Viljeshandlinger mot kollektivtransport i storbyer – trusler og tiltak

Håvard Fridheim, Tor-Erik Schjelderup og Andreas Borander

Forsvarets forskningsinstitutt (FFI)

10.06.2009

FFI-rapport 2009/01078

351001

P: ISBN 978-82-464-1592-5
E: ISBN 978-82-464-1593-2

Emneord

Kollektivtransport

Sårbarhet

Risiko

Terrorisme

Viljeshandlinger

Godkjent av

Håvard Fridheim	Prosjektleder
Jan Erik Torp	Avdelingssjef

Sammendrag

Rapporten presenterer overordnede resultater etter et oppdrag om risikovurdering av kollektivtrafikken i Oslo mot viljeshandlinger, spesielt terror og sabotasje. Arbeidet ble startet opp høsten 2007 og avsluttet våren 2009.

Det er i dag vanskelig å si at risikoen for alvorlige viljeshandlinger er påtrengende stor for kollektivtransporten i Norge. Norge har svært få erfaringer med terror, og større sabotasjehandlinger er primært en trussel i forbindelse med militære angrep. I dag er det ikke noe som tilsier en særlig økning i denne trusselen på kort sikt. Internasjonalt har man imidlertid sett flere eksempler på angrep mot kollektivtransportsystemer, i de siste årene også i form av massedrapsangrep med bruk av improviserte sprengladninger. Enkelte mindre omfattende viljeshandlinger, som hærverk og tagging, kan også i noen tilfeller føre til stans i transporttjenester, om enn kortvarig.

Sårbarhetene overfor de fleste typer viljeshandlinger er store. I dag er det ikke vanskelig å gjennomføre viljeshandlinger mot norske kollektivtrafikksystemer, så lenge man har tilgang på våpen og er motivert for å gjennomføre angrep. Potensialet for alvorlig skade ved målrettede terror- og sabotasjeangrep er stort.

Tiltak som i dag innføres mot andre typer viljeshandlinger, som hærverk, bråk og tyveri, vil ikke nødvendigvis gi god sikring mot terror og sabotasje. Rapporten foreslår derfor en rekke generelle tiltak som kan hjelpe mot slike større viljeshandlinger, så lenge de inngår i et helhetlig og målrettet sikkerhetsarbeid.

En rettesnor for sikkerhetsarbeidet i norske kollektivtransportsystemer i dag må likevel være at de skal fremstå som åpne arenaer for publikum og attraktive arbeidsplasser for ansatte. Tiltak som gir store inngrep i funksjonalitet i transporttjenestene, muligheten til fri ferdsel på offentlig sted og personkontroll bør derfor ikke inngå som en del av grunnberedskapen i transportsektoren. Slike tiltak kan imidlertid vise seg nødvendige ved høyere trusselnivå enn det vi har i dag.

English summary

This report presents simplified, non-specific results from a risk assessment of the public transport system in Oslo against malicious attacks, in particular terrorism and sabotage. The work started during the fall of 2007, and was finalized in the spring of 2009.

There are no known present threats of terrorism against Norway's public transport system, and there are no indications that the threat will change dramatically in the short term. Major sabotage attacks are usually associated with military scenarios. In Western Europe, though, there have been several major terrorist attacks in public transport systems, in later years also mass casualty attacks using improved explosive devices. Also, everyday incidents like vandalism or tagging have a potential to stop transport services for short periods of time.

The vulnerabilities against most security incidents are large, and the consequences of successful attacks can be severe. It is not hard to accomplish dramatic impacts in the Norwegian public transport system, as long as means and motives are available.

Security measures that are introduced in the mass transport system today are rarely geared towards major malicious attacks. They are mostly introduced to combat more common challenges, like theft, gang activity or vandalism. To rectify this, the report proposes several measures that can help against the more dramatic security incidents, as long as the measures are integrated into a holistic and systematic emergency preparedness strategy.

One important guideline for the suggested measures is that the public transport systems in Norway should still appear as an open arena for the passengers and an attractive place to work for the employees. Measures that are highly disruptive for the general functionality of transport services, or cumbersome for the passengers, should not be implemented in the present security climate. However, such measures have to be considered should the threat level rise.

Innhold

1	**Innledning**	**7**
1.1	Introduksjon	7
1.2	Bakgrunn for og avgrensninger i arbeidet	8
2	**Viljeshandlinger i transportsektoren?**	**9**
2.1	Begreper i tilknytning til sikkerhet	9
2.2	Aktører, motiver og virkemidler i viljeshandlinger	9
2.3	Hva kan skje i transportsektoren?	10
2.4	Viljeshandlinger kontra kollektivtransport – sårbarhet og utfordringer	12
2.4.1	Utfordringer for sikring mot viljeshandlinger	12
2.4.2	Sårbarheter overfor terrorangrep/massedrap	13
2.4.3	Sårbarheter overfor sabotasje/svikt i transporttjenestene	13
2.4.4	Sårbarhet overfor svikt i eksterne infrastrukturer	14
3	**Trusselen for viljeshandlinger mot kollektivtransportsystemer**	**14**
3.1	Trusselen mot Norge og norske interesser	14
3.2	Trusler mot transportsektoren	16
3.2.1	Terrorangrep	16
3.2.2	Sabotasje	18
3.2.3	Andre hendelser	19
3.3	Trender innenfor terrorisme, spesielt mot kollektivtransport	20
3.3.1	Generelle trender for innenfor terrorisme i EU	20
3.3.2	Angrep mot transportmål i EU i 1998-2006	21
3.3.3	Terrorisme mot norsk kollektivtransport?	23
4	**Relevante tiltak mot viljeshandlinger**	**25**
4.1	Tiltak – sikkerhet eller skuebrød?	25
4.2	Organisasjonsmessige og administrative tiltak	26
4.2.1	Avklaring av målsetting og ansvarsforhold	26
4.2.2	Samarbeidsutvalg innenfor sikkerhet mellom involverte aktører	27
4.3	Planer og sikkerhetsvurderinger	27
4.3.1	Beredskapsplaner	27
4.3.2	Evakueringsplaner	28
4.3.3	Øvelser	28
4.3.4	Etterretning og analyse	28
4.3.5	Risikoanalyser	29
4.3.6	”Penetrasjonstester”	29

4.4	Forebyggende tiltak	29
4.4.1	Adgangskontroll	29
4.4.2	Regulering av trafikk rundt store stasjoner	31
4.4.3	Kameraovervåking	31
4.4.4	Vakthold og patruljer	32
4.4.5	Rydding av områder og fjerning av gjemmesteder	33
4.4.6	Informasjon til reisende	34
4.4.7	Sensorer for deteksjon av våpen	34
4.4.8	Kontroll av bagasje og reisende	36
4.4.9	Kontroll av parkert materiell	37
4.4.10	Brannsikkerhet	37
4.4.11	Fortifikasjon av kritiske funksjoner	37
4.5	Konsekvensreduserende tiltak	38
4.5.1	Konsekvensreduserende design	38
4.5.2	Redundans og desentralisering av kritiske funksjoner	38
4.5.3	Beskyttelsesutstyr	39
4.6	Tiltak overfor eget personell	39
4.6.1	Tiltak for sikker håndtering av informasjon	39
4.6.2	Kompetanseutvikling - trening og kursing	41
4.6.3	Sosiale tiltak	42
4.7	Sikkerhet mot andre viljeshandlinger enn terror/sabotasje	42
4.8	Tiltaksstrategier	44
5	**Oppsummering og anbefaling**	**45**
Appendix A	**Sikkerhet ved VM på ski**	**46**
A.1	Utvikling innenfor sikkerhet ved OL	46
A.2	Spesifikke sikkerhetshendelser ved tidligere arrangementer	47
A.3	Eksempler på sikkerhetstiltak	49
A.3.1	Vinter-OL i Salt Lake City i 2002	49
A.3.2	Sikkerhet ved Vinter-OL i Torino i 2006	50
A.4	Konsekvenser av økt satsing på sikkerhet	51
A.5	Sikkerhet ved VM på ski i 2011	51
A.5.1	Er ski-VM et attraktivt mål for viljeshandlinger?	51
A.5.2	Utfordringer for kollektivtransporten	52
A.5.3	Aktuelle tiltak	52
Appendix B	**Forkortelsesliste**	**55**
	Referanser	**56**

1 Innledning

1.1 Introduksjon

Denne rapporten er skrevet i forbindelse med et oppdrag FFI har gjennomført for Kollektivtransportproduksjon AS (KTPAS), Oslo kommune ved Beredskapsetaten, Jernbaneverket, NSB BA, Flytoget og Ruter As, om risiko ved ulike former for viljeshandlinger mot kollektivtrafikksystemet i Oslo-området. Oppdraget ble gjennomført i perioden høsten 2007 - våren 2009, og arbeidet er dokumentert i en ikke offentlig hovedrapport.[1] Oppdragsgiverne ønsket i tillegg en offentlig tilgjengelig kortrapport, for lettere å kunne dele informasjon om arbeidet. Denne rapporten presenterer derfor en overordnet og mindre detaljert versjon av resultatene. I praksis presenterer den de generelle utfordringene som går igjen ved sikring av kollektivtransportsystemer i storbyer mot viljeshandlinger, og den skisserer i tillegg overordnede tiltak som kan inngå i transportvirksomhetenes beredskapsarbeid.

Viljeshandlinger er handlinger som er gjort med forsett av mennesker. Motivene for slike handlinger kan være å ramme eller påvirke samfunnssystemer, virksomheter eller individer, for eksempel politisk, økonomisk eller helsemessig. Mye sikkerhetsarbeid har som hensikt å motvirke viljeshandlinger som gir alvorlige samfunnsmessige konsekvenser, for eksempel militære angrep, sabotasje eller terrorhandlinger. Dette oppdraget har hatt som hovedmål å vurdere risiko, primært overfor terrorangrep med massedrap som følge, eller sabotasje som fører til langvarig forstyrrelse av transporttjenestene. Tradisjonelle militære utfordringer har ikke vært en del av arbeidet – søkelyset har vært satt på hvilke typer aksjoner enkeltpersoner eller mindre grupper kan være i stand til å gjennomføre, primært med enkle, fysiske virkemidler.[2]

Begrepet viljeshandlinger omfatter imidlertid også hendelser som kan oppfattes som mindre alvorlige for samfunnet, blant annet ran, hærverk, trusler og rampestreker. I verste fall kan også slike hendelser skape farlige situasjoner eller føre til sikkerhetsbrudd, og over tid kan de i sum utgjøre store utfordringer for publikum, transportvirksomhetene og samfunnet i form av økonomiske tap, svekket tjenestetilbud eller redusert generell trygghetsfølelse. Slike viljeshandlinger er beskrevet overordnet i oppdraget, og foreslåtte tiltak er også sett i sammenheng med disse.

Rapporten er strukturert som følger

- Kapittel 1 beskriver bakgrunnen for og innholdet i rapporten.
- Kapittel 2 definerer begrepet viljeshandlinger, og diskuterer generelt hvordan slike hendelser kan utgjøre sikkerhetsutfordringer for kollektivtransportsystemer.
- Kapittel 3 diskuterer trender og trusler når det gjelder relevante former for angrep mot kollektivtransportsystemer.

[1] Fridheim, H. Schjelderup, T.E. Borander, A. (2009): Kollektivtransport i Oslo-området som mål for viljeshandlinger - Trusselbilder, sårbarheter og forslag til tiltak, FFI/RAPPORT-2009/00890 (U.off. iht. offentleglova § 21)

[2] I praksis tilsier dette at aksjoner av størrelse som terrorangrepene i Madrid 2004 og London 2005 danner en øvre grense for hvilke scenarioer som er vurdert i oppdraget.

- Kapittel 4 presenterer generelle tiltak som kan være aktuelle overfor viljeshandlinger.
- Kapittel 5 oppsummerer rapporten.

I tillegg ble oppdraget bedt om å fremskaffe noe informasjon om sikkerhetsarbeid rundt store idrettsarrangementer, som grunnlag for planleggingen før ski-VM i Oslo i 2011. Denne informasjonen er samlet i appendiks A.

1.2 Bakgrunn for og avgrensninger i arbeidet

Oppdragets arbeid har hatt følgende hovedmålsettinger:[3]

- Bidra til økt kunnskap om trusselsituasjonen og potensielle aktører.
- Identifisere sentrale utviklingsfaktorer, gjennomgå og oppdatere eksisterende scenarioer, og vurdere nye scenarioer for ulike trusler mot kollektivtransporten.
- Forbedre beslutningsgrunnlaget for å utarbeide og gjennomføre forebyggende tiltak.
- Styrke evnen til krisehåndtering.
- Forbedre grunnberedskapen hos aktørene.

Det er gjort noen avgrensninger i hvilke trusler og utfordringer oppdraget har sett på:

- Rapporten ser på persontransport, ikke godstransport.
- Rapporten ser på lokal kollektivtrafikk i storbyer – med andre ord er ikke persontransport over lange distanser, ekspressbusser, utenlandsferger og cruiseskip osv. tatt med.
- Arbeidet har ikke sett på sikring mot tradisjonelle krigstrusler
- Arbeidet har ikke sett på tiltak for sikring av IKT-systemer mot logiske angrep (cybertrusler)
- Tiltak som er vurdert er i første rekke av forebyggende art, med andre ord tiltak som kan hindre eller vanskeliggjøre terror og sabotasje mot transportsystemet. Tiltakene er ikke kostnads- eller effektivitetsvurdert.

Arbeidet har tatt utgangspunkt i tidligere FFI-arbeider innenfor transportsektoren, bl.a. prosjektet "Beskyttelse av samfunnet 4"[4], et oppdrag våren 2005 om viljeshandlinger mot togtrafikk[5], et oppdrag sommeren 2006 om viljeshandlinger mot Oslo S[6] og et oppdrag høsten 2006 om viljeshandlinger mot innenriks sjøtransport.[7] Arbeidet baserer seg også på løpende arbeider fra FFIs TERRA-prosjekt (terrorisme og asymmetrisk krigføring). Mye av informasjonen i denne rapporten er hentet direkte fra tidligere rapporter fra de nevnte arbeidene.

[3] Ref. "Mandat for securityprosjektet for Oslos kollektivtransport" – Versjon 1.1, 16. januar 2008
[4] Hagen J et al (2003): Beskyttelse av samfunnet med fokus på transportsektoren, FFI/RAPPORT 2003/00929.
[5] Schjelderup T E et al (2005): Togtrafikken som mål for terror og sabotasje – en risikoanalyse, FFI/RAPPORT-2005/01894 (U.off)
[6] Fridheim H et al (2006): Oslo S som mål for terror og sabotasje – en risikoanalyse, FFI/RAPPORT-2006/03790 (Begrenset)
[7] Eggereide B et al (2007): Innenriks sjøtransport som mål for terror – en risikovurdering, FFI/RAPPORT-2007/00004 (Begrenset)

2 Viljeshandlinger i transportsektoren?

Oppdraget har hatt som formål å se på sikkerhet mot viljeshandlinger. Dette kapittelet definerer hva viljeshandlinger er, spesielt sett i sammenheng med andre beslektede begreper, og diskuterer kort sårbarheter overfor slike handlinger i kollektivtransportsystemer.

2.1 Begreper i tilknytning til sikkerhet

Definisjon av begrepet *sikkerhet* ble viet stor plass i Infrastrukturutvalgets rapport fra 2006.[8] Sikkerhet ble her benyttet som samlebegrep for alt beskyttelsesarbeid mot uønskede hendelser. Innenfor sikkerhetsbegrepet skjuler det seg mange dimensjoner, blant annet om de uønskede hendelsene er tilfeldigheter og ulykker, eller om de skjer som resultat av overlegg. Derfor deles sikkerhetsbegrepet ofte i to; *safety* og *security;* hvor safety omfatter det normale sikkerhetsarbeidet som skjer mot ulykker, tekniske feil og skader, mens security omhandler sikkerhet overfor tilsiktede hendelser utført eller utløst av mennesker.

Viljeshandlinger er handlinger som er gjort med forsett av mennesker. Motivene for slike handlinger kan være å ramme eller påvirke samfunnssystemer, virksomheter eller individer, for eksempel politisk, økonomisk eller helsemessig. FFI har tradisjonelt hatt et fokus på viljeshandlinger som er motivert ut fra ønsket om å oppnå alvorlige samfunnsmessige konsekvenser, f.eks. militære angrep, sabotasje eller terrorhandlinger. Begrepet viljeshandlinger omfatter imidlertid også handlinger med adskillig mindre konsekvenser enn dette, som ran, hærverk og rampestreker. Slike hendelser kan også i noen tilfeller skape farlige situasjoner eller føre til sikkerhetsbrudd med alvorlige konsekvenser.

Ut fra diskusjonen over skulle security være noe nær det samme som sikkerhet mot viljeshandlinger. Det er likevel noen nyanseforskjeller mellom begrepene, ikke minst basert på hvordan begrepet security har blitt brukt de seneste årene:

- Mange assosierer security med *store* viljeshandlinger, slik som terrorisme og sabotasje.
- EUs 7. rammeprogram inkluderer også store industriulykker og naturkatastrofer i sine forskningsprogram innen security.[9]

I enkelte kretser er dermed security i ferd med å bli et begrep for sikkerhet mot hendelser med lav sannsynlighet og tilsvarende store konsekvenser, uavhengig av årsak. På grunn av dette brukes i stedet begrepet viljeshandlinger i denne rapporten, for å sikre fokus på hendelser som er utført eller utløst av mennesker.

2.2 Aktører, motiver og virkemidler i viljeshandlinger

Det er en rekke aktører som kan tenkes å gjennomføre viljeshandlinger mot infrastrukturmål. En generell liste kan inkludere følgende aktørtyper:

- Fremmede makter

[8] Justis- og politidepartementet (2006): Når sikkerhet er viktigst, NOU 2006:6
[9] European commission (2006): Work Programme 2007 – Cooperation Theme 10 Security.

- Terrorister
- Aktivister
- Kriminelle
- Utilregnelige personer
- Pøbler
- Utro tjenere i egen organisasjon
- Vanskelige kunder
- Konkurrenter

Motiver for at slike aktører skal gjennomføre viljeshandlinger mot infrastrukturer kan også være mangslungne:

- Etterretning - fremskaffe informasjon
- Press for å påvirke prosesser og avgjørelser
- Utøve hevn
- Sabotasje - forstyrre eller stanse tjenester
- Oppnå økonomisk vinning
- Søke oppmerksomhet, moro og spenning
- Irrasjonelle hendelser

Tilsvarende er virkemidlene som kan tas i bruk under forskjellige viljeshandlinger mange:

- Konvensjonelle virkemidler for fysisk skade på personer, materiell eller bygningsmasse. Dette inkluderer virkemidler for brannstiftelse, håndvåpen og eksplosiver/sprengladninger, i tillegg mer hverdagslige gjenstander som slagvåpen, kniver/skarpe gjenstander, malingsbokser, fremmedlegemer på kjøreveier osv.
- Kjemiske, biologiske, radiologiske og kjernefysiske virkemidler
- Virkemidler for elektronisk krigføring – elektroniske pulser, mikrobølgevåpen, jamming
- Logiske virkemidler for angrep på IKT-systemer
- Sosiale virkemidler – informasjonskampanjer, bombetrusler, truende oppførsel osv.

Selv enkle lister som dette viser at en risikovurdering overfor viljeshandlinger er krevende. Antall mulige kombinasjoner av aktører, virkemidler og motivasjoner er stort. Når man skal vurdere sikkerhet mot viljeshandlinger, blir det derfor viktig å være presis på hvilke viljeshandlinger man skal sikre mot, slik at de svar som gis og tiltak som foreslås er relevante.

2.3 Hva kan skje i transportsektoren?

Bredden av mulige viljeshandlinger setter sikkerhetsarbeidet innenfor transportvirksomhetene på en stor prøve. En viktig utfordring er at ulike viljeshandlinger kan få mange forskjellige utfall og konsekvenser.

Generelt kan viljeshandlinger mot kollektivtransport føre til følgende konsekvenser:

- Ansatte, passasjerer og brukere kan bli utsatt for farlige situasjoner, med risiko for liv og helse.
- Transporttjenester kan bli stanset eller forstyrret.

- Det kan utøves materiell skade på utstyr, som medfører økonomiske tap.
- Passasjerer og ansatte kan bli utsatt for kriminelle handlinger, ran og tyveri, som medfører økonomiske tap.
- Passasjerer og ansatte kan oppleve en sterkt redusert trygghetsfølelse ved å bruke kollektivtransporttjenestene, og som følge av dette se seg om etter alternativer.

Det er viktig å være presis på hvilke konsekvenser man søker å redusere risiko overfor. Sikring mot massedrap på publikumsarealer krever f.eks. andre tiltak enn sikring mot tagging av vognparken på parkeringsplasser eller sikring av kritiske objekter for trafikkstyringen. Hvis man ikke har en klar kobling mellom trusler, mulige konsekvenser, relevante tiltak og selve transportsystemet, er det fare for å innføre sikkerhetstiltak som strengt tatt ikke gir ønsket effekt, men som er kostbare og har dramatiske konsekvenser for passasjerer og egne ansatte.

I dette oppdraget ses det spesielt på følgende viljeshandlinger:

- **Terrorangrep med massedrap som formål**. Disse kan utføres av enkeltindivider eller mindre grupper, blant annet motivert ut fra ønsker om hevn eller politisk oppmerksomhet. Flere virkemidler er relevante, men bruk av fysiske virkemidler og sprengladninger er tradisjonelt mye brukt.
- **Sabotasje med formål å stanse deler av transporttjenestene**. Normalt er dette et naturlig virkemiddel i innledende faser av militære angrep, som er utenfor dette oppdragets arbeid. Mer relevant er aksjoner utført av enkeltindivider med generell destruksjonstrang, eller sabotasje gjennomført som avledningsmanøvre i forbindelse med annen kriminell virksomhet. Dette vil naturlig nok ikke være hendelser av samme omfang og intensitet som et militært angrep, men konsekvensene kan bli alvorlige nok når de gjennomføres på riktig sted. Svikt i transporttjenestene kan også bli konsekvensen av mer uskyldig motiverte viljeshandlinger, for eksempel i forbindelse med hærverk, tyveri og spenningssøkende aktiviteter. Spekteret av mulige aktører, motiver og virkemidler for denne typen trusler er derfor stort.

Det er verdt å understreke at trusselen ved slike viljeshandlinger ikke bare kommer fra eksterne aktører. Slike hendelser kan understøttes eller faktisk også gjennomføres av egne ansatte. Medarbeiderne i en virksomhet har god kunnskap om kritiske sårbarheter som kan utnyttes i viljeshandlinger.

Utover dette er det mulig å peke på mange andre typer viljeshandlinger som er relevante for transportsektoren, for eksempel:

- Hærverk og materiell skade, spesielt tagging.
- Ran og tyveri
- Bråk og uro
- Trusler mot egne ansatte
- Etterretningsvirksomhet og stjeling av informasjon

Disse siste typene hendelser behandles ikke direkte videre i denne rapporten, men i kapittel 4 kommenteres det hvordan foreslåtte tiltak mot terror og sabotasje eventuelt kan sikre mot denne typen trusler også.

2.4 Viljeshandlinger kontra kollektivtransport – sårbarhet og utfordringer

2.4.1 Utfordringer for sikring mot viljeshandlinger

I dag er det relativt få hindre mot store viljeshandlinger innenfor kollektivtrafikksystemet i de fleste storbyer. Slike hendelser kan utnytte den grunnleggende sårbarheten som nær alle kollektivtrafikksystemer har: De skal være åpne og lett tilgjengelige for store publikumsmengder, slik at trafikkavviklingen går mest mulig effektivt.

Som følge av dette er det få hindringer for tilgang til publikumsområdene, i form av adgangskontroll eller kontroll av medbrakt bagasje. De store folkemengdene som oppsøker publikumsarealene gjør det også krevende å oppdage avvikende oppførsel som signaliserer at en viljeshandling er under oppseiling. Dette gjør at en rekke tradisjonelle sikkerhetstiltak knyttet til avsperring, inngjerding, fortifikasjon, adgangskontroll osv. har liten hensikt i store deler av transportsystemet – i praksis vil slike tiltak drepe muligheten til å avvikle trafikk i det volumet man ser i dag.

Likevel er det innført en rekke tiltak som skal sikre mot ulike viljeshandlinger. Graffiti fjernes fortløpende, kameraer er installert over store deler av systemet og kritiske anlegg utenfor publikumsområdene er låst og sperret av. En utfordring er likevel at disse tiltakene ikke dekker spennet av viljeshandlinger som er skissert i kapittel 2.2. Sikring mot terrorscenarioer er kanskje den største utfordringen, men også sikring mot virkelig alvorlige sabotasjeangrep er mangelfull. Innenfor de fleste lokale trafikksystemer er sikkerhetstiltak i første rekke rettet mot å ivareta driftssikkerhet i hverdagen. Tiltak vinkles mot hendelser som vurderes som sannsynlige, som skjer ofte og som man kjenner seg igjen i. Å skulle sikre systemet mot mer ekstreme viljeshandlinger oppleves av mange som ren ”science fiction”, og behovet for slik sikring har en tendens til å bli argumentert bort med uttalelser av typen ”hvorfor skulle noen ha interesse av å angripe vårt system?”

Skulle man likevel bestemme seg for å gjennomføre tiltak mot viljeshandlinger, blir det viktig å avklare hvem som har ansvaret for å gjøre dette. Kollektivtrafikken har de siste årene opplevd en storskala oppsplitting av tidligere store selskaper. Der man før gjerne hadde ett eller to selskaper som alene ivaretok administrasjon, eierskap, planlegging og gjennomføring av kollektivtrafikken, finner man i dag separate selskaper knyttet til de ulike oppgavene. Virksomhetene har i tillegg fjernet servicefunksjoner som vakt- og renhold, og kjøper heller disse tjenestene fra eksterne selskaper. Samtidig vil en rekke myndighetsorganer på kommunalt, fylkes- og direktoratsnivå ha funksjoner overfor transportaktørene.

I denne jungelen av involverte aktører er det ofte vanskelig å peke på hvem som er ansvarlig for å sikre de ulike delene av transportsystemet mot viljeshandlinger. Eierskapsgrenser og ansvarsforhold kan være uklare, og konkrete krav og målsettinger for sikkerhetsarbeidet varierer på tvers av aktørgrensene. Det som skjer av sikkerhetsarbeid blir da i beste fall fragmentert, i verste fall ikke relevant overfor dagens trusselbilde.

2.4.2 Sårbarheter overfor terrorangrep/massedrap

Flere terroraksjoner har vært rettet mot kollektivtransport internasjonalt de siste årene, hvor transportinfrastrukturen har blitt benyttet som arena for massedrapsaksjoner. Formålet har med andre ord vært å drepe og skade mange mennesker, ikke å stanse transporttjenestene som sådan (selv om dette ofte er en sekundær effekt av angrepene).

Inntil nylig har det ikke vært gjennomført mye sikkerhetsarbeid mot slike trusler innenfor kollektivtransporten i Norge, annet enn innenfor luftfarten og for utenriks sjøtransport. Transportsektoren har derfor mange sårbare områder for slike aksjoner, i praksis ethvert område som samler mange mennesker på et konsentrert areal. Her er det relativt enkelt å gjennomføre massedrapsaksjoner, så lenge man har nødvendige motiver og virkemidler.

Noen sårbare punkter for slike aksjoner er:

- Selve transportmidlene – busser, sporvogner, t-banevogner, togsett og båter.
- Terminaler og store stasjonsområder, og nærområder knyttet til disse.
- Angrep mot selve kjøreveien, f.eks. tunneler, bruer, utplassering av legemer på skinnegang for tog og t-bane osv.

2.4.3 Sårbarheter overfor sabotasje/svikt i transporttjenestene

I transportvirksomhetene har sabotasjetrusselen hatt større fokus enn terrorisme. Derfor er det allerede gjennomført en rekke tiltak overfor denne trusselen, f.eks. knyttet til adgangskontroll. Likevel er ikke sikkerhetstiltakene veldig avanserte, og de fleste transporttjenestene har sårbare områder som kan angripes for å sette dem ut av spill.

Det er viktig å understreke at sabotasje ikke har vært noe utpreget motiv ved gjennomførte viljeshandlinger mot transport de siste årene. Likevel kan andre typer aksjoner, f.eks. hendelser som har som formål å utøve hærverk og materiell skade, føre til at transporttjenestene stopper opp i kortere eller lengre tid.

Noen sårbare områder for sabotasje er:

- Selve kjøreveien, spesielt skinnegående transport (utplassering av fremmedlegemer for å stoppe passerende tog, ødeleggelse av kjørebanen)
- Oppstillingsplasser hvor store deler av kjøretøyparken kan skades med aksjoner av begrenset omfang.
- Trafikkstyringssentraler, spesielt for t-bane og tog
- Tekniske rom og installasjoner for støttesystemer, f.eks. datarom, signaleringssystemer, sambandsbaser, kabelgater, likerettere for kraftforsyning osv.

2.4.4 Sårbarhet overfor svikt i eksterne infrastrukturer

Transportsektoren er naturlig nok avhengig av svært mange andre samfunnsfunksjoner og infrastrukturer. Tradisjonelt fremheves *kraftforsyningen og elektronisk kommunikasjon* som to bærebjelker i moderne samfunn, og det kan forventes store samfunnsmessige konsekvenser dersom strøm eller samband svikter. Imidlertid oppstår det relativt sjelden store utfall i kraftforsyning eller elektronisk kommunikasjon som følge av viljeshandlinger. Denne sårbarheten er derfor normalt mest relevant i forbindelse med teknisk svikt og ulykker i de nevnte sektorene.

3 Trusselen for viljeshandlinger mot kollektivtransportsystemer

Dette kapittelet diskuterer relevante trusler mot kollektivtransportsystemer, basert på offentlig tilgjengelig informasjon.

3.1 Trusselen mot Norge og norske interesser

Politiets sikkerhetstjeneste (PST) utarbeider fortløpende trusselvurderinger. Årlig lages en vurdering for Justis- og politidepartementet som grunnlag for hvilke prioriteringer PST skal ha i sitt arbeid for det inneværende året. I tillegg utarbeides periodiske vurderinger og hendelsesstyrte trusselvurderinger (f.eks. ved statsbesøk og alvorlige hendelser i inn- og utland). Flere trusselvurderinger er graderte, men det utgis ofte ugraderte utgaver i tillegg.

Overfor faren for terror graderer PST trusselbildet i fire nivåer: lav, moderat, høy og ekstrem. Hva som karakteriserer hvert nivå er beskrevet i det følgende:[10]

- Lav: Sannsynligheten for en terroraksjon er lav. En eller flere aktører kan ha intensjoner om, men trolig ikke kapasitet til å ramme bestemte interesser.
- Moderat: Sannsynligheten for en terroraksjon er moderat. En eller flere aktører kan ha intensjoner om og kapasitet til å ramme bestemte interesser.
- Høy: Sannsynligheten for en terroraksjon er betydelig. En eller flere aktører har intensjoner om og kapasitet til å ramme bestemte interesser. Det foreligger en uspesifisert trussel.
- Ekstrem: Sannsynligheten for en terroraksjon er ekstremt høy. En eller flere aktører har intensjoner om å ramme bestemte interesser. Det foreligger en spesifikk trussel. Ingen ytterligere advarsler kan påregnes før en aksjon iverksettes.

Trusselnivået i Norge ble endret til lav i juni 2006, etter å ha vært på moderat nivå siden høsten 2004. Selv om Norge ikke har hatt særlig erfaring med alvorlige viljeshandlinger, peker PSTs trusselvurdering for 2009 på flere forhold som er relevante i tiden fremover. Disse beskrives kort i det følgende:[11]

[10] Politiets sikkerhetstjeneste: http://www.pst.politiet.no
[11] Tekst hentet fra PSTs åpne trusselvurdering 2009: http://www.pst.politiet.no/Filer/utgivelser/trusselvurderinger/Aapen_trusselvurdering_PST.pdf

- **Politisk motivert vold – terrorisme**
  Risikoen for politisk motivert vold utøvet av aktører som er inspirert av ekstrem islamisme, vil fortsatt representere en utfordring for Norge. Hovedtyngden av ekstrem islamistisk aktivitet i Norge er knyttet til støttevirksomhet til utlandet, men det foreligger også indikasjoner på økende radikalisering. Økt radikalisering i Norge gjør det nasjonale trusselbildet mer uforutsigbart. PST har ikke avdekket konkrete planer om terrorangrep i Norge, men trusselbildet er komplekst, og situasjonen kan endres raskt.
- **Politisk motivert vold – nasjonal ekstremisme**
  Ekstreme nasjonale grupperinger utgjør i dag ingen alvorlig trussel mot norske interesser. Det høyreekstreme miljøet er svekket av bl.a. dårlig økonomi og lite rekruttering, og trusselen herfra vil i første rekke være enkeltpersoners voldelige adferd. Når det gjelder venstresiden pekes det på mulige ordensproblemer i forbindelse med demonstrasjoner og markeringer, bl.a. mot israelske og amerikanske interesser.
- **Spredning av masseødeleggelsesvåpen**
  Trusselvurderingen peker på at spredning av masseødeleggelsesvåpen (kjemiske, biologiske og kjernefysiske våpen, samt leveringsmidler) utgjør en betydelig sikkerhetstrussel. Det er derfor viktig å forhindre at varer, kunnskap og teknologi eksporteres fra Norge til aktører som har til hensikt å utvikle og produsere masseødeleggelsesvåpen eller leveringsmidler for slike.
- **Etterretningsvirksomhet mot Norge og norske interesser**
  Fremmede staters etterretningsaktivitet mot Norge og norske interesser er på et vedvarende høyt nivå. Trusselvurderingen peker spesielt på at flere stater er i ferd med å bygge opp betydelig kapasitet innen datanettverksoperasjoner, spesielt for spionasje og målrettet informasjonsinnhenting.
- **Trusler mot myndighetspersoner**
  Trusler mot myndighetspersoner fremsettes av personer med ulik motivasjon og intensjon. Trusselvurderingen peker på at den teknologiske utviklingen har bidratt med nye kanaler for omtale av og henvendelse til myndighetspersoner, blant annet SMS, nettsteder, blogger og epost. Dette ser ut til å ha senket befolkningens generelle ytringsterskel, også når det gjelder aggressive og truende ytringer. De fleste trusler fremsettes spontant, i affekt eller under ruspåvirkning, og har sjelden sammenheng med en reell intensjon om å utføre en skadelig handling. For 2009 vil imidlertid stortingsvalget til høsten føre til at flere myndighetspersoner blir profilert sterkere enn vanlig.

3.2 Trusler mot transportsektoren

3.2.1 Terrorangrep[12]

Internasjonalt har kritisk infrastruktur de siste årene blitt en arena for massedrapsaksjoner. Terrorgrupper søker å maksimere effekten av voldsbruk gjennom å spre frykt (”terror”) for å fremme sin politiske agenda. Dette oppnår de først og fremst gjennom handlinger som skaper store oppslag i media, og massedrapsaksjoner blir derfor mer interessante enn sabotasje som medfører materiell skade eller ødelagte tjenester fra kritisk infrastruktur.

De siste årene har vi sett internasjonale terrornettverk med stor vilje og kapasitet til å gjennomføre massedrapsaksjoner. I første rekke gjelder dette det tidligere Afghanistan-baserte Al-Qaida, i tillegg til en hel rekke radikale jihadistgrupper som deler Al-Qaidas ideologi. Massedrapsaksjoner er en relativt ny utvikling innen terrorisme, og dette skaper store utfordringer for vår sikkerhetstenkning.

Transportsektoren har vist seg mer utsatt for denne typen viljeshandlinger enn andre kritiske infrastrukturer. I første rekke skyldes dette at mange terrorgrupper retter oppmerksomheten sin mot arenaer hvor de kan ramme flest mulig mennesker. Transportsektoren har flere egenskaper som gjør den til en fristende arena for massedrap:

- Store deler av infrastrukturen er åpen og lett tilgjengelig for de som bruker den. Transportsektoren er derfor utsatt for viljeshandlinger i langt større grad enn andre infrastrukturer.
- Mange personer er samlet på relativt små arealer. Konsekvensene av en vellykket viljeshandling er derfor langt mer åpenbar i transportsektoren enn for andre infrastrukturer.

De fleste offentlige transportmidler er vanligvis ubeskyttet, og tradisjonelle sikkerhetstiltak har vært rettet mot å forhindre menneskelig svikt og ulykker, ikke fiendtlige viljeshandlinger. Selv om fokus på beskyttelse mot terrorangrep har økt de siste årene, har det vist seg vanskelig å utvikle gode teknologiske løsninger for å bekjempe og avverge terrorhandlinger på offentlig infrastruktur.

Utover massedrap er den politiske effekten av aksjoner mot transportmål også et viktig moment for terrorgrupper. De fleste mennesker anvender transporttjenester fra fly, tog, buss eller båt, og aksjoner mot transportmål vil derfor ofte påvirke publikums opplevelse av trygghet og bevegelsesfrihet. Dette kan igjen få betydelige politiske og økonomiske konsekvenser.

Selv om Norge har vært forskånet fra terrorangrep mot kollektivtransportmål de seneste årene, er det flere eksempler å hente fra andre europeiske land. Det er her spesielt to hendelser som har

[12] Enkelte formuleringer i avsnittet er hentet rett fra: Schjelderup Tor-Erik, Lia Brynjar, Rodal Gry Hege (2005): Togtrafikken som mål for terror og sabotasje – en risikoanalyse, FFI/RAPPORT-2005/01894 (Unntatt offentlighet)

bidratt til økt oppmerksomhet rundt terrortrusselen mot urbane kollektivtransportsystemer: Terrorangrepene i Madrid i 2004 og London i 2005.

Om morgenen 11. mars 2004 bombet militante islamister fire pendlertog på tre forskjellige stasjonsområder i Madrid.[13] Bombene gikk av inne i togsettene. Totalt omkom 191 personer. Terroristene hadde plassert ut 14 bomber ombord i togsettene – 3 av disse detonerte ikke. Bombene var typisk bygget opp av ca 10 kg sprengstoff, spiker og skruer, en detonator og en mobiltelefon. Angrepet var i praksis skreddersydd for å ramme blindt og ta livet av flest mulig mennesker. Et interessant trekk ved aksjonene var at de ikke ble utført av selvmordsbombere, men at bombene ble satt igjen i bagasje på togsettene for utløsing på "verst mulig tidspunkt" i henhold til rutetabellene.

7. juli 2005 eksploderte tre bomber i løpet av kort tid på tre t-banevogner, mens en bombe detonerte på en buss ved Tavistock Square ca en time senere. Angrepene ble gjennomført av selvmordsbombere med hjemmelagede sprengladninger. I tillegg til gjerningsmennene omkom 52 passasjerer i angrepene.

Disse to angrepene har fått stor oppmerksomhet i ettertid på grunn av de katastrofale tapstallene de medførte. Det har imidlertid også skjedd andre typer hendelser mot transportsektoren som kunne ha gitt store konsekvenser. Noen av disse er omtalt i trendrapporter fra Europol:

- The German Trolley Bomb Case. [14] 31 juli 2006 ble to improviserte sprengladninger pakket i kofferter og satt ombord på to regiontog nær Köln i Tyskland Begge bombene bestod av en gassflaske, en vekkerklokke, en detonator og tre plastflasker med bensin. Bombene detonerte ikke, men det er antatt at mange ville blitt drept eller skadet om så hadde skjedd. To libanesiske studenter i Tyskland ble senere arrestert, mistenkt for å ha plassert ut bombene. Hendelsen skal bl.a. ha vært motivert av striden rundt de danske karikaturtegningene av profeten Muhammed. Angrepene ble opprinnelig planlagt gjennomført under VM i fotball i Tyskland samme år, men ble utsatt pga. alle sikkerhetstiltakene som var i sving under dette arrangementet.
- UK Airplane Plot. [15] 10. august 2006 ble det gjennomført flere arrestasjoner i Storbritannia, mot en gruppe mennesker mistenkt for å planlegge et selvmordsangrep mot flere fly mellom Storbritannia og USA. Planen skal ha vært å smugle komponenter for improviserte sprengladninger ombord i fly, blant annet flytende eksplosiver i plastflasker. Totalt elleve mennesker ble arrestert, i hovedsak britiske statsborgere av pakistansk opprinnelse. Aksjonen skal ha vært motivert av krigføringen i Afghanistan og Irak, og et viktig formål var å ramme både amerikanske og britiske mål samtidig.
- Glasgow International Airport.[16] 30. juni 2007 ble en brennende bil med gassflasker ombord kjørt inn i terminalbygningen ved flyplassen i Glasgow, Skottland. Gassflaskene

[13] Lia B, Nesser P (2005): Terror mot jarnvegar – Eit oversyn over typiske terroraksjonar mot togpassasjertransport. FFI/RAPPORT-2005/01451, Forsvarets forskningsinstitutt.
[14] Europol (2007): "TE-SAT 2007 - EU Terrorism Situation and Trend Report 2007"
[15] Europol (2007): "TE-SAT 2007 - EU Terrorism Situation and Trend Report 2007"
[16] Europol (2008): "TE-SAT 2008 - EU Terrorism Situation and Trend Report 2008"

eksploderte ikke, og bare et fåtall mennesker ble skadet. De to bilførerne ble arrestert, og den ene av dem døde senere på sykehuset som følge av brannskader. Det viste seg raskt at hendelsen kunne kobles til en feilslått aksjon i London dagen i forveien, hvor bomber var plassert ut i to biler nær en stor nattklubb, men ikke eksploderte.

Det er flere interessante fellestrekk ved disse aksjonene. Alle har hatt massedrap som formål, alle har vært rettet mot store kollektivtransportmål, alle har hatt sitt utspring i radikale islamistiske miljøer, og i alle har egenutviklede improviserte sprengladninger blitt anvendt.

3.2.2 Sabotasje

Med det store fokuset som har vært på massedrapsterrorisme de siste årene, har det vært tilsvarende mindre fokus på sabotasjeangrep mot transportsystemer. Dels er dette et uslag av at mange infrastruktureiere allerede har gjennomført flere sikkerhetstiltak mot sabotasje i kritiske deler av infrastrukturen. Samtidig viser ikke de mest aktive miljøene innenfor internasjonal terrorisme noen særlig interesse for å hindre gjennomføring av transporttjenester, spesielt over lengre tid. De fleste terrorgrupper er små og har for lite ressurser til å kunne gjennomføre landsomfattende og lammende sabotasjeanslag mot sivil infrastruktur.

Det er med andre ord vanskelig å se for seg velplanlagte og omfattende sabotasjeaksjoner mot transportsystemer i fredstid. Imidlertid er det flere andre aktører som kan gjennomføre mindre omfattende handlinger, som igjen kan føre til transportsvikt. Ikke minst gjelder dette egne ansatte, som av ulike grunner kan gjennomføre destruktive handlinger mot transportsystemet. Kollektivtrafikken i Oslo har sett eksempler på dette: Innenfor KTPAS har man opplevd flere forsøk på sabotasje mot t-banevogner på verkstedet på Ryen[17], som sannsynligvis er gjort av egne ansatte.

Transportsektoren er også stadig utsatt for viljeshandlinger av mindre alvorlig og målrettet karakter, f.eks. hærverk, brannstiftelse, tagging, ran og uro, og slike hendelser kan også gi materiell skade som kan føre til konsekvenser for trafikkgjennomføringen. I juli 2004 ble 21 t-banevogner på Vestli stasjon sprayet ned med maling både innvendig og utvendig, noe som førte til at man måtte sette inn buss på strekningen Vestli-Tøyen til vognene var rengjort.[18] Dette tilsier at kritiske deler av transportinfrastrukturen, spesielt steder der store deler av vognparken er parkert, kan være attraktive mål uten at hendelsene er motivert ut fra planer om å stanse trafikkgjennomføringen over tid.

Noen hærverkshendelser har også potensial til å medføre stort antall døde eller skadede. Et eksempel er utplassering av fremmedlegemer på skinnegangen, som bl.a. skjedde. 2. juli 2006[19].

[17] "Anmelder sabotasje på t-banevogner." Aftenposten 12. mars 2008. Lenke: http://www.aftenposten.no/nyheter/oslo/article745042.ece
[18] "Tagging stopper t-banen", Østlandssendingen 4. juli 2004. Lenke: http://www.nrk.no/nyheter/distrikt/nrk_ostlandssendingen/3911657.html
[19] "Sabotasje uroer passasjerer", Aftenpostens nettutgave 5. juli 2006. Lenke: http://ww.aftenposten.no/nyheter/iriks/article1377356.ece

Her ble fire betonglokk, hver på ca 35 kg, lagt over skinnegangen slik at et flytog kolliderte med dem. Den gangen oppstod det bare mindre materielle skader på lokomotivet, men en eventuell avsporing kunne ha gitt katastrofale følger.[20]

3.2.3 Andre hendelser

Selv om verken sabotasje- eller terrorangrep er regulære hendelser i norsk kollektivtransport, kan trusler om slike angrep forekomme oftere. Trusler kan fremsettes generelt mot virksomhetene, for eksempel i form av bombetrusler, gjensatte kofferter som det står "bombe" på og lignende. En mer spesifikk utfordring er at toppledere eller medieprofilerte medarbeidere kan bli utsatt for direkte trusler eller utpressingsforsøk.

Utover dette er det er en rekke hendelser som kan utfordre trygghetsfølelsen til publikum og ansatte i transportvirksomhetene, og mange slike rapporteres med store overskrifter i media. Ekebergbanen i Oslo har i perioder hatt et uroproblem, med drikking og bråk inne i trikkevognene, steinkasting mot trikken, hærverk og utplassering av gjenstander på trikkeskinnene.[21] Gjenger barker av og til sammen i masseslagsmål på publikumsarealer, som på Carl Berner i desember 2007, der et sted mellom 40 og 50 ungdommer begynte å slåss inne i en t-banevogn.[22] Narkotikaomsetning skjer åpenlyst nær store stasjonsområder, ikke minst utenfor Oslo S.[23] Profesjonelle grupper av lommetyver opererer på publikumsarealene og inne i transportmidlene.[24] Snikere på transportmidlene slår seg vrang og angriper kontrollører.[25] Selv om risikoen for å oppleve farlige situasjoner er relativt liten for reisende med kollektivtjenestene i Oslo, er det åpenbart et potensial for å oppleve ubehagelige situasjoner, og stadige oppslag av denne typen vil spre usikkerhet og utrygghet.

I tillegg kan det inntreffe hendelser som rammer kollektivtransporten indirekte. Det mest åpenbare eksemplet i nyere tid er store politiske demonstrasjoner som utarter seg i retning av opptøyer og vold, som demonstrasjonene i Oslo ifm. Israels krigføring i Gaza i januar 2009.[26] Selv om opptøyene etter disse demonstrasjonene primært rammet politiet og butikkeiere langs Karl Johans gate, har slike hendelser også potensial til å ramme transportsektoren. Dels kan

---

[20] Selv om den ikke var forårsaket av sabotasje, kan togulykken ved Eschede i Tyskland i 1998 si noe om skadepotensialet ved avsporing. Et tog med 287 passasjerer sporet da av som følge av en feil i hjulsystemet på en av vognene. Toget hadde en hastighet på ca 200 km/t og kjørte inn i en betongbro. 101 døde, 88 ble alvorlig skadet. Kilde: Wikipedia, http://en.wikipedia.org/wiki/Eschede_train_disaster

[21] "Vil ha slutt på bråk og hærverk", Nordstrands blad 22. mars 2007. Lenke: http://noblad.no/apps/pbcs.dll/article?AID=/20070322/NONYHETER/103220163

[22] "Masseslagsmål på t-banevogn", Aftenposten 8. desember 2007. Lenke: http://www.aftenposten.no/nyheter/oslo/article2143159.ece

[23] "Pågrep 120 personer i rusaksjon", Vårt land 16. april 2008. Lenke: http://www.vl.no/samfunn/article3479646.ece

[24] "Lommetyvene bruker skjorte og slips", Østkantavisa 17. mars 2008. Lenke: http://www.ostkantavisa.no/apps/pbcs.dll/article?AID=/20080317/NYHETER/843752131/1018/DEBATT

[25] "Kvinne dømt for kontrollørvold", Nettavisen 1. mars 2005. Lenke: http://pub.tv2.no/nettavisen/innenriks/article352944.ece

[26] "Her knuser demonstrantene Karl Johan", VG 8. januar 2009. Lenke: http://www.vg.no/nyheter/utenriks/midtosten/artikkel.php?artid=545880

byområder bli sperret av slik at trafikkavviklingen forstyrres, dels kan også transportmidler og infrastruktur bli utsatt for hærverk og skade.

3.3 Trender innenfor terrorisme, spesielt mot kollektivtransport

Siden terrortrusselen har vært veldig i fokus de seneste årene, er det interessant å se nærmere på utviklingstrekk og trender innenfor terrorangrep mot transportsektoren. Hvor relevant er denne trusselen for kollektivtrafikken i Norge?

3.3.1 Generelle trender for innenfor terrorisme i EU

Europol har de tre siste årene gitt ut rapporter om terrorsituasjonen i EU-området. Tabell 3.1. sammenfatter noe statistikk fra disse rapportene for antall registrerte terrorangrep, sortert på hvilket miljø hendelsene kan tilskrives.[27]

År	2006	2007	2008
Islamistisk	1	4	0
Separatistisk	424	532	397
Venstreradikal	55	21	28
Høyreradikal	1	1	0
Enkeltsak	-	1	5
Ikke spesifisert	17	24	11
Totalt antall hendelser	498	583	441
Hendelser fra UK	-	-	74

Tabell 3.1 Antall registrerte terrorangrep (gjennomførte, feilede eller avvergede) i EU for 2006-2008. Tall fra Storbritannia for 2008 avvek fra tidligere rapporteringer, i og med at man for første gang også inkluderte hendelser i Nord-Irland. Disse tallene er ikke direkte sammenlignbare med tidligere års data, og er derfor lagt til i egen rad.Kilde: Europol.

Rapportene understreker at det kan være store mørketall i antall registrerte hendelser. Datagrunnlaget gjør det også vanskelig å peke på entydige trender når det gjelder antall angrep over tid. Det er imidlertid mulig å lese ut en god del interessante sammenhenger fra dataene som ligger til grunn for tabellen. Langt de fleste registrerte hendelsene har blitt gjennomført av nasjonale separatistbevegelser, som normalt ikke vil angripe mål utenfor sine landegrenser. De landene som opplever flest angrep er da også store land som tradisjonelt har hatt problemer med slike bevegelser, som Frankrike, Spania og Storbritannia.

I tillegg understreker trendvurderingene i rapportene at de ønskede konsekvensene for aksjonene avhenger sterkt av angriperens politiske og ideologiske mål. Selv om flere av gruppene som er

[27] Europol (2007): ”TE-SAT 2007 - EU Terrorism Situation and Trend Report“.
Europol (2008): ”TE-SAT 2008 - EU Terrorism Situation and Trend Report”.
Europol (2009): ”TE-SAT 2009 - EU Terrorism Situation and Trend Report“.

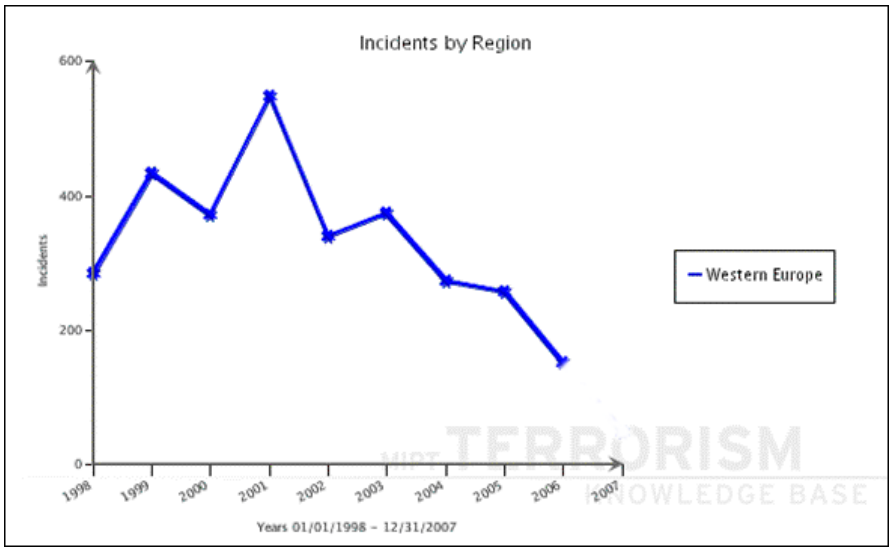
omtalt i tabell 3.1 har angrepet transportmål, er det så langt primært ekstreme islamske miljøer som har forsøkt å gjennomføre massedrapsaksjoner.

3.3.2 Angrep mot transportmål i EU i 1998-2006

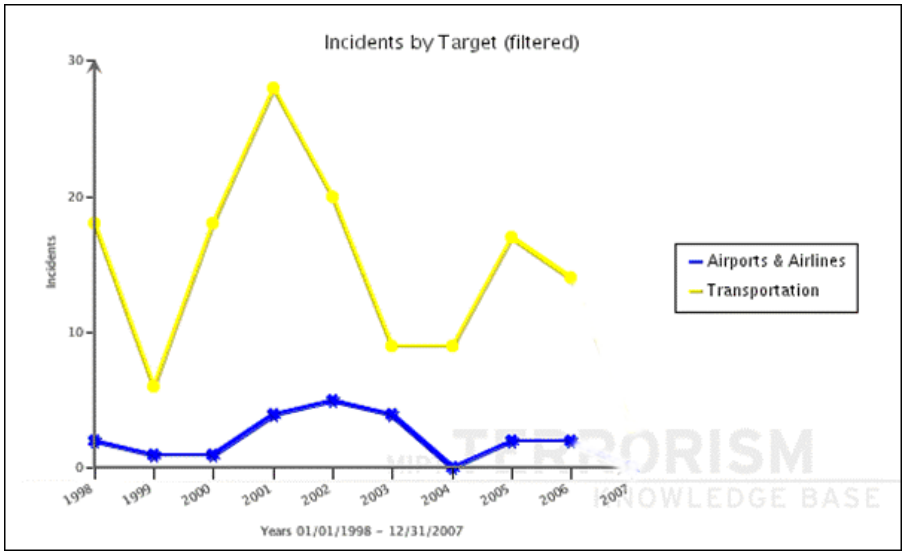
Bildet i forrige avsnitt kan utfylles ved å se på hendelser registrert i databasene fra Memorial Institute for the Prevention of Terrorism (MIPT) i USA. Instituttet drev frem til våren 2008 en egen database over registrerte terrorangrep (databasen har senere blitt lagt ned). FFI har gjennomført søk i databasen for registrerte terrorhendelser i Europa i perioden 1998-2006. I det følgende presenteres noen funn fra søket.

Totalt var det registrert 3.087 terrorhendelser i Vest-Europa i søkeperioden, med totalt 401 drepte. Transportsektoren (eksklusive luftfarten) var på sin side utsatt for 141 hendelser i samme periode, med totalt 247 drepte. Selv om angrep mot transportsektoren utgjør bare drøyt fire prosent av registrerte hendelser, stod disse for omlag halvparten av antall drepte som var registrert i basen. De registrerte drapstallene er i praksis summen av angrepene i Madrid i 2004 (191 omkomne) og London i 2005 (52 omkomne passasjerer og 4 gjerningsmenn). Det må imidlertid understrekes at tall for flere av de registrerte hendelsene er beheftet med betydelig usikkerhet.

Antall terrorhendelser per år er illustrert i figur 4.1. Tilsvarende er antall terrorhendelser bare mot transportsektoren skissert i figur 4.2.



Figur 4.1 Registrerte terrorangrep mot Vest-Europa 1998-2006. Kilde: MITP Terrorism Knowledge Base



Figur 4.2 Terrorangrep mot transportsektoren 1998-2006. Kilde: MIPT Terrorism Knowledge Base

Antall registrerte angrep går gradvis nedover etter en topp rundt 2001. Innenfor transportsektoren var det også en topp rundt 2001, men her varierer det mer i den etterfølgende perioden. Dette kan være et utslag av at registrerte hendelser er relativt få, i tillegg til det faktum at koordinerte angrep registreres som flere hendelser (angrepene i Madrid og London er registrert som fire hendelser hver).

De 141 hendelsene mot transportsektoren fordeler seg som følger:

- 50 mot busser
- 26 mot stasjonsområder for tog og t-bane
- 22 mot vognsett for tog og t-bane
- 18 mot spor og skinnegang for tog
- 16 mot annen vegbasert transport
- 6 mot tog, andre typer angrep (f.eks. angrep mot kraftforsyning til togene)
- 2 mot luftfart (feilregistreringer i databasen)
- 1 mot sjøfart (en ferge ved Korsika)

Som også Europols terrorrapporter beskriver, er langt de fleste av disse hendelsene gjennomført av nasjonale separatistbevegelser i Frankrike, Spania og Storbritannia.

Virkemidlene som ble tatt i bruk i aksjonene var som følger:

- 69 angrep med brannstiftelse og brannbomber
- 63 angrep med bruk av eksplosiver
- 4 tilfeller av kapring
- 5 andre former for angrep (f.eks. kutting av kraftkabler)

3.3.3 Terrorisme mot norsk kollektivtransport?

I vestlige land har det i lengre tid vært en generell konsensus om at faren for global terrorisme har vært økende etter 11. september 2001.[28] Tallene fra MIPT som ble presentert i kapittel 3.3.2. viser imidlertid en jevn nedgang i antall registrerte terrorangrep etter 2001, mens Europols tall fra 2006-2008 er vanskelig å trekke konklusjoner ut fra. Selv om man kanskje ikke bør ta tall for Vest-Europa som utgangspunkt for trender når det gjelder global terrorisme, kan det også på verdensbasis argumenteres for at terrortrusselen ikke er økende, i alle fall når man ser på antall hendelser som enten gjennomføres eller avsløres.

Denne problemstillingen diskuteres i detalj i Human Security Brief 2007, og hovedkonklusjonene fra denne rapporten er at det etter topper i 2004 og 2005 (med terrorangrep i bl.a. Madrid, London, Jakarta, Bali, Amman og New Delhi) har vært en dramatisk nedgang i antall drepte på verdensbasis som følge av terrorhandlinger.[29] Dette forklares bl.a. med:[30]

- Evnen til å oppdage og avverge terrorangrep før de gjennomføres har økt – beredskapen har blitt bedre.
- Det har oppstått indre stridigheter blant ekstremister, og det er uenighet om hvor effektivt terror er som kampmiddel
- Al-Qaida har mistet støtte i tidligere sympatiserende miljøer

Det er med andre ord lyspunkter å spore når det gjelder sikkerhet overfor terrorangrep. Samtidig finnes det nok av kilder som peker på at denne trusselen fortsatt er høyst aktuell, og at enkeltaksjoner har potensial for å gi dramatiske konsekvenser. I tillegg til rapporter og databaser som har vært nevnt tidligere i dette kapittelet, har Petter Nesser, FFI, dokumentert en kronologi over jihadisme i Vest-Europa for perioden 1994-2007.[31] Europa har hatt en lang tradisjon for lokalt basert politisk vold, men Nesser peker også på en økende interesse for jihadister i å bruke Europa som mål for terrorangrep. Spesielt etter 2003 har planlegging, forberedelse og gjennomføring av angrep mot europeiske land økt i relevans, i hovedsak motivert ut fra europeiske lands deltakelse i krigen i Irak.

Kronologien dokumenterer 72 terrorhendelser i perioden 1994-2007. Basert på dette konkluderes det med at islamsk terrorisme mot Vest-Europa utgjør en økende og ikke minst mer dødelig trussel, men det understrekes også at det er stor usikkerhet i tilgjengelig informasjon og data. Kartleggingen inkluderer både planlagte og gjennomførte hendelser. 16 av de kartlagte hendelsene har hatt togtrafikk som mål, mens 9 har vært rettet mot luftfart.

---

[28] Human Security Report Project (2008): Human Security Brief 2007. Lenke: http://www.humansecuritybrief.info

[29] Human Security Report Project (2008): Human Security Brief 2007. Lenke: http://www.humansecuritybrief.info

[30] "Mindre terror i verden", Utenriksanalyse av Stein Tønneson, Prio, fra Morgenbladet 30. mai 2008.

[31] Petter Nesser (2008): "Chronology of Jihadism in Western Europe 1994-2007: Planned, Prepared, and Executed Terrorist Attacks". Published in Studies in Conflict & Terrorism, Volume 31, Issue 10, (October 2008), pp. 924 – 946.

Denne rapporten skal ikke konkludere med om terrortrusselen øker eller avtar. Det vi imidlertid kan fastslå basert på informasjonen som er presentert i dette kapittelet, er følgende:

- Europa er fortsatt er en interessant arena for terrorisme.
- Transportsektoren har vært utsatt for flere angrep, ofte med massedrap som formål. Angrep er i hovedsak rettet mot luft- og skinnegående transport.
- Massedrapsaksjoner har hovedsakelig blitt gjennomført med bruk av hjemmelagde improviserte sprengladninger.

Hva så med Norge? Listen over offentlig kjente terrorangrep og trusler mot Norge de siste årene er kort, men vil inkludere: [32]

- Al-Qaidas nestkommanderende - Ayman al-Zawahiri – nevnte for noen år tilbake Norge to ganger i forbindelse med oppfordringer til angrep ifm. norske militære bidrag i Afghanistan og Irak.
- Utlendinger har drevet spaning i Norge, og dette kan kanskje ses i sammenheng med forberedelser til terrorangrep
- Det er fremsatt trusler mot eller gjennomført angrep i nærheten av norske ambassader i utlandet.

I MIPT-databasen som er omtalt i kapittel 3.3.2 var det bare registrert tre ”terrorhendelser” i Norge i perioden 1998-2007. Hvor reelle disse terrorhendelsene er kan også diskuteres – hendelsene inkluderer plasseringen av en bombe uten tennsats på bilen til Anne Orderud Paust i 1998, ruteknusing ved den tyrkiske ambassaden i 2000 og skytingen mot den jødiske synagogen i Oslo i 2006. På bakgrunn av den begrensede empirien, er det fullt mulig å kvantitativt argumentere for at terrortrusselen mot Norge er tilnærmet lik null.

Likevel har vi sett en rekke eksempler på at lokale radikaliserte grupper i Europa, f.eks. Storbritannia, Spania, Tyskland og Frankrike, kan sette i verk svært dødelige angrep. Det er vanskelig å sette frem en troverdig argumentasjon for at dette ikke også kan skje i Norge, ikke minst fordi vi vet svært lite om hvor mange mulige angrep som er blitt forhindret. PSTs trusselvurdering for 2009 understreker også at det er indikasjoner på en økende grad av radikalisering av islamistiske miljøer i Norge, og at politisk motivert vold fra islamistiske grupper vil være en utfordring for Norge i årene som kommer.[33]

Det er uansett vanskelig å sette kvantitative sannsynligheter på terrortrusselen i Norge. Det er kanskje heller ikke nødvendig. I en kronikk fra 2008 argumenterer FFI-forsker Iver Johansen i en kronikk for at det er terrorens *potensial* heller enn dens reelle styrke i øyeblikket som er viktig: ”Terroren lever på mange måter sitt eget liv i massemediene, og det er trusselscenarioene mer enn virkeligheten som driver mottiltakene.”[34] Selv om internasjonal terrorisme hittil ikke har rammet

[32] “Norsk sikkerhet i en terrorisert verden”, kronikk av Iver Johansen i ABC-Nyheter 23. mai 2008. Lenke: http://www.abcnyheter.no/node/67200
[33] PSTs åpne trusselvurdering 2008: http://www.pst.politiet.no/Filer/utgivelser/trusselvurderinger/Trusselvurdering%202008.pdf
[34] “Norsk sikkerhet i en terrorisert verden”, kronikk av Iver Johansen i ABC-Nyheter 23. mai 2008. Lenke: http://www.abcnyheter.no/node/67200

Norge direkte, tas trusselen likevel så alvorlig at den er i ferd med å skape dyptgripende endringer i samfunnet vårt. Spesielt gjelder dette hvilke tiltak som vurderes for å møte trusselen. Transportsektoren har internasjonalt vist seg som et attraktivt mål for terrorister, og selv om det er vanskelig å overføre erfaringer fra andre land direkte til norske forhold, må også norske transportaktører være bevisst på hvilke tiltak som er relevante mot denne trusselen.

4 Relevante tiltak mot viljeshandlinger

Kapittelet beskriver generelle tiltak som kan redusere risiko for viljeshandlinger i et kollektivtransportsystem. Selv om trafikksystemene i Oslo er utgangspunktet for denne vurderingen, er selve beskrivelsen av tiltak søkt gjort generell, slik at resultatene kan brukes også innenfor andre virksomheter.

4.1 Tiltak – sikkerhet eller skuebrød?

Selv om denne rapporten ikke inneholder en egen effektivitetsvurdering av de ulike tiltakene som presenteres, er det verdt å understreke at det for tiden pågår en løpende debatt internasjonalt om hvilke tiltak som er mest effektive mot terror og sabotasje. En prinsipiell diskusjon dreier seg om enkelte tiltak faktisk gir noen beskyttelse i det hele tatt, eller om det er andre motiver for å innføre dem.

Et sentralt begrep i denne debatten er ”sikkerhetsteater”. Begrepet ble innført av den amerikanske sikkerhetseksperten Bruce Schneier i boken ”Beyond Fear”, og det brukes for å beskrive tiltak som har som formål å gi en følelse av sikkerhet, mens de i realiteten gir liten eller ingen økning i det reelle sikkerhetsnivået.[35] Dette er svært synlige tiltak som er designet for å vise at man tar sikkerhet på alvor, men siden sikkerheten likevel ikke øker, fungerer de i praksis som skuebrød. De involverer ofte begrensninger i folks handlefrihet, og tiltak som å nekte folk å ha med væske i større kvanta på fly og stikkprøver med screening av passasjerer og bagasje har alle vært betegnet som sikkerhetsteater. Det er likevel vanskelig å finne omforente holdninger om et tiltak er et sikkerhetsteater eller ikke, og ofte koker debatten ned til debattantenes grunnleggende holdninger om sikkerhet kontra etiske hensyn til personvern og individets rett til fri ferdsel.

Det er ulike argumenter både for og mot tiltak som kan betegnes som sikkerhetsteater:[36]

- Tiltakene koster penger, men effektiviteten er omstridt. Dette kan stjele ressurser fra tiltak som er viktigere.
- Tiltakene kan utfordre etiske hensyn.
- Den direkte kostnaden med slike tiltak kan ofte være dramatisk mye lavere enn mer effektive tiltak (f.eks. stikkprøver kontra full kontroll av personer og bagasje).
- Synlige tiltak kan spre frykt (spesielt i hverdagen), men kan også virke beroligende (i situasjoner med økt trusselnivå).

[35] Schneier B. (2003): Beyond Fear: Thinking Sensibly About Security in an Uncertain world. Copernicus books

[36] Wikipedia: http://en.wikipedia.org/wiki/Security_theater

- Hvis tiltakene gir *inntrykk* av å være effektive, kan de reelt sett også redusere risiko.
- Slike tiltak er ofte effektive virkemidler for andre typer hendelser enn de i utgangspunktet er motivert ut fra. Selv om tiltak ofte innføres overfor terrortrusselen, vil tiltak som økt kameraovervåking, mer uniformert vaktpersonell osv. i større grad bidra til å redusere risiko for hverdagskriminalitet, som lommetyveri og hærverk.

Dette er med andre ord et komplekst felt, og denne rapporten søker ikke å gi noe svar på denne problemstillingen. Tiltak som kan fungere som "sikkerhetsteater" vurderes i rapporten, men i stor grad anbefales de ikke innført i hverdagen. Dette bør i første rekke være virkemidler som trer i kraft ved høyere trusselnivå, og de vil med dette bidra til å øke publikums oppmerksomhet når de faktisk innføres. Tiltakene kan da få en situasjonsspesifikk nytteeffekt.

4.2 Organisasjonsmessige og administrative tiltak

4.2.1 Avklaring av målsetting og ansvarsforhold

I dag er det en rekke aktører involvert i gjennomføring av kollektivtransport i storbyer:

- Administrative transportvirksomheter.
- Transportoperatørene innenfor veg, båt og bane.
- Infrastruktureiere og -ansvarlige.
- Offentlige tilsynsvirksomheter og utøvende myndigheter
- Tjenesteleverandører, dels innenfor annen kritisk infrastruktur (kraftforsyning, elektronisk kommunikasjon), dels servicetjenester til transportvirksomhetene innenfor vakttjeneste, renhold osv.

I tillegg er nødetatene viktige aktører i sikkerhetsarbeidet overfor viljeshandlinger, så vel preventivt som ved håndtering av inntrufne hendelser.

I et slikt komplisert aktørbilde kan det være vanskelig å finne en klar og omforent målsetting for sikkerhetsarbeidet mot viljeshandlinger. Slike målsettinger er ikke nødvendigvis lett å finne innenfor de enkelte aktørenes organisasjoner heller. Svakheter som ofte går igjen er uklare føringer når det gjelder sikring mot viljeshandlinger, få krav til hvilken sikring som er ønskelig og uklarhet i hvem som skal stille kravene.

Flere av aktører har likevel begynt å vurdere tiltak mot viljeshandlinger, men i hovedsak motiveres slikt arbeid ut fra hyppig forekommende hendelser som tagging, ran og uro på transportmidlene (f.eks. kameraovervåking i sporvogner og busser for å redusere bråk og uro). Sikring mot større hendelser skjer i liten grad. Arbeidet som gjøres er som regel lite koordinert med andre virksomheter.

En slik fragmentering av sikkerhetsarbeidet er uheldig. Uten en helhetlig, omforent og målrettet strategi for sikkerhet i kollektivtransportsystemet som helhet, vil sikkerhetskravene variere fra

arena til arena, og dette vil i praksis bare forskyve sårbarhetene fra de ”sikre” til de ”usikre“ delene av systemet.

Aktuelle tiltak for å forbedre dette er:

- En systematisk gjennomgang og presisering av ansvarsforhold, for å klargjøre hvem som er ansvarlig for sikkerhet i de ulike delene av systemet.
- Utarbeidelse av en sikkerhetsstrategi for *hele* kollektivtrafikksystemet, som klart kommuniserer hvilke typer hendelser man skal planlegge for, hvilken type sikkerhetsnivå man skal arbeide mot, og hvilken type tiltak som er aktuelle. Strategien må dekke balansen mellom å gi en klar retning for sikkerhetsarbeidet og det å gi en lokal tilpasning av tiltak til fagekspertisen i virksomhetene.
- Utpeking av én ansvarlig aktør på overordnet nivå, som er ansvarlig for å gjennomføre strategien, og som stiller krav til de øvrige virksomhetene basert på denne.
- I tillegg må det finnes medarbeidere med ansvar for sikkerhet mot viljeshandlinger innenfor den enkelte involverte transportvirksomhet. Dette må være stillinger som får tilstrekkelig med tid til å arbeide med sikkerhet, slik at arbeidet ikke blir slukt opp av kortsiktige gjøremål i hverdagen.

4.2.2 Samarbeidsutvalg innenfor sikkerhet mellom involverte aktører

Det er behov for et tett samarbeid mellom de ulike aktørene i et storbykollektivtrafikksystem når det gjelder sikring mot viljeshandlinger. En løsning er derfor at det opprettes et beredskapsutvalg blant de involverte aktørene, hvor forhold knyttet til sikkerhet drøftes.

Aktuelle tema for et slikt beredskapsutvalg er:

- Generell kompetanseoppbygging om viljeshandlinger mot kollektivtrafikksystemer
- Diskusjoner rundt svakheter i sikkerhetsarbeidet i systemet
- Koordinering av sikkerhetstiltak på tvers av aktørene

Hvis det utvikles en overordnet strategi for sikkerhet mot viljeshandlinger, vil gjennomføringen av denne også være et naturlig tema i samarbeidsutvalget.

4.3 Planer og sikkerhetsvurderinger

4.3.1 Beredskapsplaner

De fleste av aktørene i transportsektoren har utarbeidet beredskapsplaner som også ivaretar viljeshandlinger. Disse planene ivaretar i noen grad hvordan man skal håndtere hendelser som oppstår, med bakgrunn i varslingslister, rutinebeskrivelser og så videre. Imidlertid varierer formatet for beredskapsplanene, ofte selv innenfor samme konsern, og hvilke type hendelser man planlegger for kan også variere.

Aktuelle tiltak for å forbedre dette er:

- Samkjøring og koordinering av beredskapsplaner mellom aktørene

- Kvalitetssikre hvor gode planene er
- Sjekke at man planlegger for tilsvarende typer hendelser
- Samordne prosedyrer for håndtering av hendelser

4.3.2 Evakueringsplaner

Evakuering av bygninger eller transportmidler er nødvendig i flere relevante scenarioer for viljeshandlinger mot transportsektoren. I langt større grad enn tidligere vil våpen kunne settes av lokalt der folk oppholder seg, og en kritisk gjennomgang av hvordan evakuering skal skje og bedre merking av evakueringsveier anses derfor som en forutsetning for mange av tiltakene denne rapporten skisserer.

Et tilleggsproblem ved dette er at det ofte er bygge- og vedlikeholdsaktivitet i transportinfrastrukturen. Evakueringsplaner må derfor fortløpende vurderes iht. disse aktivitetene, for å sikre at rømningsveier faktisk er åpne tilgjengelige, og godt merket også under slike arbeider.

4.3.3 Øvelser

I tillegg til generell kursing, bør det også regelmessig gjennomføres øvelser som involverer trening på håndtering av viljeshandlinger, så vel papirøvelser og tabletops som realistiske simuleringer. Hvilken form øvelsen bør ha, avhenger av hva man søker å oppnå med den. For realistisk trening må de faktiske ressursene trenes på praktisk oppgaveløsing, mens papirøvelser er nyttige for generell kompetanseutvikling og diskusjoner rundt prinsipielle problemstillinger, gjerne rundt nye utfordringer som man foreløpig ikke har planlagt for eller trent på.

4.3.4 Etterretning og analyse

Viljeshandlinger av noe omfang krever planlegging, noe som medfører et behov for data- og informasjonsinnsamling. Ofte vil de som har til hensikt å gjennomføre viljeshandlinger være nødt til å oppsøke målet på forhånd. Dette er en aktivitet som det er mulig å oppdage hvis den oppfattes som unormal sammenlignet med vanlige trafikanters oppførsel. Eksempler kan være unormalt lange opphold på stasjonsområder, unormal interesse for eller opphold rundt kritisk infrastruktur, filming eller fotografering.

Systematisk kartlegging av slik oppførsel blir fort en etterretnings- og analyseoppgave som grenser inn mot ansvaret til Politiet og Politiets sikkerhetstjeneste. Transportvirksomhetene bør likevel vurdere behovet for interne rapporteringsrutiner om unormal adferd, og ikke minst bør de ha tenkt igjennom hvilke hendelser som skal motivere til kontakt med politiet. Opplæring av eget personell i hvilke typer adferd man bør se etter kan være et viktig virkemiddel. I tillegg bør avvikene registreres i de eksisterende kvalitets- og sikkerhetsavvikssystemene, slik at det er mulig å gjøre analyser av hendelsene. Dette kan grunngi behovet for tilgang på eksterne ressurser, som politi, og i tillegg vil dataene gi vektere muligheter for å utnytte sine ressurser bedre og danne grunnlag for risikoanalyser.

En tilleggsutfordring er at virksomhetene må være bevisst på hvordan de håndterer egen sensitiv informasjon, slik at denne ikke lett gjøres tilgjengelig for aktører som kan utnytte den i viljeshandlinger. Dette er diskutert nærmere i kapittel 4.6.1.

4.3.5 Risikoanalyser

Risikoanalyser er nyttige virkemidler for å systematisere kunnskap om sårbarheter i eget system, som grunnlag for å vurdere behov for nye sikkerhetstiltak. Det finnes imidlertid flere utfordringer ved slike analyser, og den kanskje viktigste er at sårbarheter endrer seg over tid. Spesielt er dette gyldig for avanserte teknologiske systemer som er tungt avhengige av IKT, f.eks. trafikkstyring. Her vil endringshastigheten i system og software ofte være så rask at analyser har svært kort gyldighetstid. Endringer kan også foregå hyppig i den fysiske infrastrukturen, spesielt ved vedlikeholds- og nybyggingsarbeider. Kontroll av relevansen av tidligere analyser er derfor viktig, og i noen tilfeller bør man gjenta analyser selv relativt kort tid etter at de er gjennomført.

Avslutningsvis skal det også sies at en risikoanalyse ikke er noe sikkerhetstiltak i seg selv. Med mindre analysene faktisk fører til implementering av tiltak som reduserer viktige risikoforhold, vil dette arbeidet ha liten verdi.

4.3.6 ”Penetrasjonstester”

Innenfor IKT-sektoren har man lenge benyttet penetrasjonstester, mao. aktiv utprøving av sikkerheten i systemene, for å teste om det finnes sårbarheter som kan utnyttes av eksterne angripere. Tilsvarende virkemiddel er mulig for den øvrige delen av infrastrukturen, for å kontrollere om avvik og forsøk på angrep blir oppdaget og forsøkt avverget. Mulige virkemidler kan være utplassering av bager for å se om vektere eller kamerapersonell oppdager og fjerner dem, forsøk på å ta seg inn på kritiske områder (trafikksentraler, tekniske rom) og lignende. Grenseflaten mellom slike aktiviteter og reelle øvelser er kanskje ikke stor, men noe av formålet med slike tester er at de skal skje uanmeldt. Luftfartssektoren har tradisjon for å benytte denne teknikken for evaluering av sikkerheten på flyplassene.

Tiltaket blir ikke mindre interessant av at media bruker slike teknikker. TV2 har f.eks. prøvd ut flysikkerheten på Gardermoen, med påfølgende oppslag dagene etterpå.[37] Med et økende fokus på sikkerhet innenfor kollektivtrafikksystemene i de store byene, er det ikke utenkelig at noen medieaktører vil gjøre det samme her.

4.4 Forebyggende tiltak

4.4.1 Adgangskontroll

Adgangskontroll er et tiltak med mange dimensjoner. I hovedsak er dette samlebetegnelsen for alle tiltak som begrenser muligheten for at uautorisert personell kan ta seg inn på et område. Dette kan gjøres av minst tre hensyn:

[37] “Dette fikk vi med på flyet”, Nettavisen 8. august 2006. Lenke: http://pub.tv2.no/nettavisen/innenriks/article704849.ece

- Man reduserer faren for at uvedkommende tar seg inn til sårbare områder i transportsystemet, hvor de kan utøve skade.
- Man reduserer faren for at uvedkommende tar seg inn til sensitive områder, slik at de kan stjele skjermingsverdig informasjon.
- Man hindrer at publikum tar seg inn til farlige områder, der de kan skade seg selv.

Ulike tiltak som reduserer muligheten for dette er blant annet fysiske sperringer (bommer, låste dører, gjerder), vakthold ved inngangsdører, varsling og deteksjon av forsøk på ta seg inn på et område, utstedelse av adgangskort og nøkler og prosedyrer for å begrense antall kort og nøkler som deles ut.

I noen grad er slike tiltak allerede tatt i bruk av transportvirksomhetene i dag. Adgangskontroll er imidlertid lite hensiktsmessig på arealene der publikum ferdes, siden man i hovedsak ønsker en effektiv trafikkavvikling. Da kan ikke de fysiske kontrolltiltakene bli for omfattende eller tidkrevende, annet enn inn til de virkelig kritiske objektene for trafikkgjennomføringen hvor publikum uansett ikke har noe å gjøre.

Eksempler på sensitive områder som bør vurderes ifm. adgangskontroll er:
- Rom med inntak til ventilasjonssystemer (ifm. røyk/gassutslipp)
- Rom med viktig teknisk utstyr – signalering, samband, kraftforsyning osv
- Trafikkledersentraler
- Rom under høyblokker, rom under publikumsarealer, vareleveringer under stasjoner (hvor sprenging av bomber, brannstiftelse og lignende kan få stor konsekvens for bygningsmasse eller folk over).
- Førerrom ombord i transportmidlene
- Verkstedsområder, vognoppstillingsplasser, parkeringsplasser for busser osv.

Det er en rekke tiltak som kan vurderes for generell sikring av slike områder:
- Adgangskontroll med nøkkelkort, låser o.l.
- Sensorer for deteksjon av bevegelse
- Inngjerding (og kontroll av at denne er god)
- Kameraovervåking
- Låsing av inngangspartier til stasjonsområder ved høyere trusselnivå.

I tillegg må man se på rutiner for hvilke personer som skal ha tilgang til områdene:
- Begrense tilgang til det som er strengt nødvendig.
- Gode rutiner for ”nøkkeladministrasjon”, spesielt innlevering av nøkler og kort når man ikke lenger har bruk for dem (f.eks. med støtte av ”rundeskjema” ved endt tjeneste).
- Strengere krav overfor eksterne tjenesteleverandør om bruk av fast personell, f.eks. fast renholds- og vaktpersonale.

4.4.2 Regulering av trafikk rundt store stasjoner

Bilbomber ved stasjoner eller områder med mye folk kan trekkes fram som et høyrisikoscenario knyttet til kollektivtransport. Sikring mot denne trusselen kan kreve en rekke generelle tiltak:

- Kontroll av biltrafikk rundt store stasjonsområder. Aktuelle tiltak er å sette opp bommer og sperrestativer, som evt. kan åpnes av biler som har ”lovlig” ærend ved anlegget. Områder å se etter er:
    - Åpne inngangspartier, trappenedganger eller glassdekte vinduer hvor det er mulig å kjøre biler inn i anlegget for senere detonering av bilbombe.
    - Vareleveringer i eller under anlegget.
    - Parkeringsplasser nær anlegget
    - Vegger med store glassruter, hvor glass kan sprenges inn i lokalet.
    - Steder hvor det er mulig å kjøre inn på selve stasjonsområdet via tunneler, perronger og lignende
- Reduksjon i parkeringsmuligheter nær stasjonsbygningene
- Planer for ytterligere sperring av uteplasser, torg og veier forbi anleggene ved høyt trusselnivå.

Kraftige bilbomber vil imidlertid kunne ha et stort virkningsområde, som det er vanskelig å beskytte seg mot i tett bebygde områder uten å sperre av all trafikk rundt et anlegg. Sikring mot bilbomber blir derfor ofte et spørsmål om å redusere muligheten for at uvedkommende kan kjøre inn i kritiske bygninger med bil, evt. å hindre at bombene detoneres rett ved siden av bygningen slik at deler av den raser sammen.

4.4.3 Kameraovervåking

Kameraovervåking kan være et effektivt virkemiddel i forbindelse overfor viljeshandlinger. Overvåking kan gjennomføres med ulike målsettinger:

- Hendelser skal kunne oppklares. Kamera dekker mesteparten av området på anlegget, og bilder lagres for senere etterforskning dersom noe inntreffer.
- Hendelser skal avverges. Dette kan skje enten ved at personell følger med på kameraskjermer og legger merke til viljeshandlinger under oppseiling, eller ved ”smart” kamerafunksjonalitet som gjør at f.eks. gjenglemt bagasje blir oppdaget automatisk. I tillegg kan kamera i seg selv ha en preventiv effekt på viljeshandlinger.

Det er mange kamera i drift i kollektivtrafikksystemene i Norge i dag, på stasjonsområder, ved kritiske objekter og i økende grad inne i transportmidlene. En klar og enhetlig strategi for bruk av dem er imidlertid vanskelig å finne. Ulike aktører setter opp egne kamera uten koordinering med andre. Det er åpenbare huller i kameradekningen flere steder, og i tillegg er det ikke tilrettelagt for fulltids overvåking av kamera fra vaktsentraler. Kameraovervåkningen er også i første rekke motivert ut fra hyppig forekommende viljeshandlinger, f.eks. uro på trikken, lommetyveri på stasjonsområder og tilsvarende. I mindre grad er kamera tenkt som et virkemiddel mot terrorhandlinger.

Bruk av kamera mot terrorhandlinger er et interessant tema. For slike hendelser vil argumentet om at kamera i seg selv virker preventivt være lite gyldig – om et kamera tar bilder av hendelsen som spres til media, er det sannsynligvis bare en bonus for gjerningsmennene. Erfaringer fra andre land, bl.a. Israel, tilsier også at overvåking bare i liten grad vil kunne avverge direkte angrep, f.eks. fra selvmordsbombere.[38] Unntaket måtte være om overvåkning suppleres med sterke deteksjonsmekanismer (automatiske eller godt trenet kamerapersonell), samt rask utrykning når avvik blir registrert.

Aktuelle tiltak knyttet til kameraovervåking er:

- Presisering av hva man søker å oppnå med kameradekningen på ulike områder, inkl. kvalitative spesifikasjonskrav til kameraer og opptakssystemer (forebygging eller avverging). Deretter skreddersydd design av kamerassystemet for å oppnå ønsket effekt
- Koordinering av behov for kameradekning på tvers av aktørgrenser.
- Kartlegge om alle kritiske områder er dekket – tunnelinnganger, kjøretunnel under spor med kabelkulverter, ventilasjonsinntak osv.
- Vurdere om kameraplasseringen er tilstrekkelig for oppklaring etter hendelser. Gjennomgang i samarbeid med politiet.
- Utarbeide policy for oppdatering av kameradekning ved store utbygningsarbeider, opphenging av reklameplakater/bannere som kan påvirke kameradekning osv.
- Gjennomføre datastøttet modellering av optimal kameraplassering.
- Forbedre bildekvalitet, f.eks. ved å bytte ut eldre kamera eller å forbedre lyssetting.
- Sikre at kamerapersonell kan gjennomføre forebyggende overvåking
    - Opplæring i indikatorer for angrep – hvordan vurdere om personers oppførsel tilsier at noe skal skje, informasjon om virkemidler som ofte benyttes osv.
    - Trening i bruk av kamera til forebygging.
    - Utforming av skjermer/arbeidsplass for å tilrettelegge for overvåking i sanntid.
    - Dele kameraovervåkingsfunksjoner fra generelle servicetjenester.
    - Mer personell til kameraovervåking.
- Automatiserte overvåkingsfunksjoner
    - Innføre automatisk kamerakontroll for å oppdage gjenglemt bagasje.[39]

4.4.4 Vakthold og patruljer

Private vakttjenester er mye brukt innenfor transportsektoren, og vektere patruljerer regelmessig på offentlige publikumsarealer, i noen grad også inne i transportmidlene. Vaktordninger er også i bruk ved enkelte sentrale punkter i infrastrukturen, typisk verksteder og større vognoppstillingsplasser.

Hyppigere bruk av patruljer med uniformert personell kan øke evnen til å avverge viljeshandlinger, ut fra argumentasjon om at ”synlighet gir sikkerhet”. Dette kan enten være innleide vektere eller politi. Større bruk av uniformert politi har vært et mye brukt virkemiddel i Europa etter de senere års terrorhandlinger mot jernbanetransport, bl.a. i Østerrike og Tyskland. I

[38] Notater fra Vidar Westrheim, Jernbaneverket, fra 45th Colpofer Conference, 13-14 september 2006
[39] Slike løsninger vil imidlertid kunne gi mange falske alarmer

Østerrike får uniformert personell lov til å reise gratis med tog, og dette anses også som et enkelt preventivt virkemiddel mot angrep.[40] Andre land (f.eks. Frankrike) har innført ordninger med eget togpoliti som skal ivareta sikkerheten ombord på transportmidlene.

Økt patruljering og synlighet av uniformert personell er et åpenbart virkemiddel i situasjoner der trusselnivået øker. Det kan også vurderes i hverdagen, men det må imidlertid bemerkes at en forutsetning for å ha glede av mer uniformert personell er at de har en viss grunntrening i securityrelaterte hendelser. Trening og kursing anses derfor som et viktigere tiltak for å sikre god vakttjeneste i hverdagen enn å ansette mange nye vektere.

Uansett vil det være behov for avklaringer mellom objekteier og politiet om tilgjengelige ressurser og gode løsninger for vakttjenesten på anlegget.

4.4.5 Rydding av områder og fjerning av gjemmesteder

De fleste anlegg og transportmidler har mange mulige gjemmesteder for ulike typer våpen. Dette dreier seg om hulrom og nisjer hvor det er mulig å gjemme våpen for senere detonering, f.eks. bager med sprengstoff. I tillegg er mye utstyr, reklameskilt, apparater osv. satt ut på fellesarealer innenfor transportsystemet. Dette gir dårlig oversikt for vakt- og sikringspersonell som skal se etter avvik fra det normale i forbindelse med viljeshandlinger.

Figur 4.1 Søppelbøtter kan være et skjulested for pakker eller bager med sprengstoff

Strategier for rydding av infrastrukturen kan ha effekt overfor en rekke scenarioer. Mulige tiltak er:

[40] Notater fra Vidar Westrheim, Jernbaneverket, fra 45th Colpofer Conference, 13-14 september 2006.

- Midlertidig plombering, eventuelt fjerning av søppelbøtter. Alternativt bruk av gjennomsiktige søppelbøtter.
- Midlertidig plombering av oppbevaringsbokser.
- Låsing av seter på vognene, slik at det ikke er mulig å gjemme ting under benkeplater.
- Fjerning av reklameskilt, varestativer, fotoautomater, billettautomater, benker, postpakkeautomater osv. på fellesarealer, i alle fall de som det er mulig å gjemme gjenstander under eller bak.
- "Skråstilte" tak på automater, som gjør det vanskelig å sette igjen gjenstander på toppen av dem.
- Utarbeide strategi/policy for utplassering av bannere, flagg osv. som kan hindre kameraovervåking.
- Utarbeide strategi/policy for å redusere muligheten for å gjemme farlige stoffer i transportsystemet på sikt, f.eks. krav ved innkjøp av nytt vognmateriell, utforming av nye stasjonsområder osv.

Flere av disse tiltakene kan gi store inngrep i funksjonaliteten i transportsystemet ved vanlig hverdagsdrift. På grunn av dette vil tiltakene være mest aktuelle ved høyere trusselnivå, spesielt dersom det rettes konkrete, spesifikke trusler mot transportsystemet. Imidlertid bør det allerede ved lave trusselnivåer avklares hvilke tiltak som skal gjennomføres dersom trusselen øker, og mer langsiktige strategiarbeider bør starte umiddelbart.

4.4.6 Informasjon til reisende

Dette vil være tiltak som tar sikte på å informere passasjerene om trusselen fra viljeshandlinger, slik at de evt. kan bidra til å oppdage og avverge dem, eventuelt å hjelpe seg selv dersom hendelser skulle inntreffe. Mulige tiltak er "vær varsom"-plakater (se etter gjenglemt bagasje), høyttaleropprop, video- og reklamefilmer som setter fokus på trusselen osv.

Det kan argumenteres for at slike tiltak ikke vil ha ønsket effekt dersom de innføres i hverdagen, uten at det foreligger mer eller mindre konkrete trusler. Etter hvert kan de bli en del av den vanlige "bakgrunnsstøyen" for de reisende. En mulighet er derfor at slike tiltak forberedes (plakater trykkes opp, nødvendige meldinger skrives osv), slik at de raskt kan iverksettes når situasjonen tilsier det.

4.4.7 Sensorer for deteksjon av våpen

Det har de siste årene vært fokusert på muligheter for tidlig varsling av viljeshandlinger som innebærer bruk av eksplosiver eller kjemiske, biologiske eller radioaktive (CBR) stoffer. Dette kan skje ved hjelp av stasjonære eller mobile sensorer eller "sniffere". I noen tilfeller, for eksempel overfor C-våpen, kan stasjonære detektorer koples til et alarmanlegg slik at tiltak automatisk kan iverksettes, f.eks. talevarsling om evakuering, stengning av ventilasjonsanlegg og lukking av branndører.

Deteksjon av sprengstoff er mulig, enten ved bombehunder eller teknologiske sniffere som detekterer spor av sprengstoff i luften. Bombehunder er imidlertid kostbare å trene opp, og det er

vanskelig å se for seg at aktører utenfor Politiet eller Forsvaret vil bære denne kostnaden. Tilgjengelige teknologiske løsninger gir også mange feilmeldinger, siden det er vanskelig å skille spor av sprengstoff fra andre stoffer, f.eks. kunstgjødsel eller enkelte medisiner[41].
Det er mulig å anskaffe detektorer for kjemiske stridsmidler og en del industrikjemikalier. I St.prp. 54 (2001-2002) ble DSB gitt i oppdrag å vurdere muligheter for stasjonær deteksjon av kjemiske stridsmidler[42]. Prosjektgruppen valgte en tunnelbanestasjon som prøveprosjekt, og det ble utført spredningsforsøk med røyk og damp. Ved en terrorhandling med plutselig utslipp kan personer i stasjonen utsettes for betydelige doser allerede før en eventuell alarm blir gitt. Et alarmsystem vil i første rekke varsle hjelpemannskaper om hva som er skjedd, hindre at flere personer kommer inn på området, og varsle trafikksentraler om hendelsen.

Deteksjon av kjemiske stridsmidler er imidlertid forbundet med utfordringer, spesielt med tanke på feilkilder og falske alarmer. Videre er det utallige steder et eventuelt angrep kan skje og måter det kan skje på, slik at optimal plassering av detektorene er en utfordring. Det finnes en del håndholdte detektorer for kjemiske stridsmidler på markedet, og som er i bruk i Forsvaret, Sivilforsvaret og hos noen brannvesen. Disse er forholdsvis enkle og robuste i bruk. Innkjøp av håndholdte detektorer kan derfor vurderes, men opplæring og trening i korrekt bruk er essensielt.

Utstyr for tidlig varsling av et B-angrep er under utvikling og delvis tilgjengelig, men utstyret kan ofte ha begrensninger med hensyn til sensitivitet og spesifisitet[43].

Deteksjon av radioaktiv stråling er ikke i samme grad forbundet med feilkilder og falske alarmer som deteksjon av kjemikalier. Detektorer for radioaktiv stråling er rimelige, robuste og enkle i bruk. Tiltak som kan vurderes nærmere er utplassering av noen stasjonære gammadetektorer i infrastrukturen, eller å utstyre vektere med detektor eller dosemåler. Opplæring i korrekt bruk er igjen helt essensielt.

Oppsummert er det et åpenbart problem at det ikke finnes noen god universell sensorløsning som dekker alle tenkbare våpen. I tillegg er antall feilmeldinger fremdeles stort fra slike løsninger. Selv om det fortløpende forskes på og utvikles nye sensorløsninger, vil godt etterretningsarbeid og god nok sikring av trusselstoffer på kort sikt være viktigere. Dette vil imidlertid ligge utenfor transportaktørenes ansvarsområde.

Transportvirksomhetene kan imidlertid sørge for opplæring og årvåkenhet blant vektere og eget personell. Disse vil ha en nøkkelrolle i å varsle alle typer alvorlige hendelser eller tilløp til hendelser, bistå i en effektiv evakuering av publikum, inkludert å utløse brannlarmer dersom det kan avhjelpe situasjonen. Da blir kompetanse om våpenvirkninger viktigere enn sensorer for å avdekke dem.

---

[41] US Transport Security Administration (2006): Technology for Hold Baggage Screening, presentasjon ved International Arab Civil Aviation Security Conference, Abu Dhabi 7-8 februar 2006.
[42] DSB (Direktoratet for sivilt beredskap) (2002): ”Prosjekt for å vurdere muligheter for stasjonær deteksjon av kjemiske stridsmidler”, Oslo, desember 2002.
[43] Blatny, J M, Fykse E M, Olsen J S (2006): Påvisning av biologiske trusselstoffer – Teknologinnspill til FS 07, FFI/RAPPORT-2006/01483, Forsvarets forskningsinstitutt.

4.4.8 Kontroll av bagasje og reisende

De reisendes bagasje kan skjule farlige våpen, f.eks. sprengstoff, CBR-virkemidler og brannbomber, som er planlagt brukt i viljeshandlinger. Internasjonalt er det derfor stor satsing på løsninger som gjør det mulig å kontrollere de reisendes bagasje.

Generelt representerer dette et kraftig inngrep overfor de reisende. Selv om kontroll av bagasje ikke er et ukjent virkemiddel, f.eks. fra flytrafikken, konserter og idrettsarrangementer, har dette så langt ikke vært brukt i kollektivtrafikken i byene. Det er også grunn til å stille spørsmål om hvor effektivt bagasjekontrolløsninger vil være i åpne transportnettverk. Bagasjekontroll er egnet for sikring av enkeltanlegg, men i et kollektivtransportsystem kan det være hundrevis av stasjoner og holdeplasser. Å skulle kontrollere bagasje over hele dette systemet vil være svært ressurskrevende og kostbart. Trafikkavviklingsevnen vil også avta dramatisk på grunn av tidsforsinkelsene dette ville ha medført. En alternativ løsning er imidlertid å se på mer begrensede løsninger. Stikkprøver med manuell gjennomgang av bagasje og bruk av mobile screenere kan brukes for å legge terskelen *litt* høyere for gjennomføring av viljeshandlinger.

Noen tiltak kan være:

- Tilrettelegging for merking av bagasje med mobiltelefonnummer. Tiltaket vil i første rekke bidra til at eierne av gjenglemte kolli raskt kan spores opp, slik at man slipper tidkrevende gjennomgang av bagasje med tilkalling av politi og avsperring av områder.
- Innføring av automatisk kameraovervåking som detekterer bagasje som står i ro i lengre tid på de store stasjonsområdene.
- Stikkprøver med manuell gjennomgang av bagasje. Vektere eller politi kan sette opp kontrollposter for fysisk gjennomgang av enkelte personers bagasje. Dette kan skje på ulike steder i infrastrukturen.
- Tekniske løsninger for screening av bagasje. Hvis dette kjøpes inn er det viktig å ha mobile apparater som kan flyttes rundt i systemet.
- Samarbeid med nødetatene om patruljer med bombehunder, både for å kontrollere bagasje og for preventiv beskyttelse.

Tilsvarende kan de reisende ha farlige stoffer og objekter med seg på kroppen, ikke i bagasjen. For å kontrollere dette kan det gjennomføres manuell kontroll av passasjerene, eventuelt kan det kjøpes inn sikkerhetssluser for automatisk skanning. For tiden prøves det ut skannerløsninger basert på millimeterbølger i flere land, spesielt i luftfarten. Passasjerene går inn i en sikkerhetssluse hvor de blir bestrålt, og operatørpersonellet får opp bilder som i praksis ”kler av” de reisende og avdekker eventuelt farlige objekter som er skjult på kroppen deres. Dette vil også være svært ressurskrevende løsninger i et åpent trafikksystem, og i tillegg finnes det flere etiske betenkeligheter rundt slike løsninger (vil f.eks. bilder av passasjerene kunne komme på avveie?).

På grunn av at slike tiltak er ressurskrevende og langt utover det passasjerene i kollektivtrafikken anser både som normalt og hensiktsmessig, vil de sannsynligvis først være aktuelle ved høye trusselnivå, ikke i hverdagen.

4.4.9 Kontroll av parkert materiell

Dette tiltaket innebærer en grundig gjennomgang og sjekk av transportmidlene før de tas i bruk for dagen. Årsaken til at et slikt tiltak kan være nødvendig er at transportmidlene er mulige mål for massedrapsaksjoner, og farlige stoffer kan bli utplassert på dem for å utløses på et bestemt tidspunkt. For tiden er det flere steder relativt lett tilgang til transportmidler som er parkert nattetids.

I mange tilfeller vil transportvirksomhetene gjennomføre en enkel visuell kontroll av transportmidlene før bruk, men uten å gå grundig til verks (sjekke under seter, kontrollere luker, hulrom, bagasjerom osv). Muligens vil ikke dette være nødvendig i hverdagen, men i tilfelle trusselnivået skulle øke, bør det vurderes mer grundige inspeksjonsrunder før transportmidlene tas i bruk.

4.4.10 Brannsikkerhet

Generelt god brannsikkerhet er fornuftig også når det gjelder viljeshandlinger. Brannbomber er et aktuelt virkemiddel i terror- og sabotasjesammenheng, og bruk av eksplosiver vil ofte føre til branner i tillegg.

Mange slike tiltak vil være velkjente for transportvirksomhetene allerede i dag:

- Informasjonsmessige tiltak ifm. merking, skilting og lyssetting
- Brannalarmer og varslingsanlegg
- Branndører og brannskiller
- Brannslukking, overrislingsanlegg, pulverapparater
- Kartlegging og sikring av farlige stoffer (f.eks. gasser på industriområder)
- Løpende fjerning av søppel og brennbart materiale
- Redusert bruk av brannfarlige bygningsmaterialer
- Planverk for håndtering av branner i tunneler

Det kan imidlertid være verdt å peke spesielt på brannsikkerhet i forbindelse med bygg- og vedlikeholdsarbeider. Her kan det fort samles opp mye brennbart materiell, og allerede eksisterende tiltak kan bli undergravd. Gode planer for hvordan brannsikkerhet ivaretas under slike prosesser er viktig.

4.4.11 Fortifikasjon av kritiske funksjoner

Når det gjelder beskyttelse av kritiske anlegg for transportgjennomføring, er det mulig å tenke seg en rekke bygnings- og konstruksjonsmessige tiltak som reduserer sårbarheten overfor ulike våpenvirkninger. Eksempler på tiltak kan være å flytte objekter til fjellanlegg, bruk av betong av en viss tykkelse i tak/vegger/gulv, sikring av rom med mye elektronikk mot elektromagnetiske pulser, gassikring av rom osv. Å gjennomføre slike tiltak i eksisterende bygningsmasse er imidlertid dyrt, og i flere tilfeller kan truslene heller håndteres på annen måte.

Det skal også sies at en rekke av disse tiltakene i første rekke er dimensjonert for å beskytte mot våpen levert utenfra systemet, som regel i en militær setting. Moderne terror- og sabotasjetrusler skjer imidlertid ofte fra innsiden. Utfordringen blir derfor i minst like stor grad å slippe våpeneffekter ut av anlegget, som det vil være å hindre våpnene å komme inn. Kraftig fortifikasjon kan i slike tilfeller bare øke skadepotensialet ved ulike hendelser. Tiltaket er derfor ikke vurdert videre i analysen.

4.5 Konsekvensreduserende tiltak

4.5.1 Konsekvensreduserende design

I dagens trusselbilde synes det mer sannsynlig at angrep mot transportsektoren vil ha som formål å drepe mange mennesker enn å stoppe trafikkavviklingen over tid. Denne typen trussel vil normalt bli effektuert på åpne publikumsområder eller i transportmidlene, og det er vanskelig å redusere sannsynligheten av slike angrep med fortifikatoriske tiltak eller adgangskontroll.

Imidlertid finnes det en rekke bygg- og designmessige tiltak som vil redusere konsekvensene av en gjennomført handling. Eksempler på slike tiltak er:

- Generelt design av nye stasjoner og transportmidler med hensyn til sikkerhet, f.eks. åpne stasjonsområder med enkle og intuitive evakueringsveier.
- Takkonstruksjoner som gjør at sprengkraft ledes ut av anlegget, ikke stenges inne.
- Redusere bruk av brennbart materiale på publikumsområder og i transportmidler.
- Mindre bruk av glass i vegger rundt inngangspartier.
- Bombesikre søppelbøtter

Samme typer tiltak kan tenkes mot andre trusler, f.eks. at vegger settes inn med anti-graffitimidler som gjør det lettere å fjerne maling. Flere av disse tiltakene vil imidlertid være dyre når de skal innføres i gamle konstruksjoner. Et alternativ er i stedet å etablere en policy for hvordan slike hensyn skal tas ved vedlikehold, nybygging og innkjøp av nye transportmidler, slik at løsningene kan fases inn over tid.

4.5.2 Redundans og desentralisering av kritiske funksjoner

Dette er tiltak som sørger for å redusere kritikaliteten av enkeltanlegg og -funksjoner og som bygger inn reservekapasitet i transportsystemet. Aktuelle tiltak er:

- Spre parkert vognmateriell på flere anlegg, slik at konsekvenser reduseres dersom hendelser inntreffer (et alternativt tiltak kan imidlertid være å styrke adgangskontroll og vaktsikkerhet ved de aktuelle anleggene).
- Ha backupanlegg og -systemer for trafikkstyring
- Ha noe overkapasitet av vognmateriell og transportmidler
- Sikre noe reservemateriell og bygge opp kapasitet for rask reparasjon

4.5.3 Beskyttelsesutstyr

Dette er materiell og utstyr som tar sikte på å beskytte mennesker som kan eller har blitt utsatt for viljeshandlinger. Typisk materiell å vurdere behovet for er:

- Beskyttelsesutstyr – vernedrakter, gassmasker osv. – overfor ulike våpenvirkninger, for egne ansatte
- Innkjøp av utstyr for håndtering av skadete personer (passasjerer og egne ansatte) - ulltepper, førstehjelpsutstyr osv.

4.6 Tiltak overfor eget personell

Dette er tiltak rettet mot egne ansatte. I tillegg vil en rekke av de tekniske forebyggende tiltakene i kapittel 4.4 (f.eks. adgangskontroll) også være relevante overfor egne ansatte.

4.6.1 Tiltak for sikker håndtering av informasjon

Innenfor et kollektivtrafikksystemet kan det finnes mye informasjon som kan utnyttes i viljeshandlinger. I hovedsak dreier dette seg om kunnskap om kritiske og sårbare deler av transportsystemet, for eksempel dokumentert i risikoanalyser, adgangsanalyser eller beredskapsplaner. I tillegg kan virksomhetene få behov for å behandle sensitiv informasjon fra eksterne aktører, f.eks. fra politiet/PST når det gjelder dagsaktuelle sikkerhetsutfordringer.

I dagens informasjonssamfunn blir svært mye informasjon gjort enkelt tilgjengelig i åpne kilder. Det er derfor viktig at transportvirksomhetene har et bevisst forhold til hvilken informasjon man ønsker å dele kontra det man faktisk *bør* dele. Tekniske tegninger, typetegninger av vognmateriell, systembeskrivelser og lignende er eksempler på informasjon som bør vurderes nøye før den eventuelt offentliggjøres. Slik informasjon kan være av stor interesse for mange mennesker som ikke har noe vondt i sinne, for eksempel entusiaster som driver diskusjonsfora for alt som har med skinnegående transport å gjøre, men samme type informasjon er også nyttig for de som ønsker å gjennomføre viljeshandlinger. I dag ligger slik informasjon lett tilgjengelig på Internett. Samtidig sendes annen sensitiv informasjon (analyseresultater, planverk) relativt fritt mellom medarbeidere i transportvirksomhetene over usikrede e-postløsninger.

Det er verken sannsynlig eller særlig hensiktsmessig at man klarer å hemmeligholde all informasjon som kan være av interesse for ondsinnede aktører. Imidlertid kan konsekvensene av en vellykket viljeshandling mot lokaltransporten bli så stor at dette forholdet bør tas på alvor, enda mer enn tilfellet er i dag. Virksomhetene bør derfor utvikle gode retningslinjer for sine medarbeidere når det gjelder offentlig publisering av informasjon på nettsteder, videresending per e-post o.l., basert på en gjennomgang av hvilken informasjon som anses som sensitiv.

Det lovmessig sterkeste virkemiddelet for håndtering av sensitiv informasjon i Norge er Sikkerhetsloven.[44] Denne har blant annet som formål å legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. Loven gjelder i utgangspunktet for følgende aktører:

[44] Lov om forebyggende sikkerhetstjeneste. Ikrafttredelse 1. juli 2001. http://www.lovdata.no

- Forvaltningsorganer, det vil si ethvert statlig eller kommunalt organ
- Leverandør av varer eller tjenester til et forvaltningsorgan i forbindelse med en sikkerhetsgradert anskaffelse
- I noen tilfeller også for selskaper og privat og offentlig næringsvirksomhet, som eier eller på annen måte har kontroll over eller fører tilsyn med skjermingsverdig objekt, eller som av et forvaltningsorgan gis tilgang til sikkerhetsgradert informasjon.

Loven presiserer hvordan skjermingsverdig[45] og sikkerhetsgradert[46] informasjon skal behandles, blant annet med bruk av sikkerhetsklareringer (kapittel 6 paragraf 19[47]):

- Person som skal gis tilgang til skjermingsverdig informasjon, skal autoriseres.
- Person som skal autoriseres for tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere, skal på forhånd sikkerhetsklareres.
- Person som i sitt arbeid vil kunne få tilgang til skjermingsverdig informasjon gradert KONFIDENSIELT eller høyere, skal sikkerhetsklareres dersom ikke sikkerhetstiltak for å fjerne risikoen for tilgang med rimelighet lar seg gjennomføre.

Innenfor transportsektoren er det imidlertid flere virksomheter som ikke er underlagt Sikkerhetsloven. Virksomhetene vil normalt ikke inneha informasjon som kan true rikets sikkerhet, men kunnskap om sårbarheter i infrastrukturene kan definitivt utgjøre utfordringer for vitale nasjonale interesser.

Et aktuelt tiltak er derfor å utvikle et system hvor nøkkelpersonell i transportvirksomhetene blir sikkerhetsklarert for lave sikkerhetsnivå, slik at de er i stand til å motta og håndtere informasjon inntil Begrenset. Aktuelle tiltak i forlengelsen av dette er:

- Klassifisering av hva som er skjermingsverdig informasjon innenfor virksomheten.
- Kartlegging av funksjoner og stillinger innenfor virksomheten som bør ha tilgang til skjermingsverdig informasjon.
- Sikkerhetsklarering av ansatte i nøkkelstillinger.

Skulle dette vise seg vanskelig å få til iht. Sikkerhetsloven, finnes det alternative løsninger:

- Selv om rapporter ikke er gradert iht. Sikkerhetsloven, er det likevel mulig å ha en bedriftsintern restriktiv holdning til spredning av mulig sensitiv informasjon. Her kan også større bruk av Offentlighetsloven være et virkemiddel, selv om denne ikke på langt nær gir samme grad av beskyttelse som Sikkerhetsloven.
- Man kan bruke alternative kontrolløsninger for å vurdere om en person bør ha tilgang til sensitiv informasjon. Et alternativ til sikkerhetsklarering er politiattest (en attest fra politiet med opplysninger om personens oppføringer i strafferegisteret og bøteregisteret de siste årene). I flere yrker er det krav om slike attester (f.eks. for vektere), men det er samtidig klare begrensninger på hvilke stillinger hvor politiattest kan kreves av

[45] Informasjon som **skal** merkes med sikkerhetsgrad
[46] Informasjon som **er** merket med sikkerhetsgrad
[47] Lov om endringer i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Kunngjort 11. april 2008. http://www.lovdata.no

arbeidsgiver (spesifisert i Lov om strafferegistrering). Et ytterligere alternativ kan være sertifiseringsløsninger for sikkerhetsmedarbeidere i bedriften. Ingen av disse løsningene legger imidlertid til rette for fordeling av informasjon som er gradert iht. Sikkerhetsloven, så disse vil i første rekke være egnet for å håndtere informasjon som bedriften selv angir som sensitiv.

En tilleggsutfordring kommer i forhold til eksterne tjenesteleverandører. Spesielt gjelder dette vaktselskaper, bygningsarbeidere og rengjøringsfirma som har oppgaver ved skjermingsverdige objekter eller har tilgang til steder der skjermingsverdig informasjon oppbevares. I svært mange tilfeller har man liten kontroll over hvilken person som kommer og løser oppgaver fra gang til gang, og i praksis vil man kunne oppleve at det kommer en ny person som gjør rent hver gang. I slike tilfeller vil ikke sikkerhetsklareringer være mulig, og som nevnt over vil det være klare begrensninger på muligheten til å kreve politiattester for arbeiderne. I den grad det er serviceoppgaver som må gjøres i sensitive omgivelser, må man derfor vurdere andre tiltak:

- Nekte tilgang til sensitive områder for personer man ikke har kontrollert.
- La personene gjøre arbeidet under oppsyn av kontrollert personell.
- La være å sette ut slike tjenester, og heller ha eget personell som gjør arbeidet.

4.6.2 Kompetanseutvikling - trening og kursing

Det generelle sikkerhetsarbeidet innenfor transportvirksomhetene har så langt hatt et tradisjonelt safetyfokus, mao. håndtering av ulykker, situasjoner med teknisk feil og menneskelig svikt. Fokus har i liten grad vært rettet mot viljeshandlinger, og kunnskapen om mulige viljeshandlinger er liten. Økt oppmerksomhet rundt hva viljeshandlinger er og hvordan de kan håndteres, kan imidlertid sikres gjennom ulike kurs- og øvingsopplegg. Noen aktuelle tiltak er:

- Enkle (dags)seminarer for store deler av arbeidsstyrken om viljeshandlinger, f.eks. rundt tema som PSTs trusselnivåer, faktakunnskap om ulike viljeshandlinger og mulige effekter, ansvarsforhold osv.
- Praktisk kursing av vaktpersonell og medarbeidere på transportmidlene når det gjelder indikatorer på mulige viljeshandlinger: avvikende adferd, gjenglemt bagasje osv.
- Praktisk kursing av vaktpersonell og medarbeidere på transportmidlene når det gjelder ”best practice” for oppførsel ved viljeshandlinger – prosedyrer for hva som bør gjøres i ulike scenarioer.

Trening må også gjennomføres for mer effektiv bruk av eventuelle teknologiske støttesystemer som kan sikre mot viljeshandlinger, f.eks.:

- Bruk av kameraovervåking til forebygging
- Bruk av eventuelle sensorer for deteksjon av våpen, screening av bagasje osv.

Avslutningsvis er det viktig å understreke at ytterligere trening og kursing mot viljeshandlinger ikke innebærer at transportvirksomhetene skal ta over oppgaver som er politiets ansvar. Samspillet med nødetatene bør derimot være en del av undervisningsopplegget i de kurs som evt. avholdes.

4.6.3 Sosiale tiltak

En generell hypotese i moderne sikkerhetstenkning er at ”den største trusselen kan komme innenfra”. I mange tilfeller er dette knyttet til at egne ansatte kan gjøre feil som får negative følger for sikkerhet, f.eks. at man videresender sensitiv e-post til mottakere utenfor bedriften. Imidlertid er det også en mulighet for at medarbeidere bevisst kan ønske å påføre bedriften skade. Konsekvensene av slike hendelser kan bli store, fordi de ansatte har god kunnskap om kritiske sårbarheter i systemet.

Slike hendelser kan til en viss grad avverges av generelle sikkerhetstiltak som skissert i kapittel 4.4, f.eks. overvåking og vakthold. En bekymring er imidlertid at man lett kan utvikle en sikkerhetskultur som baseres på en generell mistenkeliggjøring av egne medarbeidere. Dette kan være ytterligere problematisk for transportvirksomheter, siden disse ofte samler medarbeidere fra mange nasjonaliteter. KTPAS i Oslo har f.eks. medarbeidere fra drøyt 50 ulike nasjonaliteter.

Utover tradisjonelle kontrolltiltak, kan det derfor være verdt å se på sosiale tiltak i virksomhetene. Dette er i praksis de samme typer tiltak som man ville ha vurdert for å skape en hyggelig og trivelig arbeidsplass, slik at medarbeiderne får en lagfølelse som gir lojalitet til egen organisasjon; bedriftsidrettslag, fester, videreutdanningsmuligheter, kampanjer mot mobbing osv. Slike tiltak kan gi positive effekter for sikkerheten, ved at medarbeidere blir inkludert og føler seg som en akseptert del av virksomheten. I tillegg kan dette føre til at det utvikles sosiale kontrollmekanismer, som sørger for at mistenkelige avvik oppdages og reageres på før de utgjør en reell sikkerhetsrisiko.

4.7 Sikkerhet mot andre viljeshandlinger enn terror/sabotasje

Tiltakene som er nevnt hittil i dette kapittelet er i første rekke designet for å sikre mot. hhv. terrorhendelser og sabotasje. Likevel vil en rekke av tiltakene også bidra til å øke sikkerheten mot andre, hyppigere forekommende viljeshandlinger. Tabell 4.1 søker å illustrere dette, ved å koble sikkerhetstiltak mot ulike viljeshandlinger. I tillegg til terror og sabotasje har vi også sett på:

- Tagging – hærverk i form av nedspraying av objekter med maling.
- Gjengaktivitet, f.eks. uro, masseslagsmål, ansamlinger av uønskede elementer på transportinfrastrukturen osv.
- Trusler mot eller utøvelse av vold mot ansatte i transportvirksomhetene.

Tiltak	Terrorisme	Sabotasje	Tagging	Gjeng/uro	Vold egne ansatte
Administrative tiltak (4.2)	X	X	X	X	X
Planer/øvelser(4.3.1-4.3.3)	X	X	X	X	X
Analyser (4.3.4-4.3.6)	X	X	(x)	(x)	(x)
Adgangskontroll (4.4.1)	X	X	X		X
Regulere trafikk (4.4.2)	X	X			
Kameraovervåking (4.4.3)	(x)	X	X	X	X
Vakthold (4.4.4)	X	X	X	X	X
Rydding/gjemmesteder (4.4.5)	X	(x)			
Informasjon (4.4.6)	X	X	X	X	X
Sensorer våpen (4.4.7)	X	(x)			
Kontroll bagasje/reisende (4.4.8)	X	(x)	(x)	(x)	(x)
Kontroll transportmidler (4.4.9)	X	(x)			
Brannsikkerhet (4.4.10)	X	X			
Fortifikasjon (4.4.11)		X			
Konsekvensredusering (4.5.1)	X	X	X		
Redundans/desentralisering(4.5.2)		X			
Beskyttelsesutstyr (4.5.3)	X	X			
Informasjonssikkerhet (4.6.1)	(x)	X	(x)		
Kompetanseutvikling (4.6.2)	X	X	X	X	X
Sosiale tiltak (4.6.3)	X	X			X

Tabell 4.1 Sikkerhetstiltak og relevans overfor ulike viljeshandlinger. Tall i parentes viser i hvilket kapittel tiltaket er beskrevet. Kryss angir god effekt av tiltak overfor viljeshandlingene, kryss i parentes angir mulig effekt.

Som tabellen viser, vil en rekke av tiltakene som er aktuelle overfor terror og sabotasje også ha en effekt mot mer hverdagslige utfordringer. Spesielt gjelder dette tiltak som innebærer overvåking/kamera og vakt/patruljevirksomhet. Imidlertid kan det være tiltak mot terror/sabotasje som faktisk påvirker evnen til å håndtere andre hendelser negativt. Dersom man f.eks. bare sprer transportmidler på flere anlegg, vil man være mer sårbar overfor taggetrusselen flere steder samtidig med mindre alle anleggene blir gjenstand for en kraftig oppgradering av adgangskontrolltiltak.

I tillegg finnes det tiltak rettet spesielt mot hverdagshendelsene som ikke er omtalt over. I mange tilfeller vil imidlertid slike tiltak ikke være ansvaret til transportvirksomhetene direkte. Mot taggetrusselen kunne man kanskje vurdert forebyggende holdningskampanjer, koordinerte kampanjer for rask fjerning av graffiti, begrensninger i salg av spraybokser o.l., men dette er virkemidler som hører mer naturlig hjemme hos ulike myndighetsorganer. Mot gjenger kan

spaning, etterretning og tiltak for å bryte opp miljøene være aktuelle, men dette er politiets ansvar. Transportvirksomhetenes handlingsrom mot slike trusler blir derfor begrenset, annet enn de tiltakene som er krysset av i matrisen i tabell 4.1. Alternativt kan transportvirksomhetene inngå samarbeid med nødetater og myndigheter for å sette fokus på også de mer hverdagslige viljeshandlingene.

4.8 Tiltaksstrategier

Det er vanskelig å si hva som er ”god nok” sikring av et kollektivtransportsystem overfor viljeshandlinger. Dette problemet har mange dimensjoner:

- Systemet er sårbart overfor en rekke viljeshandlinger, men vi har få erfaringer nasjonalt med terror og sabotasje
- Det finnes ingen konkrete krav til sikringen av trafikksystemet i dag, som det er mulig å dimensjonere tiltak mot.
- Innføring av sikkerhetstiltak koster mye, og de vil ofte stå i motsetning til andre viktige hensyn som blant annet trafikkgjennomføring og personvern.

En mulig løsning for å komme videre er å gjennomføre enkle risikovurderinger, for å identifisere hvilke scenarioer som har høyest risiko i kollektivtrafikksystemet, dersom angrep faktisk inntreffer. Deretter kan tiltak vurderes i henhold til f.eks. PSTs trusselnivåer: Lav, Moderat, Høy og Ekstrem. En slik inndeling gjør det mulig å sortere ut tiltak som bør gjennomføres i hverdagen, som en del av virksomhetens grunnberedskap, og hvilke som raskt må kunne iverksettes hvis trusselnivået øker.

Forslag til tiltakspakker vil avhenge av sårbarhetene i det aktuelle transportsystemet som vurderes. En generell innretning kan være som følger:

- På lavt trusselnivå vil grunnleggende tiltak for et effektivt sikkerhetsarbeid være naturlig å vurdere. Personellmessige og administrative tiltak som gir bedre rammebetingelser for arbeidet med sikkerhet mot viljeshandlinger hører hjemme her, samt konkrete tiltak for håndtering av scenarioer med høy risiko. I tillegg bør man her ha forhåndsplanlagt tiltak som skal iverksettes på høyere trusselnivå.
- Moderat trusselnivå vil normalt ikke skille seg mye fra lavt trusselnivå når det gjelder hvilke tiltak som er aktuelle. I stor grad vil tilleggstiltak utover det som skjer i hverdagen være av administrativ art, rettet mot eget personell (oppfordre til økt årvåkenhet) og adgangskontroll. Her kan man også vurdere å iverksette forhåndsplanlagte informasjonstiltak overfor publikum, som oppfordrer til årvåkenhet og setter fokus på bagasjehåndtering, varsling av avvikende hendelser osv.
- Ved høyt trusselnivå må tiltak som skal gjennomføres være forhåndsplanlagt, slik at de kan iverksettes raskt for å gi god breddesikring mot en høy, men uspesifisert trussel. Dette kan være tiltak som innebærer rydding av infrastrukturen for gjemmesteder, økt vakthold, skjerpet kontroll av transportmidler før bruk, stikkprøvekontroller av personer og bagasje, informasjonstiltak og lignende.

- Ved ekstremt trusselnivå må tiltak kunne iverksettes umiddelbart for å møte en spesifikk trussel. Dette vil i hovedsak være forsterkninger av tiltak som allerede er vurdert ved høyt trusselnivå.

5 Oppsummering og anbefaling

Det er i dag vanskelig å si at trusselen fra store viljeshandlinger er påtrengende for kollektivtransporten i Norge. Vi har få erfaringer med terror- og sabotasjeangrep, og i dag er det ikke noe som tilsier en signifikant økning i denne trusselen på kort sikt. Sånn sett er det ikke rart at transportvirksomhetene er mest opptatt av hyppigere forekommende viljeshandlinger, som hærverk, uro og tyveri.

Imidlertid er potensialet for skade ved målrettede terror- og sabotasjeangrep stort. Tiltak som innføres for andre typer viljeshandlinger vil heller ikke nødvendigvis gi god sikring mot terror og sabotasje. Samtidig ser vi at kollektivtrafikk regelmessig trekkes frem som mulig mål for slike angrep, og internasjonalt har vi sett flere eksempler på terroraksjoner mot nettopp transportsektoren de siste årene. Dette skyldes delvis sektorens betydning for samfunnslivet, men minst like viktig er det store antall mennesker som bruker transporttjenestene hver dag.

I dag er det ikke veldig vanskelig å gjennomføre viljeshandlinger av typen som rapporten skisserer mot norske kollektivtransportsystemer, så lenge man har tilgang på våpen og motiver for å gjennomføre angrep. Spesielt gjelder dette terrorangrep. Det er imidlertid viktig å understreke at dette er konsekvensen av en ønsket situasjon. De åpne løsningene er en forutsetning for å kunne avvikle persontrafikk i stor skala og gi funksjonelle tjenester til publikum. Behov for nye sikkerhetstiltak i systemet må derfor hele tiden balanseres mot hensynet til publikum i hverdagen.

Rapporten skisserer en rekke tiltak mot viljeshandlinger, som kan iverksettes på ulike trusselnivå. Det må likevel erkjennes at sikkerheten i kollektivtrafikken mot viljeshandlinger ikke vil være fullt ivaretatt selv om tiltakene i denne rapporten implementeres. Systemene vil fremdeles være sårbare overfor angrep som kan gi store konsekvenser, spesielt på lave trusselnivå. Imidlertid kan tiltakene som er skissert gi viktige løft utover dagens sikkerhetsarbeid, dersom de settes inn i en helhetlig og målrettet sikkerhetsstrategi.

Appendix A Sikkerhet ved VM på ski

Verdensmesterskapet på ski 2011 skal arrangeres i Holmenkollen i Oslo. Arrangementet gjennomføres av selskapet Ski-VM 2011 AS, eid av Norges Skiforbund (60 %) og Skiforeningen (40 %), og avvikles i perioden 23. februar – 6. mars 2011. I tillegg tas det sikte på en rekke ulike kulturarrangementer rundt om i byen i denne perioden, og man forventer derfor stor publikumstilstrømning til Oslo disse dagene.

I forbindelse med andre store idrettsarrangementer, som VM i fotball og OL, gjennomføres det store sikkerhetsarbeider. I noen grad har disse også bidratt til å avverge eller forsinke viljeshandlinger (f.eks. et bombeangrep mot tyske tog i 2006). FFI ble derfor bedt om å utarbeide noe grunnlagsinformasjon om viljeshandlinger kontra store idrettsarrangementer, spesielt for kollektivtrafikken.

Dette kapittelet oppsummerer noen funn etter et litteratursøk rundt sikkerhet ved større idrettsarrangementer. Deretter prøver vi å koble dette til VM på ski i Oslo 2011, som innspill til den videre planleggingen av arrangementet.

A.1 Utvikling innenfor sikkerhet ved OL[48]

Det ble for første gang satt virkelig søkelys på sikkerhet ved større idrettsarrangementer etter hendelsen under OL i München i 1972, der medlemmer av organisasjonen ”Black September” tok som gisler og til slutt drepte 11 deltagere fra den israelske OL-troppen. Hendelsen viste manglene ved personell- og områdesikkerhet under arrangementet.

Sikkerhet er ofte drevet av erfaringer fra tidligere hendelser, og de neste års arrangementer hadde derfor et stort fokus på trusselen fra terrorister. I OL i Atlanta i 1996 var det et høyt fokus på område- og personellsikkerhet, og man hadde en mye bedre og mer kompetent beredskap enn tilfellet var i München. Likevel skjedde det en alvorlig sikkerhetshendelse, der én enkeltperson (med uklare motiver) utløste en bombe i en park. Dette resulterte i et dødsfall og 111 skadde personer. I ettertid ser man at mange ting kunne vært gjort bedre også i planleggingen før dette arrangementet. Blant annet var trusselbildet man planla etter dominert av trusselen fra grupper basert i Midt-Østen, mens den reelle trusselen viste seg å komme fra grupperinger og enkeltpersoner fra USA. Det ble også funnet svakheter i hvordan sikkerhetsplanleggingen var gjennomført, da koordinering og ansvarsforhold mellom de forskjellige statlige organisasjonene til tider var meget uklar.

[48] Informasjonen i dette kapittelet er i hovedsak hentet fra fire kilder:

- Jane’s (2007): Fortress Olympics - Counting the cost of major event security, hentet fra Jane’s Intelligence Review – May 01, 2007
- Johnson, C. W. (2006): A Brief Overview of Technical and Organisational Security at Olympic Events, Dept. of Computing Science, University of Glasgow
- Oquirrh Institute (2003): THE 2002 OLYMPIC WINTER GAMES SECURITY LESSONS APPLIED TO HOMELAND SECURITY, Olympic Security Review Conference, October 2003
- Romney, M. (2004): Lessons learned from Security at Past Olympic Games, tale holdt ved “Competition, Foreign Commerce, and Infrastructure Hearing” den 4. mai 2004

Etter hendelsen i Atlanta i 1996 ble sikkerhet rundt store arrangementer ikke bare rettet mot arrangementsområder, men også mot områder tilknyttet eller i nærheten av, arrangementet, for eksempel parker og bysentra. Det ble i tillegg et fokus på sikkerhetstrusselen fra demonstrasjoner, og på sikkerhet tilknyttet andre arrangementer som var planlagt nært i tid og sted til det store arrangementet. OL i Sydney i 2000 og OL i Salt Lake City i 2002 hadde et spesielt fokus på logistikk, koordinering og samordning, og spesielt Salt Lake tok fatt i problemer rundt koordinering og ansvarsforhold mellom de forskjellige statlige organisasjonene.

I 2004 arrangerte Aten sommer-OL, og brukte over 1,5 milliard USD på sikkerhet i tilknytning til arrangementet. Aten brukte erfaringene fra tidligere arrangementer, og til en viss grad også personell tilknyttet tidligere OL. I tillegg var Aten det første OL som fullstendig tok i bruk overvåkings- og etterretningsinformasjon og integrerte dette i den daglige avviklingen av arrangementet.

Denne utviklingen viser at sikkerhetsarbeidet ved store idrettsarrangementer i dag har som målsetting å skape en boble av total sikkerhet. For at OL skal ha beskyttelse mot alle tenkelige trusler, må det investeres store summer på sikkerhet. Tabell A.1 viser et anslag av de direkte sikkerhetskostnadene ved en del tidligere OL. Man ser her klart at kostnadene øker når sikkerhetsfokuset hos arrangementene blir bredere. Unntaket her er OL i Torino i 2006. Forskjellene mellom dette arrangementet og OL i Salt Lake City 4 år tidligere kan nok til en viss grad forklares med at lekene i Salt Lake skjedde bare et drøyt halvt år etter terrorangrepene i USA i september 2001. Det er også viktig å huske på at kostnadene som må brukes på sikkerhet er avhengig av den eksisterende infrastrukturen og den eksisterende sikkerhetssituasjonen der arrangementet holdes.

Barcelona 1992	USD 66,5 mill
Atlanta 1996	USD 109 mill
Sydney 2000	USD 180 mill
Salt Lake 2002	USD 345 mill
Aten 2004	USD 1500 mill
Torino 2006	USD 250 mill

Tabell A.1 Sikkerhetskostnader ved tidligere OL[49]

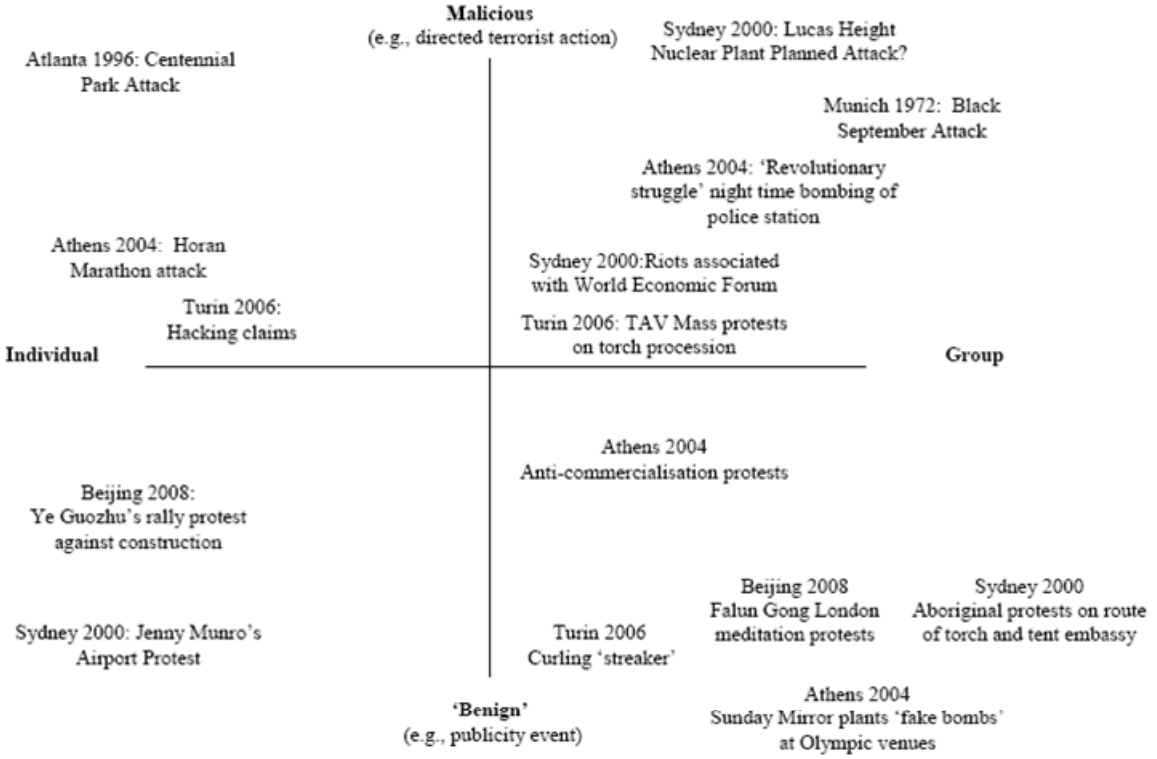
A.2 Spesifikke sikkerhetshendelser ved tidligere arrangementer

Trusler mot store idrettsarrangementer er forsøkt beskrevet med eksempler i figur A.1.[50] Her er ulike hendelser sortert på to dimensjoner: hvem som utgjør trusselen, fra enkeltindivider til

[49] Tallene er hentet fra:

- Jane's (2007), Fortress Olympics - Counting the cost of major event security, Hentet fra Jane's Intelligence Review – May 01, 2007
- Johnson, C. W. (2006), A Brief Overview of Technical and Organisational Security at Olympic Events, Dept. of Computing Science, University of Glasgow

organiserte grupper, og ”grad av ondskap” i handlingen. Det siste vil naturlig nok være en meget subjektiv bedømmelse.



Figur A.1 Dimensjoner ved sikkerhet for store idrettsarrangementer[51]

Johnson (2006) beskriver på bakgrunn av dette fire grove kategorier av trusseltyper:

- **Handlinger gjort av ondsinnede grupper.**
  Denne kategorien kan best eksemplifiseres ved hendelsen under OL i München i 1972, der ”Black September” drepte 11 deltagere fra den israelske OL-troppen. Andre hendelser kan være voldelige demonstrasjoner arrangert for å forstyrre eller stoppe det pågående arrangementet.
- **Handlinger gjort av ikke-ondsinnede grupper**[52]**.**
  Disse hendelsene er ofte fredelige demonstrasjoner med hensikt å skape publisitet rundt forskjellige saker, men kan likevel utgjøre potensielle sikkerhetstrusler mot et arrangement. Denne kategorien kan eksemplifiseres ved den fredelige demonstrasjonen for aboriginenes rettigheter som skjedde under OL i Sydney i 2000, der over hundre telt ble satt opp i Victoria Park.
- **Handlinger gjort av ondsinnede enkeltpersoner**
  Denne kategorien dekker et stort spekter av hendelser, alt fra hærverk og personangrep til terrorangrep, utført av en enkeltperson uten spesifikk hjelp fra andre personer. Denne

[50] Johnson, C. W. (2006), A Brief Overview of Technical and Organisational Security at Olympic Events, Dept. of Computing Science, University of Glasgow
[51] Johnson, C. W. (2006), A Brief Overview of Technical and Organisational Security at Olympic Events, Dept. of Computing Science, University of Glasgow, side 13.
[52] Med ”ikke ondsinnede grupper eller enkeltpersoner” menes grupper eller enkeltpersoner som ikke bruker ulovlige maktmidler, og som har som sin primære hensikt å på fredelig vis skaffe seg oppmerksomhet

typen hendelser er veldig vanskelig å beskytte seg mot. Her er rørbombeangrepet under OL i Atlanta i 1996 et godt eksempel, hvor en person la en tidsinnstilt bombe i en offentlig park der publikum vas samlet etter et OL-arrangement. Denne hendelsen resulterte i ett dødsfall og 111 skadde personer.

- **Handlinger gjort av ikke ondsinnede enkeltpersoner**[3]
  Dette er handlinger utført av enkeltindivider som ikke planlegger å true sikkerheten til noen tilknyttet arrangementet. Dette kan for eksempel være ”streakers”, altså folk som løper nakne over stadionområder. Et annet eksempel er protesten til Jenny Munro i tilknytning til OL i Sydney i 2000, der hun utførte en stille protest langs veien mellom OL-områdene og flyplassen, for å protestere mot brudd på aboriginenes rettigheter.

A.3 Eksempler på sikkerhetstiltak

Det er valg ut to case for å gi eksempler på spesifikke sikkerhetstiltak som har blitt gjort ved andre store idrettsarrangementer. Det er fokusert på vinter-OL, da det finnes lite litteratur om sikkerhetstiltak rundt tidligere ski-VM. Casene er vinter-OL i Salt Lake City, USA, i 2002 og Vinter-OL i Torino, Italia, i 2006.

A.3.1 Vinter-OL i Salt Lake City i 2002

Vinter-OL i Salt Lake City ble arrangert bare et halvt år etter terrorangrepene i USA 11. september 2001. Dette gjorde at fokuset på sikkerhet ble spesielt høyt under, og arrangementet var det første som ble erklært til å være et ”US National Special Security Event” (riktignok kom denne erklæringen før terrorangrepene 11. september 2001).

Følgende tiltak ble iverksatt under OL i Salt Lake City i 2002[53]:

- Over 10.000 sikkerhetspersonell ivaretok sikkerhet, blant annet 5.000 soldater, 200 grensevaktspesialister, 100 vakter fra U.S. Marshals Service for å passe på medisinske nødteam, og over 100 tjenestemenn fra U.S. Forest Service for å passe på fjell- og løypeområder.
- Bakgrunnssjekk av alle frivillige og ansatte.
- Utstrakt bruk av alle typer etterretning, og samarbeid med diverse statlige etterretningsorganisasjoner.
- Mobilt feltlaboratorium for å oppdage kjemiske, biologiske eller radioaktive våpen.
- Simulering av konsekvenser og spredning etter et radiologisk, kjemisk eller biologisk angrep, basert på utslipp- og spredningsmåling av svovel hexafluorid over Salt Lake City.
- Sivilt sikkerhetspersonell i folkemengder.
- Bærbare røntgenapparat for skanning av post og mistenkelige pakker.

[53] Informasjonen er hentet fra:

- Johnson, C. W. (2006), A Brief Overview of Technical and Organisational Security at Olympic Events, Dept. of Computing Science, University of Glasgow
- Oquirrh Institute (2003), THE 2002 OLYMPIC WINTER GAMES SECURITY LESSONS APPLIED TO HOMELAND SECURITY, Olympic Security Review Conference, October 2003
- Romney, M. (2004), Lessons learned from Security at Past Olympic Games, tale holdt ved “Competition, Foreign Commerce, and Infrastructure Hearing” den 4. mai 2004

- Gjennomsøk av arrangementsområder for bomber før åpning.
- Forbud mot ryggsekker og store bager ved alle arrangementsområder.
- Biometrisk identifisering og adgangskontroll av alt personell og av alle utøvere.
- En grense på 100 meter fra alle arrangementsområder der bare autoriserte kjøretøy fikk kjøre.
- Overvåkning av områder med CCTV.[54]
- Felles datasystem for å spre etterretning og hendelsesrapporter.
- GPS[55] posisjonsindikator på alle offisielle kjøretøy.

A.3.2 Sikkerhet ved Vinter-OL i Torino i 2006

Følgende tiltak ble implementert under OL i Torino i 2006[56]:

- Over 15.000 sikkerhetspersonell, blant annet 10.000 politi, 2.500 soldater, 300 snikskyttere for å passe på fjell- og løypeområder, 40 spesialsoldater på snøskutere og brannmenn med spesialisering innen kjemiske, biologiske og radiologiske angrep.
- Militærhelikoptre ble bruk til overvåking av alpint- og langrennskonkurranser.
- Gjennomsøk av arrangementsområder for bomber før åpning.
- Litt høyere sikkerhet på områder der idrettsarrangementene foregikk enn på andre områder, som premieutdelingsområde og konsertområder.
- Store samlingsområder, som torg og sentrale gater, ble sperret for kjøretøyer, og det ble gjennomført inngangskontroll av publikums sekker og vesker.
- Overvåkning av områder med CCTV og andre typer overvåkningsutstyr.
- Konsentriske sirkler med gradvis bedre sikkerhet rundt de forskjellige arrangementsområdene, med blant annet en grense på 100 meter fra alle arrangementsområder der bare autoriserte kjøretøy fikk kjøre.
- Obligatorisk gjennomsøking av vesker, bager og sekker, samt bruk av metalldetektorer ved inngang til idrettsarrangementene.
- Søk i folkemengder ved bruk av bombehunder.
- Separate innganger for media, deltagere, VIPs og publikum.
- Aktivt samarbeid og erfaringsoverføring fra blant annet Europol, Interpol, de fleste G8-landene, Israel og en del land fra Vest-Europa.
- 2.000 personer arbeidet for å opprettholde IT-infrastrukturen (pluss et ukjent antall som jobbet på IT-sikkerhet). Det ble identifisert 5 millioner IT-relaterte sikkerhetshendelser i løpet av lekene, hvorav 425 ble karakterisert som alvorlige og 20 kritiske.

[54] "Closed-Circuit Television"
[55] "Global Positioning System"
[56] Informasjonen er hentet fra:

- Around the Rings, Press Release: IOC Turin Debrief 7/14/2006, Tigjengelig fra: http://www.aroundtherings.com/articles/view.aspx?id=26667
- Johnson, C. W. (2006), A Brief Overview of Technical and Organisational Security at Olympic Events, Dept. of Computing Science, University of Glasgow

A.4 Konsekvenser av økt satsing på sikkerhet

Det er mange utfordringer knyttet til sikkerhet ved idrettsarrangementer. I tillegg til økte kostnader, vil sikkerhetstiltak ofte gå på bekostning av handlefriheten til de som berøres av dem. Aktive tiltak, som for eksempel adgangskontroll, vil skape kø og hindre publikum, media og utøvere i å bevege seg fritt. Dette har ved tidligere arrangementer vært kilder til misnøye og protester. Sikkerheten rundt utøverne kan også føre til at deres handlefrihet og bevegelser blir begrenset under hele arrangementet, og ikke bare på selve konkurransearenaen.

En rekke personkontrolltiltak har også utfordringer knyttet til personvern. Denne typen sikkerhetstiltak kan lett misbrukes, både av ansatte som har ansvar for sikkerhetstiltaket, men også av utenforstående via uautorisert tilgang til og spredning av informasjon. Utstrakt bruk av overvåkning og lagring av bildedata, bruk av ansiktsgjenkjenningssoftware på overvåkningskameraer og bruk av biometrisk adgangskontroll er eksempler på tiltak som har klare utfordringer når det gjelder personvern.

Zedner diskuterer en del av paradoksene knyttet til sikkerhet:[57]

- Mange sikkerhetstiltak vil kun flytte trusselen til et annet geografisk eller samfunnsmessig område, og bare sjelden fjerne den fullstendig. Ved høy sikkerhet på arrangementsområdene kan en terrorist finne andre, mindre sikre mål, for eksempel innenfor transport. Man kan derfor si at det totale trusselnivået i samfunnet er relativt konstant, med mindre kilden til trusselen blir fjernet.
- Økt sikkerhet ved bruk av aktive og passive sikkerhetstiltak vil gjøre disse sikkerhetstiltakene mer synlige i samfunnet. Dette vil i sin tur gjøre at samfunnet generelt blir mer oppmerksom på at det er potensielle farer som man må beskyttes mot, og på den måten kan sikkerhet være med på å øke frykten i samfunnet.
- Sikkerhetstiltak er også eksempler på gjøremål hvor man ofrer rettighetene til de få, for å beskytte rettighetene til de mange. Tiltakene er til for flertallet, og forutsetter at de få som blir sett på som truende (suspect population), blir ekskludert. Sikkerhetstiltak vil gå på bekostning av alles individuelle rettigheter, men dette er ikke likt fordelt i samfunnet. Ved såkalt ”tilfeldige” sikkerhetskontroller av personer og bagasje, vil man i større grad sjekke de personer som passer forhåndsbestemte profiler, og ofte vil disse tilhøre bestemte etniske grupper.

A.5 Sikkerhet ved VM på ski i 2011

A.5.1 Er ski-VM et attraktivt mål for viljeshandlinger?

Knyttet til viljeshandlinger er det spesielt to hensyn å vurdere i forbindelse med Ski-VM i 2011:

- Arrangementet kan være en attraktiv arena for ulike viljeshandlinger, delvis på grunn av medias oppmerksomhet, delvis på grunn av symbolverdien i å ramme et stort idrettsarrangement.

[57] Zedner, L. (2003), Too Much Security?, International Journal of the Sociology of Law 31(3): 155–84.

- Siden publikums- og medieoppmerksomheten rundt arrangementet er stort i utgangspunktet, vil ulike uønskede hendelser som skjer i denne perioden få mer omtale enn normalt.

Hvorvidt VM på ski i Oslo er stort nok til å tiltrekke seg mennesker som ønsker å gjennomføre viljeshandlinger kan diskuteres. Dette vil delvis avhenge av hva slags type viljeshandlinger man frykter (politiske demonstrasjoner og markeringer er generelt mer sannsynlig enn terroraksjoner), men ikke minst av andre forhold rundt arrangementet, for eksempel:

- Den rådende sikkerhetspolitiske situasjonen når arrangementet blir gjennomført
- Hvilke saker som opptar media i Norge/utlandet i denne perioden
- Det generelle sikkerhetsnivået ved arrangementet
- Tilstedeværelsen av VIP-personer
- Antall tilskuere, ikke minst utenlandske tilskuere

A.5.2 Utfordringer for kollektivtransporten

Ser man spesielt på transportsektoren, vil VM på ski i praksis være en Holmenkollsøndag hver dag i over to uker – mange mennesker skal transporteres til og fra byen, og deretter får man de lokale utfordringene med å transportere publikum til og fra Holmenkollen. Avviklingen av dette transportvolumet over så mange dager kan kanskje oppleves som en sikkerhetsutfordring i seg selv. Det er imidlertid noen hensyn å vurdere spesielt:

- Antall fremmedspråklige på transportmidlene vil sannsynligvis øke, og dette er noe man må ta hensyn til om det skulle skje uønskede hendelser (f.eks. ved evakuering).
- Transportvolumet vil være stort, og transportmidlene kan bli tettpakket. Konsekvensene av hendelser som oppstår kan derfor bli større enn normalt, til andre tider på døgnet enn den vanlige rushtiden.
- Hendelser som oppstår i transportsektoren i denne perioden kan slå negativt tilbake på selve arrangementet VM på ski, gi dårlig norgesreklame osv.

Likevel er det per i dag vanskelig å argumentere for at nettopp transportsektoren kommer til å være mer utsatt i løpet av de to vinterukene i 2011 enn det normalt er. I den grad viljeshandlinger faktisk rettes mot VM på ski, synes det mer sannsynlig at disse har stadionanleggene eller kulturarrangementene som mål, siden pressen allerede er der. Hvis transportsektoren likevel skulle angripes, er sårbarhetene som kan utnyttes i denne perioden akkurat de samme som systemet opplever i hverdagen. Det beste virkemiddelet transportsektoren kan gjøre for å stå godt rustet mot VM på ski, er derfor å legge grunnlaget for et generelt godt sikkerhetsarbeid i hverdagen.

A.5.3 Aktuelle tiltak

Selv om det kanskje ikke er nødvendig å implementere mange tekniske tiltak mot viljeshandlinger for ski-VM, kan det være interessant å se hvilke generelle erfaringer man har gjort seg for sikkerhet ved tidligere store idrettsarrangementer. Disse listes opp her.

En gjenganger er utfordringer knyttet til **koordinering av, og samarbeid mellom, ulike yrkesgrupper og fagfelt**. Det er helt naturlig og nødvendig at forskjellige fagfelt og etater blir

tatt inn som en del av sikkerhetsstrukturen rundt et stort idrettsarrangement, og det er viktig å få de forskjellige gruppene til å jobbe sammen på en effektiv og hensiktsmessig måte. Tidligere arrangementer har hatt stor suksess med å lage effektive ledelsesgrupper bestående av representanter fra de forskjellige fagfeltene, og disse ledelsesgruppene har blitt satt ned i god tid før arrangementet startet. Det har blitt utført mange øvelser for å gjøre gruppene kjent med hvordan de må jobbe, og det er også blitt fokusert på "teambuilding" innad i ledelsesgruppene. Slik har personene fått tillit til hverandre.

Det bør også være en lik måte å gjøre risikovurderinger på i alle de forskjellige fagfeltene som deler på sikkerhetsansvaret. Dette gjør det enklere å sammenligne trusler og fordele knappe ressurser der de trengs mest.

Det er viktig å ha et **informasjonssystem** som sprer relevant informasjonen til de riktige menneskene. Dette systemet må være robust og ha god innebygd redundans, og det må være dimensjonert til å fungere under alle forhold, for eksempel under en potensiell hendelse. Det er også nyttig å inkludere etterretningsinformasjon inn et slik informasjonssystem.

Det er viktig at det er satt av **nok tid til installering og testing av tekniske sikkerhetsløsninger,** som kommunikasjonssystem og overvåkningssystem. Hvis bygging av arrangementsområder blir utsatt, vil også starten på installering og testing av eks. overvåkningssystemer bli utsatt. OL i Aten fikk bare brukt deler av sitt overvåkningssystem på grunn av denne problematikken.

OL i Torino i 2006 hadde utfordringer med å **sikre konkurranseområdene** for idrettsgrener som gikk over store avstander, som for eksempel langrenn. Det var derimot relativt problemfritt å sikre konkurranseområder som var i fjellområder, på grunn av vanskeligheten med å komme seg dit utenom de offisielle veiene.

Media har hatt et kontinuerlig høyt fokus på sikkerhet nå det gjelder denne typen arrangementer. Det har ofte kommet kritikk fra media på bakgrunn av det som blir sett på som for høy sikkerhet, og det kommer også kritikk av tilsynelatende for lav sikkerhet. Det har også forekommet at representanter fra media aktivt har sjekket sikkerheten på diverse områder. Det er derfor viktig å ha en klar kommunikasjon til media, uten å frigi sensitiv informasjon. Erfaringer tilsier at å la én dedikert person som er godt opplært i mediehåndtering, risikokommunisering og kriseledelse uttale seg til media, er fornuftig. En god håndtering av media i en krisesituasjon kan begrense omdømmetap og oppfattet alvorlighet av krisen, mens en dårlig eller utilstrekkelig håndtering av media kan gjøre mye skade.

Det er også meget viktig å **ha et reelt og oppdatert trusselbilde** i sammenheng med et arrangement. Dette trusselbildet avgjør hvor man fokuserer sikkerheten. Imidlertid kan det også diskuteres om sikkerhetstiltak også skal brukes for å skape trygghetsfølelse utover hva det reelle trusselbildet tilsier. Følelse av trygghet er subjektivt, og oppfatning av risiko varierer fra person til person. Det er ofte en forskjell på hva befolkningen anser som de store truslene og hva

sikkerhetseksperter anser som trusler. Derfor kan man spørre seg om sikkerhetstiltak bør gjøres også der befolkningen mener den trengs, eller bare der sikkerhetsekspertene menes den trengs.

Dette er forhold som kan være viktig å ta med i planleggingen før Ski-VM i Oslo i 2011. I tillegg bør politiet og Politiets Sikkerhetstjeneste involveres for samarbeid, praktiske råd, trusselvurderinger (spesielt nær arrangementet) og lignende. Det kan også være aktuelt å kontakte andre arrangører av ski-vm, for å klarere ut hvilke tiltak som ble gjort der og hvilke erfaringer disse har gjort seg. Aktuelle kontakter er arrangørene i Val Di Fiemme/Italia 2003, Oberstdorf/Tyskland 2005, Sapporo/Japan 2007 og Liberec/Tsjekkia 2009. Praktiske erfaringer fra Lillehammer-OL i 1994 er også av interesse.

Appendix B Forkortelsesliste

CBRN	Chemical, Biological, Radiological, Nuclear
CCTV	Closed-Circuit Television
FFI	Forsvarets forskningsinstitutt
GPS	Global Positioning System
IKT	Informasjons- og kommunikasjonsteknologi
KTPAS	Kollektivtransportproduksjon AS
MIPT	Memorial Institute for the Prevention of Terrorism
NSB	Norges statsbaner
PST	Politiets sikkerhetstjeneste
ROS	Risiko- og sårbarhetsanalyse
VIP	Very Important Person

Referanser

- ABC-nyheter (2008): “Norsk sikkerhet i en terrorisert verden”, kronikk av Iver Johansen i ABC-Nyheter 23. mai 2008. Lenke: http://www.abcnyheter.no/node/67200
- Aftenposten (2006):”Sabotasje uroer passasjerer”, Aftenpostens nettutgave 5. juli 2006. Lenke: http://ww.aftenposten.no/nyheter/iriks/article1377356.ece
- Aftenposten (2007): “Brann på Oslo S lammer togtrafikken”, Aftenposten 28. november 2007: http://www.aftenposten.no/nyheter/oslo/article2124044.ece
- Aftenposten (2007): “Masseslagsmål på t-banevogn”, Aftenposten 8. desember 2007. Lenke: http://www.aftenposten.no/nyheter/oslo/article2143159.ece
- Aftenposten (2008): ”Anmelder sabotasje på t-banevogner.” Aftenposten 12. mars 2008. Lenke: http://www.aftenposten.no/nyheter/oslo/article745042.ece
- Blatny, J M, Fykse E M, Olsen J S (2006): Påvisning av biologiske trusselstoffer – Teknologinnspill til FS 07, FFI/RAPPORT-2006/01483, Forsvarets forskningsinstitutt.
- DSB (Direktoratet for sivilt beredskap) (2002): ”Prosjekt for å vurdere muligheter for stasjonær deteksjon av kjemiske stridsmidler”, Oslo, desember 2002.
- Eggereide B et al (2007): Innenriks sjøtransport som mål for terror – en risikovurdering, FFI/RAPPORT-2007/00004 (Begrenset)
- European commission (2006): Work Programme 2007 – Cooperation Theme 10 Security.
- Europol (2007): ”TE-SAT 2007 - EU Terrorism Situation and Trend Report 2007”, Europol March 2007.
- Europol (2008): ”TE-SAT 2008 - EU Terrorism Situation and Trend Report 2008”
- Europol (2009): ”TE-SAT 2007 - EU Terrorism Situation and Trend Report 2009”
- Fridheim H et al (2006): Oslo S som mål for terror og sabotasje – en risikoanalyse, FFI/RAPPORT-2006/03790 (Begrenset)
- Hagen J et al (2003): Beskyttelse av samfunnet med fokus på transportsektoren, FFI/RAPPORT 2003/00929
- Human Security Report Project (2008): Human Security Brief 2007. Lenke: http://www.humansecuritybrief.info
- IOC (2006): Around the Rings, Press Release: IOC Turin Debrief 7/14/2006, Tigjengelig fra: http://www.aroundtherings.com/articles/view.aspx?id=26667
- Jane’s (2007): Fortress Olympics - Counting the cost of major event security, hentet fra Jane’s Intelligence Review – May 01, 2007
- Johnson, C. W. (2006): A Brief Overview of Technical and Organisational Security at Olympic Events, Dept. of Computing Science, University of Glasgow
- Justis- og politidepartementet (2006): Når sikkerhet er viktigst, NOU 2006:6
- Lia B, Nesser P (2005): Terror mot jarnvegar – Eit oversyn over typiske terroraksjonar mot togpassasjertransport. FFI/RAPPORT-2005/01451, Forsvarets forskningsinstitutt.
- Lov om forebyggende sikkerhetstjeneste. Ikrafttredelse 1. juli 2001. http://www.lovdata.no
- Lov om endringer i lov om forebyggende sikkerhetstjeneste (sikkerhetsloven). Kunngjort 11. april 2008. http://www.lovdata.no

- March Network News (2006): ”Finish Capital Tackles Crime and Vandalism – Video Surveillance Helps Helsinki City Transport Battle Graffiti”. March Networks News 2006. Lenke: http://www.marchnetworks.com/Customers/CaseStudies/3.aspx
- Morgenbladet (2008): ”Mindre terror i verden”, Utenriksanalyse av Stein Tønneson, Prio, fra Morgenbladet 30. mai 2008.
- Nesser, P (2008): "Chronology of Jihadism in Western Europe 1994-2007: Planned, Prepared, and Executed Terrorist Attacks". Published in Studies in Conflict & Terrorism, Volume 31, Issue 10, (October 2008), pp. 924 – 946.
- Nettavisen (2005): ”Kvinne dømt for kontrollørvold”, Nettavisen 1. mars 2005. Lenke: http://pub.tv2.no/nettavisen/innenriks/article352944.ece
- Nettavisen (2006): “Dette fikk vi med på flyet”, Nettavisen 8. august 2006. Lenke: http://pub.tv2.no/nettavisen/innenriks/article704849.ece
- Nordstrands blad (2007): “Vil ha slutt på bråk og hærverk”, Nordstrands blad 22. mars 2007. Lenke: http://noblad.no/apps/pbcs.dll/article?AID=/20070322/NONYHETER/103220163
- Oquirrh Institute (2003): THE 2002 OLYMPIC WINTER GAMES SECURITY LESSONS APPLIED TO HOMELAND SECURITY, Olympic Security Review Conference, October 2003
- Politiets sikkerhetstjeneste (2009): Åpen trusselvurdering 2009: http://www.pst.politiet.no/Filer/utgivelser/trusselvurderinger/Aapen_trusselvurdering_PST.pdf
- Romney, M. (2004): Lessons learned from Security at Past Olympic Games, tale holdt ved “Competition, Foreign Commerce, and Infrastructure Hearing” den 4. mai 2004
- SAFETEC (2004): ”Oslo Kommune Beredskapsetaten – Hovedrapport oppdatering av ROS-analyse”, Dok nr ST-25497-RA-1-Rev01, desember 2004 (BEGRENSET).
- Schjelderup T E et al (2005): Togtrafikken som mål for terror og sabotasje – en risikoanalyse, FFI/RAPPORT-2005/01894 (U.off)
- Schneier B. (2003): Beyond Fear: Thinking Sensibly About Security in an Uncertain world. Copernicus books
- US Transport Security Administration (2006): Technology for Hold Baggage Screening, presentasjon ved International Arab Civil Aviation Security Conference, Abu Dhabi 7-8 februar 2006.
- Verdens gang (2009): ”Her knuser demonstrantene Karl Johan”, VG 8. januar 2009. Lenke: http://www.vg.no/nyheter/utenriks/midtosten/artikkel.php?artid=545880
- Vårt Land (2008): ”Pågrep 120 personer i rusaksjon”, Vårt land 16. april 2008. Lenke: http://www.vl.no/samfunn/article3479646.ece
- Zedner, L. (2003), Too Much Security?, International Journal of the Sociology of Law 31(3): 155–84.
- Østkantavisa (2008): ”Lommetyvene bruker skjorte og slips”, Østkantavisa 17. mars 2008. Lenke: http://www.ostkantavisa.no/apps/pbcs.dll/article?AID=/20080317/NYHETER/843752131/1018/DEBATT

- Østlandssendingen (2004): ”Tagging stopper t-banen”, Østlandssendingen 4. juli 2004. Lenke: http://www.nrk.no/nyheter/distrikt/nrk_ostlandssendingen/3911657.html

Vevsider:

- Politiets sikkerhetstjeneste: http://www.pst.politiet.no
- Wikipedia,
  - om sikkerhetsteater: http://en.wikipedia.org/wiki/Security_theater
  - om togulykken i Eschede 1998: http://en.wikipedia.org/wiki/Eschede_train_disaster