FORSKNINGSRAPPORT

Rymdsystem som kritisk infrastruktur: Ett systemperspektiv för att stärka cybersäkerhet i rymden

Christine Große
Leif Sundberg

LULEÅ TEKNISKA UNIVERSITET

Myndigheten för samhällsskydd och beredskap

LULEÅ TEKNISKA UNIVERSITET

UMEÅ UNIVERSITET

Rymdsystem som kritisk infrastruktur: Ett systemperspektiv för att stärka cybersäkerhet i rymden

Christine Große
Leif Sundberg

Luleå tekniska universitet
Institutionen för System- och rymdteknik
Avdelningen för Informationssystem

Luleå tekniska universitet, Grafisk produktion 2025

ISSN 1402-1528
ISBN 978-91-8048-870-9 (pdf)

Luleå 2025

www.ltu.se

Innehåll

SAMMANFATTNING I

1 INLEDNING 1

2 LÄRDOMAR FRÅN TIDIGARE STUDIER, ÖVERSIKTER OCH RAPPORTER 3

2.1 Cybersäkerhet i rymdsystem 3

2.2 Tidigare litteraturöversikter 7

3 METOD OCH MATERIAL 11

3.1 Urval 11

3.2 Analys av litteraturen 13

4 RESULTAT OCH ANALYS 16

4.1 Bibliometrisk analys av litteraturen 16

4.2 Tematisk sammanställning av litteratur 18

4.2.1 Styrning 19

4.2.2 Organisatoriska aspekter 22

4.2.3 Tekniska aspekter 24

4.3 En översiktlig modell av rymdsystemet 27

5 FÖRSLAG PÅ FRAMTIDA FORSKNING 30

5.1 Framtagning av scenarier 30

5.2 Från labbet till rymden och tillbaka 31

5.3 Resiliens mot störningar i rymdsystem 32

6 SLUTSATS 33

REFERENSER 35

Sammanfattning

Den senaste tiden har det rapporterats om flera störningar av GPS-signaler i länder vid Natos östra gräns. Dessa har inte bara drabbat militärt strategiska funktioner, men även det civila luftrummet. Denna typ av störningar av exempelvis rymdsystem och samhällsviktiga verksamheter beräknas bli vanligare framöver, i kölvattnet av användning av ny teknik i geopolitiska konflikter. Rymdsäkerhet har därför också blivit en angelägenhet för Sverige, särskilt med hänsyn till Sveriges medlemskap i Nato. Denna rapport sammanställer resultat från ett forskningsprojekt som genomfördes under våren 2025 med finansiering av Myndigheten för samhällsskydd och beredskap (MSB) för att ta fram en syntes av kunskapsläget inom området samhällsskydd och beredskap, med fokus på rymdsystem som kritisk infrastruktur. Studien bygger på en litteraturöversikt där 190 artiklar analyserades via bibliometrisk analys, tematisk analys, och systemanalys.

Litteraturen beskriver utöver relativt välbeforskade hot mot datornätverk även rymdsystemets unika egenskaper som försvårar implementering av vanliga säkerhetsåtgärder. Vi presenterar praktiska lärdomar och identifierar kunskapsluckor inom området och uppslag for fortsatt forskning, som i sin tur kan stärka samhällelig resiliens. Resultaten bidrar bland annat med kunskap om de cybersäkerhetsproblem som uppstår när aktörer, som är involverade i mer eller mindre outtalade konflikter, siktar på att vinna mark i rymden. Teknikutvecklingen och utvecklingen av forskningsfältet kan knytas till både en kommersialisering av rymdindustrin och ett starkare geopolitiskt intresse av rymden som i sin tur involverar cyberrymden som slagfält för konkurrens och maktutövande. Detta ledde oss fram till en översiktlig beskrivning av fem scenarier som ramar in framtida utvecklingen av rymdsystem och innebär en rad utmaningar för offentliga och privata organisationer, förvaltning och politik. Kunskapsöversikten skapar således en länk mellan forskning och praktik vilket lägger en grund för behovsmotiverade forskningssatsningar och kunskapsutveckling som är av praktisk relevans för aktörer inom samhällsviktiga verksamhet och beredskapssystemet.

1 Inledning

Den senaste tiden har det rapporterats om flera störningar av GPS-signaler i länder vid Natos östra gräns. Dessa har inte bara drabbat militärt strategiska funktioner, men även det civila luftrummet. Denna typ av störningar av exempelvis rymdsystem och samhällsviktiga verksamheter beräknas bli vanligare framöver, i kölvattnet av användning av ny teknik i geopolitiska konflikter (SVT, 2024). Rymdsäkerhet har därför också blivit en angelägenhet för Sverige, särskilt med hänsyn till Sveriges medlemskap i Nato.

Teknikutvecklingen har gjort det möjligt för både privata och offentliga aktörer att få tillgång till den jordnära rymden. Den kritiska infrastrukturen "rymdsystem" består både av tekniska system, till exempel satelliter, markstationer och kommunikationen de mellan, och även av flera globala aktörer, inklusive nationer och privata företag (Manulis m.fl., 2021). Dessa delsystem och aktörer interagerar i tekniska, ekonomiska, geopolitiska, och legala kontexter, och fysiska sammanhang som till exempel omloppsbanor. Det sistnämnda utgör dessutom en "ändlig resurs" (eng: scarce resource") där flera aktörer gör anspråk på samma utrymme. Detta kan ses som en utvidgning av "det offentliga rummet" där det behövs överenskommelser mellan berörda hur ett hållbart nyttjande och ansvar kan utformas och utkrävas. Den ökade andelen rymdskrot, som riskerar att avsevärt begränsa det jordnära rymdutrymmet, är ett exempel på en problematik som illustrerar dessa nya förhållanden. Redan nu behöver tusentals rymdföremål följas regelbundet med hjälp av markteleskop och geostationära satelliter för att undvika kollisioner.

Denna rapport sammanställer resultat från ett forskningsprojekt som genomfördes under våren 2025 med finansiering av Myndigheten för samhällsskydd och beredskap (MSB) för att ta fram en syntes av kunskapsläget inom området samhällsskydd och beredskap, med fokus på rymdsystem som kritisk infrastruktur. Studien inriktar sig på hur förståelsen för systemiska beroenden inom rymdsystem kan hjälpa att stärka cybersäkerhet i rymden och hur denna förståelse kunde bidra till resiliens inom samhället mot störningar i rymdsystem.

Resiliens eller motståndskraft definieras ofta som ett systems förmåga att återgå till sitt ursprungliga status efter en tillfällig störning (Holling 1973), vilket dock inte nödvändigtvis innebär att systemet, oavsett om det avser tekniska eller sociala system, måste återgå till samma läge som tidigare (Handmer och Dovers 1996) utan att anpassningar kan leda till ett nytt tillstånd. Resiliens är alltså ett (emergent) beteende hos ett system som utvecklas från dess förmåga att hantera hot och sårbarheter genom återhämtning, förändring, och anpassning till nya förhållanden, vilket innebär att det är lättare att identifiera när den har uppstått än att skapa den i förväg inom komplexa, sammankopplade system så som rymdsystem och dess användning i samhället. Detta innefattar även förmågan att klara av och hantera den stress som uppkommer vid oväntade händelser (Salehi m.fl., 2020).

Verksamheter som tillhandahåller service som är avgörande för ett fungerande samhälle och dess utveckling – kritisk infrastruktur – är idag i stor utsträckning beroende av välfungerande informations- och kommunikationssystem. Dessa system består av olika tekniker som kommunicerar via trådlösa nätverk och gör det möjligt att till exempel fjärrstyra kontrollsystem för energiproduktion och -överföring och trafikstyrning, att koppla ihop

leveranskedjor, och att koordinera krishanteringsinsatser. Rymdsystem, dvs. informations- och kommunikationssystem som inkluderar installationer i rymden, till exempel geostationära satelliter, är en essentiell komponent i dessa komplexa system-av-system.

Rymdsystem kan därför ses både som en kritisk infrastruktur i sig och som en viktig komponent i andra typer av infrastrukturer då många system (till exempel GPS, väderprognoser och globala informations- och kommunikationssystem) är beroende av rymdteknik (Fidler, 2018). Till skillnad från till andra typer av kritisk infrastruktur är dock rymdsystem relativt obeforskade ur säkerhetssynpunkt (Falco, 2018:1). Detta är ett allvarligt kunskapsgap i och med en ökad spänning i området på grund av geopolitiska konflikter, som riskerar eskalera till en militarisering av rymdtekniken. Vidare är rymdsystem relativt oreglerade och bygger på att flera aktörer med olika intressen kan och vill komma överens om hur de nyttjas. Denna otydlighet gör att det är oklart vad som exempelvis kan räknas som allmännyttiga samhällstjänster, legitima försvarsåtgärder eller militära aggressioner.

Rymdsystem som kritisk infrastruktur befinner sig därför i flera legala gråzoner samtidigt som de hot som kan förknippas med rymdsystem är högst asymmetriska (Baylon, 2014:1; Baylon 2014:2). Relevanta åtgärder handlar inte bara om att bygga bort cybertekniska hot, utan också om att se rymdsystem som ett socioteknisk system inbäddad i en särskild kontext där även policy- och styrningsfrågor blir viktiga (Falco, 2018:2; Große, 2023). Exempel inkluderar också ansvarsfrågor om nyttjande av resurser och hantering av rymdskrot.

I arbetet med kunskapsöversikten tillämpades ett systemperspektiv för att illustrera komplexiteten i rymdsystem från ett socio-tekniskt perspektiv. Vi utgick från följande frågeställning:

- Hur kan cybersäkerhet i rymdsystem förstås ur ett systemperspektiv?

Målet med studien var att ta fram ett underlag som beskriver vad som utmärker cybersäkerhet och säkerhetsarbete i rymdsystem. Utöver en syntes av kunskapsläget och forskningsfronten presenteras en systemmodell som lyfter fram systemiska beroenden och olika intressenters behov för att exemplifiera ytterligare aktiviteter som kan förbättra cybersäkerhet i rymdsystem och områden i behov av fortsatt forskning. Vi identifierar även kunskapsluckor inom området och diskutera uppslag for fortsatt forskning, som i sin tur kan stärka samhällelig resiliens inom samhällsviktiga verksamheter som är beroende av rymdbaserade tjänster. Kunskapsöversikten skapar således en länk mellan forskning och praktik vilket lägger en grund för behovsmotiverade forskningssatsningar och kunskapsutveckling som är av praktisk relevans för aktörer inom samhällsviktig verksamhet och beredskapssystemet.

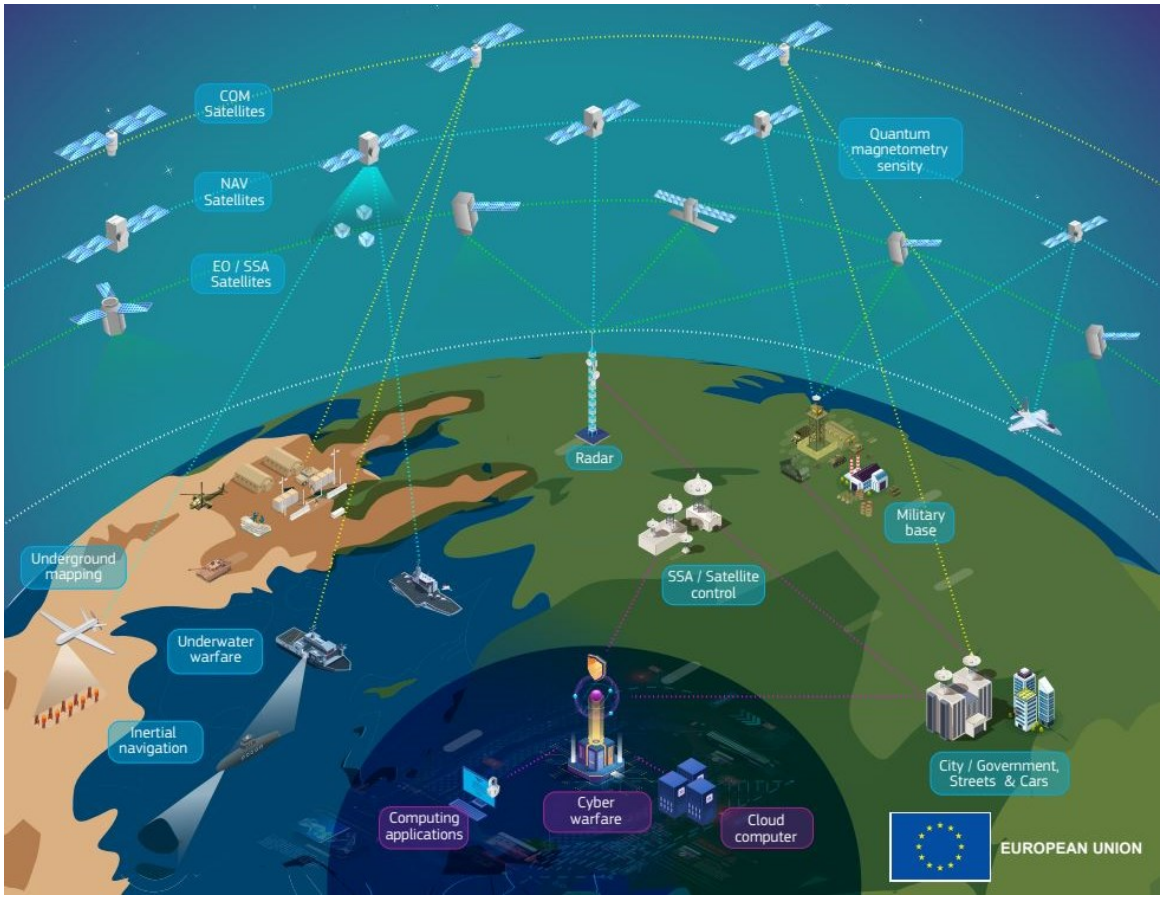
Rapporten är strukturerad på följande sätt: Efter inledningen redovisas lärdomar från tidigare översikter och rapporter (Kapitel 2). Metodkapitlet (3) beskriver datainsamling och analys av vetenskaplig litteratur. I Kapitel 4 presenteras resultaten från studien, följt av ett diskussionskapitel (5) som lyfter områden med behov av fortsatt utveckling och forskning. En kort summering och slutsatser i Kapitel 6 avrundar rapporten.

2 Lärdomar från tidigare studier, översikter och rapporter

I detta kapitel presenterar vi först branschrapporter och översikter över hot, sårbarheter och risker i förhållande till cybersäkerhet i rymdsystem i del 2.1, följt av akademiska litteraturöversikter i del 2.2.

2.1 Cybersäkerhet i rymdsystem

Rymdsystem beskrivs i litteraturen genom tre huvuddelar (se Figur 1): *rymdkomponenter*, exempelvis satelliter och andra typer av rymdfarkoster, *markstationer*, såsom antenner, uppskjutningsfaciliteter, datacenter och kontrollsystem, och *kommunikationsnätverk* mellan rymdkomponenter och markstationer (Oakley, 2020).



Figur 1. Rymdsystemets delar på marken, i rymden och där emellan (Källa: EU[1])

Det som gör rymdsystem unika är dess globala omfattning och de fysiska förhållandena i rymden. De utgör viktiga förutsättningar att beakta vid utveckling av systemets delar, till exempel gällande material, kapacitet och livscykler. Särskilt uppmärksamhet har därför lagts på rymdkomponenters design, tillverkning, uppskjutning och operation på grund av både

[1] https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en

de hårda förhållanden i rymden och de begränsade möjligheter till underhåll när de väl befinner sig på sin tilltänkta arbetsposition. Däremot har slutfasen av komponenternas livscykel först på senaste tiden fått ökat uppmärksamhet när tilltagandet av rymdskrot har börjat bli ett allvarligt hot för rymdkomponenterna och systemets funktionalitet.

Rymdsystem har utvecklats för att underlätta både observationer av jorden och rymden och kommunikation runt jorden men också till, från och mellan rymdfarkoster. I takt med att användningen av dessa tjänster har ökat, har antalet användningsområden breddats. Rymdsystem används bland annat för:

- Positionsdata för GPS-navigering,
- Precisa tidsangivelser för finansiella transaktioner,
- Satellitbaserad kommunikation i glesbefolkade områden,
- Klimat- och väderprognoser,
- Observationer av föremål i rymden och på jorden.

Dessa tjänster gör att systemet är intressant för ett stort antal samhällsaktörer inom civila och militära områden, inklusive politik och offentlig förvaltning, banksektorn, transport och logistik, matproduktion, forskning och samhällssäkerhet. När geopolitiska konflikter intensifieras (SVT, 2024) växer även intresset för rymdsystemets betydelse för samhället då störningar av relaterade tjänster anses bli vanligare framöver.

Som nämnt ovan kan rymdsystem ses både som en kritisk infrastruktur i sig och som en viktig komponent i andra kritiska infrastrukturer. Denna sammankoppling med andra system är karakteristiskt för komplexa socio-tekniska system i vilka relationerna mellan komponenterna inte är linjära/triviala - de är komplexa och därmed inte nödvändigtvis kausalt eller deterministiskt relaterade till varandra. I synnerhet behöver den globala karaktären uppmärksammas, vilket gör att lokala eller nationella ansatser har svårt att påverka alla relevanta hot och sårbarheter. Därför har uppmärksamheten gällande säkerhetsfrågor i förhållande till rymdsystem ökat och tidigare rapporter har sammanställt insikter om befintliga utmaningar och möjliga vägar framåt.

Några typiska problem som identifieras är bland annat (Hamill-Stewart och Ashdown, 2025):

- **Osäkra komponenter och leverantörskedjor**, vars sårbarheter, såsom tillgång till faciliteter, ofärdig hård- och mjukvara, olika nätverk samt information, kan attackeras på olika vis. Exempel på sådana attacker inkluderar insiderjobb, skadlig kod, avlyssning och obehörig ändring/borttagning av information.
- **Fragmenterat landskap** av säkerhetsstandarder, lagstiftning och riskuppfattningar globalt som i sin tur påverkar rymdsystemets alla komponenter, interaktioner och omgivningen samt den funktionalitet systemet tillhandahåller till samhället.
- **Brett spektrum av intressen,** exempelvis drivna av ekonomiska, geopolitiska, tekniska eller samhälleliga målbilder. Detta gör att sårbarheter och oreglerade områden kan utnyttjas genom bland annat sabotage, stöld av intellektuella tillgångar eller att skaffa sig obehöriga möjligheter till kontroll av rymdsystemets komponenter för att orsaka olika störningar.

- **Kommersialisering av rymdindustrin** till följd av lägre kostnader i sektorn har lett till en ökning av privata aktörer som agerar på marknaden. Detta bidrar till de första tre problemen ovan, exempelvis genom att användning av standardprogram och mjukvarubibliotek vid hård- och mjukvaruutveckling överför redan bekanta sårbarheter (till exempel svaga lösenord, fabriksinställningar för administrativa funktioner och att prioritera affärsnytta före säkerhet) till rymdsystemet.
- **Förutsättningar för säker utveckling och underhåll** av rymdsystem är särskilt utmanande eftersom det vanligtvis är långa processer under vilka teknik och organisationer förändras, vilket gör att även komponenter och metoder som var relativt säkra i designfasen riskerar att inte kunna leva upp till säkerhetsstandards som är aktuellt många år senare när de fortfarande är i bruk. Det är svårt att uppdatera rymdkomponenter när de är uppskjutna, vilket också försvårar användning av ny teknik för markstationer och nätverkskommunikation. Vid kommunikation mellan rymd- och markkomponenter prioriteras resurseffektivitet (hastighet, energi och kapacitet) före säkerhet, vilket gör att rymdsystem ofta saknar vissa säkerhetshöjande åtgärder, till exempel kryptering eller skydd mot intrång.
- **Automatisering och sammankoppling** med andra system följer samhällets teknikutveckling och intresset för rymdsystemets tjänster. På samma sätt som nya verktyg och arbetssätt kan underlätta för samhällsutvecklingen innebär de också en förstärkning av tidigare nämnda problem. Exempelvis kan sammankopplingen av olika system leda till att hotaktörer riktar sig mot sårbarheter hos sekundära system, underleverantörer eller kunder. Utmaningar med automatisering kan exemplifieras genom att satelliter och andra rymdfarkoster behöver manövrera självständigt och felfritt för att undvika kollisioner, inte bara med asteroider utan också rymdskrot som bland annat härstammar från förstöring av satelliter, en funktion som också kan manipuleras.
- **Hybrida hot** refererar till hotaktörer som medvetet använder sig av teknik och andra påverkansmetoder för att utöva makt på andra genom att skada, (för-)störa och destabilisera. I förhållande till rymdsystem bör särskilt olika förmågor att bekämpa satelliter (ASAT) nämnas. Då fysiska attacker mot rymdkomponenter genererar betydliga mängder rymdskrot (vilket utgör ett kaskadhot mot rymdsystem oberoende av geopolitiska avsikter, även kallat Kesslersyndromet) har strategierna bytt fokus till användning av laser, mikrovågor eller elektronisk störning / signalförfalskning. Så kallade bakdörrar som ger möjlighet till kontroll av satelliter är ytterligare av intresse vilket leder tillbaka till förstnämnda problemet gällande komponenter och leverantörskedjor.

Intensifierad geopolitisk konkurrens och konflikter innebär att hotet mot rymdsystem kommer att förbli förhöjt under överskådlig framtid.

I en rapport från Totalförsvarets forskningsinstitut (FOI) beskrivs utvecklingen av rymddomänen genom samverkan mellan domänens aktörer i tre perioder: kalla kriget, den eviga freden och den moderna rymdåldern. Analysen fokuserar på aktörsnätverk rörande två tillgångar – satelliter och uppskjutningsfaciliteter (Westman m.fl., 2025):

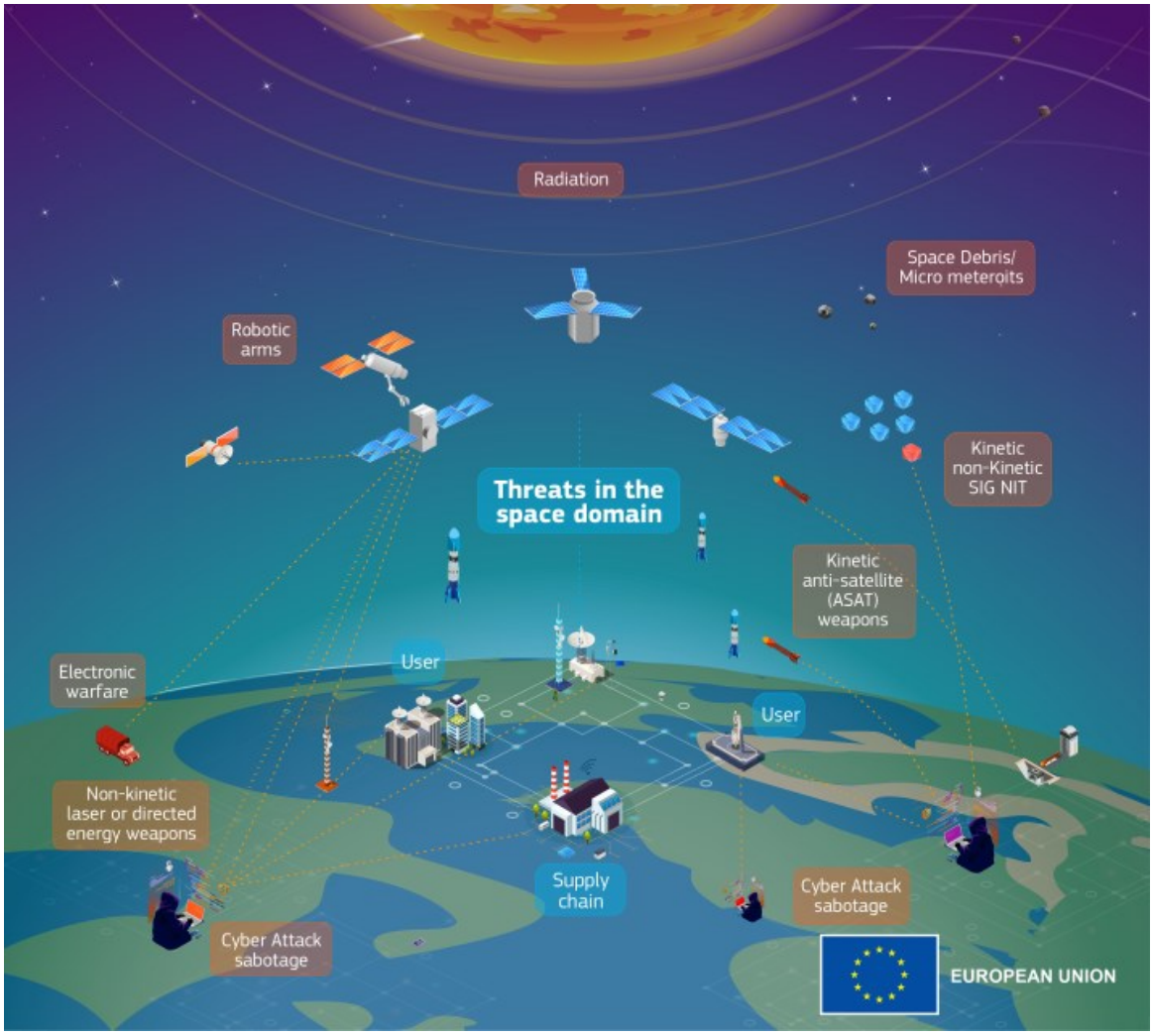
- ***Kalla kriget*** 1957–1990. Satellitnätverket under denna tid är ett mindre nätverk som dominerades av två stormakter: USA och Ryssland. Kina utgjorde en mer fristående part. Uppskjutningsnätverket synliggör däremot fyra distinkta poler som utgjordes av USA, Japan, Ryssland och Europa.
- ***Den eviga freden*** 1991–2010 som författarna refererar till som en "sammanflätad tid av samarbete", där satellitnätverket har vuxit betydligt till ett utökat, mer sammankopplat nätverk. Här finns fler kopplingar mellan USA, Ryssland och Kina tillsammans med fler aktörer som Japan och Kanada. Även uppskjutningsnätverket har blivit mer integrerat och består av tre dominerande kluster: Ryssland, USA och ett nät av aktörer från Europa.
- ***Moderna rymdåldern*** 2011–2024. Satellitnätverket har förändrats till en multipolär form av nätverk med en mångfald av aktörer där USA, Japan, Kina och Ryssland bildar tydliga poler. Indien och Sydkorea börjar också ta plats medan europeiska aktörer bildar ett stort nät av privata och statliga aktörer. Gällande uppskjutningsnätverket är det numera USA som dominerar följt av europeiska klustret medan de andra aktörer är mer integrerade. Nordkorea utgör en ny aktör i nätverket.

2019 antog Natos medlemmar en policy där rymden erkändes som en ny operativ domän, vid sidan av luft-, land-, sjö- och cyberrymden (NATO, 2024). Policyn påpekar att den jordnära rymden blir alltmer trång och konkurrensutsatt, och satelliter är sårbara för störningar. Därtill uppmärksammas utveckling och test av ett brett spektrum av tekniker för att attackera rymdsystemet, exempelvis Rysslands test av en anti-satellitrobot 2021. Policyn avser att vägleda Natos förhållningssätt till rymden och säkerställa rymdbaserat stöd till olika operationer. 2020 beslöts att Nato Space Centre ska etableras i Tyskland. 2023 offentliggjordes även planer på rymdbaserad övervakning och underrättelseverksamhet med hänvisning till förbättrad situationsmedvetenhet och beslutsfattande.

I en nyligen publicerad rapport utforskar EU:s institution för cybersäkerhet (ENISA) hotbilden för cybersäkerhet i rymden i syfte att rekommendera åtgärder och strategier för en robust utbyggnad av kommersiella satellitsystem och arkitekturer. Rapporten innehåller en livscykelmodell med tillhörande aktörer och taxonomier för tillgångar och hot. De främsta hoten mot satelliter är störningar, kapningar och exploateringar av datornätverk. I rapporten presenteras fyra riskscenarier som ligger till grund för rekommendationer, såsom minimistandarder för rymdindustrin, säkerhetsåtgärder i leveranskedjor, analys och test av komponenter innan de introduceras i produktionsmiljöer samt implementering av krypteringsåtgärder (ENISA, 2025).

European Space Policy Institute (ESPI) och Copenhagen Institute for Future Studies (CIFS) har tillsammans genomfört en framsynsanalys av rymdforskningens framtid i Europa 2040–2060. Studien beskriver fyra långsiktiga scenarier för utforskning av rymden och betonar kritiska osäkerheter och krafter som förvänta forma dess inriktning. Eftersom den europeiska rymdutforskningens framtid förväntas innehålla element från vart och ett av dessa scenarier, anses författarna att strategisk framsynthet är avgörande för dagens beslutsfattande, med ledord som alerthet, uthållighet och framåtblickande (CIFS, 2023).

2022 utarbetades EU:s första rymdstrategi för säkerhet och försvar (EU, 2024) där rymden identifierades som ett viktigt strategiskt område för att skydda rymdtillgångar, och försvara europeiska intressen samt att stärka motståndskraften hos rymdsystem och tjänster. Figur 2 illustrera de främsta hoten riktade till rymdsystem.



Figur 2. Hot mot rymdsystem. (Källa: EU[1])

2.2 Tidigare litteraturöversikter

Falco (2018; 2019) beskriver rymdsystem som kritisk infrastruktur. Författaren noterar att det saknas säkerhetsstandarder och att dessa systems unika karaktär gör dem extra utsatta. Rymdsystems unika egenskaper och förhållanden inkluderar:

- "Single point of failure" för många system som är beroende av rymdsystemet.
- Avsaknad av standarder och regleringar.
- Komplexa värdekedjor och livscykler.
- Hög användning av kommersiell "off-the-shelf" teknik som många aktörer har tillgång till (till exempel så kallade "CubeSats").
- Högt specialiserad personal, vilket gör det svårt för säkerhetsexperter att få tillgång till domänkunskap för att bygga säkerhetsåtgärder.

- Resursbegränsningar. Rymdsystem behöver vara strömsnåla och effektiva gällande nätverkskommunikation, vilket är begränsande för säkerhetsåtgärder.

Författaren presenterar följande principer för cybersäkerhet och rymdsystem:

- ***Organisation av rymdtillgångar***: Här ingår rekommendationer om arbetssätt och struktur, såsom att använda befintliga och utveckla nya standarder, att utveckla expertis för cybersäkerhet, säkerhetskultur och metoder för riskbedömning, inklusive användning av lämpliga standarder (till exempel NIST). Samarbete med forskare som är experter på säkerhetsfrågor lyfts också fram.
- ***Beslutsfattare***: Detta perspektiv riktar sig mot en strategisk nivå för att skapa förutsättningar för en säker utveckling. Det poängteras bland annat att det är viktigt att arbeta proaktivt i stället för reaktivt, klargöra säkerhetskrav på kritisk infrastruktur, och tilldela ansvar för cybersäkerhetsfrågor. Andra åtgärder är utökning av befintliga ramverk för att inkludera rymdsystem, och etablering av ett center för kunskapsdelning (Space System Information Sharing and Analysis Center (ISAC)).
- ***ISAC***: Centrets uppgifter är att upprätta informationsdelningskrav, dokumentera och uppdatera principer för cybersäkerhet och standarder, och att samarbeta med andra industrier som är beroende av rymdsystemet och dess tjänster.

Phillips m.fl. (2018) fokuserar på mjukvarusäkerhet för att reducera risker relaterade till mjukvara i satelliter. Artikeln innehåller en systematisk översikt av relevant litteratur och sex olika satellitprogram. Baserat på litteraturstudien och en enkät till experter inom dessa program undersöktes om säkerhets- och kvalitetshöjande praktiker genom mjukvaruutveckling kan förbättra satellitmjukvarans resiliens. Studien visade att sårbarheter i programvaror utgör potentiella cyberhot. Att minska antalet sårbarheter genom att förbättra arkitektur och metoder för mjukvaruutveckling anses bidra till att göra rymdsystemen mer motståndskraftiga.

Manulis m.fl. (2021) presenterar en översikt av cybersäkerhet i "New Space", en era som karaktäriseras av att en mängd olika aktörer utför aktiviteter i rymden. New Space står i kontrast till "Old Space" som kännetecknа en era som bestod av få aktörer, ofta militära, under kalla kriget (se, FOI:s rapport i del 2.1). Utöver en genomgång av satelliters livscykel, rymdsystemarkitektur och nya teknologier redogör författarna för hotbilder och incidenter relaterade till olika segment där kommunikationsnätverk är de målen som attackeras oftast. Författarna identifierade också nya utmaningar, exempelvis förknippade med det växande antalet av olika typer av satelliter som förväntas blir föremål för olika hot/attacker.

Höyhtyä m.fl. (2022) pekar på vikten av att bygga ut satellitinfrastrukturen på ett hållbart sätt i och med den ökade mängden aktörer och utvecklingen av 6G-standarden för nätverkskommunikation. Författarna presenterar en systematisk översikt över potentiella hot mot infrastrukturen, till exempel rymdtrafik, rymdskrot, och cybersäkerhet.

Kavallieratos och Katsikas (2023) presenterar en systematisk litteraturöversikt på temat cybersäkerhet i rymden. De analyserade 67 artiklar fördelade på sju aspekter: hot, attacker, risker, åtgärder, sårbarheter, lagstiftning, och kravställning för cybersäkerhet. Författarna föreslår fortsatt forskning på följande tematiska områden: säkerhet via design, metoder för

riskidentifiering i relation till kritisk rymdinfrastruktur, utveckling av ramverk för cybersäkerhet i rymden, mänskliga interaktioner, standarder och regleringar, och fokus på kaskadeffekter där man tar hänsyn till de komplexa nätverk som utgör rymdsystem.

Salim m.fl. (2024) kartlägger cyberhot och motåtgärder i förhållande till olika delar av satellitkommunikationssystem och deras livscykel från konceptstadiet till design-, tillverknings- och rymdstadiet. Studien innehåller omfattande redogörelser för cyberattackmetoder, möjliga konsekvenser, och cybersäkerhetsstrategier, med fokus på satellitsäkerhet. Författarna presenterar också en tidslinje över cyberattacker på Ukrainas satellitbaserade kommunikation år 2022.

Följande förslag på åtgärder mot cyberhot presenteras:

- ***Förebyggande av cyberattacker*** genom att fokusera på
    - efterlevnad av regler och standarder
    - kontinuerlig övervakning och hotinformation
    - planering av motståndskraft mot attacker
    - regelbunden utbildning i säkerhetsmedvetenhet
    - tredjepartsintressenters engagemang i säkerheten
- ***Försvar mot pågående cyberattacker*** genom en
    - strategi för försvar på djupet
    - gradvis begränsning av misslyckande
- ***Återhämtning efter cyberattacker***, exempelvis genom att utveckla
    - Mekanismer för självåterhämtning för rymdfarkoster
- ***Integrationen med 5G/6G*** som inkluderar implementering av åtgärder som
    - krypteringsprotokoll
    - starka autentiseringsmetoder
    - säkra system för nyckelhantering
    - kontinuerlig övervakning
    - nätverkssegmentering
    - säker kodningspraxis
    - mekanismer för återställning
    - förståelse för avancerad signalbehandling

Rapporten summerar ett antal öppna frågeställningar och olösta utmaningar som resulterar från det invecklade samspelet mellan tekniska och operativa aspekter av satellitkommunikationssystem, enligt följande:

- ***Säkerhet och sekretess***, såsom att säkerställa säker kommunikation och resurssnål autentisering, hantering av uppdateringar av firmware och programvara på ett effektivt sätt, skalbarhet och nyckelhantering, säkra leveranskedjor och försvar mot avancerade ihållande hot (Eng: advanced persistant threats)
- ***Genomströmning och energiförbrukning***, inklusive kommunikationslänkar mellan satelliter, olika typer av störningar av datatransmissionen från andra system samt energiförbrukning och -hantering
- ***Efterlevnad av regelverk***, särskilt utmanande för globala företag och leverantörskedjor som involverar olika aktörer, länder och legala ramar, vilket

kräver att organisationer kontinuerligt håller sig uppdaterade gällande lagstiftning och regelverk och också ställer krav på underleverantörer.

- ***Begränsade resurser*** är en betydande utmaning för satellitsystem. Involverade organisationer upplever utmaningar när det gäller att avsätta den tid, budget och personal som krävs för att säkerställa efterlevnad av komplexa regelverk och för att genomföra cybersäkerhetsåtgärder. Detta inkluderar utmaningar rörande brist på finansiering, begränsad tillgång till personal, föråldrad utrustning, brist på utbildning, otillräckliga riskbedömningar och en oförmåga att hålla jämna steg med nya hot.
- ***Nya kommunikationsparadigm*** är framväxande utmaning som förväntas påverka både teknikutveckling, kommunikationsprotokoll och organisatoriska och samhälleliga frågeställningar. Här nämns bland annat nya, kvantbaserade datorer och dataöverföringsteknik som baseras på mening i stället för på information (så kallad semantiska kommunikationsstrategier).

Diro m.fl. (2024) presenterar en överblick över utvecklingen av incidenter i rymdsystem från 1960-talet till 2020-talet och analyserar utvecklingen av tekniken och de hot som kan förknippas med olika delar av systemet. Författarna redogör även för hotaktörer, attackscenarier, riskreduceringsstrategier och skyddsmekanismer samt konsekvenser för till exempel geolokalisering och navigationssystem. De visar hur rymdsystem är komplexa och presenterar en modell som illustrerar denna komplexitet, samt utmaningar relaterade till denna typ av system. Författarna förespråkar utöver modell- och teknikutveckling interdisciplinära samarbeten mellan olika professioner som en väg framåt.

Varadharajan och Suri (2024) ger en översikt av cyberhot som riktas mot sårbarheter inom olika delar av rymdsystem, som de definierar ur ett tekniskt/fysiskt komponentperspektiv: rymdsegmentet, marksegmentet och länken mellan dessa segment. Författarna lyfter också fram användarsegmentet som ett tillägg till marksegmentet för att hänvisa till slutanvändare av rymdbaserade tjänster: personal, leverantörer, molntjänstleverantörer, forskningssamarbeten och andra aktörer som är potentiellt sårbara för, eller källa till cyberhot. Artikeln ger generella policyrekommendationer baserat på en diskussion av ett antal säkerhetsutmaningar, bland annat:

- De hårda förhållanden i rymden som påverkar komponenter,
- Datalagring och kommunikation,
- Säker positionering, identifiering och övervakning av rymdkomponenter
- Resurseffektiva säkerhetsprotokoll, säker nyckelhantering och routing gällande nätverkskommunikation,
- Management av systemprocesser och leverantörskedjor samt
- Gränssnitt till användarnas informationssystem.

Som många andra studier ser författarna liknelser mellan rymden och cyberrymden och framhåller kunskapsbrister gällande rymdrelaterad infrastruktur och deras roll i den globala informationsinfrastrukturen.

3 Metod och material

Studien bygger på en systematisk översikt av forskningslitteratur och andra relevanta publikationer (Webster och Watson, 2002; Okoli, 2015). Syftet är att beskriva vad som utmärker cybersäkerhet och säkerhetsarbete i rymdsystem och hur en bättre förståelse om detta kan förebygga störningar i rymdsystem för att stärka samhällelig resiliens.

Utöver en syntes av kunskapsläget och forskningsfronten skapas en systemmodell som illustrerar systemiska beroenden och olika intressenters behov. Syftet med modellen är att skapa förståelse för rymdsystems komplexitet, och bidra till att identifiera områden i behov av fortsatt forskning.

3.1 Urval

För att kartlägga forskning om cybersäkerhet i rymdsystem och deras betydelse för viktiga samhällsfunktioner var första steget att skapa ett urval av forskningsartiklar. Datainsamlingen avgränsades till sökningar i databasen Scopus. Tabell 1 illustrerar urvalsprocessen med söktermer, träffar och avgränsningar samt tillval.

Tabell 1. Söktermer och urval vid litteratursökningen i SCOPUS (01/2025)

Sökterm och urval	Antal Träffar	Läst
TITLE-ABS-KEY (cybersecurity OR "cyber security" OR "cyber-security") AND TITLE (space)	373	---
Efter första genomgång av urvalet: Relevant för kunskapsöversikten	190	Fulltext
Efter borttagning av konferensband, icke tillgängliga och felaktiga texter och texter av låg kvalitet	85	Fulltext
Ytterligare rapporter och “grå” litteratur	5	Fulltext

Urvalet förfinades i fyra steg; 1) Granskning av titlar och nyckelord, 2) Översiktlig genomgång av sammanfattningar och innehåll, 3) Identifikation av artikelns fokus och tillämpningsområde, och 4) Närläsning av artiklarna.

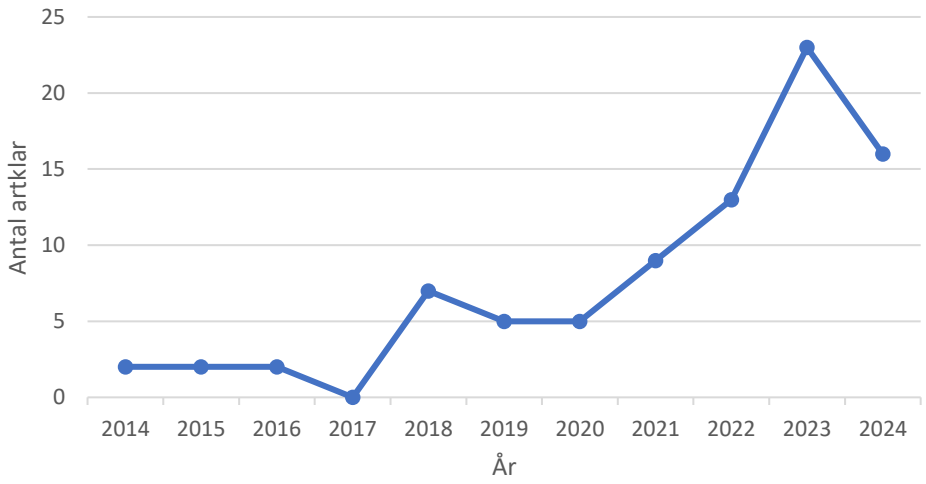
Sökningen ledde till ett urval av 373 artiklar. Nästan hälften av dessa sorterades därefter bort eftersom de inte var relevanta i den här studien: ofta behandlade de andra ”rum” (space), så som data-, offentliga, virtuella eller cyberrum (“cyber space”). Vi sorterade även bort artiklar som var av alltför spekulativ karaktär eller låg kvalitet. Den första genomgången av titlar, nyckelord och abstrakt ledde till ett urval 190 artiklar som ingick i den bibliometriska analysen. Efter en djupare granskning av publikationernas fokus bedömdes 75 artiklar som mindre relevanta för att kunna svara mot studiens mål och syfte. Dessa artiklar togs bort. Processen resulterade i ett urval bestående av 85 artiklar för vidare analys. De forskningsartiklar som ingår i den litteraturstudien har blivit publicerade mellan 2014 och 2024 av totalt ca 234 författare inom 37 olika vetenskapliga tidskrifter och konferenser.

Mycket av forsningen inom det undersökta området bedrivs och publiceras av forskare lokaliserat i USA, Storbritannien och Italien, följd av Australien, Kina, Estland, Frankrike och Tyskland. Tabell 2 visar de mest frekvent förekomna källorna i urvalet.

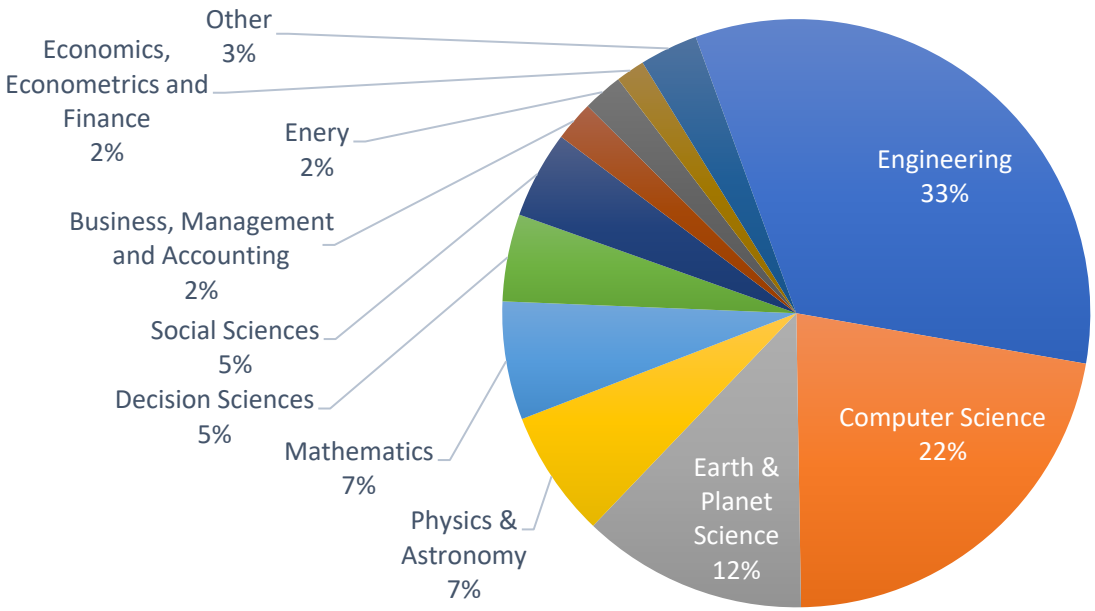
Tabell 2. Mest frekventa källor

Viktiga konferenser och tidskrifter i området
IEEE Aerospace Conference Proceedings
Proceedings Of The International Astronautical Congress Iac
International Journal Of Critical Infrastructure Protection
Lecture Notes in Computer Science
IEEE Access
Journal of Space Safety Engineering
Acta Astronautica
Space Policy

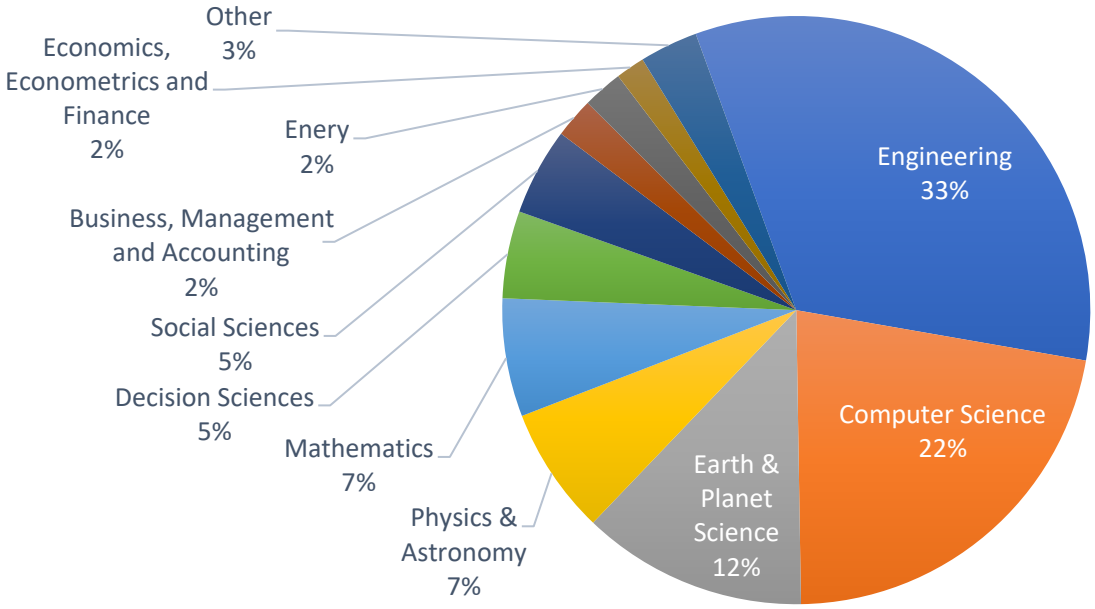
Utifrån sökningen i Scopus (se **Fel! Hittar inte referenskälla.**) går det att se en ökning a v nya publikationer sedan 2020 vilket kan kopplas till att hotbilden från cyberattacker och geopolitiska spänningar har ökat och uppmärksammats i olika sammanhang. Detta indikerar att forskningsfältet är under fortsatt utveckling vilket gör att denna studie ska förstås som en ögonblicksbild som ligger till grund för förslag på fortsatt forskning. Omkring två tredjedelar av publikationerna är konferensbidrag. Runt 30% är tidskriftsartiklar och de resterande publikationer resten är klassificerat som litteraturöversikter och bokkapitel.



Figur 3. Antal publikationer senaste tio åren.



Figur **4** illustrerar de forskningsområden där de utvalda artiklarna har publicerats. De flesta artiklar har publicerat inom ingenjörsvetenskap (33%), data- och systemvetenskaperna (22%) och jord- och planetforskning (22%), följt av forskning som har förankring i matematik (7%) samt besluts- och samhällsvetenskap (5% var).



Figur 4. Forskningsområden i urvalet.

3.2 Analys av litteraturen

Analysen av de utvalda artiklarna bygger på en metodisk ansats i tre steg:

1. Först utfördes en bibliometrisk analys av det utvalda materialet med hjälp av verktyget VOSviewer (van Eck och Waltman, 2014). Vi skapade en karta över forskningsfältet (Figur 5) baserat på hur ofta nyckelord förekommer tillsammans, med det minimala antalet förekomster inställd på fem. Analysen genererade sex kluster (Tabell 5) med 75 nyckelord. I detta steg ingick också en tolkning av vad klustren ”handlar om”. Denna analys gav en översiktlig bild av litteraturen.

2. För att skapa en fördjupad förståelse av litteraturen närläste vi artiklarna i steg 2 med syftet att identifiera teman. Här genomförde vi en tematisk analys som utgick från ett socio-teknisk system perspektiv, där tre fokusområden vägledde och strukturerade analysen: *Teknik, Organisation/Samhälle, Styrning*. Syftet var att skapa en bred förståelse för forskning med olika fokusområden. Braun och Clarkes (2006) riktlinjer för tematisk analys användes för att skapa teman under varje perspektiv och identifiera kunskapsluckor. Analysen vägleddes av frågorna i Tabell 3. För att lägga samman kunskap från den bibliometriska analysen (se steg 1) och den djupare tematiska analysen av innehållet i forskningsartiklar och andra publikationer använde vi ett ramverk bestående av fyra perspektiv: system, infrastruktur, styrning och processer (Große, 2023). Med hjälp av dessa perspektiv och fokusområden skapades underlag till både identifiering av viktiga kunskapsluckor och förslag för fortsatt forskning och utvecklingen av systemmodellen i steg 3.

Tabell 3. Forskningsguide

Perspektiv	Frågeställningar
System	• Vilka komponenter / aktörer är del av rymdsystemet? • Vilka interaktioner finns mellan komponenterna / aktörer? • Var kan gränsen dras mellan rymdsystemet och omgivningen?
Infrastruktur	• Vilken roll spelar rymdsystemet för samhället? • Vilka relationer finns till andra infrastruktursektorer? • Vilka är avnämare av tjänster som erbjuds av rymdsystem?
Styrning	• Vem kan anses äga rymdsystemet? • Vem har / ges möjlighet att påverka skapandet, operation och utveckling av rymdsystemet? • Vilka intressen finns kring rymdsystemet?
Processer	• Vad gör rymdsystemet? • Vilka krav finns riktad mot systemet och hur hanteras de? • Hur kan rymdsystemet utvecklas i framtiden?

3. Baserat på analyserna i steg 1 och 2 utvecklades också en systemmodell som kan användas som underlag för att öka förståelsen för systemiska beroenden av rymdsystem och möjligheter till att stärka resiliens inom samhällsviktig verksamhet. För att modellera det socio-tekniska system-av-system "rymdsystem” användes en

systemmodelleringsmetod utvecklad för att kartlägga olika intressenter som berörs av en situation. Metoden kan användas för att uppnå en gemensam förståelse för relevanta och nödvändiga åtgärder. I den här analysen var avsikten att skapa förståelse för systemiska beroenden inom rymdsystem och identifiera möjligheter hur cybersäkerhet i rymdsystem och resiliens i samhällsviktig verksamhet mot störningar kan vidare utvecklas. Metoden är väl beprövad och har använts i tidigare forskning med liknande avsikter för att utforska komplexa situationer och tillgodose olika intressenters behov, ofta i tidiga systemutvecklingsfaser (se exempelvis Checkland och Poulter, 2010; Große 2017, 2019; Große m.fl. 2025).

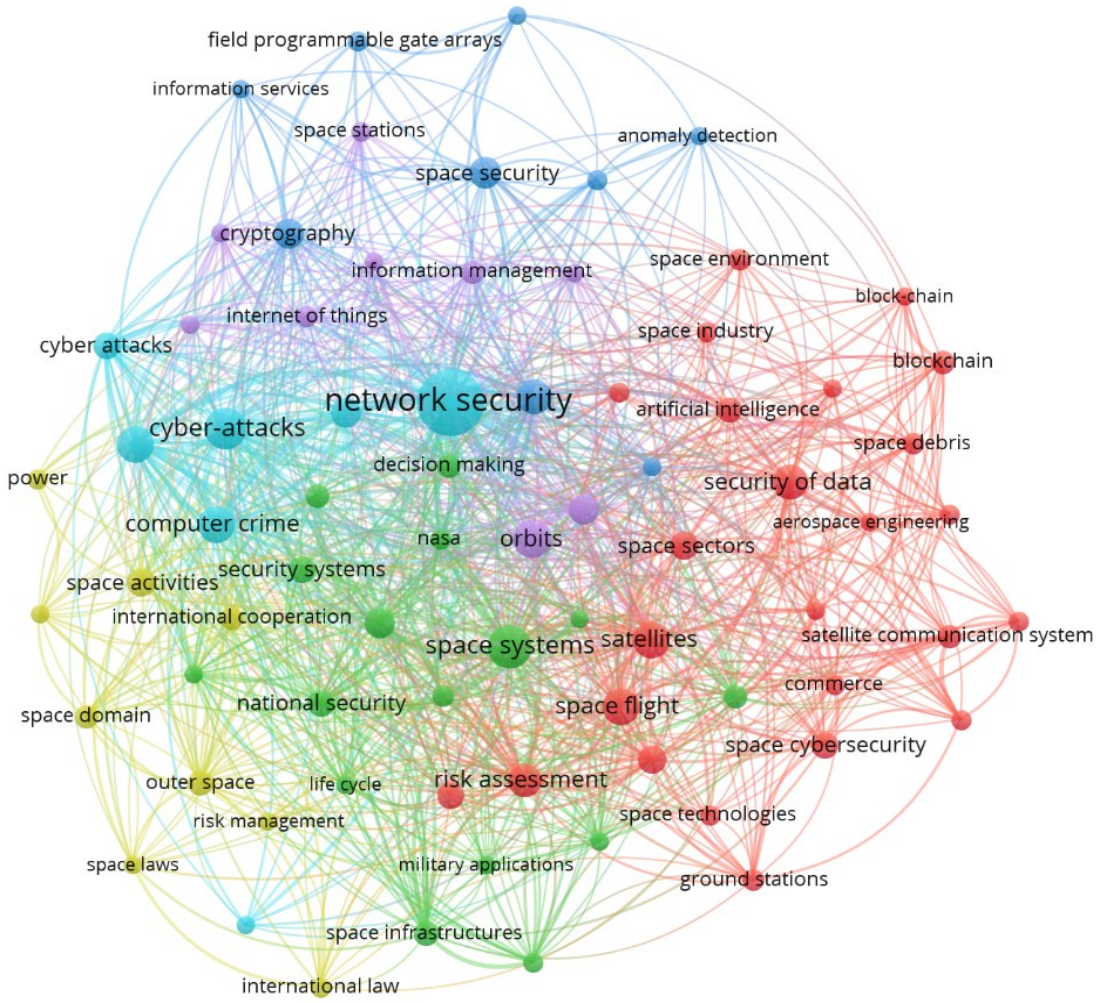
Syntesen av analyserna presenteras i det följande resultat- och analyskapitlet som strukturerades utifrån den bibliometriska analysen, den tematiska analysen, och systemanalysen för att ge en bild över områden som beforskats, utmaningar och möjligheter som lyfts fram och vilka områden som är av särskilt betydelse för att skapa ett motståndskraftigt digitalt samhälle. Med hjälp av utvalda exempel konkretiseras dessa perspektiv genom att presentera specifika teman och kunskapsluckor som uppstod när vi läste litteraturen. Implikationerna av detta för fortsatt forskning sammanställs i diskussionskapitlet.

4 Resultat och analys

Detta avsnitt innehåller resultaten av den bibliometriska analysen (4.1), tematiska analysen (4.2) och systemmodelleringen (4.3).

4.1 Bibliometrisk analys av litteraturen

I detta avsnitt presenterar vi resultaten från den bibliometriska analysen som ligger till grund för den tematiska analysen och konceptualiseringen av rymdsystemet och dess interaktioner. Analysen gav information om vilka aktörer, komponenter, interaktioner, förutsättningar, problem och lösningsansatser som finns och hur de är relevanta i samband med rymdsystemet i allmänhet och de olika delsystemen i synnerhet.



Figur 5. Nätverkskarta baserat på författarnas nyckelord.

Klustren med nyckelord (Tabell 4) bidrar med översikter av relevanta dimensioner, såsom kunder/aktörer, systemfunktioner och ägare samt viktiga perspektiv och förhållanden. Förutom olika tillgångar på marken, i omloppsbana och rymden belyser till exempel klustren ”röd” och ”grön” i Figur 5 en rad aktörer från industri och myndigheter som är involverade

i att forma och använda rymdsystemet. Relevanta nyckelord här är bland annat 'markstationer', 'satelliter', 'rymdfarkoster', 'rymdindustri', 'handel', 'NASA' och 'offentliga arbeten'. Dessa två kluster visar också på säkerhetsrelaterade problem genom nyckelord som 'rymdskrot', 'datasäkerhet', 'livscykel' och 'säkerhetssystem'.

Tabell 4. Kluster av nyckelord med beskrivningar.

Kluster	Beskrivning	Exempel på nyckelord
Röd (25 objekt)	Industriaktörer	markstationer, satelliter, rymdfarkoster, rymdindustri, leverantörskedjor, livscykel
Grön (16 objekt)	Rymd som kritisk infrastruktur	NASA, offentliga arbeten, informationsservice, nationell säkerhet, rymdapplikationer, säkerhetssystem
Blå (9 objekt)	Nätverk	Autentisering, kryptografi, nätverksarkitektur, rymdsäkerhet, anomalidetektering
Turkos (9 objekt)	Cyberhot	Databrott, cyberattacker, cyberhot
Gul (9 objekt)	Lagar och förordningar	internationellt samarbete, internationell rätt, rymdlagar, rymdverksamhet, riskhantering, informationsspridning
Lila (7 objekt)	Rymdoperationer	jorden (planet), omloppsbanor, rymdstationer, bemannad rymdfart, satellitnätverk

Klustret ''blå'' är direkt kopplat till nätverkssäkerhet för rymdsystem, vilket framgår av nyckelord som 'autentisering', 'kryptografi' och 'rymdsäkerhet'. Fokus ligger på den tekniska delen av systemet.

Klustret ''turkos'' omfattar olika hot mot rymdsystem, som representeras av nyckelord som 'databrott', 'cyberattacker' och 'cyberhot'. Klustret ''gult'' innehåller nyckelord som rör ägande och reglering, med tanke på att rymden inte följer nationella gränser, vilket väcker frågor som rör 'internationellt samarbete', 'internationell rätt' och 'rymdlagar'. Vidare anges frågor och överväganden som rör 'rymdverksamhet', 'informationsspridning' och 'riskhantering'. Slutligen innehåller det ''lila'' klustret artiklar som rör verksamhet i jordens omloppsbana, med nyckelord som 'jorden (planet)', 'omloppsbanor', 'rymdstationer' och 'bemannad rymdfart.

4.2 Tematisk sammanställning av litteratur

Resultaten från litteraturanalysen är grupperade under tre övergripande teman: Styrning (4.2.1), organisatoriska aspekter (4.2.2), och tekniska aspekter (4.2.3). Varje övergripande tema innehåller även ett antal underteman, illustrerat i Tabell 5.

Tabell 5. Teman som framkommer i litteraturen.

Tema	Utmaningar	Förslag på lösningar och fortsatt forskning
Styrning		
Lagstiftning	Det saknas gemensam och global lagstiftning.	Utgå från och utveckla befintlig lagstiftning, stifta nya lagar vid behov.
Internationellt samarbete	Spänningar mellan upprustning i rymden och "for the good of mankind".	Systemtänk! Tänk större: gå från den enskilda satelliten till ett större system.
Standarder	Det saknas implementerade standarder för cybersäkerhet i rymden.	Använd befintliga standarder, och utveckla nya vid behov.
Organisatoriska aspekter		
Kunskaps- och informationsdelning	Det saknas metoder för kunskapshantering mellan olika aktörer.	- Uppmuntra informationsdelning mellan olika parter (till exempel satellittillverkare). - Upprätta kunskapscenter för cybersäkerhet och rymdsystem. - Skapa anpassade utbildningsinsatser i cybersäkerhet för rymdpersonal.
Riskhantering	Rymdsystem och deras utveckling är komplex, vilket gör det svårt att utveckla och använda standardmetoder.	Utveckla systemisk riskstyrning och adaptiva riskhanteringsmetoder.
Tekniska aspekter		
Nätverks-kommunikation	Rymdsystem bygger i hög grad på nätverks-kommunikation mellan markstationer och rymdkomponenter. Det gör dem sårbara för diverse attacker.	- Utveckla testbäddar för att vidareutveckla de föreslagna teknikerna. - Från labbet till rymden. Det behövs mer forskning på faktiska tillämpningar.
Arkitekturer	Det saknas standardiserade lösningar för rymdsystem...	Författare beskriver tekniska lösningar för till exempel arkitektur och kryptering i rymdsystem.
Algoritmer och simuleringar	Rymdsystem är byggda för begränsad bandbredd och att vara energisnåla, etc. Det försvårar cybersäkerhetsåtgärder eftersom dessa drar mer resurser.	Författare beskriver tekniska lösningar för att skapa energisnåla cybersäkerhetsåtgärder

4.2.1 Styrning

Styrning i förhållande till cybersäkerhet i rymdsystem omfattar tre centrala aspekter: lagstiftning, internationellt samarbete, och standarder. Dessa beskrivs närmare nedan.

4.2.1.1 Lagstiftning

Cybersäkerhet i rymden är ett komplext fenomen där det saknas detaljerad global lagstiftning. I och med att rymden är en arena för geopolitiska konflikter är en av utmaningarna att de involverade aktörerna (till exempel stater) har olika synsätt, som illustreras av citatet från Bace m.fl. (2024 s.9) nedan:

> *"While this paper set out to argue that existing international law could be applied to cyberattacks on space infrastructure, it would be a mistake to ignore the reality that there is still significant ambiguity and varying interpretations, potentially impeding the unequivocal enforcement and application of these laws in such scenario." p. 9.*

Andra författare hänvisar till att lagstiftning som togs fram under kalla kriget då rymden blev en viktig del i kapplöpningen mellan stormakterna skulle kunna användas som utgångspunkt för att formulera globala lagar för cybersäkerhet. Dilworth och Osborne (2024) nämner till exempel "Outer Space Treaty" från 1967 (se även, Balleste, 2018).

Outer Space Treaty[2] innehåller till exempel formuleringar om användning av massförstörelsevapen och överenskommelser om att stater bör konsultera varandra om de planerar aktiviteter som är potentiellt störande för andra staters fredliga utforskande av rymden (Carlo och Veazoglou, 2020). Detta är särskilt relevant i kontexten anti-satellitvapen (ASAT). Ett anti-satellittest ("Y-1C ASAT ") utfört av Kina 2007 kritiserades just för att det inte föregicks av sådan dialog. Potter (2015) reflekterar över huruvida cyberattacker kan klassificeras som massförstörelsevapen, och behovet av klarhet gällande lagstiftning på området:

> *"Ground war […] has now largely become an unregulated cyber-satellite war." The paper particularly emphasises the risk of "hacking the friendly skies", that is, the cyber-related risks of commercial aviation. Examples include poorly segmented networks, low-security industrial control systems and hacked drones. Another concern is ensuring the correctness when it comes to the core of logistics as well as military operations: positioning, navigation and timing (PNT)."*

Carlo m.fl. (2020) nämner flera problembilder relaterade till cybersäkerhet och rymdsystem: ökat antal aktörer, både offentliga, privata, civila och militära, utför nu aktiviteter i rymden. Det saknas gemensamma policys och regleringar. Behov av gemensam och global lagstiftning är stort, men faller på att de inblandade aktörerna har olika intressen. Författarna menar att dessa frågor kommer att bli olösta såvida inte a) aktörerna kommer överens, eller b) de löses i efterdyningarna av en konflikt i rymden. Martin och Freeland (2023: 2024) pekar på en trend där lagstiftningen tenderar att bli fragmenterad och formulerade på nationell nivå istället för global nivå, och att detta är särskilt problematiskt i

[2] https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

kölvattnet av en snabb teknikutveckling som ändrar förutsättningarna för cybersäkerhet (till exempel utvecklingen av kvantdatorer). Breda m.fl. (2022,2023) menar att AI-teknik spelar en allt större roll i rymdsystem, till exempel för att positionera satelliter. Författarna redogör för nya sårbarheter som uppstår i och med AI-systems oberäknelighet, och föreslår insatser för att hantera dem. Exempel på sådana insatser är specifik reglering och cybersäkerhetsprinciper för användning av AI i rymdsystem. Även Carlo m.fl. (2023) pekar på vikten av att reglera användningen av AI-system i rymden.

Även Petrovici och Carlo (2018) pekar på hur fler aktörer än tidigare är intresserade av att nyttja rymden, till exempel för kommersiella aktiviteter. Författarna diskuterar denna trend (även kallad "Space 4.0" eller "New space") med utgångspunkt i europeisk och nordamerikansk lagstiftning (se även Davis m.fl., 2024; Segate, 2024):

> *"It is clear, that cooperation remains a core element of the peaceful uses of outer space. New legal mechanisms need to avoid unnecessary impediments of private space activities and at the same time have to comply with historical space law principles, such as the province of all-mankind maxim."*

Men det finns även en oro för att lagstiftningen blir en angelägenhet endast för västländer och att det krävs samarbete till exempel mellan USA och Kina (Hoffmann m.fl., 2020).

Bodeau m.fl. (2014: 2023) föreslår en systems-of-systems approach för att skapa resilienta rymdsystem och diskuterar möjliga sätt att arbeta med olika resilienshöjande åtgärder, både teknikorienterade och organisationella, som kan överföras till andra typer av globala / komplexa system. Författarna utpekar i synnerhet utmaningar relaterade till styrning av sådana system, såsom beslutsmandat, ansvars- och kostnadsfördelning samt koordination av samverkan kombinerat med interoperabilitetsproblem av olika slag.

Carlo och Breda (2024) pekar på vikten av att se rymdsystem som kritisk infrastruktur då de är viktiga förutsättningar för funktionaliteten av andra samhällsviktiga områden, exempelvis transporter och logistik, energi och matförsörjning samt en rad andra sektorer som är beroende av informationstjänsterna. Författarna utgår från dessa systems egenskaper för att söka en bättre förståelse för beroenderelationerna mellan rymdsystem och sektorer av kritisk infrastruktur och den inverkan juridiska och policy-relaterade aspekter kan ha på framtida utveckling.

4.2.1.2 Internationellt samarbete

Carlo och Roux (2022) menar att den ökade användningen av ny teknik i rymdsystem bör ackompanjeras av koordineringsinsatser för att säkerställa att denna användning sker för mänsklighetens bästa. I samma anda menar Martin (2023) att cybersäkerhet i rymden bör förstås ur två aspekter: säkra och hållbara lösningar, och säkerställandet att aktiviteter i rymden genomförs med mänsklighetens bästa i åtanke. Författaren jämför rymden med andra områden i behov av global styrning, såsom Antarktis och oceanerna och föreslår ett ramverk för cybersäkerhetsfrågor baserat på internationell lagstiftning och industristandarder.

I och med ökad polarisering mellan olika geopolitiska block menar Racionero-Garcia and Shaikh (2024) att även om vi kommer att se ökat internationellt samarbete i rymdfrågor mellan länder kommer dessa samarbeten förmodligen att ske inom ramen för olika allianser (till exempel EU och / eller NATO). Detta kan i sin tur leda till ökade militära spänningar och till och med konflikter i rymden:

> *"… the dual-use nature of space technologies and the adoption of strategic competition as the main driver of this kind of segmented international cooperation entails the impossibility of addressing collective problems that affect the entire international community, such as space debris. And, as West suggests, it could also further escalate military tensions and even conflict in outer space [West, 2020]."*

Samtidigt menar Suwijak och Li (2022) att *"International cooperation is the only way to provide a fully coordinated approach to cyberspace protection which is consistent with the fundamental premise of international cooperation and collaboration in space"*.

Sammantaget innebär den ökade mängden aktörer i rymden, i kombination med geopolitiska konflikter att det är mer nödvändigt men också svårare än någonsin att formulera och verkställa regler för samarbeten i rymden (Verco, 2021).

4.2.1.3 Standarder

Abanades m.fl. (2018) beskriver hur åtgärder för att säkerställa ansvarighet (accountability) ej implementerats i någon hög utsträckning i rymdsystem. Författarna fokuserar på åtgärder för att förbättra cybersäkerhet och föreslår efterlevnad av ISO 27000-standarden som ett minimikrav, tillsammans med användning av protokoll som till exempel LDAP (lightweight directory access protocol). Blount (2020) visar hur legala frågor kring cybersäkerhet i rymden är komplexa och involverar policys, tekniska standarder och specifikationer (till exempel ISO 27001, AIAs NAS9933 och CNSS som är ett tillägg till NIST 800–53 med specifikt fokus på rymden). Blount menar dock, i likhet med andra författare, att cybersäkerhet i rymden fortfarande är ett öppet område, och att det inte går att blint förlita sig på standarder: det krävs kollektiva insatser för att skapa gemensamma standarder, regler och metoder.

Dygnatowski (2021) pekar ut rymdsystem som en viktig del av nationell säkerhet. Författaren menar att det borde vara föremål för samma säkerhetsåtgärder som annan kritisk infrastruktur, men att rymdsystem har unika egenskaper som gör att de riskerar att bli "den svagaste länken" i en nations infrastruktur. Ett första steg borde vara att implementera standarder såsom NIST menar författaren. Finke m.fl. (2023) presenterar en testbädd baserad på NIST för att skydda kommersiella satelliter mot cyberattacker och möjliggöra fler samarbeten.

4.2.2 Organisatoriska aspekter

I denna del presenteras perspektiv som utgår från de organisationer som på ett eller flera sätt hanterar rymdsystem. Två teman identifierades i den befintliga litteraturen: informationsdelning och riskhantering.

4.2.2.1 Informationsdelning

Housen-Couriel (2023) menar att informationsdelning mellan aktörer är viktig för att minimera kunskapsgapet mellan attackerare och försvarare:

> *"In the foreseeable future, States, international organizations, and private companies will bear the lion's share of ensuring resilience to cybersecurity in outer space; and must learn to effectively share reliable and actionable information that improves their cyber situational awareness in outer space." (p. 549).*

Jones (2024) undersöker beslutsfattares uppfattningar om cybersäkerhet i satellitsystem via en enkät. Riskmedvetenheten bland deltagarna ökade mellan åren 2012 och 2022, och författaren föreslår att området behöver beforskas ytterligare, och att satellittillverkare behöver dela med sig av information om cyberattacker.

Shahzad m.fl., (2024) undersöker ingenjörers och cybersäkerhetsexperters erfarenheter och poängterar vikten av investeringar i utbildningsinsatser. På samma tema presenterar Hills m.fl. (2022) en skräddarsydd utbildning i cybersäkerhet för personal inom rymdsektorn. Utbildningen omfattar individanpassade moment, med konkreta laborationer, och anpassade scenarier, till exempel genom användning av "digitala tvillingar". Framtida forskning bör fokusera på att utveckla denna typ av skräddarsydda laborationer menar författarna.

4.2.2.2 Riskhantering

Berthoud och Agass (2021) noterar behov av resilienta satellitsystem i och med att de utgör en viktig komponent i kritisk infrastruktur. De använder modellering för att identifiera hot mot satelliter fördelade på fyra typer: Kinetiska vapen, cybersäkerhet, rymdväder, och rymdskrot. Författarna presenterar hotbilder och skapar scenarier för varje typ.

Boschetti m.fl. (2022) pekar på vikten av placering av markstationer för rymdsystem, med betoning på Finland och Sverige i och med att de befinner sig vid NATO:s östra gräns, men även nära Arktis som är föremål för geopolitisk konkurrens. Cantelli-Forti m.fl. (2021) presenterar ett system ("SCOUT") för att skydda markstationer mot cyberattacker. Författarna testade systemet genom simuleringar i Matera, Italien, men menar att det går att implementera i andra kontexter också i och med att markstationers infrastruktur är relativt lika. Det bör noteras att det som presenteras, i likhet med andra artiklar, är resultat av labbliknande experiment.

Curbo och Falco (2023) presenterar en forskningsagenda för mjukvarusäkerhet vid rymdfärder. Givet det ökade behovet av säkerhetsåtgärder på området föreslår de följande agenda: Kravformulering för resiliens, undersökning av: säkerhetsaspekter för RTOS (real

time operating systems) som ofta används vid rymdfärder, säkerhet för uppdragsapplikationer och "payloads", säkerhetsaspekter för subsystem (command and data handling, C&DH), navigationssystem, autonoma system, metoder och skydd mot hot riktad mot "flight software" (ramverken SPARTA och TREKS nämns specifikt), adversaries / malware. Dessa rekommendationer kan användas vid design av rymdsystem för att öka deras motståndskraft mot cyberattacker. Ear m.fl. (2023) försöker att ta sig an problemet att det saknas data om cyberattacker mot rymdsystem genom att skapa ett eget dataset och extrapolera 4076 attackkedjor från fyra offentliga dataset med data från 1977–2019. De använder ramverken SPARTA (se ovan) och MITRE ATT&CK. Författarna pekar på hur antalet attacker ökar, samtidigt som en stor del av dem är möjliga att stoppa. De rekommenderar fortsatt forskning på att bygga upp den här typen av dataset och hitta sätt att automatisera åtgärder.

Vessels m.fl. (2019) presenterar en riskhanteringsteknik med fokus på nätverkskommunikation. Mailloux m.fl. (2019) föreslår en systemteoretisk processanalysmetod för att förstå och beakta säkerhetskrav vid systemutveckling och ger ett exempel på ett försörjningssystem för den internationella rymdstationen ISS. Relevanta säkerhetskrav relaterar till funktion, design och arkitektur av sådana komplexa system. Nyttan med ansatsen menar författarna är att utveckla kravställning för säkerhet och resiliens som kan beaktas redan från början vid systemdesign och -utveckling och som kan mätas och verifieras.

Knez m.fl. (2016) har utvecklat en säkerhetsutvecklingsprocess baserat på olika riskanalyskoncept och testat denna på ett scenario för ett rymduppdrag. Författarna diskuterar en rad insikter om problem som kan uppstår i samband med att implementera en sådan process:

- Generiska ramverk behöver anpassas till specifika operationer, att risker i ett komplext system inte kan identifieras och beskrivas fullt ut.
- Ett uppdrags resiliensbehov behöver förstås först innan cybersäkerhetsåtgärder kan implementeras.
- Det saknas lämpliga utvärderingstal för att mäta cybersäkerhet.
- Det krävs både detaljkunskap, ett team av olika professioner som kan jobba effektivt ihop och träning.
- Det inte finns en enkel receptbok för att utveckla eller automatisera säkerhetsarbetet.

En annan automatisk riskhanteringsprocess är "BlueGen", utvecklad av McNeil m.fl. (2018).

Kaczmarek (2024) diskuterar cyberhot och attackmetoder riktade mot satelliter, rymdfarkoster, jordstationer och kommunikationsnätverk. Författaren presenterar fem exempel på genomförda attacker mot satellitsystem och utforska potentiella risker förknippat med implementation av AI. Rekommendationer för att säkerställa en bra säkerhetsnivå inkluderar att arbeta proaktiv med cyberförsvar, att använda AI på ett ansvarsfullt och etiskt sätt och att skapa globala cybersäkerhetsstandards.

4.2.3 Tekniska aspekter

I denna del presenteras artiklar med fokus på teknik relaterad till cybersäkerhet i rymdsystem. Sammanfattningsvis presenterar dessa artiklar både tekniska utmaningar respektive lösningar. Vi har samlat artiklarna i tre underkategorier: nätverkskommunikation, arkitekturer, och algoritmer och simuleringar.

4.2.3.1 Nätverkskommunikation

Hannan (2018) och Pazouki och Aydeger (2023) diskuterar hot mot ISS, i form av injektionsattacker som har potential att slå ut rymdstationens strömförsörjning. De rekommenderar säkerhetsåtgärder i form av kryptografi, brandväggar och ett "intrusion preventing system" för att säkra kommunikationerna mellan jorden och ISS.

Carter m.fl. (2020) fokuserar på "fog-cloud computing" som en teknisk lösning för säkra kommunikationer i rymdsystem. Fog-cloud computing använder "edge devices" för att säkra kommunikationer i moln och sakernas internet (IoT) miljöer. Författarna föreslår att framtida forskning ska använda simuleringar för att testa denna teknik. Crabtree och Rookard (2024) använder i sin tur simuleringar för att utvärdera olika teknikers "trust-metrics" i kontexten rymdsystem. De föreslår ytterligare forskning på området och utveckling av testbäddar.

Crocetti m.fl. (2024) presenterar en krypteringsteknik (AES-GCM) som de testar på "space-grade" FPGA:s (Field Programmable Gate Array: är en integrerad halvledarkrets som består av en uppsättning logiska block som kan konfigureras ((eller programmeras)) när de används av slutanvändaren. De är "icke-flyktiga", det vill säga kan inte omkonfigureras, är robusta mot strålning och har små fördröjningar), och föreslår fortsatt forskning för att utveckla denna teknik. Författarna (2023) presenterar även energisnål hårdvarukryptering, HMAC, för användning i rymdsystem. De (2024) presenterar även en tredje teknik för kryptering – AES-CMAC. Samtliga tekniker presenterade av författarna följer CCSDS (the Consultative Committee for Space Data Systems)-standard.

Marsili m.fl. (2023) jämför tre kommunikationsmetoder, baserat på radio, laser och neutroner. Författarna påpekar att radiokommunikation mellan satelliter är förhållandevis lätt att störa och avlyssna, att optisk kommunikation har vissa fördelar jämfört med radio, men inte är helt störningsfri och föreslår därför neutron-baserad kommunikation eftersom neutroner är mycket snabbare och kan ta sig igenom material. Detta anses göra avlyssning och störning av kommunikation svårare.

Maple m.fl. (2022) identifierar behov av säkra kommunikationer mellan till exempel rymdstationer och markstationer. Författarna presenterar olika typer av algoritmer för kryptering, och jämför deras prestanda och pris.

4.2.3.2 Arkitekturer

Boschetti m.fl. (2023) föreslår en "hybrid" rymdarkitektur med fokus på norra Europas Arktis ("high north"). Ledord i en sådan arkitektur är heterogena nätverk och ekosystem

som bidrar till ökad redundans, resiliens och skalbarhet. De föreslår fortsatt forskning att integrera studier av hybrid rymdarkitektur med cybersäkerhetsaspekter.

Bhuva och Kumar (2023) menar att blockkedjeteknik har stor potential att användas för att skapa säkrare kommunikationssystem i rymden. Det bör noteras att denna studie bygger på labbarbete och författarna rekommenderar fortsatt forskning på området. Dailey och Reed (2019) anammar ett sociotekniskt synsätt för att formulera en International Space Reference Architecture (ISRA)-arkitektur. Arkitekturen består av policy, en gemensam vokabulär, och teknisk innovation. Målet är att utveckla ett ramverk för delade normer och önskade beteenden för att säkerställa maximal socioekonomisk nytta i rymden. ISRA utgör en gemensam vision i ett splittrad reglerat landskap menar författarna och de citerar Deborah Barnhart (f.d., Chief Executive Officer and Executive Director vid U.S. Space & Rocket Center): "*Engineering is easy… policy is hard*" s.3. De föreslår blockkedjetekniken som en potentiell kandidat för att stötta arkitekturen. Även Drobyazko och Hilorme (2021) föreslår blockkedjor som en teknik för att öka rymdsystems cybersäkerhet. Dessa författare pekar även på vikten av att implementera system för att minska rymdaktiviteters negativa effekt på miljön. Falco och Gordon (2024) presenterar en blockkedjebaserad arkitektur för att möjliggöra "space infrastructure as a service" som kan delas och användas mellan olika aktörer. Ytterligare en artikel som fokuserar på blockkedjor i kontexten av rymdsystem är Yang m.fl. (2023).

Bradbury m.fl. (2020) refererar till fenomenet "New Space" som karaktäriseras av att ett allt större antal olika aktörer positionerar enheter, satelliter och system i rymden. Detta öppnar upp för flera möjligheter (attack vectors) för cyberattacker. Författarna presenterar en "Internet of Space Things, IoST"-arkitektur som utgår från hot från aktörer på fyra olika nivåer: individer (till exempel individuella hackers eller insiders), grupper (med ett visst fokus) organisationer (till exempel konkurrenter) och nationer (geopolitiska rivaler). Det bör noteras att detta är en referensarkitektur på generell nivå och bör kompletteras med metoder för att hantera hot på lägre nivåer.

4.2.3.3 Algoritmer och simuleringar

Denna kategori är bred och består främst av labbforskning där olika simuleringar av attacker genomförs, ofta tillsammans med utveckling av algoritmer som skydd mot cyberattacker.

Shaw m.fl. (2015) simulerar en attack som stör kommunikation mellan rymdfarkoster och markstationer. Pavur och Martinovic (2021) simulerar ett scenario där spionsatelliter försöker lura rymdlägesbildsdata för att missta dem som rymdskrot. Författarna använder maskininlärning för att bygga en detektor med god prestanda. Deras ansats bygger på en multidisciplinär ansats där cybersäkerhetsaspekter kombineras med kunskap från astrofysik och internationell säkerhet. Li (2023) pekar på behov av metoder för att identifiera rymdskrot, både oavsiktligt och avsiktligt skapat. Hotbilden bygger på att en fientlig aktör avsiktligt kan sätta rymdskrot i omloppsbana, till exempel genom att förstöra en rymdfarkost. Även Woodward m.fl. (2021) använder maskininlärning (djupinlärning) för att identifiera anomalier i rymdsystem. Lefcourt m.fl. (2022) hänvisar till störningstekniker (crosstalk, jamming, spoofing, replay) använda i Rysslands anfallskrig mot Ukraina, och menar att dessa

typer av störningar (Radiofrequency interference) måste karaktäriseras och använder neurala nätverk för att identifiera dessa störningstekniker. De presenterar en proof of concept (POC) och har publicerat datasetet de använde i studien. Även Zhou m.fl. (2021) menar att maskin/djupinlärning är en framtidsteknik för anomalidetektering i rymdsystem.

Byrne m.fl. (2014) pekar på behov av säkerhetsåtgärder för rymdflygningar (space flight missions). Författarna presenterar en testmiljö för att testa cybersäkerhet i denna kontext och planerar att utveckla en testbädd för detta ändamål. Schalk och Brown (2023) menar att tidigare forskning i hög grad använt sig av hypotetiska scenarier. Författarna utför en attacksimulering på NASA:s "core Flight System (cFS)" som är tillgängligt som öppen källkod.

Zhang och Du (2023) experimenterar med denial-of-service (DoS)-attacker mot markstationer och menar att placeringen av dessa stationer påverkar prestandan i olika scenarier. Madani m.fl. (2024) diskuterar hur tillförlitlighet och säkerhet av optiska kommunikationsverktyg, såsom laser-baserat kommunikation mellan rymd- och jordstationer kan förbättras. Utöver utmaningar relaterade till avstånd mellan enheterna diskuteras även störningsscenarier, exempelvis avlyssning med hjälp av "malicious" satelliter och DoS-attacker genom blockering av "line-of-sight" mellan kommunicerande enheter. Författarna diskuterar hur användning av jord- och satellitbaserade radarsystem kunde hjälpa att upptäcka sådana typer av attacker.

Carlo och Boschetti (2023) fokuserar på Space Situational Awareness (SSA) system (det vill säga system som används för att hålla reda på objekt i rymden, såsom satelliter och rymdskrot) i ytterligare en artikel med fokus på Arktis och (norra) Europa. Genom modellering identifierar författarna hot mot SSA-system, och drar slutsatsen att:

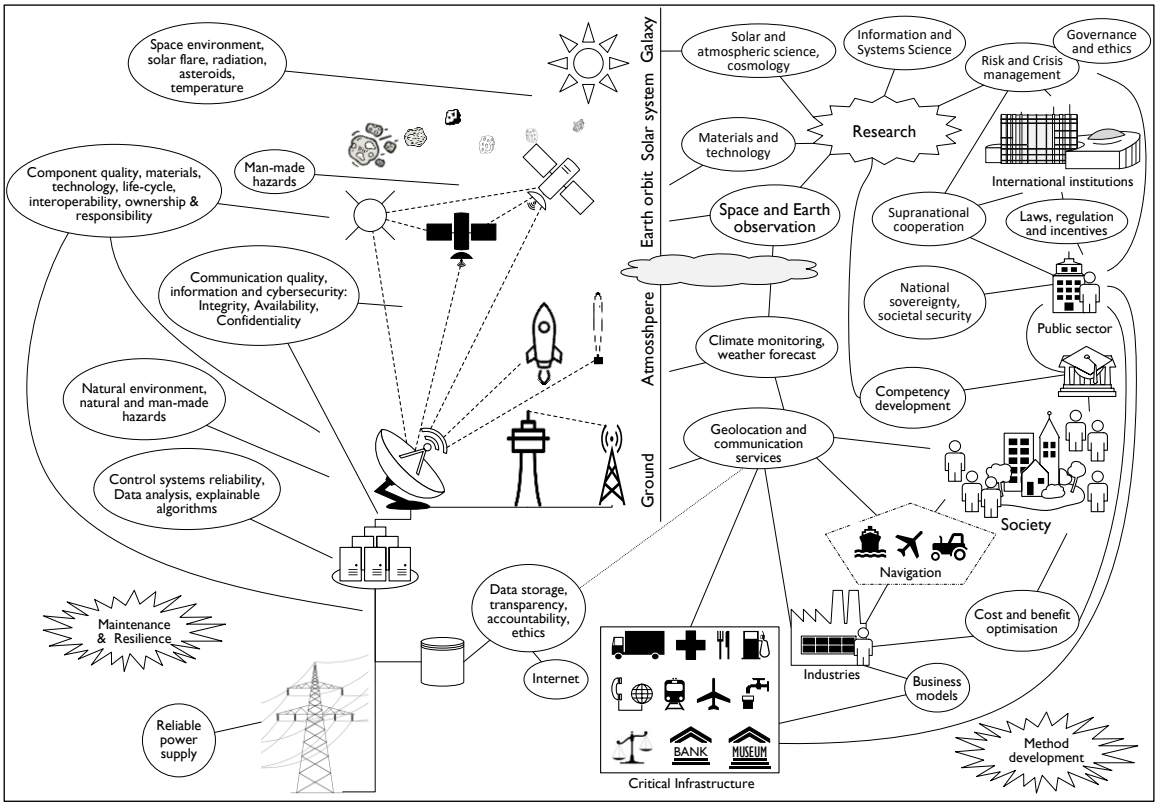
> *"Space Situational Awareness systems and networks can be targeted by malicious actors to gain strategic advantages in orbit or for intelligence purposes. The complexity of the networks and the wide variety of sensors that compose them makes the number of vital links exceptionally high, multiplying the weaknesses against external threats without increasing their redundancy. The community needs greater attention to the problem, both in the light of the international contingency and the constant increase of debris in orbit. In addition, the growth of the space sector requires more significant levels of resilience of support and control structures." p. 310.*

El-genk och Schriener (2024) använder simulering för att skapa ett scenario där en cyberattack mot en kärnreaktor i rymden avvärjs. Jenkins m.fl. (2021) presenterar en "moving target approach" för att avvärja cyberhot mot rymdsystem. Fördelen med denna metod är att den tidigt kan upptäcka en attack.

4.3 En översiktlig modell av rymdsystemet

Baserat på resultat från den biliometriska och tematiska analysen utvecklade vi en konceptuell modell av rymdsystemet. Syftet med modellen är att illustrera ett komplext system i en ”bild-om-allt” (Figur 6). Bilden kan användas som underlag för vidare diskussion med aktörer om systemet och deras förutsättningar för att bidra till systemets robusthet och möjligheter att hantera effekter av störningar i förväntad funktionalitet.

Först visualiseras grundläggande komponenter i modellen genom att beskriva rymdsystemets roll som ett nav för rymd- och jordobservation och kommunikation. Figur 6 visar den mångfald av sammankopplade aktörer, tillgångar och tjänster som utgör rymdsystemet samt relevanta avnämare och kundgrupper. Här illustreras också de gränssnitt som förbinder detta delsystem med andra delar av det globala systemet. Bilden innehåller också visualiseringar av ett urval av olika hot och problem mot rymdsystemet, till exempel gällande komponenternas utformning, kommunikations- och säkerhetsstandarder, datakvalitet och -hantering och aktörernas riskuppfattningar och geopolitiska målsättningar.



Figur 6: Rymdsystemet som kritisk infrastruktur.

Systemets förutsättningar för att utföra rymd- och jordobservation och kommunikation involverar en rad olika faktorer, från de tuffa fysiska förhållandena i rymden, till frågor om lag och rätt. I denna visualisering är markstationer och rymdkomponenter samt deras interaktioner centrala delar. Förutsättningar inkluderar tillförlitlig energiförsörjning, hållbara material och säkra komponenter samt välutbildad personal. Dessutom förlitar sig rymdsystemet på ändamålsenlig dataöverföring, bearbetning och lagring, marktjänster och

missionskontroll för att tillhandahålla relevanta tjänster för olika offentliga och privata aktörer som grupperas i höger sidan av bilden.

Rymd- och jordobservation och kommunikation är tjänster som rymdsystemet tillhandahåller som i sin tur bidrar till att skapa värde för intressenter på olika nivåer (global, nationell, regional och lokal), exempelvis genom:

- Övervakning av solaktivitet och klimatmönster.
- Observation av positionering av objekt i rymden och på jorden för att
    - Stödja navigering och automatisering av transporter och jordbruk
    - Stödja till riskhantering gällande asteroider.
    - Underlätta landskapsvård och övervakning av djurpopulationer
    - Observera vädret samt naturliga och av människor orsakade hot,
    - Bidra till samhällets och inter-/ nationell säkerhet.
- Satellitbaserad kommunikation (till exempel för områden utan andra alternativ)

Det bör noteras att rymdsystemet generellt sett orsakar utsläpp, såsom buller, föroreningar och växthusgaser, exempelvis under uppskjutningsaktiviteter, produktion och vid slutet av komponenternas livscykel. Emissionerna påverkar systemets intressenter och berörda i varierande grad. Förutom effekterna på jorden är en av de mest akuta effekterna skräpet i omloppsbana (rymdskrot) som härstammar från resterna av olika rymdfarkoster, vilket i sin tur ökar kollisionsrisken för befintliga och nya rymdfarkoster, vilket kan leda till oönskade konsekvenser för de tjänster och konsumenter som de stödjer.

Som andra del i konceptualiseringen av rymdsystemet kan en allmän och idealiserad definition av det mer generiska rymdsystemet formuleras med hjälp av CATWOE-elementen (Checkland och Scholes 1999) på följande sätt:

Rymdsystemet är ett system som ägs av världssamfundet och som bemannas av kvalificerad personal från lokala, nationella och överstatliga organisationer och som, med beaktande av (globala) rättsliga bestämmelser och tekniska begränsningar, stödjer säker och tillförlitlig rymd- och jordobservation och kommunikation. Det samlar in och tillhandahåller relevanta data, prover och information för forskning, samhällsutveckling samt risk- och krishantering.

Kund (***C****ustomer*): Rymdsystemets kunder som nyttjar dess tjänster omfattar offentliga och privata organisationer samt enskilda personer som kan befinna sig på många olika platser. Deras behov tillgodoses genom lämpliga resurser som produceras via systemets ändamålsgivande process (T). Hur och i vilket syfte en kund använder resultaten av (T) ligger dock utanför rymdsystemets kontroll och kräver ytterligare kontrollmekanismer.

Aktörer (***A****ctors*): Nyckelaktörer är privata företag och offentliga organisationer, såsom tillverkare, forskningsinstitut, tjänsteleverantörer och olika underleverantörer, som möjliggör till slut rymd- och jordobservation samt kommunikation.

Transformationsprocess (***T****ransformation process*): De behov som systemet tillgodoser är förknippade med tillförlitlig rymd- och jordobservation och kommunikation, exempelvis genom information gällande positionering av jordnära objekt och objekt på jordytan, och övervakning av solfenomen eller globala fenomen, såsom klimat och naturliga och av

människan orsakade faror. Systemet uppfyller dessa behov genom att samla in, överföra, analysera och lagra data, prover och information i rymden, på jorden och däremellan.

Världsåskådning (***W****eltanschauung*): ligger till grund för, och motiverar systemets verksamhet. Detta innebär i ett idealiserat rymdsystem att systemet kan säkerställa tillförlitliga, effektiva och hållbara metoder och nätverk för att tillhandahålla rymd- och jordobservation och kommunikation som i sin tur gynnar systemets kunder och aktörer på jorden, i rymden och på andra platser. Världsåskådningen är av stor betydelse för systemets framtagning, användning och fortsatt utveckling.

Ägare (***O****wner*): till rymdsystemet är de som kan och får avbryta hela processen (T). Om man bortser från ägandet av de många olika delsystemen är det bara världssamfundet som kan avskaffa rymdsystemet i sin helhet. Ägandeskap av rymdsystemet är därför inte i första hand en nationell angelägenhet utan varierar i form mellan omtvistat och kooperativt och påverkas av geopolitiska omständigheter.

Miljö *(****E****nvironment*): Här avses systemmiljön, det vill säga alla förutsättningar och begränsningar som det generaliserade rymdsystemet behöver hantera. De miljömässiga begränsningarna (exempelvis de svåra förhållandena i rymden), rättsliga bestämmelser och aktuella tekniska och samhälleliga begränsningar antas här som givna. Detta betyder att de anses i den konceptuella modellen ligga utanför systemets inflytande. Däremot kommer naturliga, vetenskapliga, tekniska och politiska framsteg att påverka framtida utveckling, drift och användning av rymdsystemet.

Analysen av litteraturen och rymdsystemet har lyft fram flera säkerhetsfrågor och skapar därmed en grund för vidare diskussion. Denna diskussion kan till exempel handla om spänningar mellan (T) och (W) och olika intressenters mål för delsystemen och det övergripande rymdsystemet. I samband med det framkommer definitionen av systemgränser, det vill säga vad som hör till systemet eller går utanför det (Ashby, 1956) som en viktig aspekt. Till exempel kan rymd- och jordobservation och kommunikation användas på varierande sätt för många olika ändamål. Användningen av dessa funktioner ligger dock utanför systemets kontroll, men det är fortfarande ett etiskt dilemma i vilken utsträckning systemet är ansvarigt för en avnämares aktiviteter. I detta sammanhang kan det vara lämpligt med kontrollmekanismer på högre nivå, såsom reglering och brottsbekämpning, och kollektivt ansvar. Förutom att vidta åtgärder mot systemet för att säkerställa säker och tillförlitlig funktionalitet i form av en kritisk infrastruktur, borde dessa mekanismer också ta hänsyn till potentiell (fel)användning genom användare och andra yttre hot. Som nämnts är ansvaret för rymdsystemet således en global fråga och måste innefatta en bred diskussion om dess förutsättningar.

5 Förslag på framtida forskning

I detta kapitel diskuterar vi områden för fortsatt forskning, baserat på resultaten från den bibliometriska, tematiska och systemanalysen. Vi identifierar kunskapsområden där det finns luckor som behöver beforskas mer på djupet för att skapa goda förutsättningar för att stärka cybersäkerhet i rymden och resiliens mot störningar av rymdsystemets funktionalitet.

Detta avsnitt innehåller förslag till fortsatt forskning i relation till framtagning av scenarier (5.1), utökning av labbforskning med verkliga miljöer (5.2) och resilens i samhället mot störningar av rymdsystemet (5.3).

5.1 Framtagning av scenarier

Tidigare rapporter och forskningslitteratur har en sak gemensamt: utvecklingen i rymden präglas av stor osäkerhet, baserat på relationerna mellan olika aktörer. Dessa aktörer involverar nationalstater, allianser, och privata organisationer. Rekommendationer för fortsatt forskning är därför avhängig från den geopolitiska utvecklingen. Ett första steg borde därför vara att, med lämpliga metoder såsom scenariomodellering, framtidsstudier, och/eller workshoppar, ta fram ett antal scenarier för den fortsatta utvecklingen, med inriktningar och förslag på forskning baserade på dessa. I Tabell 6 presenteras några potentiella scenarier inom två extremer: militarisering av rymden respektive internationellt samarbete.

Tabell 6. Scenarier om framtida utveckling av rymden.

Scenario	Beskrivning
#1. Militarisering	Geopolitiska konflikter utspelar sig i allt högre grad i rymden. Öppen konflikt där bland annat anti-satellitvapen används.
#2 Kallt krig	Inga öppna konfrontationer i rymden, men ett brett spektrum av maktdemonstrationer, provokationer och hybridkrigföring via optiska, radiologiska, elektroniska eller cyberattacker samt spionageverksamhet.
#3 Privatisering av rymden	Rymden utforskas och exploateras i allt högre grad av privata aktörer. Det innebär en förtätning av föremål i rymden och att konflikter i rymden karaktäriseras mer av hård affärskonkurrens än geopolitiska konflikter.
#4 Nationell samverkan	Framsteg i utforskning av rymden via nationalstater och/eller grupper av allierade länder som involverar samarbete och koordinerat användning av resurser och nyttjande av markstationer och rymdfarkoster.
#5 Internationellt samarbete	Fredlig utforskning av rymden där världssamfundet gått samman för mänsklighetens bästa.

Det är så klart stor skillnad mellan de olika scenarierna, särskilt mellan extremerna #1 och #5 där ju den geopolitiska utvecklingen och relationerna inom världssamfundet ser väsentligt olika ut. Ett rimligt mål med mänsklighetens bästa i åtanke är såklart scenario #5 som präglas av fred, vilket ju förhindras av att det är många aktörer som hellre skulle vilja se

ett scenario närmare #2 där hybridkrigföring används i syfte att omkullkasta rådande världsordning. I scenarierna #1 till #3 är också leverantörs- och produktionskedjor föremål för spionage och försök att få otillbörlig inflyttande över komponenter och processer. I dessa scenarier är skydd mot cyberattacker en viktig fokus som identifierats i litteraturen, särskilt med tanke på de asymmetriska hot som är förknippade med rymdsystem (Baylon 2014:1,2, Daxhelet 2023). Därtill betonas ytterligare områden för framtida forskning som är relevant i alla scenarier, till exempel ansvarsfrågor som rör användningen av (knappa) resurser, hanteringen av rymdskrot och styrning av komplexa system.

- *Förslag på fortsatt forskning 1*: Analys och utveckling av kvalitets- och säkerhetsprocesser längs leverantörs- och produktionskedjor gällande komponenter och leveranser av observations- och kommunikationstjänster
- *Förslag på fortsatt forskning 2*: ”Code of conduct” gällande utveckling och användning av rymdsystemet. Detta inkluderar fördjupade studier om både globala standards för komponenter och tjänster, och etiska normer för hur verktyg och tjänster borde användas samt hur utvecklingen av dessa kunde organiseras framgent.
- *Förslag på fortsatt forskning 3*: Utforskning av framtidsscenarier som fördjupar sig i hur olika aktörers kortsiktiga och långsiktiga mål kan integreras och vilka styrmedel som kan bidra till meningsfull global dialog och överenskommelser om nyttjande av resurser med resilient och hållbar utveckling i åtanke.

5.2 Från labbet till rymden och tillbaka

En stor del av litteraturen består av forskning som utförs i labbmiljöer där olika former av simuleringar och tester av ny teknik såsom artificiell intelligens genomförs för att utveckla cybersäkerhetsåtgärder i rymdsystem. Det behövs mer forskning för att undersöka om och hur denna forskning nyttiggörs i verkliga miljöer och om det finns möjligheter att utveckla starkare band mellan labb och praktik. Potentiella vägar framåt kan vara testbäddar och sammanställningar av data och detaljbeskrivningar av verkliga fall. Detta skulle underlätta fortsatt forskning om följande:

- *Förslag på fortsatt forskning 4*: Testbäddar kan exempelvis användas för att utforska mer komplexa växelverkningar inom och mellan rymdsystem, dess omgivningar och användare för att förbättra systemens livslängd och tillförlitlighet samt hantering av störningar.
- *Förslag på fortsatt forskning 5*: Framtagning av casebeskrivningar baserat på verkliga fall av störningar och tillbud. Dessa kan ligga till grund för djupare analyser av tekniska komponenter, produktions- och serviceprocesser, organisatoriska faktorer och arbetssätt, inklusive kvalitets- och säkerhetsarbete, där relevanta intressenter och deras målsättningar inkluderas.
- *Förslag på fortsatt forskning 6*: Verkliga miljöer kan också användas tillsammans med labbmiljöer för att bygga bort stuprör i kunskapsutvecklingen genom att involvera experter från olika discipliner i gemensamma forskningsaktiviteter för att öka förståelsen för komplexiteten rörande rymdsystemet och dess utveckling och

användning. Denna interdisciplinära förståelse skulle också kunna bidra till ökat skydd mot fel och störningar som är inbyggda i alla system, både tekniska, samhälleliga och organisatoriska.

5.3 Resiliens mot störningar i rymdsystem

Forskningslitteraturen domineras av artiklar som antingen fokuserar på tekniska förutsättningar, respektive den globala lagstiftningen om rymden. Forskningen om cyber- och andra hot tydliggör dock att vissa typer av störningar, oavsett hotaktör, är svåra, om inte omöjliga, att förhindra. Detta innebär att organisatoriska och samhälleliga riskhanteringsstrategier behöver ta itu med frågan hur konsekvenser av störningar i rymdsystem kan hanteras. Med andra ord, globala och komplexa system medför också risker som är systemiska (Renn, 2016) och konsekvenser kan sprida sig som ringar på vattnet över domängränser. Detta betyder att riskstyrningen bör omfatta analyser och förslag för att hantera sådana konsekvenser, utöver att minska sårbarheter och hot, för att stärka samhällets motståndskraft. Detta involverar dock också en del utmaningar gällande interdisciplinär förståelse och arbetssätt både för forskningssamhället och praktiken.

- *Förslag på fortsatt forskning 7*: I takt med uppbyggnad av totalförsvaret i Norden och Sveriges medlemskap i Nato har krav på samhällets resiliens blivit mer uttalade. Det i sin tur påverkar inte bara operatörer av samhällsviktiga verksamheter som nyttjar rymdsystemet utan också offentliga organisationer och privata aktörer. Forskning fokuserad på intressent- och nätverksanalyser kan bidra till en bredare inkludering av berörda aktörer i lämpliga risk- och krishanteringsstrategier, för utveckling av ett robust och jämställt samhälle.
- *Förslag på fortsatt forskning 8*: Som tidigare nämnts behöver även själva processerna och metoderna för systemiska riskanalyser och riskhantering utvecklas för att skapa användbara underlag för beslutsfattande om åtgärder som är relevanta och ger effekter vid störningar. En viktig utveckling är att förändra tankesättet från att anta ett lineärt förhållande mellan orsak och verkan till mer dynamiska samband som nödvändiggör en vändning bort från skuldbeläggning av aktörer (ofta användaren) till mer dialog-baserade och experimentella arbetssätt för att hantera utmaningar.
- *Förslag på fortsatt forskning 9*: Övning och lärande behöver beforskas mer på djupet för att undersöka vilka typer av övningar och alternativa arbetssätt ger effekt vid störningar av de vardagliga förhållandena i offentliga och privata organisationer. Denna forskning kan också knytas till testbäddar (se 5.2) för att utveckla samhälleliga produktions- och serviceprocesser som är mindre beroende av en permanent funktionalitet *i* rymdssystem och därmed mindre intressant för illvilliga aktörer att attackera.
- *Förslag till fortsatt forskning 10*: Utveckling av inter- och multidisciplinär förståelse och gemensamma arbetssätt inom ramen för riskstyrning, krisberedskap och civilt försvar. Traditioner och normer inom forskningsämnen påverkar forskarnas möjlighet och benägenhet till tvärdisciplinär forskning. Framtagning av nya arbets- och synsätt som accepteras i svensk forskning behöver stödjas av forskningsfinansiärer.

6 Slutsats

Syftet med studien var att sammanställa kunskapsläget med fokus på rymdsystem som kritisk infrastruktur. Studien inriktar sig på hur förståelsen för systemiska beroenden inom rymdsystem kan hjälpa att stärka cybersäkerhet i rymden och hur denna förståelse kunde bidra till resiliens inom samhället mot störningar i rymdsystem.

Arbetet med kunskapsöversikten tillämpade ett socio-tekniskt perspektiv och utgick från följande frågeställning:

- Hur kan cybersäkerhet i rymdsystem förstås ur ett systemperspektiv?

Målet med studien var att ta fram en ett underlag som beskriver vad som utmärker cybersäkerhet och säkerhetsarbete i rymdsystem. Baserat på bibliometriska, tematiska och systemanalyser presenterades en syntes av kunskapsläget och forskningsfronten som lyfter fram systemiska beroenden och olika intressenters behov för att exemplifiera hur cybersäkerhet i rymdsystem kan stärkas, och identifiera områden i behov av fortsatt forskning. Analyserna har fokuserat på rymdsystemet och dess funktionalitet. Resultaten visar exempel på studier om cyberhot som riktas mot systemkomponenter, interaktioner och miljö(er), vilket lägger grund för fortsatt forskning om säkerhetshöjande åtgärder.

Litteraturen beskriver utöver relativt välbeforskade hot mot datornätverk även rymdsystemets unika egenskaper som försvårar implementering av vanliga säkerhetsåtgärder. Vi identifierar kunskapsluckor inom området och diskuterar uppslag for fortsatt forskning, som i sin tur kan stärka samhällelig resiliens genom att ansvariga aktörer tar deras beroende av rymdbaserade tjänster mer i beaktande. Resultaten bidrar bland annat med kunskap om de cybersäkerhetsproblem som uppstår när aktörer, som är involverade i mer eller mindre outtalade konflikter, siktar på att vinna mark i rymden. Kunskapsöversikten skapar således en länk mellan forskning och praktik vilket lägger en grund för behovsmotiverade forskningssatsningar och kunskapsutveckling som är av praktisk relevans för aktörer inom samhällsviktig verksamhet och beredskapssystemet. Vår kunskapssammanställning är därmed ett svar på tidigare forsknings efterfrågan om åtgärder för att skydda och skapa en resilient utveckling i rymden (Oakley, 2020)

Att cybersäkerhet i rymdsystem är ett relativt ungt och snabbt växande ämne illustreras av en låg andel vetenskaplig litteratur som framkom i sökningen, särskilt mellan åren 2014 och 2020 (se Figur 3). Teknikutvecklingen och utvecklingen av forskningsfältet kan knytas till både en kommersialisering av rymdindustrin och ett starkare geopolitiskt intresse av rymden som i sin tur involverar cyberrymden som slagfält för konkurrens och maktutövande. Detta ledde oss fram till en översiktlig beskrivning av fem scenarier som ramar in framtida utvecklingen av rymdsystem och innebär en rad utmaningar för offentliga och privata organisationer, förvaltning och politik. Denna systematiska litteraturstudie bidrar med en kunskapsöversikt över ett flertal utmaningar som är också av relevans för Sveriges civila beredskap. Utifrån resultaten lyftes ett antal lärdomar för praktiken och teman för fortsatt forskning.

Praktiska lärdomar från den tematiska analysen:

- Utgå från och utveckla befintlig lagstiftning och standarder, stifta/skapa nya lagar/standarder (kvalitet, säkerhet, arbetssätt) vid behov.
- ”Out-of-date” är mer vanligt än förväntat, på grund av komponenternas långa design- och tillverkningsprocesser samt att de är svår eller omöjligt att uppdatera.
- Uppmuntra delning av information rörande tekniska specifikationer, säkerhetsincidenter och dess hantering mellan olika parter (till exempel satellittillverkare).
- Upprätta kunskapscenter för cybersäkerhet och rymdsystem.
- Skapa anpassade utbildningsinsatser i cybersäkerhet för rymdpersonal.
- Utveckla adaptiva metoder för riskbedömning och riskhantering.
- Utveckla testbäddar för att vidareutveckla de föreslagna teknikerna.
- Samverkan med universitet och mellan discipliner. Det behövs mer forskning på faktiska tillämpningar.

Litteraturöversikten visar också ätt rymdsystem är relativt oreglerade och bygger på att flera aktörer med olika intressen kan och vill komma överens om hur de nyttjas. Det krävs alltså överstatliga överenskommelser som sträcker sig bortom enskilda nationer och privata aktörer som driver teknikutvecklingen. Att teknik och verktyg kan användas i olika syften understryker vikten av att inte bara sträva efter en lämplig säkerhetsnivå i leverantörsled utan också att utveckla robusthet i samhället som kan leda till resiliens hos användarna mot störningar i rymdsystem genom att reducera beroendet av tjänster som dessa system erbjuder. Inom dessa områden saknas dock publikationer, vilket föranleder ett antal förslag för fortsatt forskning.

Uppslag för fortsatt forskning:

- Framtagning och utforskning av framtidsscenarier mellan extremerna ”militarisering” och ”internationellt samarbete”.
- Utveckling och bedrift av interdisciplinära testbäddar som möjliggör samarbete mellan olika discipliner i forskning och praktik.
- Framtagning av en samling av fallbeskrivningar baserat på verkliga fall av störningar och nära-till-störning-event för analys och lärande.
- Utveckla processer och metoder för systemiska riskanalyser och riskhantering.
- Införliva resiliensbegreppet i organisationsforskning och praktik genom att studera alternativa lösningar och arbetssätt som kan koexistera i vardagen och minska negativa konsekvenser vid störningar, vilket i förlängningen också kan bidra till en mer inkluderande och hållbar utveckling av samhället.
- Att främja interdisciplinär och praktiknära forskning i forskarsamfundet och djupgående analyser utifrån flera teoretiska perspektiv i praktiken.

Referenser

Ashby, W. R. (1956). An Introduction to cybernetics. Chapman & Hall, London.

Baylon, C. (2014:1). Challenges at the intersection of cyber security and space security. International Security.

Baylon, C. (2014:2). Challenges at the intersection of cyber security and space security: country and international institution perspectives. Policy Commons.

Braun, V. & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative research in psychology, 3(2), 77–101.

Checkland, P.; Scholes, J. (1999). Soft systems methodology in action: A 30-year retrospective, Wiley, Chichester, Eng., New York.

Checkland, P.¸Poulter, J. (2010). Soft Systems Methodology. In: Reynolds, M. & Holwell, S. (eds.) Systems Approaches to Managing Change: A Practical Guide. Springer, London: 191–242.

CIFS – Copenhagen Institute for futures studies, (2023). Future of Space Exploration. Strategic Scensios for European Space Exploration 2040-2060. In: ESPI – European Space Policy Institute. Online: https://www.espi.or.at/wp-content/uploads/2024/01/Future-of-European-Space-Exploration_final-version.pdf

Daxhelet, E. (2023). The Intersection between Outer-space Security and Cybersecurity. Finabel - The European Army Interoperability Centre. Online: https://finabel.org/wp-content/uploads/2023/07/May-2023.pdf

ENISA – European Union Agency for Cybersecurity (2025). Space Threat Landscape. Publications Office of the European Union. Luxembourg. DOI:10.2824/8841206

EU (2024). EU Space Strategy for Security and Defence. Factsheet. Online: https://defence-industry-space.ec.europa.eu/document/download/5e3dfcd1-2ff2-4fd1-85f7-74d0d9b62b3a_en?filename= Factsheet%20EU%20Space%20Strategy%20for%20Security%20and%20Defence.pdf

Falco, G. (2018:1). The vacuum of space cyber security. AIAA SPACE and Astronautics Forum and Exposition, 5275.

Falco, G. (2018:2). Cybersecurity principles for space systems. Journal of Aerospace Information Systems, 16(2), 61–70.

Fidler, D. P. (2018). Cybersecurity and the new era of space activities. Digital and Cyberspace Policy Program.

Große, C. (2017): Applying Systems Thinking onto Emergency Response Planning. Using Soft Systems Methodology to Structure a National Act in Sweden. ICORES. SCITEPRESS, 288–297.

Große, C. (2019): Airports as Critical Infrastructure: The Role of the Transportation-by-Air System for Regional Development and Crisis Management. IEEE Conference IEEM, 440–444.

Große, C. (2023). A Review of the Foundations of Systems, Infrastructure and Governance. Safety Science, vol. 160, 106060.

Große, C.; Sundberg, L.; Abdin, A. (2025): Space systems as critical infrastructure - A soft systems approach. 35th European Safety and Reliability and the 33th Society for Risk Analysis Europe Conference.

Hamill-Stewart, J.; Ashdown, N. (2025). Space Systems Security Assessment. Tyburn St Raphael. Online: https://www.secured-research.com/s/Space-Systems-Security-Assessment.pdf

Handmer, J. W.; Dovers, S. R. (1996): A Typology of Resilience: Rethinking Institutions for Sustainable Development. In Industrial & Environmental Crisis Quarterly 9 (4), 482–511.

Holling, C. S. (1973). Resilience and Stability of Ecological Systems. Annual Review of Ecology and Systematics 4(1), 1–23.

Manulis, M.; Bridges, C. P.; Harrison, R.; Sekar, V.; Davis, A. (2021): Cyber security in New Space. Analysis of threats, key enabling technologies and challenges. In International Journal of Information Security 20 (3), 287–311. DOI: 10.1007/s10207-020-00503-w.

Nato (2024). NATO's overarching Space Policy. Online: https://www.nato.int/cps/en/natohq/topics_175419.htm

Oakley, J. G. (2020). Cybersecurity for Space: Protecting the Final Frontier. Apress.

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. Communications of the Association for Information Systems, 37. DOI10.17705/1CAIS.03743

Renn, O. (2016) Systemic Risks: The New Kid on the Block, Environment: Science and Policy for Sustainable Development, 58:2, 26-36, DOI: 10.1080/00139157.2016.1134019

Salehi, V.; Veitch, B.; Musharraf, M. (2020). Measuring and improving adaptive capacity in resilient systems by means of an integrated DEAMachine learning approach. Applied Ergonomics, 82, 102975.

Sveriges Television, SVT (2024). https://www.svt.se/nyheter/inrikes/sverige-drabbat-i-storsta-gps-sabotaget-i-ostersjon

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26(2), xiii–xxiii.

Westman, J.; Mattsson, L.; Guldstrand, F. (2025). En multimodal nätverksanalys av rymddomänens utveckling genom tre eror. Rapport: FOI-R—5682—SE. Online: https://www.foi.se/rapporter/rapport sammanfattning.html?reportNo=FOI-R--5682--SE.

van Eck, N. J., and Waltman, L. (2014). Visualizing Bibliometric Networks. In Y. Ding, R. Rousseau, and D. Wolfram (Eds.), Measuring scholarly impact. Methods and practice. Cham: Springer.

Forskningsartiklar som ingår i rapporten

Abanades, J. A.; Vivero, J.; Martínez, M. (2018). Introducing accountability in space operations. In: SpaceOps 2018 Conference. DOI: 10.2514/6.2018-2480

Bace, B.; Gökce, Y.; Tatar, U. (2024): Law in orbit. International legal perspectives on cyberattacks targeting space systems. In Telecommunications Policy 48 (4). DOI: 10.1016/j.telpol.2024.102739.

Balleste, R. (2018). Reconsidering rules of engagement in outer space. In: Proceedings of the International Institute of Space Law 2018, 727–734.

Berthoud, L.; Agass, S (2022). Identifying Space Threats for SpaceAware Resilience- a Spacecraft and Satellite Service Resilience Model. In: 2022 IEEE Aerospace Conference proceedings. DOI:10.1109/AERO53065.2022.9843343.

Bhuva, D.; Kumar, S. (2023). Securing Space Cognitive Communication with Blockchain. In: 2023 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW). DOI: 10.1109/CCAAW57883.2023.10219188.

Blount, P. J. (2020) CYA. A legal perspective on how to do cybersecurity in space. In: Proceedings of the International Institute of Space Law 2020, 457–466.

Bodeau, D.; Brtis, J.; Graubart, R.; Salwen, J. (2014). Resiliency techniques for systems-of-systems extending and applying the Cyber Resiliency Engineering Framework to the space domain. In: 2014 IEEE 7th International Symposium on Resilient Control Systems (ISRCS).

Boschetti, N.; Gordon, N.; Sigholm, J.; Falco, G. (2022). Commercial Space Risk Framework Assessing the Satellite Ground Station Security Landscape for NATO in the Arctic and High North. In: 2022 IEEE Military Communications Conference (MILCOM), pp. 679–686. DOI: 10.1109/MILCOM55135.2022.10017538.

Boschetti, N.; Sigholm, J.; Wallen, M.; Falco, G. (2023). A Hybrid Space Architecture for Robust and Resilient Satellite Services. In: 2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT). DOI: 10.1109/SMC-IT56444.2023.00021.

Bradbury, M.; Maple, C.; Yuan, H.; Atmaca, U. I.; Cannizzaro, S. (2020). Identifying Attack Surfaces in the Evolving Space Industry Using Reference Architectures. In: 2020 IEEE Aerospace Conference.

Breda, P.; Markova, R.; Abdin, A. F.; Jha, D.; Carlo, A.; Mantı, N. P. (2022). Cyber Vulnerabilities and Risks of AI Technologies in Space Applications. In: 73rd International Astronautical Congress (IAC).

Breda, P.; Markova, R.; Abdin, A. F.; Mantı, N. P.; Carlo, A.; Jha, D. (2023): An extended review on cyber vulnerabilities of AI technologies in space applications. Technological challenges and international governance of AI. In Journal of Space Safety Engineering 10 (4), pp. 447–458. DOI: 10.1016/j.jsse.2023.08.003.

Byrne, D. J.; Morgan, David; Tan, Kymie; Johnson, Bryan; Dorros, Chris (2014): Cyber Defense of Space-based Assets. Verifying and Validating Defensive Designs and Implementations. In Procedia Computer Science 28, pp. 522–530. DOI: 10.1016/j.procs.2014.03.064.

Cantelli-Forti, A.; Capria, A.; Saverino, A. L.; Berizzi, F.; Adami, D.; Callegari, C. (2021): Critical infrastructure protection system design based on SCOUT multitech seCurity system for intercOnnected space control groUnd staTions. In International Journal of Critical Infrastructure Protection 32. DOI: 10.1016/j.ijcip.2020.100407.

Carlo, A.; Boschetti, N.: (2023). Modelling the Impact of Space Situational Awareness Disruption on the European and Arctic Security Landscape. In: MESAS 2022, 13866 LNCS, 299–311.

Carlo, A.; Cesari, L.; Lacroix, L. (2020). The challenge of protecting space-based assets against cyber threats. In: 71th International Astronautical Congress 2020. The CyberSpace Edition, 12-14 October 2020. IAC-20-E9,2.D5.4,x59386.

Carlo, A.; Mantı, N. P.; W. A. M, B.A.S.; Casamassima, F.; Boschetti, N.; Breda, P.; Rahloff, T. (2023): The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications. In Journal of Space Safety Engineering 10 (4), pp. 474–482. DOI: 10.1016/j.jsse.2023.08.002.

Carlo, A.; Roux, L. (2022). Emerging Technologies and Space. In: MESAS 2021, 13207 LNCS, 494–508.

Carlo, A.; Veazoglou, N. (2020). ASAT Weapons. Enhancing NATO's Operational Capabilities in the Emerging Space Dependent Era. In: MESAS 2019, 11995 LNCS, 417-426.

Carter, J. M.; Narman, H. S.; Cosgun, O.; Liu, J. (2020). Trade-off model of fog-cloud computing for space information networks. In: 2020 IEEE Cloud Summit, 91–96.

Crabtree, A.; Rookard, C. (2024). SSITH. Secure Space Infrastructure with Trust metrics backed by Hardware. In: 2024 IEEE Aerospace Conference.

Crocetti, L.; Falaschi, F.; Saponara, S.; Fanucci, L. (2024). Highly-Efficient Galois Counter Mode Symmetric Encryption Core for the Space Data Link Security Protocol. In: ApplePies 2023, 1110 LNEE, 297–303.

Crocetti, L.; Falaschi, F.; Saponara, S.; Fanucci, L. (2023): Implementation of a Hash-based Secure Core for Integrity and Authentication of Data in Space Applications on Space-grade FPGAs. In: 2023 IEEE 2nd Industrial Electronics Society Annual On-Line Conference (ONCON). DOI: 10.1109/ONCON60463.2023.10431035.

Crocetti, L.; Falaschi, F.; Saponara, S.; Fanucci, L. (2024). Secure Data Authentication in Space Communications by High-Efficient AES-CMAC Core in Space-Grade FPGA. In: ApplePies 2023, 1110 LNEE, 49-54.

Curbo, J.; Falco, G. (2023). A Research Agenda for Space Flight Software Security. In: 2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT). DOI: 10.1109/SMC-IT56444.2023.00016.

Dailey, N.; Reed, H. (2019). International space reference architecture. In: International Astronautical Congress 2019. IAC-19-E3.4.10x50471.

Davis, R.; Bace, B.; Tatar, U. (2024): Space as a critical infrastructure. An in-depth analysis of U.S. and EU approaches. In Acta Astronautica 225, 263–272. DOI: 10.1016/j.actaastro.2024.08.053.

Dilworth, S. W.; Osborne, D. D. (2022). Cyber Threats Against and in the Space Domain. Legal Remedies. In: 2022 14th International Conference on Cyber Conflict, 235–247.

Diro, A.; Kaisar, S.; Vasilakos, A. V.; Anwar, A.; Nasirian, A.; Olani, G. (2024): Anomaly detection for space information networks. A survey of challenges, techniques, and future directions. In Computers and Security 139. DOI: 10.1016/j.cose.2024.103705.

Drobyazko, S.; Hilorme, T. (2021): Influence of Sustainable Development of Space Activities on Earth Ecology. In IOP Conf. Ser.: Earth Environ. Sci. 940 (1), 12014. DOI: 10.1088/1755-1315/940/1/012014.

Dygnatowski, S. (2021): Space systems as the weakest link. In Advances in Military Technology 16 (1), 133–147. DOI: 10.3849/aimt.01409.

Ear, E.; Remy, J.L.C.; Feffer, A.; Xu, S. (2023): Characterizing Cyber Attacks against Space Systems with Missing Data. Framework and Case Study. In: 2023 IEEE Conference on Communications and Network Security (CNS). DOI: 10.1109/CNS59707.2023.10289045.

El-Genk, M. S.; Schriener, T. M. (2024): Simulation and Mitigation of False Data Injection Cyberattacks on a Space Nuclear Reactor Power System. In Nuclear Technology. DOI: 10.1080/00295450.2024.2380952.

Falco, G. (2018:1): The vacuum of space cybersecurity. In: 2018 AIAA SPACE and Astronautics Forum and Exposition.

Falco, G. (2019): Cybersecurity principles for space systems. In Journal of Aerospace Information Systems 16 (2), pp. 61–70. DOI: 10.2514/1.I010693.

Falco, G.; Gordon, N. G. (2024): A Zero-Trust Satellite Services Marketplace Enabling Space Infrastructure as a Service. In IEEE Access 12, 71066–71075. DOI: 10.1109/ACCESS.2024.3403483.

Finke, J.; Thummala, R.; Elbasheer, R.; Hansen, P.; Henry, W.; Mamula, D.; Noor, A.M.; York, T.; Zheng, K.; Falco, G. (2023). Satellite Cybersecurity Testbed to Improve Commercial Space Security. In: ASCEND 2023. DOI: 10.2514/6.2023-4768

Hannan, N. (2018): An assessment of supply-chain cyber resilience for the international space station. In RUSI Journal 163 (2), pp. 28–32. DOI: 10.1080/03071847.2018.1469249.

Hills, G.; Baldasare, J.; Henry, W.; Connell, W. (2022). A Customized Approach to Cybersecurity Education for Space Professionals. In : 2022 IEEE Military Communications Conference (MILCOM). DOI: 10.1109/MILCOM55135.2022.10017583.

Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: how China's technical standards could fragment the internet. Journal of Cyber Policy, 5(2), 239–264. DOI: 10.1080/23738871.2020.1805482

Housen-Couriel, D. (2023): IAC-21-E-9 (Paper ID. 67116) Information sharing for the mitigation of outer space–related cybersecurity threats. In Acta Astronautica 203, pp. 546–550. DOI: 10.1016/j.actaastro.2022.11.012.

Höyhtyä, M.; Boumard, S.; Yastrebova, A.; Järvensivu, P.; Kiviranta, M.; Anttonen, A. (2022): Sustainable Satellite Communications in the 6G Era. A European View for Multilayer Systems and Space Safety. In IEEE Access 10, pp. 99973–100005. DOI: 10.1109/ACCESS.2022.3206862.

Jenkins, C.; Vugrin, E.; Manickam, I.; Troutman, N.; Hazelbaker, J.; Krakowiak, S., Maxwell, J,; Brown, R. (2021). Moving target defense for space systems. In: 2021 IEEE Space Computing Conference (SCC), 60–71.

Jones, R. C. (2024): Survey of Space Professionals' Perception of Satellite Cybersecurity from 2012 to 2022. Decision-Makers' Thoughts on Satellite Cybersecurity Evolving. In New Space 12 (4), 259–272. DOI: 10.1089/space.2024.0015.

Kaczmarek, S. (2024): Cybersecurity challenges in space exploration. In Cutter business technology journal 37 (2), 26–35.

Kavallieratos, G.; Katsikas, S. (2023): An exploratory analysis of the last frontier. A systematic literature review of cybersecurity in space. In International Journal of Critical Infrastructure Protection 43. DOI: 10.1016/j.ijcip.2023.100640.

Knez, C.; Llanso, T.; Pearson, D.; Schonfeld, T.; Sotzen, K. (2016). Lessons learned from applying cyber risk management and survivability concepts to a space mission. In: 2016 IEEE Aerospace Conference.

Lefcourt, S.; Gordon, N.; Wong, H.; Falco, G. (2022). Space Cognitive Communications. Characterizing Radiofrequency Interference to Improve Digital Space Domain Awareness. In: 2022 International Conference on Localization and GNSS (ICL-GNSS). DOI: 10.1109/ICL-GNSS54081.2022.9797033.

Li, D. (2023): Upgrading space debris mitigation measures to cope with proliferating cyber threats to space activities. In Advances in Space Research 71 (10), pp. 4185–4195. DOI: 10.1016/j.asr.2022.12.055.

Madani, P.; McGregor, C. (2024). Cybersecurity Issues in Space Optical Communication Networks and Future of Secure Space Health Systems. In: 2024 IEEE Aerospace Conference. DOI: 10.1109/AERO58975.2024.10521087.

Mailloux, L. O.; Span, M. L.; Mills, R. F.; Young, W. L. (2019). A top down approach for eliciting systems security requirements for a notional autonomous space system. In: 2019 IEEE International Systems Conference (SysCon).

Manulis, M.; Bridges, C. P.; Harrison, R.; Sekar, V.; Davis, A. (2021): Cyber security in New Space. Analysis of threats, key enabling technologies and challenges. In International Journal of Information Security 20 (3), 287–311. DOI: 10.1007/s10207-020-00503-w.

Maple, C.; Epiphaniou, G.; Hathal, W.; Atmaca, U. I.; Sheik, A. T.; Cruickshank, H.; Falco, G. (2022). The Impact of Message Encryption on Teleoperation for Space Applications. In: 2022 IEEE Aerospace Conference (AERO).

Marsili, D.; Boschetti, N.; Gordon, N.; Nikas, Y.; Leger, W.; Joyce, M.; Falco, G. (2023). Slipping Through Attackers' Fingers. Fast Neutron Communications for Space Cybersecurity. In: 2023 IEEE Aerospace Conference. DOI: 10.1109/AERO55745.2023.10115666.

Martin, A.-S. (2023): Outer Space, the Final Frontier of Cyberspace. Regulating Cybersecurity Issues in Two Interwoven Domains. In Astropolitics 21 (1), 1–22. DOI: 10.1080/14777622.2023.2195101.

Martin, A.-S.; Freeland, S. (2023). Encoding and Securing Space Activities. Legal Challenges Arising from the Advent of 'Quantum Technology for Space'. In: Proceedings of the International Institute of Space Law 2023, 239–254.

McNeil, M.; Llanso, T.; Pearson, D. (2018). Application of capability-based cyber risk assessment methodology to a space system. In: HoTSoS 2018, Association for Computing Machinery. DOI:10.1145/3190619.3190644

Pavur, J.; Martinovic, I. (2021). On Detecting Deception in Space Situational Awareness. In: ASIA CCS '21: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, 280–291.

Pazouki, S.; Aydeger, A. (2023): Securing International Space Station Against Recent Cyber Threats. In Xin-She Yang, Simon Sherratt, Nilanjan Dey, Amit Joshi (Eds.): Proceedings of 7th International Congress on Information and Communication Technology. ICICT 2022, London, vol. 464. Singapore: Springer Nature (LNNS).

Petrovici, G.; Carlo, A. (2018). Legal Challenges of space 4.0. The framework conditions of legal certainty among states, international organisations and private actors in the changing landscape of space activities. In: Proceedings of the International Institute of Space Law 2018, 71–87.

Phillips, D. M.; Mazzuchi, T. A.; Sarkani, S. (2018): An architecture, system engineering, and acquisition approach for space system software resiliency. In Information and Software Technology 94, 150–164. DOI: 10.1016/j.infsof.2017.10.006.

Potter, M. (2015). Cybersecurity in the space age. In: Proceedings of the International Institute of Space Law 2015, 267–383.

Racionero-Garcia, J.; Shaikh, S. A. (2024): Space and cybersecurity. Challenges and opportunities emerging from national strategy narratives. In Space Policy 70. DOI: 10.1016/j.spacepol.2024.101648.

Salim, S.; Moustafa, N.; Reisslein, M. (2024): Cybersecurity of Satellite Communications Systems. A Comprehensive Survey of the Space, Ground, and Links Segments. In IEEE Communications Surveys and Tutorials. DOI: 10.1109/COMST.2024.3408277.

Schalk, A.; Brown, D. (2023). Detection and Mitigation of Vulnerabilities in Space Network Software Bus Architectures. In: 2023 IEEE Aerospace Conference. DOI: 10.1109/AERO55745.2023.10115986.

Segate, R. V. (2024): Drafting a Cybersecurity Standard for Outer Space Missions. On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach. In Journal of Asian Security and International Affairs 11 (3), 345–375. DOI: 10.1177/23477970241261432.

Shahzad, S.; Joiner, K.; Qiao, L.; Deane, F.; Plested, J. (2024): Cyber Resilience Limitations in Space Systems Design Process. Insights from Space Designers. In Systems 12 (10). DOI: 10.3390/systems12100434.

Shaw, H. C.; McLaughlin, B.; Stocklin, F.; Fortin, A.; Israel, D.; Dissanayake, A., Gilliand, D.; LaFontaine, R.; Broomandan, R.; Hyunh, N. (2015). Applying a space-based security recovery scheme for critical homeland security cyberinfrastructure utilizing the NASA Tracking and Data Relay (TDRS) based Space Network. In: 2015 IEEE International Symposium on Technologies for Homeland Security (HST).

Suwijak, C.; Li, S. (2022): Global Internet Access from the Low Earth Orbit. Legal Issues regarding Cybersecurity in Outer Space. In Journal of East Asia and International Law 15 (1), 93–108. DOI: 10.14330/jeail.2022.15.1.05.

Varadharajan, V.; Suri, N. (2024): Security challenges when space merges with cyberspace. In Space Policy 67. DOI: 10.1016/j.spacepol.2023.101600.

Vessels, L.; Heffner, K.; Johnson, D. (2019). Cybersecurity risk assessment for space systems, In: 2019 IEEE Space Computing Conference (SCC), 11–19. DOI 10.1109/SpaceComp.2019.00006.

Verco, E. (2021). Satellites are cyber insecure: We need regulation to avoid a disaster. ANU Journal of Law and Technology, 2(2), 57–94. DOI: 10.3316/informit.20220516066953

West, J.L. (2020). Space Security Cooperation: Changing Dynamics. Springer International Publishing, 145–162.

Woodward, D.; Hobbs, M.; Gilbertson, J. A.; Cohen, N. (2021). Uncertainty Quantification for Trusted Machine Learning in Space System Cyber Security. In : 2021 IEEE 8th International Conference on Space Mission Challenges for Information Technology (SMC-IT), 38–43. DOI: 10.1109/SMC-IT51442.2021.00012.

Yang, Z.; Shaofeng, L.; Chenyang, T. (2023). Research on Security Protection of Space-Earth Integrated Network Wireless Link Based on Consortium Blockchain Technology and Application. In: 2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA). DOI: 10.1109/EEBDA56825.2023.10090811.

Zhang, L.; Du, Y. (2023): Resilience enhancement scheme for gateway placement in space information networks. In Computer Networks 222. DOI: 10.1016/j.comnet.2022.109555.

Zhuo, M.; Liu, L.; Zhou, S.; Tian, Z. (2021): Survey on security issues of routing and anomaly detection for space information networks. In Scientific Reports 11 (1). DOI: 10.1038/s41598-021-01638-z.