FOI MEMO
Projekt
SABEK – Risker kopplade till smarta städer
Sidnr
1 (28)

Projektnummer
A1120084
Kund
Justitiedepartementet
FoT-område
Inget FoT-område

Författare
Nils Karanta
Viktor Strömberg

Datum
2020-12-17
Memo nummer
FOI Memo 7439

Smarta städer – En internationell utblick

Sändlista

Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen

Titel
Smarta städer – En internationell utblick

Memo nummer
FOI Memo 7439

Sammanfattning

Detta memo ingår som en del i ett större uppdrag från Regeringskansliet (Justitiedepartementet) inom ramen för anslagsprojektet SABEK (Samhällets beredskap i kris och krig). Anslagsprojektet utgör en del av Regeringskansliets inriktning till FOI avseende Säkerhets- och försvarspolitisk forskning och analys (SOFFA).

Studiens syfte är att genomföra en internationell utblick och inhämta olika exempel på hur städer har arbetat med konceptet smart stad. Detta genomförs i form av en fallstudie bestående av några av världens städer som bedömts ha kommit längst i arbetet med konceptet smart stad, nämligen Singapore, Oslo, Amsterdam och San Francisco. Studien söker svar på vad städerna har för vision för den smarta staden, vilka konkreta projekt städerna har genomfört eller planerar att genomföra samt vilka risker och sårbarheter som städerna har identifierat.

Studien finner att samtliga städers vision på ett eller annat sätt har som övergripande syfte att förbättra livet för stadens invånare. Däremot har städerna lite olika inriktning, där vissa exempelvis fokuserar på miljöfrågor och andra på transporter. Sett till vilka projekt städerna bedriver för att uppnå detta genomför samtliga städer någon typ av projekt kopplat till autonoma fordon. Det finns även exempel på projekt som är mer unika och intressanta att undersöka vidare, exempelvis Amsterdams *Schoonschip* som kan tänkas ha förmågan att öka stadens robusthet. Beträffande risker och sårbarheter är det endast en av städerna som verkar arbeta på lokal nivå med sårbarheter direkt kopplade till den smarta staden. Analyser kopplade till övriga städer handlar oftast mer om risker och sårbarheter kring digitalisering i allmänhet. Hur överförbara dessa är till den smarta staden är emellertid något som man behöver fundera kring. Slutligen innefattar den smarta staden andra risker än rent tekniska, varav den mest tydliga torde vara behovet av att inkludera alla stadens invånare, oavsett ekonomiska resurser eller kunskap, i det nya samhällsbygget.

Innehåll

1 Introduktion

Idén om en digitaliserad eller även kallad smart stad är inget nytt, redan under internets genombrott föddes idén om att inkorporera *informations- och kommunikationsteknik* (IKT) i det vardagliga livet. I akademiska artiklar sedan 1994 och framåt har förekomsten av begreppen *digital city* och *smart city* vuxit med en jämn takt, men en stark ökning av förekomsten av begreppet *smart city* har skett sedan 2010. Den starka ökningen sammanfaller med EU:s introduktion av begreppet i samband med projektet *EU Setis* för kvalificering av projekt för hållbara städer och urban utveckling, samt Apples lansering av ordet ”smart” i beskrivning av hemelektronik såsom mobiltelefoner.[1] Det finns idag ingen vedertagen definition av vad en smart stad är. Överlag kretsar begreppsdiskussionen kring hur en stad kan förbättras, framförallt hur digitalisering kan bidra till en förbättring av miljö och livskvalité samt effektiviseringar av hur samhället fungerar.[2]

I det här memot gör vi en fallstudie av fyra utländska städer, där vi studerar hur Singapore, Oslo, Amsterdam och San Francisco arbetar med konceptet smart stad. Syftet med studien är att genomföra en internationell utblick och inhämta exempel på olika smarta städer-projekt i världen. Studien görs med en ambition om att öka förståelsen för vad en smart stad är och vilka risker som finns.

För att uppnå syftet avser studien att besvara följande frågeställningar:

1. *Vision* – Vad är syftet och målbilden med den smarta staden?
2. *Projekt* – Vilka projekt har genomförts, eller planerar att genomföras, kopplat till den smarta staden?
3. *Risker och sårbarheter* – Vilka kända risker och sårbarheter finns det med den smarta staden?

I rapporten *Vilse i Lasagnen – En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur* beskrivs riskerna med den ökade digitaliseringen som främst kopplade till utbyggnaden av ”Sakernas Internet” – även kallat IoT efter engelskans begrepp *Internet of Things*. IoT består av produkter uppkopplade mot ett centralt system, där produkterna kan vara riktade till privatkonsumenter i form av hushållselektronik, till industrier som vill effektivisera sin produktion samt till offentliga aktörer som vill effektivisera sin verksamhet. Riskerna med IoT kretsar kring att uppkopplingen gör det möjligt för en angripare att slå ut många system samtidigt, genom att från en enhet kunna ta sig vidare till flera uppkopplade enheter i samma system.[3]

Den ökade digitaliseringen får konsekvenser för den smarta stadens riskbild eftersom digitala lösningar inkorporeras i stadens funktion i allt större utsträckning. Riskbilden påverkas dels av hur staden hanterar integrationen av den nya tekniken i befintliga system, dels av hur sammankopplingen mellan den fysiska och digitala världen ska hanteras. Ett exempel på det senare kan vara hur riskbilden påverkas av att styrsystem i industrin blir uppkopplade. Ju större del av staden som är uppkopplad, desto mer ökar dessutom sårbarheterna kopplade till digitaliseringen. Policyarbetet kring digitalisering och cybersäkerhet tros också få stor påverkan på den smarta stadens riskbild.[4]

Memot inleds med en kortare metodbeskrivning i kapitel 2. Denna följs av en genomgång av de valda städernas visioner, projekt kopplade till den smarta staden samt identifierade risker och sårbarheter i kapitel 3. Därefter genomförs en djupare analys i kapitel 4 av vad som har framkommit i de tidigare avsnitten. Avslutningsvis presenteras studiens slutsatser i kapitel 5.

---

[1] Dameri & Cocchia. *Smart City and Digital City: Twenty Years of Terminology Evolution*.
[2] Albino, Berardi & Dangelico. *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*.
[3] Ingemarsdotter, Eidenskog & Hedtjärn Swaling. *Vilse i Lasagnen?- En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*, FOI-R--4814--SE.
[4] Kelkar, Golden, Pandey, & Peasley. *Making smart cities safer*.

2 Design och metod

Frågeställningarna kommer att undersökas genom en fallstudie avgränsad till städerna Singapore, Oslo, Amsterdam och San Francisco. Designen utgår från den undersökningsstrategi som på vissa håll kallats *enstaka fallstudie* och som är en strategi som lämpar sig väl för att undersöka och beskriva ett fåtal fall i detalj.[5] Urvalet har gjorts i syfte att maximera variationen och på så sätt ta fram flera olika exempel på smarta städer. Ett sådant upplägg torde vara av mer intresse i en deskriptiv studie av denna typ, som mot bakgrund av fåtalet fall ändå skulle få svårt att generera ett representativt urval.

Urvalsprocessen har tagit sin utgångspunkt i toppskiktet på den ranking över smarta städer i världen som den schweiziska handelshögskolan *IMD Business School* har gjort.[6] Rankingen baseras på hur invånare i 102 städer världen över uppfattar vidden och påverkan av de insatser som genomförs i syfte att göra deras stad smart. Därefter har urvalet skett baserat på geografisk placering samt en initial bedömning av vad för typ av vision staden har och hur mycket data som finns tillgänglig. Bakom urvalet ligger en tanke om att städer i olika delar av världen i någon mån skiljer sig åt, exempelvis hade ett urval av enbart städer inom Europa riskerat att endast inkludera städer som alla på olika sätt påverkas av EU, bland annat genom lagstiftning och villkor kopplade till olika EU-projekt. Studien har inte som målsättning att ge en representativ bild av vad som menas med smarta städer, utan syftar i huvudsak till att visa på fyra exempel.

Datainsamlingen har genomförts med hjälp av existerande källor företrädesvis bestående av städernas egna offentliga kommunikation och policydokument, men även av medierapporteringar och akademiska artiklar. I syfte att skapa en ökad förståelse – framförallt kring risker och sårbarheter, som inte tycks återfinnas i någon större omfattning i existerande öppna källor – skickades även ett mejl med en kortare enkät ut till respektive stad. Mejlet ställdes till den befattningshavare eller det departement som var, eller i varje fall kunde antas vara, inblandad i arbetet med den smarta staden. Av de fyra städerna var det endast Oslo som inkom med ett svar på enkäten.

Eftersom smart stad-begreppet i sig är väldigt spretigt och elastiskt så är det inte heller helt tydligt vilka av städernas satsningar eller projekt som faller in under begreppet. Identifieringen av vad som är att betrakta som smarta städer-projekt har därför skett med hjälp av två vägledande kriterier.

Enligt dessa kriterier är ett projekt att betrakta som en smart stad-satsning om antingen:

1. Staden refererat till projektet som en smart stad-satsning, eller
2. Om det går att betrakta projektet som en smart stad-satsning utifrån stadens vision för en smart stad.

Samtliga projekt som städerna har redovisat eller som har kunnat identifieras har emellertid inte inkluderats. Detta då vissa av städerna har listat ett så pass stort antal projekt på sina hemsidor att det inte funnits plats att, åtminstone inte på ett meningsfullt sätt, inkludera dessa. Projekten i studien är således, likt fallstudien i sin helhet, att betrakta som *exempel* på smarta städer-projekt och inte som en uttömmande eller representativ redogörelse. Studien har inte heller gjort någon djupare undersökning av hur långt städerna har kommit i implementeringen av projekten, vilket innebär att projektens status är att betrakta som okänd om inte annat anges.

[5] Teorell & Svensson. *Att fråga och att svara: samhällsvetenskaplig metod*. s. 74ff.
[6] IMD Business School. *Smart City Index 2019*.

3 Smarta städer

I detta kapitel beskrivs de olika städerna Singapore, Oslo, Amsterdam och San Francisco. Inledningsvis beskrivs visionen för staden, därefter listas de projekt som har kunnat identifieras och slutligen följer en redogörelse över eventuella risker och sårbarheter. Indelningen av olika projekt i kategorier har gjorts endast i syfte att öka läsbarheten och fyller således ingen analytisk funktion. Kapitlet avslutas med en sammanfattande tabell över samtliga städer.

3.1 Singapore

Vision

Singapores *Smart Nation Programme* iscensattes 2014, med syfte att förbättra det vardagliga livet för invånare samt förbättra företagsklimatet i landet genom att implementera digitala lösningar, i både det privata och det offentliga. Singapore har valt att implementera ett helnationsperspektiv, vilket innebär att hela nationen från regering och myndigheter till företag och invånare ska vara delaktiga i digitaliseringsprocessen.[7] Helnationsperspektivet innebär att Singapores statsledning har valt att driva digitaliseringsprocessen från toppen som en ensamt styrande aktör. Staten ser det dock som avgörande att företag och invånare tar till sig den nya tekniken.[8]

Projekt

Singapore har erfarenhet från tidigare nationsomfattande program som har implementerats i samband med skiften i teknikparadigm, exempelvis 1980-talets datorisering och millennieskiftets framsteg inom kommunikationsteknik. Totalt har sex stycken program för de olika teknikskiftena införts, från nationell datorisering till E-förvaltning. Följande fem områden har idag identifierats som särskilt betydelsefulla i Singapores digitaliseringsprocess: Sjukvård, Ekonomi, Urbana lösningar, Transport och Utbildning.[9]

Nedan följer en redogörelse över identifierade satsningar som ryms inom ramen för smarta städer-begreppet.

Hälsa – Förbättra sjukvården genom att använda personliga sensorer och smarta telefoner för att övervaka hälsotillståndet hos brukaren.

- Exempel på projekt är *Health Hub*, en portal som samlar patienters sjukvårdsdata på en digital plattform. Plattformen ger åtkomst till patientens samlade journaler för vårdgivare, ifall tillåtelse har givits.[10]

Utbildning – Skapa ett holistiskt lärande genom digitalisering, där fysisk och digital undervisning kopplas samman. Automatisera repetitiva arbetsuppgifter för att effektivisera lärarnas arbete.

- Ett exempel på projekt är *The Parents Gateway App* som möjliggör för effektivisering av administrativ kontakt mellan föräldrar och lärare.[11]

Transport och trafik – Autonoma fordon, smarta system och dataanalys ska effektivisera framtidens trafikplanering och praktiska genomförande.

---

[7] Smart Nation Singapore. *Smart nation: The Way Forward 2018.*
[8] Ibid.
[9] Ibid.
[10] Smart Nation Singapore. *HealthHub.*
[11] Smart Nation Singapore. *Parents gateway.*

- Data hämtas från kollektivtrafiken genom resenärers resekort, samt genom sensorer installerade på bussar som ger information om deras position i realtid. Användning av data som policystöd har resulterat i en 92%-ig minskning av överfulla bussar samt en minskad väntetid på 3-7 minuter. [12]

Urbana lösningar – Ökad hållbarhet och säkerhet i städerna genom datainsamling från sensorer och smarta system.

- Singapore använder drönare i syfte att förhindra utbrott av denguefeber. Drönarna används för att övervaka stuprännor i syfte att upptäcka vattensamlingar, som är en fortplantningsplats för myggor vilka sprider sjukdomen. Drönarna är också utrustade med bekämpningsmedel.[13]
- *Smart Elderly Alert System* är ett system som genom sensorer installerade i brukarens lägenhet övervakar rörelse, med syfte att öka tryggheten för de äldre. Avläsningarna kan sedan avläsas av anhöriga via en mobil-app.[14]
- *myENV App* syftar till att ge användaren information om miljön i staden genom exempelvis väderprognoser och varningar, information om luftkvalité samt möjlighet till att rapportera miljörelaterade olyckor.[15]

Ekonomi – Tillämpa *fintech*-lösningar (it-teknologi inom finansvärlden) för att effektivisera och öka konkurrenskraften.

- Med syfte att stödja utvecklingen av *fintech* och skapa legala ramverk har *Monetary Authority of Singapore* (MAS) planer på att bygga ett smart finanscentrum.[16]
- *Punggol Digital District* (PDD) planeras att bli en ny stadsdel i Singapore, där företag och universitet gemensamt ska kunna verka. Syftet är att skapa positiva synergier mellan aktörerna och främja ekonomisk tillväxt. I stadsdelen kommer smarta system att installeras såsom ett smart elnätverk, en centraliserad logistik-central, ett smart sopsystem som använder vakuum och ett centraliserat kylsystem.[17]

Risker och sårbarheter

Cybersäkerhet och datasäkerhet beskrivs som en av de viktigaste grundstenarna i Singapore utveckling av den smarta staden samtidigt som *digitalt försvar* beskrivs som en av sex grundpelare i Singapores totalförsvarsplan.[18]

År 2015 grundades myndigheten *Cyber Security Agency of Singapore* (CSA) vars uppdrag är att övervaka den digitala miljön. CSA ansvarar för att förebygga och identifiera risker samt hantera dessa om de inträffar.[19] Risker som identifierats är virusattacker, bankbedrägerier, spionage och attacker mot IT-infrastrukturen. Dessa risker ses som angelägna att hantera, inte bara för de direkta skadeverkningarna dessa kan ge, utan också ur ett längre perspektiv för att bibehålla förtroendet för den nya tekniken bland invånare och företag. [20]

[12] Smart Nation Singapore. *Open data and analytics for urban transportation*.
[13] Smart Nation Singapore. *Drones to survey dengue hotspots*.
[14] Smart Nation Singapore. *Smart Elderly Alert System.*
[15] Smart Nation Singapore. *myENV app.*
[16] Smart Nation Singapore. *Fintech Sandbox.*
[17] Smart Nation Singapore. *Punggol Digital District.*
[18] Ministry of defence. *Total defence*.
[19] Cyber Security Agency of Singapore. *Our organisation.*
[20] Cyber Security Agency of Singapore. *Singapore´s Cybersecurity Strategy 2016.*

Fyra områden har identifierats i *Singapores Cybersecurity Strategy 2016* som särskilt betydelsefulla att skydda och utveckla för att förebygga IT-attacker. [21]

- *IT-infrastruktur* – Servicesektorn (både privat och offentlig), elförsörjning, vattenförsörjning, telekommunikation och transport är samtliga områden som är beroende av en motståndskraftig och pålitlig IT-infrastruktur. Singapore vill därför öka IT-säkerheten genom att införa ett standardiserat riskbedömningssystem, att använda sig av *Security by design*, det vill säga att säkerhetsarbetet ska vara med från början och inte efterkonstrueras samt att ha tydliga policys och riktlinjer för säkerhetsarbetet.
- *IT-miljö – National Cybercrime Action Plan* (NCAP) sjösattes 2016 för att etablera en koordinerad handlingsplan för bekämpning av cyberbrott. Det ska ske genom att utbilda allmänheten, öka myndigheternas kapacitet att bekämpa cyberbrott, stärka lagstiftningen och utöka internationellt samarbete.
- *Öka kunskap bland företag och invånare* – Singapore vill utveckla vad de kallar ett *cybersecurity ecosystem*, vilket återspeglar en vilja att bli ”självförsörjande” inom IT-säkerhet. Det ska ske genom att ha en utbildad arbetskraft inom IT-säkerhet, starka lokala företag och satsningar på forskning inom IT-säkerhet.
- *Internationella partnerskap* – Grundat i att hot mot cybervärlden är ett globalt problem och att brottslingar kan utnyttja juridiska skillnader mellan länderna vill Singapore utveckla internationella partnerskap. Det ska ske genom samarbete inom brottsbekämpning, utveckling och juridik samt policys.

CSA släpper årligen rapporten *Singapore Cyber Landscape* som redogör för det gångna årets säkerhetsarbete och framtida risker. Rapporten innefattar även utblickar mot omvärlden, där trender och säkerhetsintrång analyseras. Exempel på ett riskområde som tas upp är den ökade användningen av IoT. I syfte att förbättra säkerheten och informera användarna om säkerhetsriskerna planerar CSA att under 2020 lansera ett system för säkerhetsmärkning av IoT-produkter. Märkningen skulle möjliggöra för konsumenter att på ett enkelt sätt beakta säkerhetsaspekten vid inköp av IoT-produkter.[22]

En nationell strategi med särskilt fokus på *driftsystem* (eng. *Operational Technology*, OT) och *industriella informations- och styrsystem* (eng. *Industrial Control Systems*, ICS) lanserades 2019, vilken innefattar säkerhetsarbete kring allt från uppkopplade trafikljus till styrenheter i industrin. Fokus ligger på att utbilda personal, starta ett samlingsorgan för informationsdelning och analys kring säkerhetsrisker, stärka policyriktlinjer samt utveckla nya teknologier för systemtillförlitlighet.[23]

En viktig del av CSA:s strategi är information till allmänheten om hur grundläggande skyddsåtgärder kan förhindra IT-intrång. Ett konkret exempel på detta arbete är *Cybersecurity Awareness Campaign* med syfte att, för både privatpersoner och företag, öka kännedomen om vilka risker digitaliseringen medför och hur dessa risker kan hanteras.[24] Ett annat exempel är *GoSafeOnline* som är en digital plattform riktad till företag och privatpersoner med syfte att öka kunskapen samt bidra med råd för ökat säkerhetsarbete.[25]

3.2 Oslo

Oslos arbete med att bli en smart stad började 2011 efter ett initiativ från ett privat telekomföretag med ambitionen att göra Oslo till en internationell pionjär inom nya, innovativa, miljövänliga transport- och stadsutvecklingslösningar.[26] Oslo kommuns officiella vision är att bli en smartare,

[21] Cyber Security Agency of Singapore. *Singapore´s Cybersecurity Strategy 2016*. s.12
[22] Cyber Security Agency of Singapore. *Singapore Cyber Landscape 2019*.
[23] Cyber Security Agency of Singapore. *Singapore's Operational Technology Cybersecurity Masterplan 2019*.
[24] Cyber Security Agency of Singapore. *Singapore´s Cybersecurity Strategy 2016*.
[25] Cyber Security Agency of Singapore. *GoSafeOnline*.
[26] Mejl från Oslo kommuns Byrå för stadsmiljö (*nor. Bymiljøetaten*). inkommet 6 november 2020.

grönare och mer kreativ stad för alla invånare som utvecklas med deras intressen och välmående i fokus.[27] Visionen beskrivs övergripande som ett ”urbant utvecklingsuppdrag”.[28] Denna kan i sin tur delas upp i tre kategorier: mål, medel och verktyg. Det grundläggande överordnade målet handlar ytterst om att förbättra livet för stadens invånare. För att uppnå det övergripande målet finns vad som kan beskrivas som medel – eller delmål – vilka består i att staden ska vara öppen, hållbar, sammankopplad och innovativ samt att staden behöver involvera och samarbeta med intressenter (eng. *stakeholders*). Verktygen för att uppnå delmålen består av säkra tekniska lösningar kopplade till IKT och IoT.[29]

Projekt

Inom ramen för sin smart stad-strategi har kommunen lanserat en rad konkreta satsningar.[30] Nedan följer en redogörelse över identifierade satsningar som ryms inom ramen för smart stad-begreppet.

Hälsa

- *Demensvänliga boenden* – Demonstrationsanläggning kopplad till kommunens geriatrik-avdelning med syfte att fungera som demonstrationslägenhet och kompetenscentrum för tillgänglighetsteknologi.[31]

Urbana lösningar

- *Applikationer för medborgarorienterade tjänster* – Flertalet applikationer för att underlätta kommunikation och interaktion med invånarna, exempelvis applikationer för att anmäla fel och nedskräpning, betala parkeringsavgifter och få åtkomst till offentlig statistik. [32]

Miljö och energi

- *Utsläppsfria byggarbetsplatser* – Från och med 2017 innehåller offentliga upphandlingar krav om fossilfria maskiner och fordon där målet är att samtliga byggarbetsplatser ska vara utsläppsfria 2025.[33]
- *Kretsloppsbaserad återvinning* – Källsortering i olikfärgade påsar som automatiskt sorteras och där organiskt avfall blir biogas och biogödsel, plastavfall blir nya plastprodukter och brännbart avfall används för uppvärmning.[34]
- *Resultatpanel för miljödata* – Pilotprojekt i form av en specifik skärm eller mjukvara som visualiserar klimat- och miljödata i realtid samt gör prognoser med hjälp av maskininlärning och historiska data.[35]

Transport och trafik

- *Utsläppsfria bussar* – En pågående infasning av en ny fordonsflotta med bussar som drivs av vätgas eller elektricitet, vilken beräknas vara helt klar 2028.[36]

---

[27] Oslo kommun. *Smart Oslo*.
[28] Oslo kommun. *Oslo Smart City Strategy*.
[29] Ibid.
[30] Oslo kommun. *Smart Oslo: Project*.
[31] Oslo kommun. *Dementia-friendly solutions*.
[32] Oslo kommun. *Public city apps.*
[33] Oslo kommun. *Zero-Emission Construction Sites*.
[34] Oslo kommun. *Circular economy and waste management*.
[35] Oslo kommun. *Climate Dashboard*.
[36] Ruter. *Emission Free public transport in Oslo and Akershus.*

- *Självkörande mindre bussar* – Ett pågående pilotprojekt där självkörande fordon testas på olika sträckor i syfte att introducera fordonen för invånarna och utveckla kollektivtrafiksbolagets kompetens inom området.[37]
- *Cykelpooler* – Tillgång till cyklar via stadens applikation för offentliga transporter. Till plattformen finns även en mjukvara som samlar in statistik och prognostiserar användningen i syfte att kunna maximera utnyttjandet av cyklarna.[38]
- *Mobilitetspunkt Filipstad* – Pilotprojekt inrättat 2019 i form av en specifik plats där elektriska transportmedel i form av elcyklar, elsparkcyklar och elbilar finns tillgängliga för allmänheten.[39]
- *Traffic Light Assistance (TLA)* – Pilotprojekt i form av trafikljus som kan kommunicera med omgivningen. Detta testas ihop med de självkörande bussarna för att utvärdera hur dessa interagerar med trafikljusen.[40]

Övrigt

- *Dikesfri rördragning* – Teknik där borrning sker horisontellt från byggnaders källare, vilket gör att dessa kan anslutas till vattennätet utan att det behöver grävas igenom markytan.[41] Tekniken var färdigutvecklad 2017.[42]

Risker och sårbarheter

Enligt Oslo kommun är stadens säkerhetsarbete kopplat till den smarta staden främst fokuserat på trafiksäkerhet.[43] Andra risker och sårbarheter, dock utan explicit koppling till den smarta staden, återfinns i Oslos kommunala riskbild (KRB) i vilken 17 stycken scenarier presenteras.[44] Av dessa går det att urskilja åtminstone fyra som kan anses ha en tydlig koppling till smarta städer:

- Förlorad vattenförsörjning[45]
- Elransonering
- Cyberangrepp
- 100-års solstorm[46]

Cyberangrepp och förlorad vattenförsörjning bedöms vara de scenarier som kommer att vara mest utmanande för kommunens krishanteringsförmåga. Vidare bedömer kommunen även att cyberangrepp och 100-årig solstorm är de scenarier som skapar störst påfrestningar för de kritiska samhällsfunktionerna. Sett till vilka som drabbas av respektive scenario anses förlorad vattenförsörjning vara det scenario som har störst påverkan på invånarna medan elransonering anses ha störst påverkan på samhällets funktionalitet.

Cyberangrepp verkar emellertid vara det scenario som är av störst intresse, detta då både sannolikheten för, och konsekvenserna av, ett cyberangrepp anses vara höga relativt andra scenarier. I rapporten pekar kommunen dessutom på att fem av nio kritiska samhällsfunktioner anses påverkas kraftigt av ett cyberangrepp som leder till kommunikationsbortfall. Det hänvisas även till det flernivåberoende

[37] Ruter. *Self-driving vehicles*.
[38] The Explorer. "Smart platform for shared bicycles".
[39] Ruter. *Mobilitetspunkt Filipstad*.
[40] Mejl från Oslo kommuns Byrå för stadsmiljö (*nor. Bymiljøetaten*). inkommet 6 november 2020.
[41] Oslo kommun. *No-Dig Challenge*.
[42] Byggeindustrien. "NoDig Challenge fullført".
[43] Mejl från Oslo kommuns Byrå för stadsmiljö (*nor. Bymiljøetaten*). inkommet 6 november 2020.
[44] Oslo kommun. *Kommunalt risikobilde 2017 (kortversjon)*.
[45] Kopplingen mellan smarta städer och *förlorad vattenförsörjning* grundar sig i en tanke om att industriella informations- och styrsystem (eng. ICS) förekommer i vattenhanteringen. Det är emellertid inte helt klarlagt att så är fallet i just Oslo.
[46] Solstormar är utbrott på solen som riskerar att störa ut elförsörjning och elektronisk kommunikation. Se MSB:s publikation *Extrema solstormar*: *Konsekvenser för samhällsviktig verksamhet*.

som finns, där kommunen för att kunna utföra sina uppgifter är beroende av elektroniska kommunikationstjänster vilka i sin tur är beroende av den elektroniska infrastrukturen. Man menar därför att ett cyberangrepp mot den elektroniska infrastrukturen indirekt skulle slå mot kommunens förmåga att utföra sina uppgifter och därigenom påverka medborgarnas säkerhet.

För att motverka en sådan situation menar kommunen att det är viktigt att identifiera sårbarheter i kedjan och etablera skydd mot dessa. Här betonas även vikten av att alla aktörer tar ansvar för sina områden för att på så sätt minska kommunens samlade sårbarhet.

3.3 Amsterdam

Vision

Amsterdams arbete för att bli en smart stad inleddes 2007 som ett samarbete mellan Amsterdam Innovation Motor (AIM), elnätverksoperatören Liander och Amsterdam stad, vilka lade grunden för *Amsterdam Smart City Programme*. Dessa organisationer är idag drivande och jobbar aktivt för att implementera nya lösningar och driva utvecklingen framåt. Det huvudsakliga syftet är att använda IKT för att lösa miljöproblem och bygga en stad som är hållbar. Strategin bygger på uppfattningen att IKT har potential att förbättra hur en stad fungerar. Strategin har politiskt stöd och har överlevt förändringar i det politiska styret.[47]

Professorerna Luca Mora och Roberto Bolici har brutit ner Amsterdams strategi i fem faser:[48]

1. **Uppstart**
   Med syftet att minska utsläpp av växthusgaser startar AIM, Liander och Amsterdam Stad projektet med ansvar utifrån organisationernas kompetens och arbetsområde.
2. **Planering**
   Med utgångspunkt i planen för *New Amsterdam Climate Program 2025* har boende, arbetsplatser, transport och offentliga miljöer identifierats som betydelsefulla utsläppskällor av växthusgaser. Det ska dock tilläggas att sedan starten av Amsterdams arbete mot att bli en smart stad har en uppdaterad version av *New Amsterdam Climate Program* publicerats med en uppdaterad kategoriindelning, inom vilken bebyggelse, transport, elektricitet, industri och Amsterdam hamn ingår.[49] Med grund i utvecklingen av IKT har projekt för respektive område påbörjats. Efter en testperiod och analys av resultatet så antingen avslutas, eller implementeras projektet i större skala.
3. **Projektutveckling**
   Strategin är byggd på kontinuerlig utveckling av IKT-baserade projekt. Projekt initieras antingen av *Amsterdam Smart City Foundation* eller från utomstående aktörer. Förslagen utvärderas främst utifrån genomförbarhet, kostnad och vilken potentiell utsläppsminskning projektet kan ge.
4. **Övervakning och utvärdering**
   Utvärdering av de olika projektens resultat utgår från projektens initiala målbild, vilken potential projektet visar och huruvida implementation kan ske på en större skala.
5. **Kommunikation**
   I syfte att skapa nya samarbeten och inspirera andra städer delas resultaten från de olika projekten öppet.

[47] Mora & Bolici. *How To Become A Smart City: Learning From Amsterdam.*
[48] Ibid.
[49] New Amsterdam Climate. *Amsterdam Climate Neutral Roadmap 2050.*

Projekt

I Amsterdams officiella strategi för att bli en klimatneutral stad, *Amsterdam Climate Neutral 2050*, finns en rad satsningar som kan tillskrivas utvecklingen av den smarta staden. Satsningarna kretsar kring hur staden ska byggas och rekonstrueras för att minska utsläpp av växthusgaser, men även kunna fortsätta att växa. Utifrån *Amsterdam Climate Neutral 2050* kan framförallt energi och transport kopplas till utvecklingen av den smarta staden.[50]

En betydande del av Amsterdams strategi är uppbyggnaden av *Amsterdam Smart City Platform*, där både företag och privata aktörer kan dela med sig av projekt inom ramen för smarta städer. De listade projekten har ofta en tydlig miljöprofil, men det genomförs även projekt som har som syfte att förbättra det vardagliga livet med hjälp av IKT.[51]

Nedan följer ett antal exempel hämtade från *Amsterdam Climate Neutral* och *Amsterdam Smart City Platform*.

Transport

- Projektet *Smart Mobility* har som syfte att effektivisera trafikflödet i staden. Med fokus både på lösningar för logistik och lösningar för att göra privatpersoners resande mer effektivt och klimatvänligt. Lösningar innefattar bland annat bilpooler, kombinerade godstransporter och autonoma fordon, i syfte att minska antal förorenande körda mil.[52]
- *StreetSense*-projektet går ut på att installera sensorer på vägar som trådlöst sänder information om antalet bilar som nyttjar vägen samt aktuella vägförhållanden. Insamlade data kan sedan användas som policystöd. Projektet är för nuvarande i teststadiet.[53]
- Till följd av det ökande antalet el-bilar i Amsterdam syftar projektet *Flexpower Amsterdam* till att öka användning av förnyelsebar energi för laddning av el-bilar. Det sker genom att i det offentliga laddningssystemet för el-bilar schemalägga laddning när större mängd förnyelsebar energi är tillgänglig, exempelvis solenergi under dagtid samt schemalägga laddning när behovet på elmarknaden är mindre, vilket leder till lägre energipriser.[54]

Energi och miljö

- Staden vill modernisera sin energiinfrastruktur, där ett exempel på projekt är området *Schoonschip*. Området kommer bestå av 46 flytande hushåll, utrustade med solceller för elproduktion och värmepumpar som utvinner värme ur havet. Varje hushåll har ett eget batteri sammankopplat till ett digitaliserat elnät som är gemensamt med de övriga hushållen. Elnätet tillåter sammankoppling av batterierna som sedan fördelar energin mellan hushållen efter behov, vilket lett till mindre elkonsumtion från det offentliga elnätet.[55]
- *The Energy Storage System* syftar som ett pilotprojekt till att skapa klimatneutrala evenemang. Detta sker genom användandet av begagnande elbilsbatterier för att lagra energi i Amsterdam Arena, kombinerat med el från solceller på Amsterdam Arena. Det möjliggör att man kan hantera toppar i arenans energiförbrukning men även att man, när energiförbrukningen är låg, kan fördela energin på det offentliga elnätverket.[56]

[50] New Amsterdam Climate. *Amsterdam Climate Neutral Roadmap 2050.*
[51] Amsterdam Smart City. *Projects.*
[52] Ibid. s. 109f & 193.
[53] Amsterdam Smart City. *Street Sense*.
[54] Amsterdam Smart City. *Flexpower Amsterdam.*
[55] Schoonschip Amsterdam [webbsida].
[56] Amsterdam Smart City. *The Energy Storage System.*

Urbana lösningar

- Amsterdam är en del av *CityFlows*-projektet som är ett delvis EU-finansierat samarbete för utveckling av *crowd management* (hantering av folkmassor). Syftet är att med hjälp av data-insamling analysera beteendet hos folkmassor. Projektdelen i Amsterdam har till följd av Covid-19-pandemin fokuserat på folksamlingar och hur lokala regler följs.[57]
- *Energy Atlas* är en interaktiv karttjänst som syftar till att öka kunskapen om energianvändande i staden. Genom karttjänsten kan användare få information kring olika byggnaders energi-konsumtion och energieffektivitet. Tjänsten innehåller även information kring förutsättningar för installation av solceller på specifika byggnader.[58]
- *Digital Perimeter* är ett projekt ursprungligen tänkt till fotbolls-EM 2020, med syfte att öka tryggheten på evenemang, samt minska behovet av personal på evenemang. Detta sker med hjälp av sensorer för att hitta pyrotekniska pjäser, kroppskameror uppkopplade mot 5G-nätet och ansiktsigenkänning.[59]

Risker och sårbarheter

Den nederländska myndigheten *Ministry of Justice and Security*, med ansvar för cybersäkerhet, publicerade 2019 rapporten *Cyber Security Assessment Netherlands.* Rapporten fokuserar inte explicit på utvecklingen av den smarta staden, men den nära kopplingen mellan digitalisering och den smarta staden gör den ändå relevant för vår studie. Rapporten fokuserar på vilka risker den ökade digitaliseringen medför, utifrån attacker riktade mot system i Nederländerna, men även trender och framtidsutsikter inom cyberhot.[60]

Aktörerna som utgör ett hot mot cybersäkerheten anses ha olika avsikter och förutsättningar att utföra attacker. Avsikterna med attackerna definieras som spionage, disruptiva avsikter/händelser, sabotage, system- och datamanipulation och datastöld. Även oavsiktliga incidenter identifieras som ett hot och kan resultera i disruptiva händelser eller läckor. Delarna av samhället har kategoriserats som regering, samhällsviktiga funktioner, privata företag och invånare. Följande grupper av aktörer och vilka hot de utgör har identifierats: [61]

- *Främmande makt* – Vilja och förutsättningar att utföra attacker mot samtliga delar av samhället i form av spionage, datamanipulation, sabotage och störningar. Exempel på angrepp skedde 2017 och 2018 då utländsk underrättelsetjänst genomförde attacker mot nederländska ambassader i Mellanöstern och Asien.
- *Kriminella* – Vilja och förutsättningar för störningar, datamanipulation, systemmanipulation och datastöld i samtliga delar av samhället. Senaste årens trend är att kriminella grupper har fokuserat på att sprida *cryptominers* (mjukvara som stjäl processorkraft för att utvinna Bitcoins).
- *Terrorister* – Vilja att utföra sabotage mot regering och samhällsviktiga funktioner finns, men attacker har antingen avbrutits eller så saknas förutsättningar.
- *Enskilda aktörer, hacktivister, insiders* – Vilja och förutsättningar finns för störningar samt datastöld riktade mot regering, samhällsviktiga funktioner och privata företag. Majoriteten av attacker utförda av dessa aktörer är överbelastningsattacker, så kallade DDoS-attacker, vilka har potentialen att tillfälligt överbelasta och därmed omöjliggöra åtkomst till tjänsten.
- O*lyckshändelser* – Riskerna med olyckshändelser utan uppsåt kan resultera i störningar och dataläckor i samtliga delar av samhället.

Att enskilda individer beskrivs som möjliga aktörer grundar sig i att det idag inte krävs avancerade kunskaper för att utföra angrepp, vilket möjliggör även för enskilda individer att utföra enklare

[57] Cityflows Europe. *Covid-19 living lab.*
[58] Amsterdam Smart City. *Energy Atlas.*
[59] Amsterdam Smart City. *Digital Perimeter.*
[60] Ministry of Justice and Security. *Cyber Security Assessment Netherlands.*
[61] Ministry of Justice and Security. *Cyber Security Assessment Netherlands.*

attacker. Även om identifierade sårbarheter till stor del är kopplade till attacker utifrån, kan även system- eller handhavandefel utgöra en betydelsefull säkerhetsrisk. Genom den ökade digitaliseringen kan dessa fel leda till stora konsekvenser för samhället om system stängs ner, ett problem som förstärks när allt fler system är sammankopplas, då fel i ett system kan påverka andra.[62]

Enligt *Cyber Security Assessment Netherlands* kommer både riskerna och vikten av säkerhetsarbetet att öka till följd av den ökade digitaliseringen. Digitaliseringen kan leda till att nya risker och sårbarheter uppkommer, vilket också den ökade komplexiteten av system bidrar till. Implikationerna från attacker tros också bli större ju fler delar av samhället som är sammankopplade. Ökade geopolitiska motsättningar tros också öka riskerna för angrepp från främmande makt. Ökad användning av IoT inom nya branscher, såsom sjukvård och industri, tros ge en ökad attackyta.[63]

3.4 San Francisco

San Franciscos vision för en smart stad tycks huvudsakligen vara kopplad till transport och kollektivtrafik. Den uttalade visionen handlar om att göra det säkrare, lättare och bättre för alla i staden att förflytta sig mellan olika punkter. Detta sker genom att skapa gemensamma och effektiva transportsystem, som även ökar tillgängligheten för socioekonomiskt svaga grupper.[64]

Staden har under många år deltagit i ett nationellt smart stad-projekt utlyst av det amerikanska transportdepartementet.[65] Inom ramen för projektet har staden samlat ett team från stadens lokala myndigheter, företag, icke-statliga organisationer, regionala myndigheter och universitet.[66] Det finns dock även smart stad-satsningar som inte är direkt kopplade till transportsektorn. Detta återspeglas exempelvis i ett dokument från stadens *Kommitté för informationsteknologi* där det istället talas om en effektiv, datadriven och ansvarsfull förvaltning samt rena, säkra och levande samhällen.[67] En anledning till att just transportfrågorna generellt tycks ha fått sådant fokus kan vara att staden deltar i det amerikanska transportdepartementets projekt, men även det faktum att staden faktiskt, som man skriver:

> ”[…] inte kan bygga bredare gator för att anpassa sig till den växande populationen. Det finns inte plats. Istället måste vi [staden] anpassa transportsystemet till att bli mer effektivt och ta mindre plats.” [68]

Projekt

Nedan följer en redogörelse över identifierade satsningar som ryms inom ramen för smart stad-begreppet.

Urbana lösningar

- *Tillgängliggörande av IT-tjänster för låginkomsttagare* – Tillse att även låginkomsttagare får tillgång till IT-tjänster genom att tillhandahålla smarta telefoner, banktjänster och fritt offentligt Wi-Fi.[69]
- *Smarta soptunnor* – Soptunnor som övervakar och kartlägger mängden sopor för att automatiskt avgöra när tunnorna behöver tömmas.[70]
- *Smarta gatlampor* – Gatlampor placerade på vissa platser med dimbart ljus, WiFi-anslutning, kameror och mikrofoner.[71]

[62] Ibid. s.19.
[63] Ibid. s.37.
[64] San Francisco. *Our Vision*.
[65] U.S. Department of Transportation, *Smart City Challenge*.
[66] San Francisco. *Partners.*
[67] San Francisco Committee on Information Technology: Budget & Performance subcommittee. *Regular Meeting February 3 2017.*
[68] San Francisco. *Our Vision* [författarens översättning].
[69] San Francisco. *Smart City Challenge, San Francisco: Harnessing the Future of Shared Mobility*.
[70] San Francisco Committee on Information Technology. *Information and Communication Technology Plan: FY 2020-24*, s. 24.
[71] Ibid.

- *Smart byggnad* – Specifik byggnad utrustad med ytterglas som med hjälp av ett intelligent system kan justera exponeringen mot solen för att hålla jämn temperatur inne i byggnaden.[72]
- *Applikationer* – Diverse applikationer för att felanmäla saker i staden, samla in geodata från cyklister samt mäta antalet parkeringsplatser och prissätta dessa utifrån efterfrågan.[73]
- *DataSF* – Hemsida med diverse öppen data fritt tillgänglig för allmänheten att ta del av, antingen via interaktiva kartor och tabeller på hemsidan eller genom att ladda ner dessa som dataset.[74]
- *Kloaksensorer* – Sensorer med 15 års batteritid placerade i kloakerna för att, i nästintill realtid, övervaka vattenrelaterade data, som exempelvis kan användas för att räkna ut hur mycket havsvatten som har tagit sig in i kloakerna.[75, 76]

Transport och trafik

- *Eldriven och smart bilpool* – En satsning på att förbättra infrastrukturen i staden för eldrivna och uppkopplade fordon, med bland annat dedikerade körfält och upphämtningszoner.[77] Fordonen ska bland annat kunna undvika kollisioner genom att identifiera andra fordon, fotgängare och cyklister. Målsättningen är även att fordonen så småningom ska bli självkörande.[78]
- *Smarta trafiksignaler* – Trafiksignaler som ger prioritet åt kollektivtrafik och utryckningsfordon.[79]
- *Datainsamling från fordon i kollektivtrafiken* – Fordon i kollektivtrafiken överför automatiskt data till ett kontrollcenter där de används som beslutsunderlag eller för att göra prediktiva analyser och ge resenärer reseförslag.[80]
- *Smart flygplats* – Biometrisk autentisering för passagerare, navigering för synskadade genom riktmärken (eng. *beacons*) och GPS-baserade landningszoner för flygplan.[81]

Övrigt

- *Frigöring av yta* – Minskat behov av parkeringsplatser till följd av smarta transportlösningar, vilket frigör yta som kan användas till annat.[82]

Risker och sårbarheter

Något dokument som direkt berör risker och sårbarheter kring utvecklingen av den smarta staden har inte kunnat återfinnas. Däremot finns det dokument som indirekt berör frågan, dels i form av lokala policyer för cybersäkerhet, dels i form av nationella riskanalyser kring smarta städer.

Ett dokument som beskriver hur cyberhot ska hanteras är San Franciscos *Citywide Cybersecurity Strategy*.[83] Det övergripande målet i strategin handlar om att stödja, upprätthålla och säkra upp kritisk infrastruktur och datasystem. Strategin, som riktar sig till stadens departement, innehåller bland annat följande åtgärder som dessa ska vidta:

---

[72] Ibid.
[73] Hancock, Hu & Lee. "Towards an Effective Framework for Building Smart Cities: Lessons from Seoul and San Francisco". s. 85ff.
[74] San Francisco. *DataSF: Open Data.*
[75] Puri. "Ayyeka Sigfox IoT sensors monitor sewage deep underground San Francisco".
[76] San Francisco Committee on Information Technology: Budget & Performance subcommittee. *Regular Meeting February 3 2017.*
[77] City of San Francisco. Meeting at the Smart City Challenge Volume 1.
[78] San Francisco. *Smart City Challenge, San Francisco: Harnessing the Future of Shared Mobility*.
[79] Ibid.
[80] San Francisco Committee on Information Technology. *Information and Communication Technology Plan: FY 2020-24*. s. 24.
[81] Ibid.
[82] San Francisco. *Smart City Challenge, San Francisco: Harnessing the Future of Shared Mobility*.
[83] San Francisco Committee on Information Technology. *Citywide Cybersecurity Policy.*

- Utse en IT-säkerhetsdirektör för departementet, en så kallad CISO (eng. för *Chief Information Security Officer*).
- Skapa ett ramverk som bas för arbetet med cybersäkerhet, vilket enligt rekommendation bör baseras på riktlinjer från *National Institute for Standard and Technology* (NIST).
- Genomföra riskvärderingar kopplade till cybersäkerhet.
- Tillse att krav på cybersäkerhet finns och att dessa efterföljs.

Utöver åtgärderna innehåller strategin även en lista där det anges mer i detalj vilken befattning inom departementen som ansvarar för genomförandet av olika åtgärder.

Ett annat dokument som tar upp risker med IT-system är San Franciscos IT-fokuserade policy för beredskapsplaner.[84] I denna konstateras det att resiliensen i IT-system är ett kritiskt element i beredskapen för att kunna hantera natur-, eller mänskligt orsakade, katastrofer. Vidare konstateras det även att ökad resiliens uppnås genom skydd av systemen och dess miljöer samt genom förmågan att snabbt återställa dessa vid en katastrof. Målet är att upprätthålla kritiska IT-beroende tjänster vid en incident eller katastrof. För att säkerställa detta ska alla stadens departement utveckla, testa och upprätthålla en IT-beredskapsplan. Målen med beredskapsplanen är att:

- Skydda och återställa data.
- Skydda hårdvara, mjukvara och fysiska anläggningar.
- Återstarta kritiska processer genom hög tillgänglighet och en strategi för reservomkoppling.

Dokumentet innehåller även beskrivningar i detalj om hur utvecklingen och implementeringen av beredskapsplanen ska gå till samt vilket ansvar som faller på vilken befattning inom respektive departement.

För att hitta sårbarheter och risker kopplade direkt till smarta städer och inte till cyberangrepp i allmänhet verkar blickarna behöva lyftas till den nationella nivån. Ett sådant dokument är en rapport från 2015 av det amerikanska inrikessäkerhetsdepartementet (*Department of Homeland Security*) som undersöker risker i smarta städer kopplat till cyber-fysisk infrastruktur.[85] Ett av de områden som undersöks i rapporten är risker kopplade till autonoma fordon samt risker kopplade till kommunikation mellan olika fordon eller kommunikation mellan fordon och omkringliggande infrastruktur.

När det gäller autonoma fordon presenteras två exempel på attacker. Den första handlar om en illvillig aktör som attackerar fordonets datorsystem och på så sätt tar kontroll över bilens styrfunktioner, antingen direkt eller genom en modifiering av mjukvaran som får bilen att göra olika manövrar under vissa förutsättningar – exempelvis vid en viss hastighet. Det andra exemplet handlar om en illvillig aktör som stör fordonets sensorer och på så sätt skapar förvirring som kan leda till farliga körförhållanden och olyckor. I rapporten görs ett flertal observation kring detta. En av dessa handlar om svårigheter med att implementera säkerhetsuppdateringar och att dessa i många fall kan vara beroende av att fordonsägare själva tar ansvar och besöker en verkstad. En annan handlar om att mångfalden av tillverkare gör att det finns en mångfald av programvaror och säkerhetslösningar, vilket öppnar upp för fler sårbarheter och därmed möjligheter för illvilliga aktörer att angripa systemen. En tredje handlar om att antalet attackvektorer ökar med antalet trådlösa anslutningar och antalet mindre komponenter utvecklade för en specifik uppgift med avsaknad av ett omfattande säkerhetstänk, exempelvis däcktryckssensorer.[86]

Det andra området handlar om kommunikation fordon-till-fordon (V2V) och fordon-till-infrastruktur (V2I) – ett exempel på det senare kan vara fordon som kommunicerar med trafikljus för att hastigheten ska kunna anpassas till kommande trafiksignaler. Det första exemplet på detta område handlar om en

[84] San Francisco Committee on Information Technology. *Citywide IT focused- Disaster Preparedness, Response, Recovery, and Resilience Policy.*
[85] U.S. Department of Homeland Security's Office of Cyber and Infrastructure Analysis. *The Future Of Smart Cities: Cyber-physical Infrastructure Risk.*
[86] Ibid.

illvillig aktör som stör ut eller manipulerar information som skickas mellan enheterna vilket kan skapa oreda och farliga körförhållanden i trafiken. Det andra exemplet handlar om illvilliga aktörer som har förmågan att störa ut kommunikationen mellan enheter och använder detta för att utpressa tillverkare eller ägare, till exempel genom att hota att publicera information om sårbarheten eller att själv genomföra en attack. Observationerna som görs på detta område är i huvudsak desamma som gjordes beträffande autonoma fordon. En ny observation som är unik för detta område är emellertid att förarkompetensen eroderas när det finns allt mer system för att automatisera körningen och varna föraren. Detta ökar risken för olyckor och trafikproblem vid systemfel eller avbrott.[87]

Sammanfattningsvis är hoten som har identifierats i de tre ovanstående dokumenten följande:

- Naturkatastrofer[88]
- Cyberincidenter[89]
- Fysiska angrepp[90]
- Illvilliga aktörer[91]

3.5 Sammanfattande tabell

Tabell 3.5 åskådliggör vad som framkommit i kapitel 3 beträffande respektives stads vision, projekt samt identifierade risker och sårbarheter med den smarta staden. Tabellen är av sammanfattande karaktär och syftar till att ge läsaren en övergripande återblick. Antalet asterisker i tredje kolumnen ”Risker och sårbarheter” symboliserar hur nära kopplingen är till den smarta staden, se tabellnot.

	Vision	Projekt	Risker och sårbarheter
Singapore	Implementering av IKT i hela samhället i syfte att förbättra för med borgare och företag.	**Ekonomi** - Smart finanscentrum - Punggol Digital District **Hälsa** - Health Hub **IKT-lösningar** - Denguefeberbekämpning med drönare - Smart Elderly Alert System - myENV App **Transport och trafik** - Datainsamling i kollektivtrafiken **Utbildning** - The Parents Gateway App	**Säkerhetsarbete** - *Cyber Security Agency of Singapore (CSA)* - *Singapore Cyber Landscape* / *** - *Singapores Cybersecurity Strategy 2016* / *** **Identifierade risker** - IoT - IT-attacker - Attacker mot IT-infrastrukturen **Åtgärder** - Säkerhetsmärkning av IoT-produkter - Nationell strategi för OT och ICS - Utbildning av allmänheten - Internationella partnerskap - *National Cybercrime Action Plan* - ”Security By Design”

[87] Ibid.
[88] San Francisco Committee on Information Technology. *Citywide IT focused- Disaster Preparedness, Response, Recovery, and Resilience Policy.*
[89] Ibid.
[90] Ibid
[91] U.S. Department of Homeland Security’s Office of Cyber and Infrastructure Analysis. *The Future Of Smart Cities: Cyber-physical Infrastructure Risk*

Oslo	Smartare, grönare och kreativare stad för alla invånare.	**Hälsa** - Demensvänliga boenden **IKT-lösningar** - Applikationer för medborgarorienterade tjänster **Miljö och energi** - Utsläppsfria byggarbetsplatser - Kretsloppsbaserad återvinning - Resultatpanel för miljödata **Transport och trafik** - Utsläppsfria bussar - Självkörande mindre bussar - Cykelpooler - Mobilitetspunkt Filipstad - Traffic Light Assistance (TLA) **Övrigt** - Dikesfri rördragning	**Säkerhetsarbete** - *Kommunal riskbild (KRB)*** **Identifierade risker** - Förlorad vattenförsörjning - Elransonering - Cyberangrepp - 100-års solstorm - Risk att kommunen inte kan utföra sina uppgifter **Åtgärder** - Identifiera sårbarheter - Etablera skydd mot sårbarheter - Ansvar hos varje aktör
Amsterdam	Användandet av IKT för att lösa miljöproblem och skapa en hållbar stad.	**IKT-lösningar** - CityFlows - Energy Atlas - Digital Perimeter **Miljö och energi** - Schoonschip - The Energy Storage System **Transport och trafik** - Smart Mobility - StreetSense - Amsterdam	**Säkerhetsarbete** - *Cyber Security Assessment Netherlands** **Identifierade risker** - Digitalisering - Publika och privata IKT-system - System- och handhavandefel - Risk för allvarliga samhällsstörningar - System- och handhavandefel **Åtgärder**
San Francisco	Göra det lättare för alla invånare att förflytta sig mellan olika platser.	**IKT-lösningar** - Tillgängliggörande av IT-tjänster - Smarta soptunnor - Smarta gatlampor - Smart byggnad - Applikationer - DataSF - Kloaksensorer **Transport och trafik** - Eldriven och smart bilpool - Smarta trafiksignaler - Datainsamling från kollektivtrafiken - Smart flygplats **Övrigt** - Frigöring av yta	**Säkerhetsarbete** - *Citywide Cybersecurity Strategy*** - IT-fokuserad policy för beredskapsplaner** - DHS-rapport cyber-fysisk infrastruktur*** **Identifierade risker** - Naturkatastrofer - Cyberangrepp - Fysiska angrepp - Autonoma fordon - Illvilliga aktörer **Åtgärder** - Cybersäkerhetsåtgärder för varje departement - IT-fokuserad beredskapsplan

* Nationell rapport med indirekt koppling till den smarta staden.
** Lokal (kommunal) rapport med indirekt koppling till den smarta staden.
*** Nationell rapport med direkt koppling till den smarta staden.

4 Analys

I denna del avser vi att göra en djupare analys av vad som har framkommit i de tidigare kapitlen. Analysen tar fokus på trender och likheter som vi kan identifiera mellan städerna samt potentiella risker och framtida implikationer med den smarta staden och dess projekt. Kopplat till risker och sårbarheter genomförs även en SWOT-analys för respektive stad. Analysen är strukturerad enligt tidigare avsnitt – inledningsvis behandlas städernas vision, därefter konkreta projekt och avslutningsvis risker och sårbarheter.

4.1 Vision

Gemensamt för alla städers vision är syftet att förbättra livet för människor i staden. Inom visionen ryms för alla städer en vilja att effektivisera och förbättra förvaltning, transport och miljö. Fokus för visionen, åtminstone hur den har kommunicerats utåt skiljer sig däremot mellan städerna. Singapore och Oslo har ett tillsynes mer övergripande fokus, där visionen innehåller samtliga ovanstående aspekter. I San Francisco och Amsterdam finns mer tydliga fokus på transport respektive miljö. Oavsett hur visionen är kommunicerad externt är likheterna slående i hur visionerna tar praktisk form. Den främsta förklaring till det anser vi är att de utmaningar städer har idag, särskilt gällande transport och miljö som kan anses vara globala utmaningar för hela världen. Detta tillsammans med det faktum att teknikutveckling idag inte är direkt kopplat till ett land eller en stad, något som möjliggör för städer över hela världen att ta del av teknikutvecklingen och även se exempel på hur andra städer har arbetat med digitalisering.

Den stora skillnaden ligger i tillvägagångsättet städerna har valt för att försöka uppnå sin vision. Staden som skiljer sig mest i det avseendet är Singapore, då dess speciella förutsättningar som stadsstat möjliggjort för ett mer toppstyrt arbete. I Singapore är det ytterst den nationella politiska ledningen i landet som är drivande, jämfört med resterande städer i vår studie, där arbetet framförallt sker på en lokal nivå. Det borde ge Singapore bättre förutsättningar att driva sin vision över hela samhället, där även säkerhetsaspekter kan tas i beaktan. Den mer direkta kopplingen till styrande instanser i samhället borde vara något som ger bättre förutsättningar för genomgående säkerhetsarbete.

Tillvägagångsättet för att ta fram projekt inom ramen för stadens vision skiljer sig också mellan städerna. Särskilt gällande Amsterdam, där uppbyggnaden av den smarta staden utgår till stor del från mottagna förslag från företag och även privatpersoner till projekt som kan vara relevanta. Det är ett system som inte återfinns lika tydligt i resterande städer, även fast övriga städer vill samarbeta med den privata sektorn. Det kan möjligen förklara den stora variationen av projekt som återfinns i Amsterdam. Utöver projekt som är tydligt kopplade till Amsterdams vision finns även projekt vars syfte vi på förhand inte skulle klassa som en smart stad-satsning.

4.2 Projekt

Beträffande projekten kan inledningsvis två huvudsakliga övergripande likheter identifieras. Den första likheten är att samtliga städer genomför projekt som involverar någon typ av autonoma fordon. Däremot tycks den mer konkreta formen för dessa skilja sig åt. I Oslo är det exempelvis kollektivtrafikbolagen som testar mindre typer av självkörande bussar medan det i San Francisco handlar om etableringen av en bilpool med fordon som allmänheten kan nyttja. Den andra likheten handlar om att det i samtliga städer finns en återkommande tendens att arbeta med olika typer av datainsamling, exempelvis genom att mäta antalet lediga parkeringsplatser eller antalet cyklister på vissa platser under vissa tider. Insamlade data ska ofta användas för att kunna ge olika beslutfattare ett bättre underlag samt skapa automatiserade prediktiva analyser som ska underlätta för invånarna, exempelvis genom att skapa reseförslag för resenärer i kollektivtrafiken. Detta är egentligen inte förvånande då en central del av smarta städer, åtminstone utifrån ett tekniskt perspektiv, handlar om att samla in och dela olika typer av data.

Något som även finns i flera av städerna är diverse mobilapplikationer, till exempel olika typer av interaktiva kartor eller betalnings- och reseplaneringstjänster för kollektivtrafiken. Frågan är dock hur unikt detta är för just smarta städer – som jämförelse kan nämnas att nästan hälften av Sveriges kommuner redan 2014 hade någon form av mobilapplikation.[92] Samtidigt är applikationer i sig ingen homogen kategori utan den tekniska och innovativa nivån kan variera ganska kraftigt. Huruvida applikationer i sig ska anses vara en smart stad-satsning eller endast ett naturligt led i den allmänna digitaliseringen är inte självklart. Här bör man dock kunna hämta inspiration från en av de grundläggande aspekterna av smart stad-begreppet – nämligen sammankoppling – och fråga sig om applikationen utgör en del i ett större system, vars ”smarthet” först uppstår när alla dess komponenter kopplas samman och interagerar. Ur ett sådant perspektiv kan applikationer, som sedda var för sig inte verkar särskilt smarta eller sofistikerade, ändå betraktas som en smart stad-satsning när dessa väl sätts in i sitt sammanhang.

Bland de projekt som kan anses mest ”udda” eller unika i sammanhanget finner vi *Dikesfrirördragning* och *Utsläppsfria byggarbetsplatser* – båda från Oslo. Dessa projekt är intressanta eftersom de båda handlar om byggnation och samtidigt sticker ut från vad som återfinns i de andra städerna. Det kan dock diskuteras i vilken mån projekten kan anses rymmas inom ramen för en allmän förståelse av smart stad och om det även i de andra städerna finns byggarbetsplatser med miljövänliga fordon och verktyg men att de inte har betecknats som en smart stad-satsning.

Ett av de mest intressanta projekten torde vara Amsterdams *Schoonschip* som – till skillnad från många andra smart stad-satsningar – bör kunna skapa en *ökad* robusthet. Detta då elförsörjningen blir mer robust i ett system där varje hushåll har en viss egen produktion och lagring av elektricitet, som dessutom kan omfördelas till hushåll i dess närhet. Ett sådant system bör – åtminstone temporärt – minska påverkan av en attack eller olycka som drabbar elkraftverk eller elnät. Hur stor påverkan är, i termer av tid och begränsad funktionalitet för hushållen, beror på självförsörjningsgraden, det vill säga hur mycket el hushållen kan producera. Även om hushållen inte är helt självförsörjande i vardagen, utan istället beroende av en viss mängd extern elektricitet, bör ett sådant system kunna konfigureras för att vid en eventuell strömförlust begränsa användningen av icke-kritiska system och på så sätt bli självförsörjande under en sådan situation. Samtidigt kan dessa typer av lösningar skapa nya sårbarheter. Exempelvis finns det en risk att den ökade IT-infrastrukturen som krävs för att hantera ett sådant system utgör en ny öppning för en angripare. Således kan en konsekvens vara att den fördelaktiga attackvektorn för en angripare flyttas från regionala elkraftverk och elnät till mer lokalt placerade IT-system i städerna.

4.3 Risker och sårbarheter

I detta avsnitt följer bland annat fyra stycken SWOT-analyser över risker och sårbarheter med den smarta staden i respektive stad. I matriserna står SC-koppling för *Smart City*-koppling och indikerar således att något har en direkt eller indirekt koppling till den smarta staden. Olika typer av riskanalyser benämns som Risk- och sårbarhetsanalyser (RSA), dessa ska dock inte förstås som en direkt motsvarighet till det svenska begreppet. Efter SWOT-analysen följer ett avsnitt av diskussionskaraktär som även lyfter blicken framåt och funderar kring hur konceptet smart stad i sig ger upphov till nya typer av risker.

[92] Sverige Kommuner och Landsting. *E-tjänster och appar – hur är läget i kommunerna*? s. 21.

4.3.1 SWOT-analys

	Positiva	Negativa
Interna	*Styrkor:* - Genomgående, toppstyrt säkerhetsarbete med direkt SC-koppling - Toppstyrt säkerhetsarbete - Tidigare erfarenheter - Cybersäkerhet inkluderat i totalförsvaret	*Svagheter:* - Bristfällig riskmedevetenhet hos företag och invånare
Externa	*Möjligheter:* - Omvärldsanalyser	*Hot (identifierade av staden):* - Illvilliga aktörer

Figur 4.3.1 åskådliggör en genomförd SWOT-analys över risker och sårbarheter med den smarta staden i **Singapore**.

	Positiva	Negativa
Interna	*Styrkor:* - RSA med indirekt SC-koppling - Trafiksäkerhetsarbete med direkt SC-koppling	*Svagheter:* - Avsaknad av RSA med direkt SC-koppling - Trafiksäkerhet som enda område med direkt SC-koppling - Risk för elransonering
Externa	*Möjligheter:* - RSA med hänsyn till naturkatastrofer	*Hot (identifierade av staden):* - Illvilliga aktörer - Naturkatastrofer

Figur 4.3.2 åskådliggör en genomförd SWOT-analys över risker och sårbarheter med den smarta staden i **Oslo**.

	Positiva	Negativa
Interna	*Styrkor:* - RSA med indirekt SC-koppling	*Svagheter:* - Avsaknad av RSA med direkt SC-koppling - Stort antal aktörer och projekt - Ökande digitalisering - Cyberincidenter utan uppsåt
Externa	*Möjligheter:* - Informationsutbyte med andra länder	*Hot (identifierade av staden):* - Illvilliga aktörer - Främmande makt - Terrorism

Figur 4.3.3 åskådliggör en genomförd SWOT-analys över risker och sårbarheter med den smarta staden i **Amsterdam**.

	Positiva	Negativa
Interna	*Styrkor:* - Inkludering av socioekonomiskt svaga - Beredskapsplaner kopplade till IT	*Svagheter:* - Ingen RSA med direkt SC-koppling - Cyberincidenter utan uppsåt
Externa	*Möjligheter:* - RSA med direkt SC-koppling från DHS	*Hot (identifierade av staden):* - Illvilliga aktörer - Naturkatastrofer

Figur 4.3.4 åskådliggör en genomförd SWOT-analys över risker och sårbarheter med den smarta staden i **San Francisco**.

Positiva

De positiva aspekterna som framkommit från SWOT-analysen kretsar kring hur städernas säkerhetsarbete kring den smarta staden kan ge en positiv effekt på förebyggandet av de risker som är kopplade till den smarta staden.

En gemensam positiv intern aspekt för samtliga städer i vår studie är att de har gjort en risk- och sårbarhetsanalys kopplat till digitalisering. Singapore särskiljer sig här utifrån att det är den enda staden som har ett dedikerat säkerhetsarbete riktad direkt till den smarta staden, något som tydligt återspeglas av att cyberförsvar ses som en av grundpelarna i Singapores totalförsvarsplan.

Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen

Vi tror att även fast städerna inte har gjort egna risk- och sårbarhetsanalyser finns det en möjlighet att förbättra sitt riskarbete genom att använda rapporter kopplade till digitalisering som grund för säkerhetsarbetet. San Francisco är ett tydligt exempel, framförallt genom kopplingen till transportsektorn och autonoma fordon samt den rapport som finns från amerikanska inrikessäkerhetsdepartementet på samma tema. Staden kan exempelvis antingen inkorporera dess slutsatser i sitt eget arbete, etablera ett samarbete med departementet inom området eller utföra en egen liknande studie. Externa styrkor vi finner hos Amsterdam och Singapore är att båda vill blicka utåt i omvärlden för samarbete och analyser av förekommande hot mot cybervärlden.

Negativa

De negativa aspekterna som har framkommit utifrån SWOT-analysen kretsar kring risker utifrån städernas arbete för att bli en smart stad och kopplat till digitalisering i allmänhet.

Den tydligaste negativa aspekten är att endast en stad i vår studie har gjort en risk- och sårbarhetsanalys kopplat direkt till den smarta staden. Singapore är den enda staden i vår studie som har säkerhetsrisker och säkerhetsarbete direkt kopplade till den smarta staden, åtminstone den som har sådant kommunicerat öppet. San Francisco har gjort en risk- och sårbarhetsanalys kopplad till cyber- och datasäkerhet, därutöver har det gjorts en rapport på nationell nivå av den amerikanska staten om risker och sårbarheter med smarta städer i allmänhet.[93] I Oslo har staden gjort allmänna risk- och sårbarhetsanalyser där cyber- och datasäkerhet ingår. För Amsterdam har nationella risk- och sårbarhetsanalyser utifrån cyberhot och digitalisering gjorts, men dessa är inte uttalat kopplade direkt till den smarta staden.

Gemensamt för samtliga städer är att det finns ett externt hot i form av attacker utifrån den egna staden eller landet. Amsterdam har identifierat tänkbara angripare som antingen främmande makt, enskilda individer och terroristgrupper. Vi tror att dessa grupper är tänkbara angripare av samtliga städer i vår studie, oavsett om de har kommunicerat ut det offentligt. Det som däremot kan skilja sig är vilka aktörer som utgör det största hotet, då exempelvis risken för terrorbrott skiljer sig mellan länder och även städer. Oslo är den stad som tydligast inkluderat ett hänsynstagande till naturkatastrofer som en risk, främst genom scenariot med solstormar.

4.3.2 Diskussion

Hur städerna har arbetat med risker kring digitaliseringen och uppbyggnaden av den smarta staden skiljer sig åt. På grund av att de flesta projekt inom ramen för den smarta staden är kopplade till digitalisering är det rimligt att anta att de sårbarheterna som tas upp kommer att öka riskerna vid ökad digitalisering. Huruvida det är ett direkt problem att städernas risk- och sårbarhetsanalyser är fristående beror på huruvida städernas fristående smarta stad-projekt tar risker i beaktan. Sårbarheten vi kan se när det är en mängd olika aktörer som bidrar till utvecklingen av den smarta staden utan någon tydlig ansvarskedja för säkerhetsarbetet är att bristen på styrning och riktlinjer kan bidra till en mer utsatt digital miljö. Detta stöds även av FOI:s rapport *Vilse i lasagnen*, i vilken det skrivs att när fler aktörer utvecklar system inom samma område kan det ge negativa konsekvenser för ett genomgående säkerhetsarbete på grund av bristen på samordning.[94]

Svårigheten med att diskutera risker inom ramen för smarta städer är att vad som utgör en smart stad beror på vilka projekt vi väljer att klassa som smart stad-projekt. Att det finns risker med digitalisering är ingen hemlighet och oavsett hur vi väljer att definiera den smarta staden är digitalisering till synes en stor del av processen. Frågan vi då får ställa oss när vi resonerar kring riskerna är om det väsentliga är huruvida staden klassar projekten som en smart stad-satsning, eller om vi ska se det som en naturlig del av digitaliseringen av samhället. Ifall det är en naturlig del av utvecklingen kan vi även se det som en del av de redan etablerade riskerna med digitaliseringen. Ifall vi anser att utvecklingen av smarta

[93] U.S. Department of Homeland Security's Office of Cyber and Infrastructure Analysis. *The Future Of Smart Cities: Cyber-physical Infrastructure Risk.*
[94] Ingemarsdotter, Eidenskog & Hedtjärn Swaling. *Vilse i Lasagnen?* s. 41.

staden ska ses som något nytt, frånskilt digitaliseringen, skulle det däremot kunna medföra behov av nya riskbedömningar. Tanken grundar sig i att utvecklingen av den smarta staden innefattar någon typ av samhällsförändring, som innefattar andra värden än explicit tekniska förändringar. Det leder oss till frågan om dagens riskanalyser grundade i cyberhot är tillräckliga, eller om andra värden och aspekter måste tas i beaktan i riskarbetet.

En viktig aspekt av den smarta staden, som flera städer har uppmärksammat, är vikten av att tillse att samtliga invånare kan delta i den smarta och digitaliserade staden. Även om digitaliseringen är tänkt att öka tillgängligheten – och troligtvis gör det för merparten av invånarna – så riskerar den ökande digitaliseringen paradoxalt nog att minska tillgängligheten för vissa grupper av invånare med sämre tekniska kunskaper eller ekonomiska resurser. San Francisco har till exempel försökt att delvis möta detta problem genom att tillhandahålla gratis internetuppkoppling och smarta telefoner.

Frågan vi vill lyfta handlar om hur människors och företags agerande kan komma att förändras i en smart stad. Det kan handla om hur samhället ser till att alla grupper kan ta del av den smarta staden för att undvika utanförskap, hur det nya ”smarta samhället” kan komma att förändra de nuvarande samhällsstrukturerna och hur det kan förändra riskbilden vi står inför. En aspekt av hur samhällsstrukturerna kan anses förändras i och med utvecklingen av den smarta staden är hur ny teknik och datainsamling påverkar människors förtroende för samhället. Vi menar att för att kunna bygga en smart stad måste starkt förtroende för både de styrande men även de företag som ansvarar för insamlad data finnas.

5 Slutsats

Utifrån det som har framkommit i vår studie finner vi inga större skillnader i vilket syfte städerna har med att utveckla den smarta staden. Samtliga städer vill på något sätt förbättra livet för invånarna i staden, i den mån syftet skiljer sig mellan städerna är det främst avseende vilka specifika inriktningar staden har kommunicerat utåt. Exempelvis Amsterdam har kommunicerat ett tydligt miljöperspektiv i sin vision medans San Francisco har lyft transportfrågan.

Vilken vision städerna kommunicerat har till synes inte tagit tydligt uttryck i de projekt som respektive stad har utfört. Typen av projekt har i samtliga städer haft stora likheter med varandra, dock ska nämnas att San Francisco har till större del projekt kopplade till transport, även fast liknande projekt återfinns i samtliga städer. Däremot, finner vi en större mängd av projekt i Amsterdam, där vi på förhand inte skulle klassa alla som smart stad-projekt. Det är något vi tror kan attribueras till stadens strategi men även det faktum att det inte finns någon vedertagen definition av vad ett smart stad-projekt är.

Utifrån vår SWOT-analys finner vi att alla städer möts av samma externa hot: illvilliga aktörer. Hur städerna har beskrivit dessa aktörer skiljer sig, men typen av hot är desamma. Den stad som skiljer sig tydligast från de övriga med avseende på säkerhetsarbetet är Singapore, som enda stad med ett säkerhetsarbete kopplat direkt till den smarta staden, något som borde ge förutsättningar för ett mer genomgripande säkerhetsarbete. Det vi främst ser som en säkerhetsrisk i övriga städer utan ett dedikerat säkerhetsarbete för den smarta staden är att säkerhetsfrågan helt enkelt negligeras eller ses som en naturlig del av digitalisering. Det gäller särskilt för städer likt Amsterdam med en stor mängd projekt sjösatta av olika aktörer. Utan tydliga säkerhetskrav tror vi att incitamenten för säkerhetsarbete och riskmedvetenheten kommer minska, vilket ökar sårbarheterna. En lösning på det problemet skulle kunna vara att likt i San Francisco tillse att varje projekt eller berörd myndighet har en utsedd IT-säkerhetsdirektör eller motsvarande.

Referenser

Albino, Vito, Berardi, Umberto & Dangelico, Rosa. *Smart Cities: Definitions, Dimensions, Performance, and Initiatives*. 2015. Journal of Urban Technology. 22. s. 3-21.

Amsterdam Smart City *Digital* Perimeter. https://amsterdamsmartcity.com/updates/project/digital-perimeter (Hämtad 2020-11-13).

Amsterdam Smart City. *Energy Atlas.* https://amsterdamsmartcity.com/projects/energy-atlas (Hämtad 2020-11-13).

Amsterdam Smart City. *Flexpower Amsterdam.* https://amsterdamsmartcity.com/updates/project/flexpower-amsterdam (Hämtad 2020-11-16).

Amsterdam Smart City. *Projects.* https://amsterdamsmartcity.com/projects/ (Hämtad 2020-10-26).

Amsterdam Smart City. *Street Sense* https://amsterdamsmartcity.com/updates/project/street-sense (Hämtad 2020-11-16).

Amsterdam Smart City. *The Energy Storage System.* https://amsterdamsmartcity.com/updates/project/energy-storage-system (Hämtad 2020-11-16).

Byggeindustrien, ”NoDig Challenge fullført”. *Bygg.no*, 5 september 2017. http://www.bygg.no/article/1324798 (Hämtad 2020-09-15).

City of Amsterdam. *Amsterdam Climate Neutral Roadmap 2050*. 2019. https://assets.amsterdam.nl/publish/pages/943415/roadmap_climate_neutral.pdf

Cityflows Europe. *Covid-19 living lab.* Juni 2020. https://cityflows-project.eu/covid-19-living-lab/ (Hämtad 2020-10-25).

Cyber Security Agency of Singapore. *GoSafeOnline.* Juli 2020. https://www.csa.gov.sg/gosafeonline (Hämtad 2020-10-26).

Cyber Security Agency of Singapore. *Our organisation.* April 2020. https://www.csa.gov.sg/who-we-are/our-organisation (Hämtad 2020-10-26).

Cyber Security Agency of Singapore. *Singapore´s Cybersecurity Strategy 2016.* 2016. https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy

Dameri, R. P. & Annalisa Cocchia. *Smart City and Digital City: Twenty Years of Terminology Evolution*. 2011. Conference of the Italian Chapter of AIS, ITAIS2013. 1-8.

IMD Business School. *Smart City Index 2019*. https://www.imd.org/research-knowledge/reports/imd-smart-city-index-2019/ (Hämtad 2020-09-09).

Ingemarsdotter, Johanna, Daniel Eidenskog, & Vidar Hedtjärn Swaling. 2020 *Vilse i lasagnen? –En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur*. FOI-R--4814--SE. Stockholm: Totalförsvarets forskningsinstitut.

Kelkar, Mahesh, Golden, Deborah, Pandey, Piyush & Peasley Sean. *Making smart cities safer.* 2019. Deloitte Insights.

Lee, Jung Hoon, Marguerite Gong Hancock, and Mei-Chih Hu. "Towards an Effective Framework for Building Smart Cities: Lessons from Seoul and San Francisco". *Technological Forecasting & Social Change*, vol. 89/(2014;2013;), s. 80-99.

Ministry of defence. *Total defence*. Februari 2020. https://www.scdf.gov.sg/home/community-volunteers/community-preparedness/total-defence (Hämtad 2020-10-21).

Ministry of Justice and Security. *Cyber Security Assessment Netherlands.* 2019. https://english.ncsc.nl/binaries/ncsc-en/documents/publications/2019/09/13/cyber-secrurity-assessment-netherlands-2019/Cyber-+Security-+Assessment-+Netherlands-+2019.pdf

Mora, Luca & Bolici, Roberto. *How to Become a Smart City: Learning from Amsterdam*. 2017. DOI https://doi.org/10.1007/978-3-319-44899-2_15. Smart and Sustainable Planning for Cities and Regions: Results of SSPCR 2015 (s.251-266)

Myndigheten för samhällsskydd och beredskap [MSB]. *Extrema solstormar*: *Konsekvenser för samhällsviktig verksamhet* [MSB 1318]. Januari 2019. https://www.msb.se/sv/publikationer/extrema-solstormar--konsekvenser-for-samhallsviktig-verksamhet/ (Hämtad 2020-09-28).

Oslo kommun. *Circular economy and waste management*. https://www.oslo.kommune.no/politics-and-administration/green-oslo/best-practices/circular-economy-in-practice/ (Hämtad 2020-09-15).

Oslo kommun. *Climate Dashboard*. https://www.oslo.kommune.no/politics-and-administration/smart-oslo/projects/climate-dashboard/ (Hämtad 2020-09-15).

Oslo kommun. *Dementia-friendly solutions.* https://www.oslo.kommune.no/politics-and-administration/smart-oslo/projects/dementia-friendly-solutions/ (Hämtad 2020-09-15).

Oslo kommun. *Kommunalt risikobilde 2017 (kortversjon)*. Oslo: Oslo kommun, beredskapsetaten, 2017. https://www.oslo.kommune.no/egenberedskap/kommunens-arbeid-med-samfunnssikkerhet-og-beredskap/ (Hämtad 2020-09-14).

Oslo kommun. *No-Dig Challenge*. https://www.oslo.kommune.no/politics-and-administration/smart-oslo/projects/no-dig-challenge/ (Hämtad 2020-09-15).

Oslo kommun. *Public city apps*. https://www.oslo.kommune.no/politics-and-administration/smart-oslo/apps/ (Hämtad 2020-09-15).

Oslo kommun. *Smart Oslo*. https://www.oslo.kommune.no/politics-and-administration/smart-oslo (Hämtad 2020-09-14).

Oslo kommun. *Smart Oslo: Projekt.* https://www.oslo.kommune.no/politics-and-administration/smart-oslo/projects (Hämtad 2020-09-15).

Oslo kommun. *Zero-Emission Construction Sites*. https://www.oslo.kommune.no/politics-and-administration/smart-oslo/projects/zero-emission-construction-sites/ (Hämtad 2020-09-15).

Oslo kommuns Byrå för stadsmiljö (*nor. Bymiljøetaten*). Mejl inkommet den 6 november 2020 [personlig kommunikation].

Puri, Deepak. "Ayyeka Sigfox IoT sensors monitor sewage deep underground San Francisco". *Network World*, 2017. https://www.networkworld.com/article/3171072/ayyeka-sigfox-iot-sensors-monitor-sewage-deep-underground-san-francisco.html (Hämtad 2020-09-21).

Ruter. *Emission Free public transport in Oslo and Akershus*. 2018, version 10. https://ruter.no/en/about-ruter/reports-projects-plans/fossilfree2020/ (Hämtad 2020-09-20).

Ruter. *Mobilitetspunkt Filipstad*. https://ruter.no/om-ruter/prosjekter/mobilitetspunkt-filipstad/ (Hämtad 2020-11-09).

Ruter. *Self-driving vehicles*. https://ruter.no/en/about-ruter/reports-projects-plans/autonomous-vehicles/ (Hämtad 2020-09-15).

Samuel Gibbs. "Ransomware attack on San Francisco public transit gives everyone a free ride". *The Guardian*, 2016. https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware (Hämtad 2020-09-21).

San Francisco Committee on Information Technology. *Citywide Cybersecurity Policy*. 21 november 2019. https://sfcoit.org/cybersecurity (Hämtad 2020-11-02).

San Francisco Committee on Information Technology. *Citywide IT focused- Disaster Preparedness, Response, Recovery, and Resilience Policy*. 18 november 2018. https://sfcoit.org/dpr3 (Hämtad 2020-11-02).

San Francisco Committee on Information Technology. *Information and Communication Technology Plan: FY 2020-24*. https://sfcoit.org/strategy (Hämtad 2020-09-16).

San Francisco Committee on Information Technology: Budget & Performance subcommittee. *Regular Meeting February 3 2017* [presentation]. https://sfcoit.org/node/100000638 (Hämtad 2020-09-16).

San Francisco. *DataSF: Open Data*. https://datasf.org/opendata/ (Hämtad 2020-10-27).

San Francisco. *Explore*. http://smartcitysf.com/how.html (Hämtad 2020-09-21).

San Francisco. *Our Vision*. http://smartcitysf.com/ (Hämtad 2020-09-21).

San Francisco. *Partners*. http://smartcitysf.com/ (Hämtad 2020-10-19).

San Francisco. *Smart City Challenge, San Francisco: Harnessing the Future of Shared Mobility* [faktablad]. http://smartcitysf.com/ (Hämtad 2020-09-15).

Schoonschip Amsterdam. https://schoonschipamsterdam.org/ (Hämtad 2020-11-02).

Smart Nation Singapore. *HealthHub.* https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Health/healthhub (Hämtad 2020-10-29).

Smart Nation Singapore. *Drones to survey dengue hotspots.* https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Urban-Living/drones-to-survey-dengue-hotspots-1 (Hämtad 2020-11-13).

Smart Nation Singapore. *Fintech Sandbox.* https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Startups-and-Businesses/fintech-sandbox (Hämtad 2020-11-13).

Smart Nation Singapore. *Open data and analytics for urban transportation.* https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Transport/open-data-and-analytics-for-urban-transportation-1 (Hämtad 2020-11-13).

Smart Nation Singapore. *Parents gateway.* https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Digital-Government-Services/parents-gateway (Hämtad 2020-10-2).

Smart Nation Singapore. *Punggol Digital District.* https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Startups-and-Businesses/punggol-digital-district (Hämtad 2020-11-13).

Smart Nation Singapore. *Smart Elderly Alert System*. https://www.smartnation.gov.sg/what-is-smart-nation/initiatives/Urban-Living/smart-elderly-alert-system (Hämtad 2020-11-13).

Smart Nation Singapore. *Smart nation: The Way Forward 2018.* https://www.smartnation.gov.sg/docs/default-source/default-document-library/smart-nation-strategy_nov2018.pdf?sfvrsn=3f5c2af8_2 (Hämtad 2020-10-26).

Sverige Kommuner och Landsting [SKL; numera SKR]. *E-tjänster och appar – hur är läget i kommunerna?* 2014. https://internetstiftelsen.se/docs/skl-undersokning-2014-etjanstappar.pdf (Hämtad 2020-10-20).

Teorell, Jan & Torsten Svensson. *Att fråga och att svara: samhällsvetenskaplig metod*. Stockholm: Liber. 2007.

The Explorer. "Smart platform for shared bicycles". *Theexplorer.no*. https://www.theexplorer.no/solutions/urban-sharing-smart-platform-for-shared-bicycles/ (Hämtad 2020-09-15).

U.S. Department of Homeland Security's Office of Cyber and Infrastructure Analysis [DHS/OCIA]. *The Future Of Smart Cities: Cyber-physical Infrastructure Risk.* Augusti, 2015. https://us-cert.cisa.gov/ics/Future-Smart-Cities-Cyber-Physical-Infrastructure-Risk (Hämtad 2020-11-02).

U.S. Department of Transportation. *Smart City Challenge*. 2017. https://www.transportation.gov/smartcity (Hämtad 2020-09-21).