



Statens vegvesen



Teknologi og digitalisering i transportsektoren

Anders R. Hovdum

fagdirektør sikkerhet og beredskap

Strategiske mål 2030



Statens vegvesen



Tilrettelegge for
framtidens
transportsystem



Utvikle og ta vare
på vegnettet på en
profesjonell måte



Bidra til trygge
trafikanter og sikre
kjøretøy



Fremme bærekraft og
redusere
klimagassutslipp



Styrke vår
gjennomførings-evne

Tilrettelegge for framtidens transportsystem

Vårt mål er at etaten utvikler en myndighets- og regulatorrolle i et helhetlig intelligent transportsystem.

Hovedgrep 2018-2021

- Etablere Statens vegvesen som myndighet og regulator i utviklingen av et intelligent transportsystem
- Utforme regelverk for ITS basert på internasjonale standarder
- Avklare statens eierskap og tilgang til veg- og trafikkdata
- Bruke teknologi som et av flere verktøy for å oppnå nullvisjonen
- Utvikle transport som eget kjerneområde i organisasjonen



- Personvern
- Sikkerhet og sårbarhet
- **Samfunnssikkerhet og nasjonal sikkerhet**

- Datakvalitet
- Big Data – store datamengder

- **Forretningsmodeller – er det Google som legger premissene**

- Harmonisering/standardisering
- Sosiale medier
- Målrettet reklame

Samfunnssikkerhet



Statens vegvesen

«Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger.»
St.meld. 10 (2016–2017) “Risiko i et trygt samfunn”

« (...) kunnskapen om trusler og risikoområder generelt sett er altfor lav. Norske virksomheter har verken god nok oversikt over sine verdier eller risikoen de er utsatt for, og dermed heller ikke oversikt over skader og kostnader sikkerhetsbrudd og cyberangrep kan påføre dem.»

Mørketallsundersøkelsen 2018

- Kjøretøyer tilkobles Internett for levering av kjøretøyrelaterte eller brukerstyrte tjenester
 - skaper komplekse avhengigheter
 - feil et sted kan få følger og slå ut et helt annet sted
 - masseprodusert elektronikk
 - manglende standarder
- Lange og uoversiktlige digitale verdikjeder med mange aktører hvor feil forplanter seg
- Økende avhengighet av GPS-baserte tjenester og satellittkommunikasjon
 - forstyrrelser av GPS-signaler
 - forfalskning av lokasjonsinformasjon
- Ny teknologi innføres ikke likt og til samme tid, dvs. vi til enhver tid har en blanding av eldre og nyere teknologi
- Avhengighet av elektronisk kommunikasjon

Trusselaktørene



Statens vegvesen

- Statlige aktører
- Kriminelle nettverk
- Innsideaktører

- Rekke former for angrep og metoder som hackere og kriminelle bruker:
 - utpressingsprogramvare som låser datamaskinen og krever løsepenger
 - Spionasje
 - tyveri av eposter
 - publisering av sensitiv informasjon om noen (doxing)
 - vandalisme mot nettsider
 - Datatyveri
 - angrep for å ødelegge nettsider eller data

- Bilen din blir kryptert, eller overtatt og forårsaker en kollisjon som fører til skade på mennesker eller eiendom.

Hva kan gjøres



Statens vegvesen

- Samfunnssikkerhetsutfordringer som følger av økt bruk av C-ITS i transportsektoren må kartlegges / konkretiseres
 - Robuste løsninger
 - Alternative / redundante systemer
 - Restitusjon og nedetid
- Myndighetenes rolle og evne til å regulere innføring og bruk av C-ITS i transportsektoren må tydeliggjøres
- Beredskapsprinsippene nærhet, likhet og ansvar ikke tilstrekkelig for å ivareta samfunnssikkerheten – må erkjennes
 - Markedsaktørene er pådrivere
 - Beredskap og sikkerhet krever en overhead aktørene ikke har
- Summen av alle aktørenes forberedelser ikke tilstrekkelig for å ivareta sikkerhet og beredskap i en digitalisert transportsektor
- Investeringer i C-ITS for å redusere digitale sårbarheter bør likestilles med investeringer i fysisk infrastruktur og bli en del av NTP- planforslag