POLITIET

POLITIDIREKTORATET

Det kongelige Justis- og politidepartementet
Postboks 8005 Dep.,
0030 OSLO

Deres referanse	*Vår referanse*	*Dato*
	2003/00664-64 053	13.04.2007

Oversendelse av rapport

Vi viser til Deres brev datert 25. november 2006, hvor det bes om en gjennomgang av virkemåte og de tekniske forutsetningene for ordningen med mobile voldsalarmer, og Politidirektoratets brev hvor det angis at en slik tilbakemelding skal gis innen 1. mai 2007.

Anmodningen kom i etterkant av en drapssak i Vest-Oppland politidistrikt samme måned. I møte med Politiets data- og materielltjeneste (PDMT) 9. februar 2007, ba POD om at det så raskt som mulig ble utarbeidet en rapport om tekniske og bruksmessige begrensninger ved dagens system, samt aktuelle muligheter for forbedringer.

Rapporten fra PDMT (Vedlegg 1) ble levert til Politidirektoratet 30. mars 2007. PDMT har gitt en beskrivelse av begrensningene og sårbarhetene ved voldsalarmsystemet. Det er ikke funnet begrensninger utover det man tidligere har hatt kjennskap til. PDMT har for øvrig foreslått tiltak som kan redusere systemets sårbarhet. Rapporten fra PDMT behandler tekniske løsningene knyttet til en situasjon hvor en alarm utløses. Det beskrives fem områder hvor en ser klare begrensninger i systemet, og disse knytter seg til alarmenhetenes muligheter for posisjonering, responstid for politiet, "nede-tid" på stormaskinen (Strasak eller søk i Strasak er ikke mulig i en kort periode en gang ukentlig) eller server, og til slutt hvordan alarm-enheten håndteres av bruker.

En full gjennomgang av dagens system vurdert opp mot andre og nyere systemer krever ekstern vurdering og bistand, og vil dessuten ta lengre tid. PDMTs rapport gir imidlertid en god vurdering av systemet og erfaringene, og er et nødvendig grunnlag for å kunne gå videre med saken. POD har etter å ha mottatt rapporten tatt initiativ til et møte med PDMT for å vurdere behov og rammer for videre arbeid med ekstern bistand.

Videre har PDMT identifisert fire sårbare forhold ved systemet. Det første de peker på er at MVA-meldinger ikke vil kunne vises i Geopol dersom den sentrale serveren som betjener dette systemet er nede. Dette problemet kan løses ved innkjøp av en ny server.
Videre er det slik at MVA-meldinger ikke vises i Geopol i et politidistrikt dersom den lokale serveren i distriktet er nede. Dette kan løses ved at en installerer ekstra lokale servere i hvert distrikt, noe som anslagsvis vil koste 6-7 millioner kroner på landsbasis.

Politidirektoratet

Post: Postboks 8051 Dep., 0031 Oslo
Besøk: Hammersborggata 12
Tlf: 23 36 41 00 Faks: 23 36 42 96
E-post: politidirektoratet@politiet.no

Org. nr.: 982 531 950 mva
Bankgiro: 7694.05.02388

Det tredje som trekkes frem som et sårbart forhold, er at dersom noen skulle ønske å blokkere SMSer som sendes fra alarm-enheten til Telenor, så finnes det ulike metoder for å gjøre dette. Risikoen for en slik situasjon er imidlertid ansett som liten, og anskaffelse av utstyr for å hindre dette er derfor ikke anbefalt som særlig aktuelt.
En fjerde og mer sannsynlig sårbarhet, er overbelastning av mobilnettet. Dette vil være en aktuell problemstilling så lenge en velger å ha et alarmsystem som er basert på slike meldinger.

I rapporten påpekes at de alarmenhetene som brukes per i dag, er av "første generasjons type", og at det nå begynner å komme på markedet "tredje generasjons type" enheter som muligens har bedre følsomhet på enkelte områder. PDMT opplyser at disse modellene under enhver omstendighet vil bli nærmere vurdert i en planlagt anbudsrunde i løpet av 2007/2008. Politidirektoratet mener imidlertid at arbeidet med testing av alternative enheter bør igangsettes umiddelbart.

I rapporten fremheves at informasjon og god opplæring av alarm-brukerne er helt vesentlig. Politidirektoratet har helt fra innføringen av ordningen med mobile voldsalarmer vært opptatt av at den trusselutsatte skal få informasjon om begrensninger og svakheter ved systemet. Det er viktig at det gis grundig opplæring i hvordan en påser at alarmen har tilstrekkelig posisjonsinformasjon, hvordan den bæres eller plasseres riktig for å kunne motta/gi signaler osv. Denne type informasjon og opplæring har kontinuerlig blitt formidlet og den enkelte bruker har i tillegg fått detaljert skriftlig rettledning (Vedlegg 2) ved tildeling av alarm. Politidirektoratet vil imidlertid foreta en fornyet gjennomgang av rutinen for formidlingen av informasjon, for å se om noe bør gjøres annerledes. Vi vil også på nytt understreke overfor politidistriktene at det må gis en grundig opplæring av hver enkelt bruker i forbindelse med tildeling av alarm, slik at det ikke er tvil om at alarm-brukeren vet hva slags beskyttelse alarmen gir, og hvilke begrensninger som ligger i systemet. Informasjon vedrørende systemet er også redegjort for på Internett (Vedlegg 3).

Politidirektoratet ba om en redegjørelse fra Vest-Oppland politidistrikt vedrørende den aktuelle saken der. Politidirektoratet (POD) mottok 21. februar d.å. en redegjørelse fra Vest-Oppland politidistrikt (Vedlegg 4). Den gjengir hva som skjedde i den konkrete drapssaken, samt politidistriktets vurderinger av hvordan den aktuelle voldsalarmen fungerte.

Til slutt kan det nevnes at Politidirektoratet har bedt Agder politidistrikt om en redegjørelse i forbindelse med en drapssak den 30. mars d.å. Det var også i denne saken dessverre slik at en person som hadde fått tildelt en mobil voldsalarm, ble drept. Departementet vil bli ytterligere informert så snart redegjørelsen fra politidistriktet foreligger.

Med hilsen

Ingelin Killengreen

Tor Tanke Holm
seksjonssjef

Saksbehandler:
Ingvild Hoel
Tlf: 99207726

POLITIET

DIREKTØREN FOR PDMT

Politidirektoratet
Postboks 8051 dep
0031 OSLO

Deres referanse	*Vår referanse*	*Dato*
	2007/00039-3 44-06	30.03.2007

Rapport om mobil voldsalarmsystemet (MVA)

15. desember 2006 fikk PDMT i oppdrag av Politidirektoratet og foreta en teknisk utredning av alle sider ved mobil voldsalarmsystemet som benyttes av politiet.

Det opprinnelige oppdraget forutsatte at PDMT har tilgang til spesiell kompetanse som PDMT ikke besitter. I tillegg ønsker PDMT at det utføres en vurdering av MVA-systemet av en uavhengig instans, som ikke har deltatt i utviklingen og driften av systemet.

Oppdraget ble derfor i møte med Politidirektoratet 9.2.07 redusert til å beskrive begrensninger og sårbarheter i mobil voldsalarmsystemet, samt mulig tiltak for å redusere disse. Av denne grunn er utredningen omgjort til rapport.

Rapporten behandler kun den tekniske løsningen fra og med alarmen utløses. Rapporten kommer kun inn på den saksbehandlingsmessige siden av mobil voldsalarm der det er naturlig i forbindelse med beskrivelse av den tekniske løsningen. Det foreslås likevel tiltak i forbindelse med tildeling av alarmenheten til trusselutsatt og bruk av alarmen i det daglige. Det er ikke foretatt risiko eller sannsynlighetsberegning for mulige sårbarhetsscenario.

Uten at det har fått innvirkning på denne rapporten, vil PDMT fortsatt anbefale en uavhengig gjennomgang av totaliteten av mobil voldsalarmsystemet.

Kort om GPS-teknologi og feilkilder

Politiets data- og materiellt jeneste

Direktøren for Politiets data- og materiellt jeneste,
besøk: Sørkedalsveien 27
Post: Postboks 8031 Dep, 0030 OSLO
Tlf: 61 31 80 00 Faks: 61 31 80 01
E-post: post.pdmt@politiet.no

Org. nr.: 974 761 157
Bankgiro: 7694.05.08343

GPS-systemet består av 24 satellitter som kretser i 20 000 km høyde i nøyaktige baner rundt jorden to ganger pr døgn. Satellittene sender radiosignaler som inneholder identifikasjon av satellitten og tidspunkt for sendingen. For at en GPS-mottager skal kunne beregne GPS-posisjon, er enheten avhengig av at minst 3 satellitter er synlig på samme tidspunkt. Posisjonering gjøres ved at enheten foretar enveis avstandsmåling til satellittene basert på tidspunkt for sending sammenlignet med tidspunkt for mottak av sendingen. GPS-mottageren beregner så trepunkts kryssjekk på bakgrunn av avstandsmålingen. Hvis 4 eller flere satellitter er tilgjenglige, kan posisjonering gis i tre dimensjoner (lengdegrad, breddegrad og høyde). I prinsippet er det slik at jo flere satellitter, jo større nøyaktighet på posisjoneringen. Imidlertid har dette prinsippet i praksis noe begrenset gyldighet i og med at det finnes en del feilkilder i forbindelse med GPS-signalering.

Disse er i korthet (dominans i rekkefølge):

- Feil i korreksjon av psaudorangemålinger forårsaket av ionosfæren (Ionosfærisk påvirkning)
- Feil i den overførte posisjonen fra satellitten (Ephemerisdatafeil).
- Feil i den utsendte klokkeangivelsen fra satellitten (Satellittklokkefeil)
- Feil i korreksjon av psaudorangemålinger forårsaket av troposfæren (Troposfærisk påvirkning)
- Feil skapt av reflekterte signaler mottatt av mottagerantennen (Flerveistransmisjon)
- Feil i mottagerens måling av avstand skapt av termisk støy, nøyaktighet i programvare og kanalstøy (Mottakerfeil)

Hertil kommer satellittenes geometri og posisjon på himmelen, som igjen varierer med tidspunktet siden både satellittene og mottakeren beveger seg. Generelt er det slik at jo nærmere polene man befinner seg, jo færre satellitter er synlige for GPS-enhetene i størstedelen av døgnet.

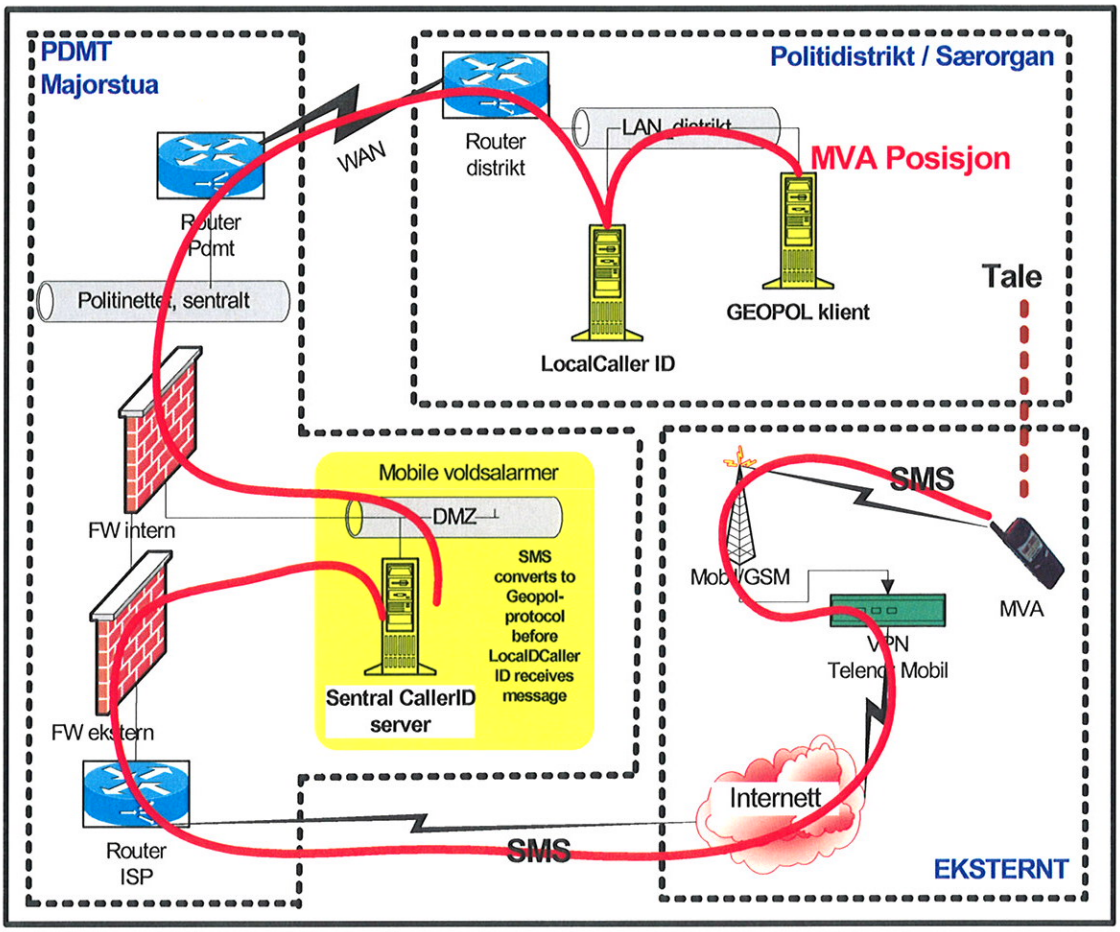
I tillegg vil de enkelte feilkilder individuelt påvirke hverandre i større eller mindre grad.

Internasjonale undersøkelser har imidlertid vist at metroligiske forhold som regnvær eller kraftig skydekke ikke påvirker GPS-signaler i vesentlig grad. Den dominante feilkilden er ionosfæriske forhold som i liten grad kan påvirkes av mennesker eller teknologi, da graden av ionosfæriske forstyrrelser på et gitt tidspunkt er meget vanskelig å forutse. Her nest kommer feil i ephemerisdata (feil i overføring) og feil i satellittklokke. Korrigering av satellittklokkene foregår kontinuerlig hver gang satellittene passerer kontrollstasjoner på jorden.

* kilde: Tomas Vangen, "Bruk av GPS i vanskelige omgivelser " Masteroppgave 2006 NTNU

Teknisk skisse av MVA-systemet:

Nedenfor følger skisse over Mobil Voldsalarmsystemet slik det er konstruert av PDMT. Rapporten omhandler primært de to rutene som heter "PDMT Majorstua" og "Politidistrikt/Særorgan". Ruten som heter "Eksternt" er i liten grad beskrevet, da prosessene i denne ruten kjøpes eksternt.



* Svalbard har ikke tilgang til MVA-systemet.
* Sok i Strasak er ikke en del av det aktive MVA-systemet og derfor ikke inntegnet.

Teknisk beskrivelse av MVA-systemet:

Det finnes 2 forskjellige typer mobile voldsalarmer (MVA) i bruk av politiet i dag. Begge fungerer på samme måte. Når trusselutsatt utløser alarm, ringer MVA-enheten ringer opp operasjonssentralen i det distrikt som tildelte voldsalarmen. MVA-enheten er programmert til å ringe lokalt telefonnummer til utstedende distrikts operasjonssentral (ikke 112). Hvis distriktet ikke er tilgjengelig, eller hvis alarmen ikke er registrert i Sentral Caller ID server, blir alarmen sendt til et forhåndsdefinert distrikt (konfigurert fra sentralt hold).

Samtidig sender MVA-enheten SMS med sist kjente GPS-posisjon til Sentral Caller ID server som driftes av PDMT. Sentral Caller ID server utfører "polling", mottak og videresending av mobile voldsalarmer via SMS Access. SMS Access er en storskala SMS service levert fra Telenor. Samme krypterte VPN forbindelse mellom PDMT og Telenor som benyttes for posisjonering av kjøretøy, benyttes for overføring av posisjoneringsdata fra mobile voldsalarmer. MVA-enhetens telefonnummer er i denne server lagret sammen med trusselutsatts navn og saksnummer fra BL/Strasak. Trusselutsattes navn, Strasaknummer og GPS-posisjonen blir så rutet videre til operasjonssentralens Geopol-installasjon i det distrikt som utstedte den MVA, slik at operatøren ser voldsalarmens geografiske posisjon vist i kartet, samtidig som den trusselutsattes samtale kobles opp på operasjonssentralen.

Hvis alarmen ikke er GPS-posisjonert, kan operatøren "polle" (søke) alarmenheten. Man få da opp et skravert felt i kartet som indikerer dekningsområdet for den basestasjonen alarmenheten har koblet seg opp i. Geopol forteller med fargekoder i vinduet for innkommende voldsalarm hvor gammel posisjonering fra MVA-enheten er. Grønn farge indikerer at MVA-enheten nylig har fått

posisjonsangivelse, rød farge indikerer ar posisjonen i MVA-enheten er eldre og det kan da være grunnlag for å undersøke om enheten faktisk er på samme sted som posisjonshenvisningen tilsier.

Operatør vil kunne foreta oppslag i Søk i Strasak på bakgrunn av MVA-enhetens telefonnummer som vises i Geopol-installasjonen og i nødsamtalemottaket. For å begrense innsyn i MVA-saker, er det i Søk i Strasak kun mulig å se en MVA-sak med disse to inngangsparametre.

Alle alarmer i MVA-systemet blir logget på sentral Caller ID server. I tillegg blir "pollinger" som utføres av operasjonssentralen for å spørre hvor MVA-enheten er, lagret.

Følgende begrensinger er identifisert:

- Generelt kan det være begrensninger i MVA-enhetens posisjonsoppdatering i for eksempel byer hvor bygninger sperrer sikt mot himmelen/satellittene, i tunneler, i hanskerommet på biler, innendørs og hvis MVA-enheten oppbevares skjult, for eksempel innenfor klærne eller i en veske. MVA-enheten fungerer best når den har fri sikt mot himmelen. Risikoen for feil bruk vurderes som stor hvis ikke den trusselutsatte får god nok informasjon om disse forholdene.

- MVA-enheten ringer kun opp operasjonssentralen i det distriktet som utstedte MVA-enheten, også i de tilfeller hvor den trusselutsatte befinner seg i et annet distrikt. Operasjonssentralen som mottar nødsamtalen må derfor ringe opp operasjonssentralen i distriktet hvor trusselutsatt befinner seg og orientere, evt. sette telefonsamtalen videre til, operasjonssentralen i det distrikt den trusselutsatte befinner seg. Dette er en begrensning i MVA-systemet som kan innvirke på responstid for å yte bistand til den trusselutsatte.

- Hvis stormaskin, Strasak el Søk i Strasak ikke er tilgjengelig vil nevnte systemer være utilgjengelige og operasjonssentralen vil ikke kunne hente bakgrunnsinformasjonen om innkommende MVA-melding i elektronisk form. I slik tilfelle er det gitt beskjed til politidistriktene om jevnlig å kjøre ut papirlister over aktive MVA-saker. Det er laget en egen jobb for dette i Strasak. Det vites imidlertid ikke om alle distrikt følger denne rutinen til enhver tid. Konsekvensen av at Søk i Strasak ikke er tilgjengelig er at operasjonssentralen som mottar MVA-melding ikke får innsyn i operative forhold som ligger til grunn for at den trusselutsatt har fått tildelt MVA-enhet. Dette fører til at operatør ikke kan forberede patruljen som responderer på MVA-meldingen som igjen blir avskåret fra å kunne foreta avgjørelser på bakgrunn av opplysninger som de i nevnte tilfeller er avskåret fra. Stormaskin er utilgjengelig hver torsdag kl. 05.55 – ca. 07.15. Risikoen for den trusselutsatte bedømmes til liten, all den tid både MVA-meldingen og tale vil gå til operasjonssentralen uhindret og det gjelder et begrenset tidsrom på et tidspunkt hvor det er lav oppdragsmengde for politiet, og det skal finnes papirutskrifter som inneholder de samme opplysninger som Søk i Strasak.

- Hvis overføringen av opplysninger fra BL/Strasak til Sentral Caller ID server er nede ved utlevering av MVA-enheten, vil ikke Sentral Caller ID server bli oppdatert før kommunikasjonen igjen er etablert. Det forholdet vurderes som ikke kritisk da slik manglende kommunikasjon vil bli avdekkes gjennom testen som foretas ved utlevering av MVA-enheten. Konsekvensen er at utlevering av MVA-enheten må utsettes til kommunikasjonen er reetablert.

- Tester, erfaring og feilmeldinger mottatt av PDMT har avdekket begrensninger i hvordan MVA-enheten bør håndteres. Spesielt modellen fra Benefon er det ikke tilrådelig å gå med på innelommen når MVA-enheten er snudd mot kroppen (pga. retningsavhengig antenne). Generelt er det heller ikke tilrådelig å oppbevare MVA-enheten i en veske el. lignende.

Spesielt MVA-enheten Hiper bruker til dels lang tid på å finne posisjon første gangen den startes opp (opptil 20 min. ved kald start av enheten). Den samme enheten bruker også noe tid på å finne posisjon hvis den blir flyttet uten å ha mulighet til kontinuerlig posisjonsoppdatering (varm start av enheten).

Følgende sårbarheter er identifisert:

- Hvis **Sentral** Caller ID server er nede, vil ikke MVA-meldingen vises i Geopol og operasjonssentralen må behandle alarmen som en ordinær nødsamtale. Dette betyr igjen at operatør ikke vet hvor den trusselutsatte befinner seg. Nedetid på Sentral Caller ID server betyr at alle operasjonssentraler i landet vil være uten grafisk posisjonering i Geopol. Å kjøre uten redundans på denne sentrale komponenten vurderes som en stor risiko. Løsning for å redusere denne risiko er å opprette redundans ved å dublere Sentral Caller ID server med ekstra server.

- Hvis **lokal** Caller ID server er nede, vil ikke MVA-meldingen vises i Geopol og operasjonssentralen må behandle alarmen som ordinær nødsamtale - se over. Nedetid på lokal Caller ID server betyr at distriktet er uten mulighet til å posisjonere MVA-enhetene grafisk i Geopol. Et mulig tiltak for å redusere denne risiko er å installere redundant lokal Caller ID server i hvert politidistrikt. Kostnaden ved dublering av lokal Caller ID server er 27 x 250 000,- totalt kr. 6 750 000,-.

- Det er ingen form for beskyttelse av SMS fra MVA-enheten før SMS er mottatt av SMS Access hos Telenor. Teoretisk kan man derfor med ulike metoder blokkere SMS i et område med utstyr som riktignok koster en del, men som er fritt tilgjengelig (jfr. beslag gjort i NOKAS-saken). Risikoen for at dette vil inntreffe vurderes derimot som liten.

- En annen sårbarhet, med større sannsynlighet, er overbelastning av mobilnettet. Typisk ved årsskifte hvor det er utstrakt bruk av SMS-sendinger, har man erfart stor forsinkelse av SMS-meldinger. Risikoen for at dette scenario vil inntreffe vurderes som stor. Konsekvensen er at MVA-meldingen og samtalen ikke når igjennom.

Følgende presisering bør gis den trusselutsatte ved tildeling av MVA-enhet

- Den trusselutsatte bør oppfordres til med jevne mellomrom å sjekke at MVA-enheten har oppdatert posisjonsinformasjon (symbol på MVA-enheten). Dette er spesielt viktig før den trusselutsatte går inn i store bygninger, hvor muligheten for signalbrudd med satellitter er stor.

- Den trusselutsatte bør oppfordres til å jevnlig holde alarmen i fri sikt for å sikre oppdatert posisjonsinformasjon. MVA-enheten varsler når den har beregnet posisjonen med lyssignal.

- Den trusselutsatte bør gjøres oppmerksom på at MVA-enheten kan få problemer med å finne posisjon hvis den oppbevares i en veske, under klærne eller innendørs.

- Den trusselutsatte bør gjøres oppmerksom på at etter passering av lengre tunneler/opphold i store bygninger kan MVA-enheten bruke tid på å oppdatere posisjon.

Mulige tiltak:

- Dublering av Sentral Caller ID server. Kostnad kr. 250 000,- inkl. mva.

- Vurdering av markedet samt foreta tester av alternative MVA-enheter for å finne enheter med bedre følsomhet for GPS-posisjonering.

- Vurdering av mulige løsninger for alternativ transport av MVA-melding, til erstatning for SMS.

- Vurdering av mulige løsninger for viderekobling av MVA-meldinger til andre distrikt.

- Revisjon av teksten over sjekkpunkter ved utdeling av MVA-enhet i BL med sikte på å gjøre polititjenestemannen bedre i stand til å gjøre den trusselutsatte oppmerksom på begrensinger i bruk av MVA-enheten.

- Tjenestemenn som behandler MVA-saker bør gjennomgå opplæring i begrensningene i GPS-teknologi generelt og håndtering av MVA-enheter spesielt.

MVA-enhetene politiet i dag benytter er av 1. generasjons type. Etter en kort og meget overfladisk undersøkelse av markedet, er det ikke funnet MVA-enheter med **dokumentert** bedre følsomhet enn de som er i bruk pr. dd. Imidlertid begynner det nå å komme enheter på markedet av 3. generasjons type. PDMT tester for tiden ut en MVA-enhet som har bedre følsomhet, men det er litt tidlig i prosessen til å trekke entydige konklusjoner på bakgrunn av disse testene. Denne modellen vil bli vurdert på lik linje med øvrige tilbydere ved neste anbudsrunde, som er planlagt igangsatt i løpet av 2007 med ferdigstilling i 2008.

Med hilsen

Lars H. Bøhler
direktør

Mats Berg
produktleder