen* (2016:319) *om skydd för geografisk information*, TF och förbud mot avbildning av skyddsobjekt vilket regleras i skyddslagen (2010:305).

Sammantaget finns alltså behov av vidare utredning av tillämpliga juridiska ramverk, andra potentiella hot och risker, kartläggning av alternativa datakällor samt utveckling av en passande metod för att i samverkan bedöma möjliga hot och risker med att tillgängliggöra offentliga aktörers digitala information.

6 Slutsatser

Typhändelserna som utvecklats i detta arbete illustrerar att tillgängliggörande av offentliga aktörers öppna data kan orsaka eller underlätta hot och risker genom att:

1. förenkla för olika hotaktörer genom att paketera en stor mängd relevanta data som annars skulle kräva stora resurser att anskaffa
2. tillåta avancerade rumsliga analyser som skulle vara svåra eller omöjliga att utföra utan dessa data
3. tillåta aggregering av öppna geodata, andra öppna och dolda data samt enskilt inhämtade data för att därigenom extrahera potentiellt säkerhetskänslig information.

Enskilda tjänstemän eller offentliga aktörer kan förmodligen inte själva överblicka alla aggregeringsmöjligheter eller potentiella hot och risker med att tillgängliggöra öppna data. Dessa svårigheter accentueras förmodligen ytterligare av den hastiga teknikutvecklingen inom maskininlärning och artificiell intelligens samt införandet av mer detaljerade och nya typer av geodata. Därför bör bedömning av hot och risker samt erforderliga åtgärder göras löpande i samverkan mellan olika offentliga aktörer.

7 Källförteckning

Andreatta, D., Favarin, S., Lisciandra, M. & Millemaci, E. (2023). Digging into waste: an analysis of waste crime in the Italian provinces. *Regional Studies*, 57(7), 1367–1379. doi:10.1080/00343404.2022.2135697.

Baber, M. (2018). Geospatial Intelligence and National Security. *The Geographic Information Science & Technology Body of Knowledge*.

Baker, J. C., Lachman, B. E., Frelinger, D. R., O'Connell, K. M., Hou, A. C., Tseng, M. S., Orletsky, D. & Yost, C. (2004). *Mapping the Risks: Assessing the Homeland Security Implications of Publicly Available Geospatial Information*. RAND Corporation. Santa Monica, USA, 195 s.

Bedi, R. (2008). Mumbai attacks: Indian suit against Google Earth over image use by terrorists. *The Telegraph*, 09 december 2008.

Brunet, J. & Claudon, N. (2015). Military and Big Data Revolution. I Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, P. S. (red.). *Application of Big Data for National Security*. Butterworth-Heinemann, ss. 81–107.

Chassay, C. & Johnson, B. (2007). Google Earth used to target Israel. *The Guardian*, 25 oktober 2007.

Clarke, K. C. (2020). Geospatial Intelligence. I Kobayashi, A. (red.). *International Encyclopedia of Human Geography (Second Edition)*. Oxford: Elsevier, ss. 127–130.

Coetzee, S., Ivánová, I., Mitasova, H. & Brovelli, M. A. (2020). Open Geospatial Software and Data: A Review of the Current State and A Perspective into the Future. *ISPRS International Journal of Geo-Information*, 9(2), doi:10.3390/ijgi9020090.

de Smith, M. J., Goodchild, M. F. & Longley, P. A. (2007). *Geospatial Analysis. A Comprehensive Guide to Principles, Techniques and Software Tools*. 2:a uppl. Leicester, UK: Winchelsea Press.

de Smith, M. J., Goodchild, M. F. & Longley, P. A. (2021). *Geospatial Analysis. A Comprehensive Guide to Principles, Techniques and Software Tools*. https://www.spatialanalysisonline.com/HTML/index.html [2023-11-08].

Domstolsverket (2020). *Remissyttrande över Öppna data-utredningens huvudbetänkande Innovation genom information, SOU 2020:55*. DOV 2020/1271.

Ekström, D. & Johannesson, J. (2020). *Värdet av öppna data - Samhällsekonomisk nyttoanalys av tillgängliggörande av särskilt värdefulla data*. Stockholm, Sverige: Damvad Analytics.

Fleming, S., Jordan, T., Madden, M., Usery, E. L. & Welch, R. (2009). GIS applications for military operations in coastal zones. *ISPRS Journal of Photogrammetry and Remote Sensing*, 64(2), 213–222. doi:10.1016/j.isprsjprs.2008.10.004.

FOI (2020). *Remissvar gällande betänkandet Innovation genom information (SOU 2020:55)*. FOI-2020-487.

FRA (2020). *Remissyttrande. Öppna data-utredningens huvudbetänkande Innovation genom information, SOU 2020:55*. FRA beteckning 3.2:4012/20:2.

Franch-Pardo, I., Napoletano, B. M., Rosete-Verges, F. & Billa, L. (2020). Spatial analysis and GIS in the study of COVID-19. A review. *Science of The Total Environment*, 739 140033. doi:10.1016/j.scitotenv.2020.140033.

Försvarsmakten (2020). *Försvarsmaktens remissvar angående huvudbetänkande från Öppna data-utredningen: Innovation genom information (SOU 2020:55)*. FM2020-20794:2.

Geissler, D., Bär, D., Pröllochs, N. & Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ Data Science*, 12(1), doi:10.1140/epjds/s13688-023-00414-5.

Ghioni, R., Taddeo, M. & Floridi, L. (2023). Open source intelligence and AI: a systematic review of the GELSI literature. *AI & SOCIETY*, doi:10.1007/s00146-023-01628-x.

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

Horváth, J., Baireddy, S., Hao, H., Montserrat, D. M. & Delp, E. J. (2021). Manipulation Detection in Satellite Images Using Vision Transformer. I *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. Presenterad vid 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), ss. 1032–1041.

Hung, T.-C. & Hung, T.-W. (2022). How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars. *Journal of Global Security Studies*, 7(4), ogac016. doi:10.1093/jogss/ogac016.

Jonsson, D. K., Johansson, B., Lindgren, F., Veibäck, E. & Bergstrand, M. (2017). *Scenariobaserad planering för civilt försvar inom energiområdet*. Totalförsvarets forskningsinstitut, FOI-R--4356--SE. Stockholm, Sverige, 49 s.

Jonsson, M. & Gustafsson, J. (2022). *Espionage by Europeans 2010-2021. A Preliminary Review of Court Cases*. Stockholm, Sweden: Totalförsvarets forskningsinstitut. FOI-R--5312--SE.

Klatell, J. (2007). 4 Charged In New York Airport Terror Plot. *CBS News*, 02 juni 2007.

Komulainen, A. (2020). *Upptäcktsavstånd för taktiska radionät*. Totalförsvarets forskningsinstitut, FOI-R--5007--SE. Stockholm, Sverige, 31 s.

Lewis, D. (2015). "Illiberal Spaces:" Uzbekistan's extraterritorial security practices and the spatial politics of contemporary authoritarianism. *Nationalities Papers*, 43(1), 140–159. doi:10.1080/00905992.2014.980796.

Li, J., Qin, H., Wang, J. & Li, J. (2022). OpenStreetMap-Based Autonomous Navigation for the Four Wheel-Legged Robot Via 3D-Lidar and CCD Camera. *IEEE Transactions on Industrial Electronics*, 69(3), 2708–2717. doi:10.1109/TIE.2021.3070508.

Linvill, D. L. & Warren, P. L. (2020). Troll Factories: Manufacturing Specialized Disinformation on Twitter. *Political Communication*, 37(4), 447–467. doi:10.1080/10584609.2020.1718257.

Lukito, J. (2020). Coordinating a Multi-Platform Disinformation Campaign: Internet Research Agency Activity on Three U.S. Social Media Platforms, 2015 to 2017. *Political Communication*, 37(2), 238–255. doi:10.1080/10584609.2019.1661889.

Malmberg Andersson, F., Gozzi, J. & Hedtjärn Swaling, V. (2014). *Risk- och sårbarhetsanalys för Totalförsvarets forskningsinstitut (FOI) 2014*. Totalförsvarets forskningsinstitut, FOI-R--3959--SE. Stockholm, Sverige, 86 s.

Massari, M. & Monzini, P. (2004). Dirty Businesses in Italy: A Case-study of Illegal Trafficking in Hazardous Waste. *Global Crime*, 6(3–4), 285–304. doi:10.1080/17440570500273416.

MSB (2020). *Remissvar. Betänkandet SOU 2020:55 Innovation genom information*. Ärendenr 2020-12389.

Narayanan, A. & Shmatikov, V. (2009). De-anonymizing Social Networks. I *2009 30th IEEE Symposium on Security and Privacy*. Presenterad vid 2009 30th IEEE Symposium on Security and Privacy, ss. 173–187.

Post- och telestyrelsen (2020). *PTS svar på betänkandet Innovation genom information (SOU 2020:55)*. 20-10917.

Rocher, L., Hendrickx, J. M. & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10(1), 3069. doi:10.1038/s41467-019-10933-3.

Skatteverket (2020). *Öppna data-utredningens huvudbetänkande Innovation genom information, SOU 2020:55*.

SKR (2020). *Yttrande. Innovation genom information SOU 2020:55*. Ärendenr 20/01298.

Säkerhetspolisen (2020). *Remissvar. Innovation genom information*. Diarienummer 2020-20562-2.

Säkerhetspolisen (2023). *Säkerhetspolisens årsbok 2022/2023*.

Söderman, U., Ahlberg, S. & Tolt, G. (2017). Geografisk information – en vital resurs i förändring. I Hull Wiklund, C., Faria, D., Johansson, B., & Öhrn-Lundin, J. (red.). *Strategisk utblick 7. Närområdet och nationell säkerhet*. Stockholm: Totalförsvarets forskningsinstitut, ss. 69–74.

Thornton, R. (2017). The Russian Military's New 'Main Emphasis'. *The RUSI Journal*, 162(4), 18–28. doi:10.1080/03071847.2017.1381401.

Twetman, H. & Bergmanis-Korats, G. (2021). *Data brokers and security. Risks and vulnerabilities related to commercially available data*. NATO Strategic Communications Centre of Excellence. Riga, 40 s.

UN-GGIM (2020). *Future trends in geospatial information management: the five to ten year vision, 3rd ed.* United Nations Committee of Experts on Global Geospatial Information Management.

van Prooijen, J.-W. & Douglas, K. M. (2017). Conspiracy theories as part of history: The role of societal crisis situations. *Memory Studies*, 10 323–333. doi:10.1177/1750698017701615.

Winehav, M. & Nevhage, B. (red.). (2011). *FOI:s modell för risk- och sårbarhetsanalys (FORSA)*. Totalförsvarets forskningsinstitut, FOI-R--3288--SE. Stockholm, Sverige, 140 s.

Włodarczyk-Sielicka, M., Połap, D., Prokop, K., Połap, K. & Stateczny, A. (2023). Spatial Visualization Based on Geodata Fusion Using an Autonomous Unmanned Vessel. *Remote Sensing*, 15(7), doi:10.3390/rs15071763.

Xi, Y. & Luo, Q. (2018). A morphology-based method for building change detection using multi-temporal airborne LiDAR data. *Remote Sensing Letters*, 9(2), 131–139. doi:10.1080/2150704X.2017.1402384.

Yuchen, N., Xiangling, D., Wenyi, Z. & Yulin, Z. (2023). A Systematic Review on Detection of Manipulated Satellite Images. I *2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. Presenterad vid 2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom), ss. 6–11.

Zhang, C. & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. *Journal of Industrial Information Integration*, 23 100224. doi:10.1016/j.jii.2021.100224.

Zhang, G., Lu, S. & Zhang, W. (2019). CAD-Net: A Context-Aware Detection Network for Objects in Remote Sensing Imagery. *IEEE Transactions on Geoscience and Remote Sensing*, 57(12), 10015–10024. doi:10.1109/TGRS.2019.2930982.

Zhang, J., Pan, B., Zhang, Y., Liu, Z. & Zheng, X. (2022). Building Change Detection in Remote Sensing Images Based on Dual Multi-Scale Attention. *Remote Sensing*, 14(21), doi:10.3390/rs14215405.

Zhao, B., Zhang, S., Xu, C., Sun, Y. & Deng, C. (2021). Deep fake geography? When geospatial data encounter Artificial Intelligence. *Cartography and Geographic Information Science*, 48(4), 338–352. doi:10.1080/15230406.2021.1910075.

Ödlund, A. & Olsson, M. (2019). Totalförsvar, informationsdelning och nya gränsytor. I Rossbach, N. H., Öhrn-Lundin, J., Jonsson, D. K., Sundberg, A., Olsson, S., Gustafsson, J., & Trané, C. (red.). *Strategisk utblick 8. Totalförsvarets tillväxt – utmaningar och möjligheter*. Stockholm: Totalförsvarets forskningsinstitut, ss. 33–37.

Öztürk, A. E. & Taş, H. (2020). The Repertoire of Extraterritorial Repression: Diasporas and Home States. *Migration Letters*, 17(1), 59–69. doi:10.33182/ml.v17i1.853.