OVERVÅKINGS HÅNDBOKA

BARE FOR DEG SOM IKKE BLIR PARANOID ELLER ENGSTELIG

FOR Å
BRUKE TELEFON, POST ELLER DATA,
MARKERE AKP PÅ GATA,
DRIVE MASSEARBEID,
BYGGE ENHETSFRONTEN OG PARTIET,

men som likevel synes det kan være greit å vite.

AKP april 1997 **kr 20**

OVERVÅKINGSHÅNDBOKA.

INNHOLD:

1. **Du setter elektroniske spor hvor du går - den nye digitale teknologien.**
   Et døgn i ditt liv. Slik blir du overvåka i løpet av 24 timer. Nye kort kartlegger handlemønsteret ditt.

2. **Innledning**
   Hvorfor lager vi denne håndboka, hvorfor vi trenger organisasjonsvern, forholdet mellom massearbeid og sikkerhet. Situasjonen i verden. Et parti av AKP's type.

3. **Hva sier Lund-rapporten.**
   Romavlytting. Post-, telefon- og telegramkontroll. Registrering av overskuddsinformasjon. Ransaking og beslag. Bruk av andre overvåkingstiltak. Konkret om overvåkinga av SUF og AKP(ml). Spaning og aktiv bruk av informanter. Provokasjon.

4. **Hvem var/er vi interessante for.**
   Norges hemmelige hær. Overvåking fra nazistene.

5. **De tradisjonelle metodene:**
   Postkontroll. Telefonavlytting. GSM-systemet. Hvordan foregår avlyttinga.
   GSM-telefonen avslører deg. Tapping av personsøkere. Noen tiltak.

6. **Datasikkerhet.**
   Overvåking av Internett. Overvåking av Internett i Norge. Sjefen kan lese e-posten din uten lov. Overvåking av nettverk. Hvordan man kan trenge inn i harddisken utafra. Noen forholdsregler. Kryptering av data.

7. **En overvåkingstjeneste for framtida.**
   Justisminister Valla om omorganiseringa av POT. S-tjenesten får utvida fullmakt. Sortinget positivt til romavlytting - metodeutvalgets innstilling. Overvåkingssystemet innafor Schengen; SIS og Sirene. Du er registrert 500 ganger. Fri flyt av persondata i Europa.
   Ting skjer fort.

8. **Hjelpemidler i overvåkinga. Hva finnes på markedet.**
   Hvor kan det skaffes og hvem kan få tak i det.

1. Du setter elektroniske spor hvor du går. Den nye datateknologiens muligheter for overvåking.

Et døgn i ditt liv.....

Slik blir du overvåka og registrert i løpet av 24 timer.

Vær også oppmerksom på at vi setter elektroniske spor ved bruk av kort ol., såkalt transaksjonsregistrering, det vil si ved flyt av penger og informasjon fra hvem til hvem, post, bank, fax, BBS, modem osv.

Vi kan ta for oss et tenkt eksempel som illustrerer dette:
0730: Drar fra parkeringshuset.
Du blir tatt opp av overvåkingskameraer. Nøyaktig tidspunkt for avreise blir elektronisk lagra i p-kortet.

0740: Kjører inn mot byen og passerer bomstasjonen.
Tidspunkt og sted for passering blir lagra elektronisk når bompengebrikka passerer bomstasjonen. Bomselskapet sender ny regning når gjeldende abbonement går ut.

0748: Blir sittende fast i trafikk-kork og ringer jobben.
Mobiltelefonen avlyttes, og opplysninger om hvem du ringer og hvor lenge du prater blir automatisk lagra hos telefonselskapet. Har du en GSM-telefon er det mulig å følge dine bevegelser fra sekund til sekund så lenge den er påslått.

0813: Ankommer parkeringshus.
Kort registrerer når du kommer, kameraer overvåker garasjen.

0816: Går inn hovedinngangen på jobben.
Elektronisk adgangskort registrerer når du kommer, enkelte kort gjør det også mulig for andre å finne ut nøyaktig hvor du er i bygningen til enhver tid.

0822: Logger inn på datanettverket.
Systemet registrerer tidspunktet.
0829: Sender personlig e-post til venner og beskjeder til kolleger.
Begge dler kan leses av dine overordnede. Selv om du sleter beskjedene, ligger de fortsatt lagra på datamaskinens harddisk.

0905: Ringer mora di.
Arbeidsgiver kan lagre opplysninger om hvor du ringer.

1015: Bestiller flybillett.
Navnet registreres i flyselskapets database, der uvedkommende kan få tak i reisetidspunkt og sted.

1100: Låner firmabil for å dra ut et ærend.
Enkelte firmaer i utlandet har innstallert utstyr i bilene som registrerer kjørestil og kjørelengde.

1115: Stopper ved en minibankterminal for å ta ut penger.
Datasystemet registrerer detaljer om alle transaksjoner. Kameraer i maskinen eller like ved overvåker uttaket. Opptaket oppbevares i 3 måneder.

1130: Kjøper gave til en venn.
Bruk av kredittkort registreres og din kredittverdighet sjekkes med banken mens du venter. Kundekort gir bonus eller avslag på prisen. Opplysninger om din kortbruk benyttes av bankene til å lage en kredittprofil når du søker lån.

1230: Avtale hos legen.
Din legejournal vil snart inneholde en liten datachip som inneholder din totale medisinske historie. Blodprøver inneholder DNA, som i stadig større utstrekning benyttes til å avdekke genetiske og slektskapsmessige trekk. Legens diagnose må i visse tilfeller også gjøres tilgjengelige for ditt forsikringsselskap dersom du har en livs- eller invalideforsikring.

1300: Tar med resepten til apoteket.
Apoteket registrerer navn, preparat, lege og fødselsdata. Oppbevares i praksis opptil ett år. Apoteket har i dag ikke lov til å utveksle opplysninger med andre apoteker.

1330: Kommer tilbake på jobb.
Kort og overvåkingskameraer registrerer når du kommer.

1530: Møte i bedriftens sikkerhetsområde.
Går gjennom sikkerhetskontroll der all bagasje røntgen-gjennomlyses og dine fingeravtrykk scannes for å fastslå om du er den du utgir deg for.

1730: Ferdig med første utkast av rapport.
Lagrer innholdet på datamaskinen, som også kan registrere arbeidshastighet, feil som blir gjort, lengden på pauser og andre arbeidsopphold under skrivinga.

1815: Drar fra jobben.
Du registreres av datanettverket når du logger deg ut. Overvåkingskameraer og kort gir eksakt tidspunkt for når du drar fra parkeringshuset.

1830: Handler matvarer.
Kredittkort-kjøpet registreres, saldoen sjekkes mens du venter.

1845: Leier video.
Videobutikkens datamaskin lagrer fødselsnummer, adresse, telefonnummer og hvilke filmer du leier. Disse opplysningene kan benyttes til å gi deg gode tilbud med utgangspunkt i filmer du vanligvis ser, selv om dette ikke er lovlig.

1855: Fyller bensin.
Betaler med selskapets eget betalingskort, får godskrevet bonus, og registreres i systemet.

1920: Hjemme. Hører gjennom telefonbesjeder.
Svareren din har registrert hvilket telefonnummer folk har ringt deg fra. Også telefonnummeret ditt vil vises når du ringer andre, med mindre du gir beskjed til teleleverandøren.

2020: Bestiller klær gjennom postordre.
Selskapet registrerer dine personlige opplysninger og kredittkort-nummer. Mange selskaper selger informasjon til private databaser.

2030: Fornyer abbonementet på Klassekampen.
Mange aviser og blader selger rutinemessig adresselistene sine til firmaer som bruker dem til reklameutsendinger.

2035: Du blir oppringt av en markedsundersøker.
Slike firmaer samler inn opplysninger om politiske meninger, sosiale holdninger og personlige oppfatninger. Enkelte «undersøkelser» er rene salgsframstøt, der de opplysningene du gir blir lagra for senere bruk.

2100: Ringer og bestiller pizza.
Ordren registreres i pizzabakeriets datasystem, sammen med navn, adresse, telefonnummer.

2110: Logger deg inn på Internett.
All overføring av informasjon, valg av samtalegrupper, nyhetsgrupper og e-postbeskjeder kan med stor letthet avlyttes, for eksempel av politiet. Enkelte nett-servere registrerer også alle besøk. Bruker du kredittkort til varekjøp på nettet, risikerer du at andre fanger opp ditt kontonummer og misbruker det. Du kan kode beskjedene dine på Internett, men heller ikke dette er noen fullgod sikkerhetsgaranti.

- Og de personene man ikke greier å følge på denne måten, f.eks. dem som har tatt noen forholdsregler mot å bli registrert hele veien, de er i hvert fall mistenkelige, overfor dem må det i hvert fall taes noen tiltak!

Datatilsynet har siden opprettelsen i 1980 gitt konsesjon til hele 65 000 registre.
Bare i 1995 ble det gitt konsesjon til 2507 registre. Men søknadene var langt flere.

Nye kort kartlegger handlemønsteret ditt.
I disse dager (februar -97) blir 2 forskjellige rabattkort lansert på markedet, Trumf og Domino. De har begge konsesjon fra datatilsynet, og registrerer handlevaner hos brukerne. De opplysningene som kan registreres innafor disse systemene er følgende: Navn, adresse, bank- eller postkontonummer, kjønn, telefonnummer, nummer på bensin-rabattkort, mobiltelefonabbonement, alder på husstandsmedlemmer, dato for transaksjon og kvittering, brukersted, kjede, beløp, bonus og opplysninger om uttak av bonus. I og for seg uskyldige opplysninger - eller egentlig **ganske mange** opplysninger.
Disse opplysningene kan ikke, i følge konsesjonen, utleveres til andre - uten at kunden samtykker.

2. Innledning.

Hvorfor lager vi denne håndboka.

AKP har både teori og mange erfaringer på overvåkingas område.
Denne teorien og disse lærdommene vil vi gjerne dele med andre!

Vi vil ikke at kommunister skal bli engstelige eller hysteriske. Vi vil at AKP skal bli synlig og offensivt, og at vi skal pådra oss masse oppmerksomhet. Samtidig vil vi at partiet og andre progressive og revolusjonære skal ha mest mulig konkret viten om de faktiske overvåkingmulighetene som finnes, hva som møter oss når vi stikker hodet fram.

For noen vil sikkert opplysningene i denne håndboka virke overveldende og som et slag i trynet, sjøl om vi sier at dette har vi alltid visst. Det som er forskjellig fra før, er at den teknologiske utviklinga har bragt helt andre muligheter for dagen. «Storebror ser deg» er idag en teknisk, om ennå ikke en politisk realitet.

Det verste vi kan gjøre i en sånn situasjon er å bli defaitistiske, og si at her nytter det lite hva vi enn gjør, overvåka blir vi samma faen. Tvert imot må vi tenke at det nytter ikke å stoppe en bevegelse som vår med tekniske hjelpemidler. Det har aldri nytta før, og det kommer ikke til å nytte i framtida. Amerikanerne prøvde terrorisere vietnameserne til taushet ved å teppebombe dem, men vietnameserne fant løsninger, overlevde og seira. Det finnes mange flere eksempler på dette i historia.

Vi må betrakte den voldsomme utviklinga av overvåkingssystemer som nå vokser fram, særlig innafor Schengen, som et uttrykk for herskerklassens uløselige problem: De er nødt til å undertrykke folk for å overleve. Det er også et ugjendrivelig faktum at det til syvende og sist **trengs folk for å undertrykke folk**. All verdens nye teknologi kan ikke dekke over dette, sjøl om borgerskapet ønsker at vi tror noe annet.

Poenget er at vi må snu dette til vår fordel, vi må finne løsninger. Vi må lære oss å forholde oss til den nye situasjonen. I sikkerhetsarbeidet må vi være reelle, ikke rituelle. En sikkerhetspolitikk som bare er basert på ritualer vil fort kunne føre til at vi lurer oss sjøl. Vi tror vi har en sikkerhetspolitikk, men i virkeligheten har vi ingen analyse av den relle truselen. Og vi kan bare utvikle tiltak som er reelle, og ikke basert på antakelser, når vi vet hva vi skal utvikle tiltak mot. Kunnskap gir oss mulighet til å analysere den konkrete siyuasjonen og grunnlag til å ta riktige beslutninger.

Det hjelper tradisjonellt lite å stikke hodet i sanda, som materialister har vi erfaring for det. Vi vil vite hva vi har å gjøre med. Derfor denne lille håndboka. Sikkert ikke perfekt, men et forsøk på å samle det vi har av kunnskaper. Det er også muligheter for at den kan oppdateres ettersom ny kunnskap kommer for dagen. Disse kunnskapene vil vi gjerne spre, i partiet og til andre.

Som revolusjonære må vi greie to ting på en gang: Vi må drive aktivt massearbeid og propaganda, samtidig som vi må verne folk og organisasjon mot trakassering, yrkesforbud og opprulling. For å understreke hvordan vi mener at motsigelsen mellom det å være et offentlig og utadretta parti og det å være overvåka skal behandles politisk, åpner vi denne framstillinga med en politisk begrunnelse.

Hvorfor partier av AKP's type trenger et organisasjonsvern. Forholdet mellom massearbeid og sikkerhet.
Situasjonen i verden.

Verden anno 1997 er preget av hurtige endringer, hvor utviklinga går over i en råere og mer aggressiv, imperialistisk utbytting. Vi ser allerede tendenser til fascifisering og hardere maktbruk, og utviklinga gir god grobunn for rasistisk og nazistisk organisering og voldsbruk. Nynazistiske grupper er igjen i ferd med å bli en økende trusel mot progressive organisasjoner og enkeltindivider. I Norge er alle revolusjonære enige om at overvåkinga mot oss ikke er slutt. Vi må tvert imot forvente at den tiltar, den internasjonale situasjonen tilsier at partiet må være forberedt på raske endringer med hensyn til demokratiske rettigheter. Over hele verden undergraves de borgerlig-demokratiske rettighetene allerede i dag. I Norge ser vi dette bl.a. i forbindelse med konsekvensene av EØS-avtalen og forslaget om å undergrave streikeretten.

Et parti av AKP's type
Et parti av vår type, med kommunisme og sosialistisk revolusjon på programmet, som ikke er forberedt på å møte slik undertrykking, vil ikke kunne spille noen rolle i den samfunnsutviklinga vi ser foran oss. Vår bevegelse har som mål å erstatte dagens kapitalistiske system med et klasseløst, kommunistisk samfunn. Dette skal skje gjennom en sosialistisk revolusjon. Bare disse måla i seg sjøl er nok til at det er viktig for makthaverne at vi ikke vokser oss sterke.

Ved skjerpede politiske forhold som kriser, unntakstilstand og krig må vi regne med at partier av vår type, og andre revolusjonære massebevegelser vil være spesiellt utsatt for forfølgelse av ulik art. Både den relativt fredelige situasjonen vi har nå og den situasjonen vi kan se for oss i nær framtid krever av et parti av vår type at vi behersker **både** de åpne og de skjulte, de legale og de illegale arbeidsformene. Det er et dialektisk forhold mellom det ytre, utadvendte arbeidet og det indre, organisatoriske. Om hovedvekta skal ligge på den ene eller den andre sida av denne motsigelsen, avgjøres av både ytre forhold, som graden av etteretning mot oss, og av situasjonen i partiet og partiets stilling i samfunnet.

Dagens situasjon tilsier at vi må ta hensyn til begge disse forholda. På den ene sida må vi legge avgjørende vekt på å nå ut til stadig nye grupper av folk med vår revolusjonære politikk og propaganda, både for å rekruttere og for å vinne støtte for våre standpunkter. Folk må møte AKP, AKP må ut til folk, vi kan ikke bygge et parti som ikke "finnes". På den andre sida viser året som har gått, med Lund-rapport og nazi-etteretning, at vi trenger politikk, linjer og rutiner som tar sikte på å ivareta både organisasjon og folk mot trakassering, yrkesforbud og opprulling. Hvis vi ser for oss en situasjon med innskrenka borgerlig-demokratiske rettigheter tilsier også dette at vi **nå** må ta noen tiltak. Vi kan fort komme i en situasjon hvor mye kan være for seint. En del av vår sikkerhetspolitikk i dag er å lage materiell og spre informasjon om statens klassekarakter, om overvåkinga og hvordan demokratiet vi har i dag i realiteten er et diktatur som har redskaper og er klare til å gripe inn når det trengs.

Vårt viktigste vern er vår støtte i befolkninga. Både under de fredelige forhold vi har nå og under forhold med åpen undertrykking er det viktigste spørsmålet for oss at vi har mange som vi samarbeider med, og i ekstreme situasjoner, beskytter oss. Derfor må vi nå legge vekt på å bygge et ytre, utadvendt nett med kontakt med mange folk, bevegelser og organisasjoner, samtidig som vi trenger et sterkt, indre organisasjonsnett. Disse to strukturene bør holdes adskilt fra hverandre. Når den åpne virksomheten blir via stor oppmerksomhet, vil det i skyggen av dette også bli enklere for oss å bevare og bygge den indre organisasjonsstrukturen.

Lund-rapporten har avslørt at regjeringa og sentrale deler av herskereliten i Norge har hatt hele det norske maktapparatet til sin rådighet for å forsøke å kneble all opposisjon mot seg sjøl. De har benytta alle midler, "lovlige" og ulovlige, og har ikke latt noe være uprøvd. Metodene for etteretning mot en indre opposisjon og lovlig politisk virksomhet er avanserte og utvikles stadig. Den nye teknologien frambringer stadig mer sofistikerte metoder. I en sånn situasjon er det lett å bli defaitistiske og hevde at det nytter så lite hva vi gjør. Samtidig har vi satt oss som mål å gjenreise den kommunistiske bevegelsen i Norge. Hvis vi greier det vil det bety at vi blir mer interessante enn vi har vært på noen år nå. Vi vet også at innvandrerorganisasjoner er spesiellt i søkelyset nå. Det stiller krav til partiet og enkeltkamerater som arbeider i forhold til slike organisasjoner, og for disse organisasjonene sjøl.

Formålet med en sikkerhetspolitikk er ikke å gjøre en organisasjon som vår handlingslamma, snarere tvert imot. Formålet er å bevare kampkrafta, sjøl under ekstrem undertrykking fra borgerskapets side.

Dette forslaget har ikke som mål at vi skal tilbake til 70-tallet, men gjennom en diskusjon utarbeide nye retningslinjer for en nødvendig sikkerhetspolitikk som tar utgangspunkt i den politiske virkeligheten og de politiske oppgavene partiet står overfor nå, også sett i forhold til folk og bevegelser rundt oss. Samtidig som vi tar vare på de åpenbart helt riktige sidene ved den sikkerhetspolitikken som ble utarbeida på 70-tallet. Med et modent og voksent parti som vi nå har blitt, er det fullt mulig å kvitte seg med barnesykdommene.

Vi tror ikke på dem som sier at overvåkinga mot oss er slutt men at den fortsetter, muligens med andre typer begrunnelser. Når overvåkingspolitiet sier at «ingen personer er overvåka» mener de at det ikke opprettes nye personsaker i personregisteret. Det er ingenting i situasjonen som tilsier at vi bør føle oss sikre på at de ikke vil opprette nye personsaker i tida framover. Men i tillegg til personregister opererer de med både emneregister og arbeidsregister som brukes som tidligere. Det sto 8100 navn i personregisteret når Lund-kommisjonen avslutta arbeidet sitt.

Målet med en sikkerhetspolitikk må være å gjøre oppgaven for overvåkerne så vanskelig som mulig. Det vil si å skaffe dem mest mulig hodebry ved hjelp av enkle tiltak som bruk av dekknavn osv. De innrømmer sjøl i Lund-rapporten at overvåkinga av oss har vært «mer sporadisk og tilfeldig enn for NKP».

Et eksempel: Det at Lund-rapporten inneholder lite oplysninger som tyder på at AKP's landsmøter har vært overvåka, kan bety to ting: Enten at de ikke har greid å skaffe seg opplysninger om dem, eller at de ikke ser det som opportunt å gå ut med slike opplysninger. Det kan imidlertid herske liten tvil om at landsmøtene våre må ha vært interessante, både i forhold til å kartlegge organisasjonen og å få kunnskap om enkeltpersoner. I tillegg til hensynet til organisasjonsvernet skal landsmøtene være hemmelige også fordi det er en demokratisk rett for alle partimedlemmer å delta på landsmøtene, sjøl om de ikke kan framstå som offentlig kjente medlemmer. Vi vil også ha retten til å si og mene hva vi vil på landsmøtene, uten innsyn fra utenforstående. Det er også dokumentert i Lund-rapporten at det har vært og er et poeng i seg sjøl å følge med i den politiske utviklinga til partiet, for om mulig å finne bekreftelse på at det er nødvendig og riktig å overvåke oss.

En god masselinje vil til alle tider være vårt viktigste vern. Partilag og enkeltkamerater må operere slik at de svømmer som fisken i vannet. Det vil si å delta aktivt i klassekampen, knytte nære forbindelser til arbeidskamerater og naboer og utnytte de demokratiske frihetene til å fremme folkets kamp, sammen med folk. Men hvis det skal være hovedlinja i sikkerhetsarbeidet vårt betinger det for det første at vi **har** en masselinje, og for det andre at vi har en rett forståelse av hva masselinje er, hvilken betydning masselinja har i et revolusjonært perspektiv, hva masselinja skal brukes til.

Hvis vi legger all vekt på at massene skal beskytte oss, uten å ta tiltak på å verne organisasjonen, kan vi også havne i en ugunstig situasjon under skjerpede forhold. Uansett om partiet har en god og korrekt masselinje, vil det være behov for en **særegen** politikk for vern av organisasjonen, om linjer, forbindelser, ledelse og struktur. Dette forslaget handler ikke om vårt eksterne arbeid, men hvordan alle medlemmer og organer i partiet kan bidra til å verne det vi **vil** verne, vårt indre-organisatoriske arbeid. Det handler om å heve bevisstheten gjennom diskusjon - i løpet av de siste åra har vi kommet ut av trening med å tenke sikkerhet - gjennom å ta i bruk fantasi og skaperevne for å gjøre de små tinga som gjør det vanskeligere for overvåkerne å overvåke oss.

Organisasjonsvern må være både et kollektivt og individuellt ansvar, slik at en glipp ikke ødelegger for andre. Selv om "sikkerhet aldri blir bedre enn det svakeste leddet", er det det **alle** gjør feil **hele tida** som er den største risikoen. Det ligger i formuleringa at hvis **en del** av organisasjonen gjør systematisk feil, kan dette gi innsyn i resten av organisasjonen. Hvis en eller noen få gjør feil, behøver det ikke å være katastrofalt hvis 99% er riktig. Den daglige praksisen er viktigst. Å ta for lett på disse ulike truslene kan få alvorlige konsekvenser både for enkeltmedlemmer og partiet som sådan. Dette er hovedgrunnen til at vi har behov for retningslinjer som dette. Med det siste årets avsløringer og overvåkingsskandaler vil vi offentlig kunne hevde at AKP har rett til et organisasjonsvern.

3. Hva sier Lundrapporten.

Alle avsnitt er sitater fra rapporten.

Fra kapitel 2.2.6, s. 17 ff.
Romavlytting.
Romavlytting med tekniske hjelpemidler har vært ulovlig i hele granskingsperioden. Etter vedtakelsen av straffelovens § 145 a i 1958 har det i seg selv vært straffbart. Tidligere kunne romavlytting i det offentliges regi eventuelt straffes som tjenesteforsømmelse. Kommisjonens undersøkelser har avdekket at Politiets overvåkingsstjeneste i 1950-årene avlyttet kommunistmøter og i 1960-årene også annen venstreradikal møtevirksomhet, dels ved faste avlyttingsopplegg på steder hvor møter jevnlig ble holdt, dels ved enkeltstående avlyttingsoperasjoner.

I begynnelsen av 1950-årene etablerte overvåkingstjenesten et fast opplegg for avlytting av Folkets Hus i Oslo. Også andre steder i Oslo ble kommunistmøter avlyttet på 1950-tallet

Det må antas at medlemmene i Koordineringsutvalget tidvis har gitt sine foresatte generell informasjon om virksomheten. Dette må antas selv om det, som blant annet påpekt for kommisjonen av et medlem av Koordineringsutvalget, nok kunne hende at medlemmene har skjermet sine politiske foresatte mot opplysninger som kunne være konstitusjonelt eller politisk belastende. I den utstrekning dette er skjedd har de politiske myndigheter vært innforstått med det. Det innebærer i så fall at de har valgt å lukke øynene for en virksomhet de hadde styrings- og kontrollansvar for, med den følge at ansvaret er blitt misligholdt. Dette fritar dem således ikke for kritikk.

Når det gjelder romavlyttingsvirksomheten fra 1955 frem til slutten av 1960-årene, har kommisjonen ikke funnet å kunne utelukke at regjeringsmedlemmer fra tid til annen har fått kjennskap til eller mistanke om at avlyttingsvirksomhet fremdeles forekom. Den kjenner i alle fall til at ett slikt tilfelle ble gjort kjent for Koordineringsutvalget. Kommisjonen har pekt på at landets politiske ledelse gjennom sine holdninger opprinnelig skapte en oppfatning i de hemmelige tjenester om at slik virksomhet kunne aksepteres og at det derfor er rimelig å plassere et medansvar for virksomheten i denne ledelsen, i første rekke hos statsministeren.

Etter 1958, da avlyttingsvirksomheten ble gjort straffbar, må den politiske ledelse etter hvert ha hatt rimelig grunn til å regne med at all slik virksomhet var avsluttet.

Kommisjonen har funnet noen få tilfeller hvor ulovlig romavlytting har vært rettet mot individuelle norske borgere, men ser ikke bort fra at det kan ha vært flere.

Telefonkontroll.

Etter forskriften av august 1960, kreves *rettens samtykke* for å iverksette telefonkontroll. Kontroll kan bare iverksettes overfor *personer* som *med grunn mistenkes* for å ha *begått nærmere angitte straffbare handlinger* og bare når kontrollen er *påkrevet av hensyn til rikets sikkerhet*.

Fra kapitel 9.4.1.1 - s. 300 ff.
Post-, telegram- og telefonkontroll.

Etter straffelovens § 145, jf § 122 er det forbudt å bryte andres brev eller lukkete skrifter eller bane seg adgang til andres låste gjemmer. Straffelovens § 116 retter seg blant annet mot offentlige tjenestemenn som foretar ulovlig beslagleggelse av brev eller telegrammer. I straffelovens § 145 a, som ble tilføyd ved lov av 12. desember 1958, er det satt forbud mot, ved hjelp av tekniske innretninger, å avlytte eller gjøre opptak av samtaler eller lukkete møter man ikke selv deltar i. Disse forbudene gjelder også for politiet, med mindre det er gitt samtykke i henhold til lov om kontroll med post- og telegrafforsendelser og med telefonsamtaler av 24. juni 1915 nr 5 med tilhørende forskrifter. Loven fikk sin nåværende form i 1950, da kontroll med telefonsamtaler ble tilføyet. Etter lovens § 1 kan Kongen eller den han gir fullmakt utferdige bestemmelser om kontroll når dette anses påkrevd av hensyn til rikets sikkerhet. Men utenfor krigstid kan det bare iverksettes kontroll overfor *personer* som mistenkes for *overtredelse* av lovbestemmelser til vern om rikets sikkerhet. Lovbestemmelsene er de samme som er nevnt i overvåkingsinstruksen. Mistanke om at noe ulovlig *planlegges eller forberedes* er således ikke nok, med mindre forberedelseshandlingen i seg selv er gjort straffbar. Loven hjemler ikke kontroll av organisasjoner.

Ved kgl res av 27. august 1915 ble det i henhold til loven av 1915 gitt bestemmelser om undersøkelse og tilbakeholdelse av postforsendelser og telegrammer, jf. nærmere under 9.6.3.1.
Forskriften var gjeldende for kontroll av post og telegrammer helt til den ble avløst ved forskrift gitt ved kgl res av 19. august 1960 om post-, telegram- og telefonkontroll. Før dette tidspunkt forelå ingen forskrift om telefonkontroll, og slik kontroll var da - etter 1958 - i prinsippet straffbar etter straffelovens § 145 a. Inntil denne bestemmelsen ble gitt, må det legges til grunn at telefonkontroll var ulovlig som stridende mot legalitetsprinsippet, jf om den rettslige synsvinkel under 6.2.4. Dessuten ville telefonavlytting i offentlig regi kunne straffes som tjenesteforsømmelse, jf straffelovens kapittel 33.

Det er for øvrig gitt generelle regler om postkontroll i straffeprosesslovens §§ 211 og 212.

Loven av 1915 og forskriften av 1960 må i lys av den teknologiske utvikling forstås slik at alt telesamband kan avlyttes, hva enten det er linjebasert eller ikke og uavhengig av om det er naturlig å se det som samtale eller telegram. Også telefax må f eks kunne avlyttes.

Etter forskriften av 1960 må politiet innhente rettens samtykke til å iverksette telefonavlytting eller post- og telegramkontroll. I særlig påtrengende tilfelle kan kontroll settes i verk etter beslutning av påtalemyndigheten. Dette må i så fall straks meddeles retten som avgjør om kontrollen skal opprettholdes. Beslutningen skal angi en tidsbegrensning for kontrollen, men hverken loven eller forskriftene setter grenser for varigheten. Kontrollen skal holdes hemmelig for den som overvåkes, og det blir ikke oppnevnt advokat for ham.

Videre fra kapitel 2.2.6.
Kommisjonen har ikke funnet tilfelle der telefonkontroll er iverksatt overfor norske borgere uten forhørsrettens samtykke etter august 1960. I denne perioden er det truffet et meget stort antall beslutninger om telefonkontroll av norske borgere. Etter lovgrunnlaget kan telefonkontroll bare brukes som ledd i etterforskingen av begåtte straffbare handlinger. Likevel er kontroll bare i noen ytterst få tilfeller besluttet overfor personer som siden er satt under tiltale. Kommisjonens gjennomgang av praksis viser at telefonkontroll i svært mange tilfeller er besluttet uten at lovens vilkår har vært oppfylt.
Kommisjonen har sett nærmere på grunnlaget for telefonkontroll der beslutningene omfatter rett til å kontrollere samtaler på telefoner som innehas av organisasjoner med politisk tilsnitt, i første rekke i Oslo, Bergen, Trondheim og Tromsø. I hovedsak er følgende kontroller grunnlag for kommisjonens vurderinger:

* Kontortelefonene til AKP (m-l) i Oslo ble avlyttet fra 1975 til 1979. Beslutningene var knyttet til tre personer, mistenkt for overtredelse av straffelovens § 97 a.
* AKP (m-l)s kontortelefoner ble igjen avlyttet fra 1982 til 1987. Kontrollen var suksessivt knyttet til to personer, mistenkt for overtredelse av straffelovens §§ 94, 98, 104 a og 134.
* Avisen Klassekampens kontortelefon i Oslo ble avlyttet fra 1976 til 1979. Kontrollen var knyttet til én person med grunnlag i mistanke om overtredelse av straffelovens
§ 97 a.
* Kontortelefonen til Norges Kommunistiske Parti i Oslo ble avlyttet fra 1986 til 1989. Avlyttingen var suksessivt knyttet til to personer mistenkt for overtredelse av straffelovens § 97 a.
* Kontortelefonen til AKP(m-l) i Bergen ble avlyttet fra 1975 til 1979. Kontrollen var suksessivt knyttet til to personer mistenkt for overtredelse av straffelovens §§ 98 og
104 a.
* I Trondheim ble kontoret til Oktober Forlag avlyttet fra 1973 til 1979 med ca et års avbrudd i 1974-75 og AKP(m-l)s kontortelefon fra 1976 til 1979. Mistanken var dels samtidig, dels suksessivt knyttet til flere personer mistenkt for overtredelse av straffelovens §§ 98 og 104 a.

Kommisjonen har som utgangspunkt for sine vurderinger blant annet understreket at telefonavlytting og brevkontroll er meget inngripende etterforskingsmetoder som holdes hemmelig for den de retter seg mot. At vedkommende ikke gis adgang til å ta til gjenmæle, stiller særlige krav til rettens kontroll og saksbehandling. Dreier det seg om avlytting av kontortelefoner til politiske partier, støter avlyttingen ikke bare an mot personvernhensyn, men også mot det grunnleggende demokratiske prinsipp om fritt å kunne drive politisk virksomhet. Ved avlytting av avisredaksjoner aktualiseres forholdet til informasjonsfriheten og avisens rett til beskyttelse av sine kilder.

Etter loven kreves at kontrollen må være *påkrevet* av hensyn til rikets sikkerhet. Ikke enhver overtredelse av de bestemmelser det henvises til i loven og forskriftene innebærer en fare for rikets sikkerhet. Jo lenger kontrollen varer, jo strengere krav må stilles til påvisningen av at kontrollen fortsatt er nødvendig av hensyn til rikets sikkerhet.

Telefonkontroll kan ikke brukes som *forebyggende overvåkingstiltak* rettet mot personer eller organisasjoner med sikte på å klarlegge om det forberedes straffbare handlinger eller annen virksomhet som er relevant etter overvåkingsinstruksen.

Kommisjonens undersøkelser har vist at forhørsrettens beslutninger gjennomgående er svært utilfredsstillende. Langt de fleste beslutninger er standardbeslutninger. De inneholder utelukkende en henvisning til eller en helt korfattet gjengivelse av overvåkingspolitiets begjæring og den begrunnelse som der fremgår, fastslår at kontrollen er påkrevet av hensyn til rikets sikkerhet og at den skjer for å fremskaffe bevis i straffesak. Det er lite tilfredsstillende at beslutninger av en så inngripende karakter treffes i form av standardbeslutninger som ikke viser at retten foretar en selvstendig og individuell vurdering av hvert enkelt tilfelle. De straffbare forhold som angis i politiets begjæringer, og som standardbeslutningene henviser til, er i regelen svært lite konkrete og ikke nærmere underbygde. På tross av dette forekommer det så å si ikke at rettens beslutninger inneholder selvstendige vurderinger, selv ikke når det i år etter år gis samtykke til at kontrollen foregår uten at det kan ses å være fremkommet noe som i nevneverdig grad er egnet til å styrke mistanken.

Tidligere overvåkingssjef Jostein Erstad har for kommisjonen gitt uttrykk for at forhørsrettens begrunnelse

> "ofte [hadde] preg av standardformuleringer. Generelt vil Erstad si at det var svært så lett, kanskje for lett, å få rettens medhold i begjæringer om telefonkontroll. Han husker bare et par avslag, ett fra Oslo og ett fra i Vestfold"

Erstad var overvåkingssjef fra 1982 til 1990. Ikke i noen av de saker kommisjonen har gjennomgått om avlytting av kontortelefonene til politiske organisasjoner mv har forhørsretten - med ett nokså spesielt unntak - nektet å ta en begjæring til følge. Bare i ett av disse tilfellene ble telefonkontrollen nedkoblet på grunn av rettens holdning.

For øvrig har kommisjonen pekt på at saksbehandlingen ved Oslo forhørsrett inneholder elementer som er rettssikkerhetsmessig lite betryggende. Beslutningene blir i Oslo truffet i Overvåkingssentralens lokaler. Rettsprotokollen med forhørsrettens standardbeslutning er regulært utskrevet på forhånd av overvåkingspolitiet. Justitiarius i Oslo byrett ga i slutten av 1980-årene uttrykk for at telefonkontroll ikke kunne brukes som en passiv overvåkingsmetode, men at det i tillegg måtte foretas andre etterforskingsskritt. Det er uklart for kommisjonen om dette innebærer noen endring i senere års praksis, som ikke er inngående undersøkt av kommisjonen. Fremdeles er imidlertid saksbehandlingen ved Oslo byrett den samme. Kommisjonen har funnet at forhørsrettenes kontroll ikke har fungert som den rettssikkerhetsgaranti den var ment å være.

Telefonavlytting har, i strid med lovgrunnlaget, vært sett som en mulighet til å følge med i organisasjonens virksomhet - med det overvåkingsmessige siktepunkt å klarlegge om noe ulovlig kunne være under forberedelse. Denne realitet synes forhørsrettene å måtte ha vært innforstått med.

Det er på det rene at overvåkingstjenesten har sett telefonkontroll av politiske partier og organisasjoner som en hensiktsmessig metode for å skaffe seg opplysninger om virksomheten, om ledere, om medlemmer og sympatisører mv, opplysninger av generell overvåkingsmessig interesse. Dette blir enda klarere når man tar i betraktning tjenestens omfattende registrering av overskuddsinformasjon fra telefonkontroll.

Registrering av overskuddsinformasjon fra telefonkontrollvirksomheten.
Etter § 3 i forskriftene om telefonkontroll av august 1960 har overvåkingstjenesten ikke adgang til å registrere opplysninger som er uten betydning for etterforsking av straffbare forhold, men som utelukkende er av overvåkingsmessig interesse eller er av betydning for personkontrolltjenesten.

Kommisjonens undersøkelser viser at tjenesten ikke har oppfattet bestemmelsen i § 3 som en begrensing i adgangen til registrering av overskuddsinformasjon. Oppfatningen har vært at enhver opplysning fra telefonkontroll har kunnet nedtegnes hvis den har vært av interesse for tjenesten. Opplysninger av politisk karakter, om personer eller organisasjoners virksomhet, er i betydelig utstrekning nedtegnet på grunnlag av informasjon fra telefonkontroll. Dette gjelder også avlyttete samtaler hvor den som er under etterforsking ikke selv deltar. I mange tilfeller er det for øvrig nedtegnet informasjon fra telefonkontroll som vanskelig kan ses å ha noen som helst betydning for tjenesten. Kommisjonen har antatt at mangel på kritisk holdning til hvilke opplysninger som oppbevares og manglende rutiner for makulering av betydningsløs informasjon, i mange tilfeller har ført til at opplysninger er blitt oppbevart.

Ransaking, beslag og beslaglignende tiltak.
Ransaking og beslag er straffeprosessuelle tvangsmidler, som skal gjøres kjent for den de retter seg mot. Hemmelig ransaking og beslag er forbudt.

Kommisjonen har kommet over noen, men ikke mange tilfeller av ulovlig ransaking av hus eller husrom.

Derimot er det funnet mange tilfeller av ulovlig beslag, foretatt hos personer med tilknytning til AKP(m-l) og NKP. Beslagene er skjedd i forbindelse med legale etterforskingstiltak - ransakinger, undersøkelser etter sprengninger, brann mv - med eller uten tilknytning til spørsmål som gjelder rikets sikkerhet. Materiale som ikke er av betydning som bevis for straffbare forhold, er overskuddsinformasjon . Dette kan ikke beslaglegges og skal leveres tilbake hvis det i første omgang er tatt med for gjennomsyn. Likevel er slike opplysninger i mange tilfeller blitt formidlet til overvåkingstjenesten i form av kopiering oa, eventuelt slik at dette er gjort av overvåkingspolitiet selv etter å ha blitt tilkalt av det ordinære politi.

Også dokumenter politiet har kommet over ved utførelse av rent ordensmessige oppgaver er i flere tilfeller ulovlig kopiert og registrert i overvåkingstjenestens arkiver. Dette gjelder f eks dokumenter som er funnet i vesker mv innbrakt som hittegods.

Opplysninger fra søknader om politiske demonstrasjoner, plakatbukk mv og opplysninger fra flyplassregistrering av reisende til kommuniststyrte land, er i stor utstrekning formidlet videre til overvåkingspolitiet og registrert der.

Overvåkingstjenesten unnlater for øvrig å varsle kontoinnehaver når banker pålegges å utlevere kontoopplysninger i henhold til straffeprosesslovens § 210. Dette er ulovlig. Kommisjonen har også sett eksempler på at denne ulovlige praksis har støtte i beslutning av forhørsretten.

Bruk av andre overvåkingstiltak.
I 1970 ble det ved rundskriv utferdiget av overvåkingssjefen i samråd med justisministeren, slått fast at politisk virksomhet *i seg selv* ikke kunne gi grunnlag for aktive overvåkingstiltak.

Kommisjonen har antatt at det på 1970-tallet som utgangspunkt ikke var instruksstridig at overvåkingstjenesten søkte å kartlegge ml-bevegelsens organisasjoner og medlemmer ved bruk av spaning og informanter. Kommisjonen kan likevel ikke se at den omfattende og systematiske bruk av informanter ved skolene med sikte på registrering av skoleelever helt ned på ungdomsskoletrinnet, var forsvarlig innenfor instruksverkets rammer.

På 1980-tallet var bruken av aktive tiltak mot ml-bevegelsen sterkt redusert. Den opphørte imidlertid ikke, selv ikke i forhold til vanlige medlemmer. Kommisjonen har funnet det kritikkverdig at spaning så sent som i 1986 ble brukt mot AKP(m-l)s sommerleirer med sikte på identifikasjon av deltakere.

Kommisjonen har gitt uttrykk for at ml-bevegelsen var blitt fulgt meget nøye av overvåkingstjenesten i mer enn ti år, uten at det i den tiden var fremkommet opplysninger som bestyrket mistanken om at væpnet revolusjon var under forberedelse. På denne bakgrunn ville det vært naturlig å vente at Overvåkingssentralen hadde utarbeidet en analyse av den sikkerhetstrussel partiet eventuelt fortsatt representerte, og hvilken virksomhet dette i så fall ga grunnlag for fra tjenestens side. Kommisjonen kan ikke se at en slik analyse ble utarbeidet på noe tidspunkt. Virksomheten gir tvert imot inntrykk av mangel på overordnet analyse og styring.

Fra kapitel 8.4.5.4 - s. 219 ff.
Overvåking.

(Konkret om SUF og AKPml).

Romavlytting
Det er grunn til å tro at SUF-møter som ble holdt i Folkets Hus ble romavlyttet på slutten av 1960-tallet. Kommisjonen har funnet et udatert notat fra "E" til "R.B". Kommisjonen legger til grunn at E er Erik Næss og RB er Ronald Bye. Notatet omhandler personer som ventelig vil bli foreslått som medlemmer i sentralstyret på det kommende landsmøtet i SUF. Ut fra notatets utforming og innhold kan man med høy grad av sannsynlighet konstatere at notatet bygger på romavlytting. Notatet er mest sannsynlig fra 1968.

Telefonkontroll
Telefonkontroll har pågått i flere perioder og flere steder i landet. Selv om rettens beslutninger, slik loven og forskriften krever, rettet seg mot personer, har kontrollen av kontortelefoner medført at overvåkingstjenesten har kunnet følge med på virksomheten blant annet til AKP(m-l), Oktober og Klassekampen.

Oslo
Telefonen til *AKP(m-l)s partikontor* i Oslo ble avlyttet fra juli 1975 til desember 1979 og fra desember 1982 til august 1987. Rettens beslutninger ble gitt for seks måneder om gangen og omfattet flere personer.

I den første perioden gjaldt mistanken overtredelse av straffeloven § 97 a, som forbyr nordmenn å ta i mot økonomisk støtte fra fremmed makt mv "for å påvirke allmennhetens mening om statens styreform eller utenrikspolitikk eller til partiformål". Oslo forhørsretts beslutninger gjaldt flere personer som var tilknyttet partikontoret. I den opprinnelige begjæringen om telefonkontroll vises til at de to mistenkte under konspirative omstendigheter hadde hatt kontakt med en utenlandsk statsborger. Denne skulle i sitt eget land

jevnlig ha mottatt betydelige pengebeløp fra den kinesiske ambassade til subsidiering av marxist-leninistiske grupper, som han var sekretær for.

Fra desember 1982 til august 1987 ble partiets kontortelefoner igjen avlyttet. Rettens beslutninger var suksessivt knyttet til to personer, som hadde sitt virke ved partikontoret. Beslutningene omfattet også kontroll av post og telegrammer. Den første beslutningen, som er av 10. desember 1982, inneholder en henvisning til straffelovens § 98 og 104 a, som tidligere hadde blitt benyttet som grunnlag for å avlytte AKP(m-l)s kontorer i Trondheim og Bergen, jf nedenfor. I tillegg vises det til §§ 94 og 134. Om straffebestemmelsene vises til 6.3.3 foran.

Partiets og nærstående organisasjoners kontorer hadde vært avlyttet i årevis på 1970-tallet uten at det var fremkommet bevis for en ulovlig virksomhet som gjorde det nødvendig å gripe inn av hensyn til rikets sikkerhet. På denne bakgrunn ville det ha vært naturlig å vente at Overvåkingssentralen ga en nærmere redegjørelse for hvorfor det nå igjen var nødvendig av hensyn til rikets sikkerhet å etterforske ledere i partiet gjennom avlytting av deres egne og partikontorets telefoner. Noen slik redegjørelse ble ikke gitt.

I begjæringen fra Overvåkingssentralen anføres som grunnlag at AKP(m-l) "i sitt prinsipp-program har uttalt seg om forhold som blant annet må tolkes som forberedelse til og/eller overtredelse av straffelovens kap. 9 og kap. 12". Det eneste nye som fremkommer er dette:

> "Væpnede aksjoner har ikke vært gjennomført i vårt land av AKP(m-l). Likevel er det på det rene at det var to sympatisører/medlemmer som sto bak sprengningsforsøket av en bro over Tverrelva i Finnmark den 20. mars d.å. Partiledelsen i AKP(m-l) gav full støtte til handlingen, og partiets avis Klassekampen, kjente saken før politiet fikk melding om den."

I begjæringen vises til at partiet har et betydelig antall aktivister, og at partiet søker å hemmeligholde sin organisasjon, sitt lederapparat og sitt medlemstall. Det ble ansett nødvendig å få oversikt over partiapparatet, tillitsmennene og partiets generelle virksomhet. Det fremheves at den personen begjæringen rettet seg mot, er sentral i partiet.

Vedlagt begjæringen var et notat fra en tjenestemann som hadde arbeidet med saksfeltet i omkring to år. Notatet anfører en rekke forhold som man ved Overvåkingssentralen hadde antatt i årevis, således at

- partiet gikk inn for væpnet revolusjon
- partiet drev subversjonsvirksomhet, infiltrerte næringslivet og skapte uro
- partiet gikk inn for såkalt politisk militærtjeneste, medlemmene skulle avtjene verneplikt, lære våpenbruk mv

I notatet gis videre uttrykk for at "en anser at det er en god grunn til å anta at AKP-erne vil komme til å infiltrere institusjoner som befalsskoler, krigsskoler, Heimevernet samt skytterorganisasjoner".

Etter hvert dukket også § 97 a opp i begjæringene. Det anføres tidligere å ha vært indikasjoner på at partiet mottok økonomisk støtte fra fremmed makt, og det var kommet opplysninger om at en giver som kalte seg "Østen er rød" hadde gitt 100.000 kr til bevegelsen. Dessuten var det oppgitt en adresse som ikke eksisterte. Forhørsrettens beslutninger viser til begjæringene.
I februar 1986 ble kontrollen knyttet til en ny person ved partikontoret. Grunnlaget var så å si identisk med tidligere. I begjæringene hevdes personen å være nøkkelmannen bak partiets militærpolitiske program og tesen om "væpna revolusjon". Forhørsrettens beslutninger henviser utelukkende til politiets begjæringer.

Overvåkingssjef Jostein Erstad har forklart for kommisjonen

> "at begrunnelsen i det alt vesentlige var programposten om væpnet revolusjon. Når det gjaldt grunnlag for mistanke ut over dette, skulle det svært lite til. Erstad kan ikke i dag erindre hvilke konkrete omstendigheter som ble anført som grunnlag for mistanke i tillegg til den generelle henvisnngen til væpnet revolusjon."

Ved telefonavlyttingen kom det ikke frem opplysninger i nevneverdig grad som styrket mistanken om straffbare forhold. Avlyttingen av partikontoret medførte at overvåkingspolitiet fikk bedre oversikt over AKP(m-l)s ledelse, virksomhet og internasjonale forbindelser enn man tidligere hadde hatt. Gjennom avlyttingen fikk man også god oversikt over personer med tilknytning til partiet.

Rød Ungdoms kontor ble avlyttet fra juli 1975 til desember 1979. Grunnlaget for rettens beslutning var mistanke om overtredelse av straffeloven § 97 a.

Telefonen til *Klassekampens redaksjon* i Oslo ble avlyttet fra desember 1976 til desember 1979. Rettens beslutning rettet seg mot flere personer. Mistanken gjaldt overtredelse av straffeloven § 97 a. Det faktiske grunnlaget var så å si identisk med grunnlaget for beslutningen om avlytting av partikontoret. Det var mistanke om kontakt med den utenlandske statsborger som der er omtalt. Ved telefonkontrollen fremkom det ikke noe som støttet mistanken, men det kan ikke ses at forhørsretten har vurdert dette ved begjæringene om forlengelser. Kontrollen ble nedkoblet i desember 1979 etter beslutning fra overvåkingspolitiet.

Gjennom denne avlyttingen oppnådde overvåkingstjenesten innsyn i avisens virksomhet. Telefonkontrollen gjorde det også lettere for tjenesten å ha oversikt over kommisjonærer og abonnenter ved at alle henvendelser til avisen ble registrert. Telefonkontroll av avisredaksjoner reiser særlige betenkeligheter. Telefonen til *Oktober Forlag* har vært avlyttet fra juli 1975 til desember 1979. Grunnlaget var det samme som angitt ovenfor vedrørende avlytting av Klassekampen.

Bergen
Telefonen til AKP(m-l)s kontor i Bergen ble avlyttet i tidsrommet fra desember 1975 til desember 1976. Grunnlaget var mistanke om overtredelse av straffeloven §§ 98 og 104 a. Det ble blant annet vist til at den person beslutningen gjaldt, var fremtredende medlem av AKP(m-l), styremedlem i Rød Front og at han aktivt gikk inn for organisasjonens program med "voldelig overgang til sosialisme".

Videre ble kontoret avlyttet i perioden fra januar 1977 til desember 1979. Beslutningen rettet seg nå mot en annen person. Begjæringen om telefonkontroll var grunngitt med at han var en av partiets fremste ideologer og aktivt gikk inn for organisasjonens program om voldelig overgang til sosialisme. Han hadde tillitsverv i partiet.

På et distriktssentralmøte i 1973 ble det sitert fra et brev som var sendt til Oktober bokhandel i Bergen. Etter det kommisjonen kan se har det ikke foreligget rettslig beslutning om brevkontroll på denne tiden. Det er uklart hvorledes brevet har kommet overvåkingstjenesten i hende.

Trondheim
I Trondheim pågikk telefonavlytting det meste av perioden fra juli 1973 til november 1979. Avlyttingen omfattet AKP(m-l)s kontor og Oktober bokhandel. Beslutningene gjaldt flere personer. AKP(m-l)s kontor synes å ha blitt avlyttet fra februar 1976 til november 1979. Oktober Bokhandel ble avlyttet fra juli 1973 til januar 1974 og fra april 1975 til september 1979.

Grunnlaget var for alle personer mistanke om overtredelse av straffeloven §§ 98 og 104 a. Til illustrasjon nevnes rettens beslutning i 1975 om kontroll av telefonen til Oktober bokhandel. Denne beslutningen rettet seg mot to personer. Retten viste til at den ene aktivt gikk inn for AKP(m-l)s program om væpnet revolusjon. Den andre ble antatt å være en av topplederne i ml-bevegelsen i Trøndelag, som man mistenkte for å drive våpenøvelser. Oktober bokhandel fungerte etter rettens oppfatning som sentral og kontaktsted/kontor for all ml-virksomhet i Trøndelag. Det var her planlegging av demonstrasjoner foregikk og materiell til demonstrasjoner ble til. Retten mente på dette grunnlag at telefonkontroll mot dem begge var påkrevd av hensyn til rikets sikkerhet.

Ulovlig beslag.

Kommisjonen har under granskingen funnet flere tilfeller av ulovlig beslag.
Et vilkår for beslag av dokumenter er at dokumentene har betydning som bevis for en straffbar handling, jf strpl § 203. Den som beslaget rammer, skal varsles om dette, jf strpl § 205 jf § 200. Medmindre det foreligger beslutning om brevkontroll etter 1915-loven, kommer kopiering av dokumenter i samme stilling som beslag. Beslag i strid med disse regler er bare tillatt dersom vilkårene for nødrett foreligger.

Et klart tilfelle av ulovlig beslag skjedde under etterforskingen av sprengningen av Oktober bokhandel i Tromsø den 20. mars 1977. I forbindelse med at politiet gjennomgikk bokhandelen etter eksplosjonen, fant man postkvitteringer og flere lister med navn på personer som hadde kjøpt bøker, eller som var abonnenter på publikasjoner som ble forhandlet gjennom bokhandelen. Overvåkingspolitiet sikret seg disse dokumentene. Opplysningene ble registrert på sak.

I februar 1971 gjennomførte politiet ransaking og beslag hos en vernepliktig ved Evjemoen. Grunnlaget for ransakingen var en siktelse i narkotikasak. Under ransakingen og etterfølgende avhør kom det frem at han var medlem av SUF. I notat datert 19. februar 1971 skriver en tjenestemann som deltok ved ransakingen:

> "Mens ransakingen foregikk tillot jeg meg å "låne" et brev dat. Oslo 25.1.71 til "kamerat" og undertegnet "Chau". Brevet ble lyskopiert og lagt tilbake. Ingenting ble beslaglagt. Av brevet fremgår

at "SUF" har sympatisører og kontakter på Evjemoen, Gimlemoen, Kjevik, Odderøya, Moseidmoen (?) og i Kr.sand. Flg navn er nevnt: ..."

Brevet omhandler revolusjonært arbeid i Forsvaret. Fra brevet gjengis:

> "Vi har nå drevet arbeid i militæret i ett og ett halvt år. Den første tida var prega av forsiktige undersøkelser, innsamling av erfaringer mht massearbeid, sikkerheten o.s.v. I løpet av fjoråra endret arbeidet karakter - vi gikk fram til å lede til dels store og høgt utvikla massekamper og vant ei rekke grunnleggende erfaringer for arbeidet framover. Vi lærte at de objektive forholda for revolusjonært arbeid i det militæret er meget gode, at massene raskt reiser seg til kamp under vår ledelse. Vi lærte at det er oss massene setter sin lit til i kampene og når klassefienden setter inn sine angrep. Og vi lærte at massene fullt ut er villige til å beskytte sine revolusjonære kamerater på grunnlag av vår propaganda om sikkerheten og nødvendigheten av å beskytte den ledende kjernen mot angrep fra offiserene. De progressive massene både i og utafor det militære slutter stadig sterkere opp om vår politikk og kommer til oss for råd og vegledning. Mulighetene for nye framstøt på det militærpolitiske området er absolutt gode."

Deretter gir brevet opplysninger om medlemmer i SUF(m-l) og sympatisører ved forskjellige forsvarsanlegg i distriktet. Overvåkingstjenesten sendte kopi av brevet til flere enheter i Forsvaret. Denne mistanken om undergravingsvirksomhet ledet til en større aksjon våren 1971, hvor både brevkontroll og spaning ble brukt.

Det finnes også flere andre eksempler fra 1970-tallet og første halvdel av 1980-tallet på ulovlige beslag gjort under lovlig ransaking.

I flere tilfeller har dokumenter i vesker innlevert til politiet som hittegods blitt gjennomgått av overvåkingstjenesten. Dokumentene er kopiert eller opplysninger notert. Her skal nevnes et par eksempler:

I oktober 1968 gjennomgikk Bergen politikammer innholdet av en veske som var innlevert som hittegods. Det viste seg at eieren var tilknyttet SUF(m-l). I vesken lå blant annet lister med deltakere på studieringer og oversikt over personer som solgte materiell. Dokumentene ble kopiert og oversendt Overvåkingssentralen.

I 1972 glemte en soldat igjen en veske på bussen. I tillegg til klær, bøker mv inneholdt vesken et brev fra en kamerat, et sjekkhefte og en notisbok. Dokumentene viste at soldaten var medlem av SUF(m-l). Brevet ble kopiert. Notisboken ble beholdt og skrevet av, og overvåkingstjenesten innhentet nærmere opplysninger blant annet om personer som var nevnt i notisboken. Opplysningene i noteringsheftet som lå ved sjekkheftet, ble skrevet av og nøye gjennomgått.

Spaning og aktiv bruk av informanter

Søknader til politiet om tillatelse til å holde stands eller arrangere demonstrasjoner ble kopiert til overvåkingstjenesten. I noen grad ble det ved hjelp av spaning klarlagt hvem som sto på stands og hvem som deltok i demonstrasjoner. Spaning ble også foretatt mot enkelte møter.

Ved kartleggingen av ml-erne bygget overvåkingstjenesten i stor grad på opplysninger fra informanter. Granskingen viser at informantene var mange. Særlig gjaldt dette ved skoler, høgskoler og universiteter, og på arbeidsplassene i offentlig og privat sektor. Informantene synes å ha blitt brukt aktivt. Formålet var å få opplysninger om hvem som var medlemmer av AKP(m-l), hvem som sympatiserte med partiet og om ml-ernes virksomhet.

Kommisjonen legger til grunn at overvåkingstjenesten på 1970-tallet også drev aktiv infiltrasjon i den forstand at man - eventuelt gjennom mellommenn - oppfordret personer til å engasjere seg i ml-bevegelsen for å skaffe informasjon, herunder interne dokumenter.

Overvåkingstjenesten fulgte nøye med på sommerleirene. Man spanet mot leirene, og informanter ble brukt aktivt. Som eksempel nevnes et notat utarbeidet av overvåkingstjenesten om telefontrafikken til og fra en sommerleir i 1972. Samtalene ble ikke avlyttet, men notatet gir opplysninger om hvem som ringte til hvem. Det kan se ut som disse opplysningene stammer fra en informant i Televerket. I en viss utstrekning spanet man også mot kurs for å klarlegge hvem som deltok. Spaning pågikk så sent som midt på 1980-tallet. I 1986 ble således et seminar i Trøndelag påspanet, og samme år brukte overvåkingstjenesten spaning for å klarlegge hvem som deltok på sommerleirer i Meråker og på Hvaler.

Provokasjon.

Under granskingen har kommisjonen blitt oppmerksom på ett tilfelle av provokasjon. Dette fant sted først på 1980-tallet og formålet var å klarlegge AKP(m-l)s interesse for våpen. Man ønsket å finne ut hvor stor denne interessen var, og hvem som var interessert. Overvåkingstjenesten anskaffet en brukt panservernrakettkaster M72 med bistand fra Forsvaret. M72 er et våpen til engangsbruk. Man tok deretter kontakt med en person med tilknytning til AKP(m-l). Vedkommende ble forevist rakettkasteren og var interessert. Han ga uttrykk for at han ikke hadde rede på våpen, men ville ta kontakt med "rette vedkommende". Noen tid senere fant visning og overlevering av rakettkasteren sted, og "rette vedkommende" ga uttrykk for stor interesse. Han uttalte at han var interessert i "skarpe", noe overvåkingstjenesten oppfattet som ubrukte panservernrakettkastere og våpen for øvrig. Han antydet ulike måter våpen kunne skaffes på. Personen ble identifisert av overvåkingstjenesten umiddelbart etter dette møtet.

4. Hvem er vi interessante for.

* Den offentlige etteretninga, dvs. politi, militære og statlige organer.
* Nazigrupperinger og høyreekstreme bevegelser.
* Arbeidsgivere, DNA, borgerskapet. Tradisjonellt viktige overvåkere for å unngå oppviglere på arbeidsplassen.
* Kriminelle miljøer, mafia (porno, puppebarer, narkotika, streikebryteri etc.).
* Utenlandsk etteretning, CIA, MI5, israelsk, russisk, tysk, svensk.
* EU, særlig Schengen.

Norges hemmelige hær.
I Lund-høringene har både Oddmund Hammerstad og Ronald Bye hevda et det finnes såkalte «frie grupper» med forbindelse til de hemmelige tjenestene. «De er trolig i tilbakegang», sier Ronald Bye, «men blir det bare igjen 50 % av det Hammersted fortalte om, blir det mer enn nok for dere å stelle med framover. Gruppene blir brukt til overvåkingsaktivitet, til dels av de hemmelige tjenestene, og de driver militærlignende aktiviteter. De er en struktur som fungerer på impulser som tas i bruk av noen av de hemmelige tjenestene, og er aktive fordi de mener at de er i en god saks tjeneste. De driver beredskapsaktivitet i frykt for at det skal skje ett eller annet på venstresida».
(Ronald Bye til Klassekampen 25.2.97).

For mer stoff om dette viser vi til Ronald Bye, Finn Sjue:
Norges hemmelige hær. Historien om Stay Behind. Tiden forlag, 1995.
Boka tar for seg oppbygginga av Stay behind-hæren og de private gruppene som «Kjettingmannen» og andre. Om lignende tjenester i andre europeiske land, om rolla til CIA og MI 6.

I januar fikk RV's stortingsgruppe overlevert arkivmateriale fra Stay Behinds virksomhet på 70-tallet. Materialet viser at Stay Behind har vært involvert i politisk kartlegging, bl.a. brev, rundskriv og instrukser fra Gunnar Bjålie, leder for Blue Mix (med oppgave å evakuere kongehus og andre nøkkelpersoner i tilfelle okkupasjon), til lokale ledd i organisasjonen. I et sirkulære fra 1971 blir nettverk og lokale kontakter mobilisert mot den nye kommunistiske bevegelsen som vokste fram, med navnelister, skoleringsmateriale og forespørsel om tilbakemelding. Dette skjedde parallellt med at POT begynte å bygge opp sine arkiver.

Informasjonene om navn og aktiviteter innafor SUF er omtrent sammenfallende med de «Notatene om SUF» som ble sendt ut fra Den norske Creditbank i 1971. Det peker på det store alvoret for vårt land, om den nedbrytende virksomheten SUF bedriver innafor næringslivet, at mange nå snakker om hårde midler, politiinnsats o.l. og at forholdsregler bør tas, at alle gode krefter bør samarbeide for å ta denne truselen alvorlig og bekjempe den med alle tilgjengelige midler.

Det er ennå ikke klarlagt hva slags rolle dette apparatet har spilt og spiller fortsatt. Det er viktig at disse opplysningene kommer fram, og at dem som har noe å fortelle får snakke fritt.

Om overvåking fra nazistene.
Det er flere ting som tyder på at nazister driver aktiv etteretning mot oss og våre nærmeste organisasjoner. Mange av våre kjente eksterne folk blir ofte oppringt med mer eller mindre godt skjulte trusler. Særlig gjelder dette kjente aktivister innafor det anti-rasistiske arbeidet.

Men både AKP, RV og RU er i søkelyset. De vet godt hvor vi holder til.

De holder også godt øye med andre organisasjoner:

I Mikael Knudsens nazi-blad «Fritt Forum» nr. 1 -96 sto det en 4-siders artikkel med en relativt grundig oversikt over organisasjonene på venstresida, spekka med navn. Artikkelen innleder med følgende:
«I denne oversikten skal vi se nærmere på de venstreekstreme gruppene i Norge. Vi skal også påvise den nære kontakten mellom de såkalte «antirasistiske» grupper og organisert kommunisme». Hvorpå beskrivelser kommer av SOS, Rød Ungdom og Rebell, RV og AKP, Antirasistisk senter, Blitz/AFA, IS, Revolusjonært Forbund og en del andre organisasjoner og lokale antirasistiske organisasjoner. Som sagt med en ganske god oversikt over personer, hvem som sitter i ledleser og styrer, hvilke publikasjoner som utgis mm.

Alt er riktignok ikke helt korrekt, men hovedsida er at oppslaget viser at de jobber med saken, de har en brukbar stamme med opplysninger som det vil være relativt enkelt å korrigere.

Fra tidligere kjenner vi til registret til Anti-Antifa over kjente antirasister og blitzere i Oslo og østlandsområdet. Her finner vi beskrivelse av utseende, adresse, spesielle kjennetegn, oppførsel, alder, bilmerke, kjennemerke og hvilke demonstrasjoner og aksjoner de har deltatt i. På enkelte av listene står det notert «prioritert angrepsmål».

I forbindelse med politiets razzia hos og arrestasjon av nazister i april 1997, hvor det ble avslørt attentatplaner mot kjente personer og institusjoner, er det funnet lister over medlemmer og sympatisører av Rød Ungdom. Dagbladet kunne 16. april melde at avisa hadde sett materialet som består av medlemsoversikt, innbetalingsblanketter til RU's pinseleir, bilder fra studietur i Kurdistan, adresse og telefonnumre til kurdere i Tyrkia, egenvurdering i forbindelse med kandidatur til RU's distriktsstyre, samt en rekke andre detaljopplysninger fra RU's og RV's møter.

Disse opplysningene, som danner grunnlag for nazistenes registre, har de etter det Dagbladet melder, skaffa seg ved innbrudd i det tidligere partikontoret i Gøteborggata 8 i 1995. Dagbladets kilder forteller at det er HAT - Hvit Arisk Terror som står bak tyveriet. HAT har nær tilknytning til Anti-Antifa.

5. De tradisjonelle metodene.

Poståpning.

Det er alminnelig antatt at overvåking av post foregår i mindre utstrekning enn avlytting av telefon. Lund-kommisjonen avdekker at postkontroll er en metode som blir benytta, og vi vet at det eksisterer maskiner for åpning av post som har de egenskapene at åpninga er umulig å oppdage. Opplysninger den senere tida viser at f.eks tollvesenet som åpner post uhemma på jakt etter narkotika.

«Tollvesenet må avklare med justisdepartementet sin praksis med åpning av private brev» sier Georg Apenes til Aftenposten. Toll- og avgiftsdirektoretet og Posten er uenige om tollvesenet har rett til å åpne private brev utenat det foreligger rettslig kjennelse. Fra januar til august 1996 har tollvesenet i sin jakt på narkotika og annet ulovlig materiale åpnet hele 5000 private brev, med resultat 169 anmeldte funn.

Vær oppmerksom på åpning av post, særlig hvis du ellers regner deg som overvåka.
Her, som på de fleste andre områder går det an å ta enkle forholdsregler ved å bruke fantasien ved f.eks. å bruke forskjellige konvolutter, håndskrift, forskjellige postkasser og -kontorer.

Telefonavlytting.

Metodene for telefonavlytting har utvikla seg enormt med den nye teknologien. Det er helt ukomplisert å registrere hvem som ringer til hvem, analyse av avlytta innhold i telefonsamtalene krever forholdsvis mer ressurser, og forbeholdes antakelig de mest interessante stedene, partikontorer, KK, sentrale kamerater, folk med internasjonale kontakter.

Det vi må være klar over, er at alle telefonforbindelser, hvem som ringer til hvem, blir automatisk registrert og lagra. Dette gjøres rutinemessig når du ber om spesifisert telefonregning.

Sjøl med de juridiske begrensningene som foreligger, går det ikke lang tid mellom personlig opplevde historier om avspilte bånd og merkelige lyder innafor vår bevegelse og i vårt miljø.

En telefon kan bli avlytta uten at du behøver å løfta på røret. En vanlig analog telefon er ikke aktiv mot omverdenen når røret ligger på plass i gaffelen. Dermed kan den ikke avlyttes med mindre en samtale er er satt opp. Da stiller det seg annerledes med en ISDN-telefon. Her er apparatelektronikken aktiv hele tiden,

bl.a. for å kunne dra nytte av automatisk mottak av data, fax osv. Dette åpner for tilkopling av mikrofonen i telefonrøret uten at det kommer noe ringesignal fra apparatet. Eksperter er uenige om man må legge inn en spesiell kode i telefonapparetet, eller om det holder å sende avgårde et signal i form av en kommando fra ISDN-sentralen til apparatet.

GSM-systemet - de nyeste mobiltelefonene.
Det heldigitale GSM-systemet avløste det analog/digitale NMT mobiltelefonsystemet. Det heter at radioforbindelsen mellom apparatene og basestasjonene er koda og krypterte. Men geskjeftige hacker-ungdommer kan melde at det kan skaffes utstyr som kan fjerne krypteringen på GSM-samtaler. Det dreier seg om et apparat på størrelse med en vanlig PC til en pris på 40-50 000 kroner. Utstyret er laga i utlandet, og det må en del "hacking" til å få det til å fungere i Norge. "Hackere" utveksler slik informasjon over Internet, og de sier at GSM ikke er vanskelig å knekke.

Disse kodenøklene for GSM-kryptering finnes høyst sannsynlig hos POT, slik at de kan avlytte enkeltpersoner etter å ha fått (eller uten å ha fått) rettslig kjennelse, som ved trådbaserte telefoner.

Hvordan foregår avlyttinga.
Vi snakker her om den sentraliserte avlyttinga som foregår i Telenor, hos POT, i forsvaret...og hvilke andre steder? De store, nye telefonsentralene er digre datamaskiner, som er kobla sammen i et nettverk. Det er ikke vanskelig å programmere inn avlytting av en eller flere telefoner, både trådbaserte og mobiltelefoner. Man trenger en enkel programkode, og går fram som følger:

Alle telefonnummer er lagra i datamaskiner i Telenor. Den som skal avlytte setter et merke ved vedkommendes telefonnummer(e) og distribuerer dette merket til alle landets digitale telefonsentraler. Kommandoen som på denne måten blir lagt inn i sentralene medfører at hver gang det merkede telefonnummeret blir aktivert, inngående eller utgående, blir samtalene automatisk lagt på harddisk. Det kan også legges inn automatisk overføring av de avlyttede samtalene til de tjenestene som bestilte avlyttinga. Hva disse folka bruker denne informasjonen til, er ikke Telenors ansvar. Avlyttinga foregår uten at du merker noen verdens ting.

Det har også blitt mye enklere å avlese den informasjonen som er samla inn. Man trenger ikka å sitte i timevis foran båndopptakeren å lytte til tullprat. Ved hjelp av databaser med stikkord (f.eks partiet, revolusjon, kurdere, PKK, demonstrasjon, crack, nazi) og talegjenkjenning kan mye av grovsorteringa foregå automatisk.

GSM-telefonen avslører deg.
Signalene fra en GSM mobiltelefon gir politiet mulighet til å følge en persons bevegelser med en margin helt ned til 1-200 meters nøyaktighet til enhver tid. Teknologien er bygget opp slik at selskapet hele tiden vet hvilken basestasjon din mobiltelefon bruker, og det er det store antall basestasjoner i byene som gjør det mulig å peile seg inn. På denne måten er det lett å finne ut hvor du befinner deg.
Mobiltelefonen trenger ikke å være i bruk, men den må være påslått fordi den da hvert sekund sender signaler til nærmeste banestasjon. Signaler med informasjon om hvilken mobiltelefon du bruker. I tillegg til hvor du oppholder deg, registrerer telefonselskapene også alle samtaler, både ut og inn, hvem du snakker med og hvor lenge du snakker.

Med rettslig kjennelse kan politiet få disse opplysningene utlevert. Politiet kan be om oversikt over alle samtaler i et bestemt område i et gitt tidsrom. På denne måten blir din og min samtale en del av etterforskningsgrunnlaget. Denne metoden har blitt så viktig at mobiltelefonoperatørene får daglig flere slike henvendelser fra politiet. I prinsippet er det ingen begrensninger på hvilke informasjoner politiet kan få på denne måten. Datatilsynet har gitt teleselskapene konsesjon til å oppbevare data om mobiltelefonbruken i seks måneder
.

Politiet bruker stadig oftere denne formen for overvåking av personer som er etterlyst, eller i forbindelse med mistanke om narkotikaforbrytelser, hvor dette har blitt rutine. I økende grad brukes metoden også i redningsoperasjoner. Men det finnes også eksempler på at metoden har vært benytta med stort hell også i andre saker. For eksempel til hjelp til pågripelse av en mann som gjentatte ganger har plaga eks-kjæresten med trusler. Og vi kan jo tenke oss anvendelsesområdet overfor venstresida.

Tapping av personsøkere.

En PC-bruker kan med letthet tappe samtlige personlige tekstmeldinger og telefonnumre som sender til personsøkerabbonenter over hele landet. Det kan fungere som et forbløffende effektivt overvåkingsmaskineri. Programvaren, som hentes fra Internett, kan til og med logge spesielle søkernumre, og man kan på denne måten sjekke alle meldinger som har gått til en bestemt person i et gitt tidsrom. Informasjonen fra personsøkerne kan også misbrukes ved at alle meldinger til alle abbonenter legges inn på en harddisk. Etterpå kan datamaskinen søke gjennom teksten og lete fram ønskede navn eller søkeord.

Det foregår på denne måten:
- Tekstmelding til personsøker skrives inn på PC og sendes ut på nettet viamodem.
- Fra radiosenderen sendes hver personsøkermelding utover hele landet som vanlige radiosignaler. Meldingene til hver bruker kan derfor avlyttes.
- Meldingen mottas av personsøkerabbonenten.
- En radioscanner, innkjøpt lovlig i Sverige (ulovlig i Norge) er innstilt på en spesiell frekvens og fanger opp alle meldinger til alle brukere samtidig som de vises på personsøkerne.
- Signalene konverteres til PC-signaler ved hjelp av en elektronisk kobling. Koblingen kan bygges av en person med grunnleggende elektronikk-kunnskaper, og koster 20 kroner, eller kjøpes ferdig via Internett.
- En PC utstyrt med program tilgjengelig fra Internett, snapper opp alle meldinger og viser dem som tekst på en skjerm. For en ekstra kostnad på 200 kroner kan programmet loggføre alle meldinger som sendes til opptil 250 personsøkernumre.

**Tapperen kan ikke automatisk se hvilket telefonnummer som mottar en melding.
I stedet ser tapperen det elektroniske identifikasjonsnummeret til personsøkeren,
altså hvilken melding som går til hvilken mottaker.**

For å kunne overvåke en person må derfor en falsk melding sendes. Når denne blir registrert, ser tapperen hvilket ID-nummer et personsøkernummer har. Får du derfor en mistenkelig melding på personsøkeren din, kan det være grunn til å være på vakt.

Det er mulig å få kjøpt personsøkere som kan motta krypterte meldinger, men dette er foreløpig dyrt. Som eksempel kan nevnes at en tjeneste som krypterer børsinformasjon og valutakurser koster 1200 kroner pr. mnd.

Noen tiltak.
Det gamle prinsippet om «politikken åpen, organisasjonen skjult» er fremdeles en bra retningslinje.Tenk masselinje når du bruker telefon: Jo større kontaktflate du har, jo større omgangskrets og jo flere typer mennesker du ringer, desto mindre oversiktlig for overvåkerne. Vær spesiellt oppmerksom ved bruk av telefon i forkant av store begivenheter i bevegelsen. Da er det svært enkelt for overvåkerne å plukke ut sentrale personer, og gjennom å avlytte dem avdekke mønstre som sier mye om hvordan vi er organisert.

Det går an å scramble eller kryptere telefonsamtaler med utstyr som finnes tilgjengelig hos internasjonale leverandører. Men dersom en rutineavlytting av en telefon avslører en karakteristisk “kraksing” som høres når linja er scrambla, fungerer dette som et signal til overvåkerne, og de vil kanskje iverksette spaning i stedenfor.

**Hvis summetonen ikke kommer med en gang du løfter av røret
kan det være et tegn på at telefonen er avlytta.**

Det samme er rare lyder, statisk bråk på linja, volumforandringer, hvis det kommer lyder når røret ligger på, hvis telefonen ringer og ingen svarer. Og sjølsagt hvis du kommer andre steder enn du har ringt, hvis du kommer inn på andre linjer og hvis du får tidligere telefonsamtaler avspilt.

Dette er det vel ikke stort vi kan gjøre med, bortsett fra å ta tiltak i forkant, tenke på hva vi sier og hvem vi sier det til.

Vær enkel i telefonen, bruk hue, ikke slarv, si det som er nødvendig. Det kan være fornuftig å kombinere telefon og brev, men ikke regn det som sikkert at post ikke blir åpna, særlig hvis du regner deg som overvåka.

Samtlige telefokjosker er det ingen som har kapasitet til å avlytte, men regn med avlytting av alle sentrale telefonkjosker.

6. Datasikkerhet.

Overvåking av Internett.

Hvis du tror at du er anonym når du surfer på Internett, tar du veldig feil.

Straks du logger deg på nettet setter du spor etter deg gjennom brukernavn/ident/konto. Dette følger deg hele den tida du er på nettet og kan leses av alle.

De fleste web-sider kan nemlig spore hvilke sider du besøker, hvor lege du oppholder deg på hver og hvor du var før. Denne informasjonen gir web-steder muligheten til å dokumentere hvilke sider som er mest populære, og å lage personanalyser ved å kombinere bevegelsene dine på Internett med demografiske data, som inneholder langt flere opplysninger om deg enn du selv ønsker å bringe for dagen.

Hvis du for eksempel har oppgitt navnet ditt eller e-postadressen på et web-sted eller kjøpt et produkt med kredittkort, kan web-stedet følge deg hver gang du kommer tilbake, ved å sende en spesiell fil som kalles en «cookie» til datamaskinen din. Cookies inneholder mye informasjon, bl.a. dato og klokkeslett for besøkene dine. Det er ingen lov som tilsier at du skal informeres om slik personlig datainnsamling, det eksisterer nesten ingen restriksjoner rundt bruk eller salg av slike aktiviteter.

I motsetning til en vanlig bokhandel, kan web-stedet spore hver bevegelse du gjør mens du er der, dvs de kan se hver bok du kikker på og hver side du blar gjennom mens du vandrer fra ett web-sted til ett annet. Ettersom slik overvåking er stadig mer utbredt dukker det opp selskaper som har oppdaga lønnsomheten i dette markedet. Amerikanske sporfølgingsfirmaer, som Internet Profiles Corp. <www.ipro.com> og Net-Count <www.netcount.com> hjelper web-steder med å finne detaljerte demografiske data (alder, jobb, inntekt osv) om de besøkende som har gitt ut sine navn eller e-postadresser.

Andre selskaper, som Interse Corp. <www.interse.com> og Accrue Software Inc. <www.accrue.com> har utviklet programvarer som automatisk sporer de besøkendes bevegelser, og lager rapporter og diagrammer ut fra denne informasjonen. Disse rapportene kan inneholde informasjon om hvilke hobbyer du dyrker, din politiske overbevisning, dine innkjøpsvaner osv.

hvis du surfer på Internett fra arbeidsplassen din, er det ennå lettere å kikke over skulderen din. WinWhatWhere Corp. <www.winwhatwhere.com> har laget en programvare som gjør det mulig for nettverksadministratoren i firmaet ditt å spore hvert web-sted du besøker og hver applikasjon du bruker på det lokale nettverket. Sjefer har ikke lov til å avlytte telefonsamtaler eller installere skjulte videokameraer på f.eks toalettene, men i de fleste land har har firmaer lov til å lese de ansattes e-postbeskjeder. Ulike tiltak er underveis for å begrense denne formen for overvåking på nettet.

Den amerikanske organisasjonen The Center for Democracy and Technology <www.cdt.org> har et ikon på hjemmesiden hvor brukerne kan sjekke sin egen cookie-informasjon. Et annet web-sted som blir flittig brukt heter Anonymizer <www.anonymizer.com>. Her kan Internett-brukere kople seg til for å fjerne personlige kjennetegn mens de beveger seg gjennom det virtuelle rommet.

Noe som bekymrer mange flere enn venstresida er at sensitiv informasjon skal havne i hendene på f.eks forsikringsselskaper eller politiske overvåkere. De tekniske mulighetene er til stede i fullt monn.

Overvåking av Internett i Norge.

Det er en erkjent sak at norsk politi har i en årrekke infiltrert Internett i narkotikasaker. Det nye er at politiet også har begynt med å infiltrere pedofile miljøer på samme måte.
«Infiltrasjon skal bare brukes i helt spesielle tilfeller og da først etter at tillatelse fra påtalemyndighet er gitt. Det er viktig at vi er inne i mediet Internett. Dermed kan vi skafe oss adgang til opplysninger og gjennom det drive politiarbeid. Men dette arbeidet må skje innen eksisterende lovverk - et lovverk som ikke er laget for Internett. To årsverk innen politiet er satt av til dette».
(Fung. kripos-sjef Tom Brunsell til Aftenposten 27.10.96).

Sjefen kan lese e-posten din uten lov.
I Norge finnes det ikke noe lovfestet vern mot innsyn i e-post. Dermed står arbeidsgiver fritt til å lage bestemmelser som gir innsyn i de ansattes e-post. Datatilsynet etterlyser klarere retningslinjer og sier at personvernet må gjelde her på samme måte som ved telefonavlytting. «Arbeidsgivere bør opplyse de ansatte om at e-post kan bli lest. Alle e-postbrukere må være klar over at de løper en risiko for å bli overvåket»
Hege Njaa, Datatilsynet.

«Jeg er ikke optimist. Det finnes knapt en eneste arbeidsavtale som tar opp dette spørsmålet, og jeg tviler på om arbeidstakerorganisasjonene er villige til å gjøre det».
Jon Bing, professor, Institutt for rettsinformatikk.
(Aftenposten 1.2.97).

Datanettverk.
De fleste som har PC på jobben er tilknyttet et nettverk. Nettverket består ofte av pc'er, skrivere og servere. Serverne er kraftige datamaskiner med stor diskplass og har lagret programvare og data.
Alle pc'er tilknyttet nettverk blir som regel overvåket av systemansvarlig. Ofte har systemansvarlige i en bedrift oppgaven med å "rydde" på den enkeltes pc i tillegg til å vedlikeholde servere og annet utstyr. Dette betyr at ingen data på et nettverk er sikret mot tilgang og tapping fra systemansvarlige. Regn derfor med at alt du skriver og lagrer kan tappes, enten du lagrer data på serverens eller pc'ens harddisk.

Et lokalt nettverk kan koples til andre nettverk. En bedrift kan fks. ha kontorer på flere steder, i samme by eller i ulike byer. Disse stedene er ofte knyttet sammen i større data- og telefonnettverk. Slike nettverk kan være landsomfattende og bestå av hundrevis / tusener av pc'er. Selv om sikkerheten på større nett kan virke solid, så må du regne med at du kan overvåkes av langt flere enn om nettverket ditt var lite. I tillegg til systemansvarlige kan fks. en nazi-sympatiserende kollega med en del IT-kunnskap skaffe seg oversikt over og tilgang til dine data.

Dersom datanettverket på jobben din har tilgang til Internet kan dette gi uautorisert tilgang til data på jobben din. Dette kan være ubehagelig for jobben din, men også for deg sjøl. Pc'en din kan i noen tilfeller være "åpen" for andre mens du surfer rundt på Internet. Som oftest er det riktignok de sentrale maskinene / serverne som utsettes for "innbrudd" og det er jo rimelig nok for her ligger jo alle dataene.
Det finnes ulike sikringsmekanismer mot uautorisert tilgang (såkalte brannmurer), men ingen av disse er 100% sikre. Nylig blei fks 11.000 hjemmesider hos Norges største Internet-leverandør, Telenor, slettet av en utenforstående.

Oppsummert betyr det at alle dine dokumenter som vedrører partiet eller dokumenter du vil holde hemmelig ikke må skrives og absolutt ikke lagres på jobbens pc.

Noen forholdsregler.
Datamaskiner bør brukes med forsiktighet.
Dataarbeid som vedrører partiet skal ikke **lagres** på PC på jobb, uansett om det er din egen maskin.
Bruk av data på jobb bør generelt begrenses, og vær spesiellt obs på nettverk hvor systemansvarlig har tilgang til alt i nettverket, når som helst.

Bruk kryptering ved transport og overføring av data.

Ha kunnskap om hvordan du sletter alle data på PC, dvs. harddisken.
Vurder behovet for sikkerhetskopiering og oppbevaringen av dette.

Det er viktig at partiet behersker e-post/Internet og har god datakompetanse.
Jo mindre kunnskap du har, desto forsiktigere bør du være.

All bruk av tekstbehandlere, PCer og databehandling setter spor. Under bearbeiding av data mellomlagres det i minnet i PC, på harddisken, og eventuelt på disketten du bruker, eventuelt på lagringsmedia sentralt i nettverket du er tilknyttet. Ved avslutning av et dokument risikerer du at disse «mellomkopiene» blir liggende igjen en stund før de overskrives på et senere tidspunkt.
Ved sletting av filer ligger det igjen fullt lesbare kopier som kan hentes fram ved lett tilgjengelige programmer som «undelete».

Vurder derfor nøye hvor du benytter en PC, hva du lagrer og hvor du lagrer. Vurder også hvem som du låner din personlige PC til.

All skriving til adresser i Internet registreres automatisk. Det er også enkelt å overvåke hvilke adresser som kommuniserer med hverandre i nett. Velg derfor hvilken person i avd. som skal fungere som «kjent» nettverksadresse. Politiet har egne eksperter for infiltrering og oppfølging av interessante Internet-sider. Vi må regne med at også andre grupperinger har kompetanse om dette. Regn med at alt du gjør på nettverk blir registrert.

Det er veldig mye lettere å overvåke digital informasjon enn «gammeldags» telefonavlytting.

All digital overvåking gjennomføres av datamaskiner (roboter) som er i virksomhet 24 timer i døgnet, 365 dager i året.

Kort om kryptering.

Kryptering betyr å forvanske (kode) informasjon slik at den ikke kan leses. Krypteringen kan reverseres ved å benytte en tilsvarende prossess, gjerne kalt dekryptering (dekoding). Krypteringen kan gjøres individuell ved hjelp av såkalte nøkler, eller kryptoalgoritmer. Mottakeren av informasjonen kan dermed gis eksklusiv adgang til informasjonen ved at vedkommende får den aktuelle nøkkelen. Dette setter også krav til en sikkerhetsmessig administrasjon av nøklene, som f.eks. rutinemessig skifte av nøklene og beskyttelse under transport, lagring og bruk.

Standard krypteringsvalg i Word, Word Perfect o.a. er enkle å knekke med lett tilgjengelig programvare.

For den som er spesiellt interessert, her følger et avsnitt om PGP.

Hva er PGP?

Pgp er et krypteringsprogram som fungerer på den måten at en kan sende e-post til hverandre, uten at det er mulig for andre enn mottakeren å lese meldinga. Systemet er så godt som 100% sikkert ved riktig bruk. Kan du ikke pgp ordentlig, så risikerer du imidlertid å gjøre feil som gjør at systemet ikke er 100% sikkert lengre.

Hvordan fungerer dette?

Pgp fungerer på følgende vis: Du lager deg 2 nøkler. Den ene er din private nøkkel, den andre er en offentlig nøkkel.

Disse nøklene fungerer sånn: Den offisielle nøkkelen er en nøkkel som du deler ut til alle dine venner. Denne nøkkelen bruker du altså ikke selv. Med denne offentlige nøkkelen kan dine venner kryptere meldinger til deg. Den offentlige nøkkelen din krypterer (koder) meldinger som bare kan dekodes med din private nøkkel. Den offentlige nøkkelen kan altså bare kode, ikke dekode. Når en melding er kryptert med den offentlige nøkkelen, er det altså ikke noen enn den hemmelige nøkkelen som kan dekode meldingen igjen. Poenget er altså at dersom du skal sende en melding til f.eks. Kåre, så må du ha Kåres offentlige nøkkel. Denne nøkkelen kan Kåre sende deg over e-post, eller på diskett. Det er imidlertid en ting du må forsikre deg om:

Forsikre deg om at du har ruktig offentlig nøkkel!

Dersom Kåre sender sin offentlige nøkkel til deg, så blir den offentlige nøkkelen liggende ute på en «fremmed» datamaskin på internett (din internett-tilbyders e-post server). Her kan f.eks. overvåkingspolitiet bytte ut denne nøkkelen med en offentlig nøkkel som de kaller for Kåre. På denne måten kan de ta alle meldinger som du sender til Kåre, lese dem, for så å sende dem videre til Kåre. For å forsikre deg mot dette bør du enten få Kåres offentlige nøkkel på diskett, eller du kan ta noe som kalles fingeravtrykk (fingerprints) av Kåres offentlige nøkkel.

Dette går ut på at du ser på noen tall som følger med den offentlige nøkkelen, og så kan du selv over telefon (med Kåre) sjekke om dette er de samme tallene som Kåre har. Dersom tallene stemmer, er du garantert at det er Kåre's virkelige hemmelige nøkkel du har, og dere har dermed garantert hemmelig e-postforbindelse for framtida.

Det finnes ingen Windows versjon av pgp.

Derfor må du bruke en dos versjon. Dette er naturlig nok en svært tungvint måte å bruke pgp på. Her må du nemlig skrive koder. Det finnes relativt enkle og oversiktlige oppskrifter på hvordan man kan gjøre dette.

7. En overvåkingstjeneste for framtida.

Fra justisminister Vallas pressemelding om omorganisering av POT
Flere har i overvåkingsdebatten hevda at POT ligger med brukket rygg, og mange mener at overvåkingstjenesten har kompromittert seg gjennom offentliggjøringa av Lund-rapporten. Jagland tok til orde for en omorganisering av POT og en organisering av en overvåkingstjeneste skikka til å møte framtidas utfordringer. Hvilke utfordringer dreier det seg om? Og hvilke virkemidler skal man i 1997 sette i verk for å kontrollere venstresida og andre opprørske elementer? For sjøl om den organiserte venstresida ikke representerer den samme truselen som på 70-tallet, har tendensene til opprør styrka seg.

28. februar 1997 heter det i en pressemelding fra justisdepartementet at regjeringa har oppnevnt utvalget som skal vurdere ulike sider ved Politiets overvåkingstjeneste. Utvalget blir leda av Åge Danielsen, direktør på Rikshospitalet, og består ellers av to høyesterettsadvokater, en konstituert overvåkingssjef, en professor, en direktør til, (NUPI), en lovrådgiver og nestlederen i norsk politiforbund.

Utvalget skal
- vurdere i hvilken grad rammer og regelverk for POT skal trekkes opp av stortinget, evt. fremme forslag til slik lovgivning,
- utarbeide evt. nytt regelverk,
- vurdere POT's organisasjonsmessige tilknytning og ansvarsforhold overfor justisdepartementet,
- vurdere forholdet mellom straffeprossessloven og overvåkingsinstruksen, herunder vilkåra for registrering av personopplysninger, krav til innhold, bruk og etterfølgende sletting av personopplysninger,
- vurdere hvordan POT bør være organisert for at den skal være i stand til å tilpasse seg ulike truselbilder til enhver tid,
- og vurdere hvilken kompetanse tjenesten evt. bør tilføres.

«Det er viktig å rette blikket framover», sier Valla, «jeg er glad for at det også er solid oppslutning om at vi nå iverksetter en ny vurdering av oppgaver, organisering og regelverk».

S-tjenesten får utvida fullmakt.
Forslag til ny lov om forebyggende sikkerhetstjeneste får høringsfrist på 1 måned. Forsvarsdepartementet beklager den korte høringsfristen, men vil at loven blir behandla av det sittende storting.

Formålet med loven er å «legge forholdene til rette for effektivt å kunne motvirke trusler mot rikets sikkerhet eller selvstendighet og andre vitale nasjonale sikkerhetsinteresser». «Forebyggende sikkerhetstjeneste omfatter alle tiltak for å sikre skjermingsverdig informasjon og skjermingsverdige objeter mot spionasje, sabotasje, terrorhandlinger og undergravingsvirksomhet. Med skjermingsverdig informasjon menes informasjon som er av betydning for landets forsvar, rikets eller alliertes sikkerhet, det internasjonale forsvarspolitiske samarbeid eller andre vitale nasjonale sikkerhetsinteresser...»

Det ligger i begrepet «forebyggende» at det gjelder både ytre og indre sikkerhet, og at man må ta all tenkelig informasjon med i betraktningen, også dem som i øyeblikket ikke er særlig påtrengende, men som på sikt kan vise seg å ha betydning.

Når det gjelder truselbeskrivelsen henvises det til kgl. res. av 14. mars 1980 om instruks for samarbeidet mellom Forsvaret og politiet til trygging av rikets sikkerhet (samarbeidsinstruksen), og Forsvarssjefens hovedretningslinjer for sikkerhetstjenesten, fastsatt 4. januar 1994. Hvilken trusel loven retter seg mot konkretiseres ikke nærmere i forslaget. Men det sies at «rikets sikkerhet» bør utvides til å omfatte alle vitale samfunnsinteresser som økonomisk nasjonal handlefrihet (menes det EU og EØS?), beskyttelse av teknologiske fortrinn og ressurskontroll. Teknologi, vitenskap, økonomi og politikk har utvikla seg til å bli stadig viktigere etteretningsmål.

Tidligere har disse interessene vært utforma i forskjellige instrukser og direktiver, utferdiga for forskjellige organer og forskjellige nivåer, alt dette skal nå samles og hjemles i en lov med tilhørende forskrifter. Loven foreslås ikka bare å omfatte forsvaret og statlige organer som nå, men skal utvides til å gjelde hele den offentlige forvaltninga, også på kommunalt plan, samt bedrifter og andre som leverer varer eller tjenester til forvaltningen i forbindelse med sikkerhetsgraderte anskaffelser. Denne utvidelsen skjer i det man erkjenner at informasjonsteknologien fører med seg nye sikkerhetsmessige utfordringer. Det handler ikke bare om å nekte uvedkommende innsyn i sensitiv informasjon, men hindre at informasjonen blir endra og gjort utilgjengelig. (Virus og annen ødeleggelse av data).

Forsvarets sikkerhetstjeneste (s-tjenesten) skal i framtida ha lov til å overvåke databruken til flere hundre tusen offentlig ansatte som behandler «skjermingsverdig informasjon». I dag gjelder s-tjenestens myndighet bare for regjeringa og departementene, men med det nye lovforslaget vi den omfatte alle ansatte i kommuner og statsbedrifter, og også sivile virksomheter som leverer sikkerhetsgraderte varer. Dette skal skje innafor «rammen av totalforsvarskonseptet». Ansvaret for sikkerheten skal også nedover i systemet, ved at linjeledelser i de virksomhetene som loven skal gjelde for blir gjort personlig ansvarlige.

S-tjenesten får blant annet adgang til å «monitorere» og overvåke utveksling av datainformasjon, samt «penetrering» av informasjonssystemer, utafor det militære nettet. Den får også myndighet til å gjøre tekniske sikkerhetsundersøkelser ved alle landets kommuner og foretak som behandler «skjermingsverdig informasjon». samtidig skal de militære kunne gjøre «innbrudd» og hacking på datasystemene for å «utprøve motstandsdyktigheten».

Nasjonal sikkerhetsmyndighet (det vil si Forsvarssjefen og Forsvarets overkommando/sikkerhetsstaben) eller den instans den bemyndiger kan foreta undersøkelser av lokaler og bygninger som eies eller kontrolleres av en virksomhet som loven gjelder for, TSU, Tekniske sikkerhetsundersøkelser. Dette skal kunne skje uten at kommunene eller foretaka er kjent med eller har gitt samtykke til undersøkelsene.

Lovforslaget behandler også personellsikkerhet og retningslinjer for klarering av personer som skal ha tilgang til skjermingsverdig informasjon. Man skal ikke drive virksomhet for fremmed makt, ha gjort straffbare handlinger, presser andre for fremmede lands interesser, misbruker rusgifter, er psykisk sjuk osv. Det understrekes at det er viktig å vurdere om det er grunn til å frykte at vedkommende vil kunne komme til å opptre i strid med sikkerhetsmessige interesser. Det er viktig å få fastslått om vedkommende setter egne personlige interesse og meninger over samfunnets lover og regler, eller om det foreligger «andre bindinger som vil kunne gå foran». Det brukes begreper som lojalitet og pålitelighet.

Det understrekes at overvåkingsinstruksens § 4 skal lovfestes, det vil si at medlemsskap i lovlig politisk organisasjon ikke **alene** skal gi grunnlag for innhenting eller registrering av informasjon, dette gjelder også for ytterste venstre og høyre politiske fløy. Det står imidlertid at «ekstrem politisk virksomhet som tar i bruk ulovlige virkemidler for å oppnå sin målsetting er ikke forenlig med sikkerhetsmessig skikkethet». Man henviser til den juridiske uenigheten som har oppstått i debatten rundt Lund-rappoerten om hva som er lovlig og hva som er ulovlig politisk virksomhet, og tar ikke stilling til dette.

Norges allianse- og sikkerhetspolitikk, dvs underordninga under NATO og nå VEU, påfører også Norge en rekke direktiver og forpliktelser av sikkerhetsmessig art. F.eks krever NATO at Norge monitorerer datainformasjon og foretar tekniske sikkerhetsundersøjkelser. Dessuten vil Norges deltakelse i internasjonale «freds»operasjoner, militære øvelser og forsvarspolitisk samarbeid tvinge med seg en harmonisering av regelverket.

Forsvarsminister Kosmo sier i denne sammenhengen (Aftenposten 21. mars 1997) at Norge har forsikra amerikanerne at norsk etteretning er en pålitelig partner. Han har funnet det nødvendig å berolige amerikanerne, på eget initiativ, om at det fortsatt er trygt for deres etteretningsfolk å utveksle opplysninger med norske kolleger. På bakgrunn av Lund-rapporten har han vært bekymra for hvordan troverdogheten til vår e-tjeneste bedømmes ute. Vitnemålet til Oddmund Hammerstad har sikkert blitt lagt merke til, og det går muligens litt tyngre for oss å få opplysninger fra USA's og andre lands etteretning. Men nå har altså Kosmo forsikra om at Norge er til å stole på, og han synes at han har fått en god tilbakemelding.

Loven innebærer også at straffereglene skjerpes overfor offentlig ansatte for å «bevare streng taushet». Den innfører en lovbestemt, straffesanksjonert taushetsplikt overfor offentlig ansatte som kommer i kontakt med slik informasjon. Strafferamma for taushetsbrudd er bøter eller fengsel inntil 6 måneder. Medvirkning straffes tilsvarende. Hvis forholdet er grovt uaktsomt er straffen bøter eller fengsel inntil 1 år.

Dette av hensyn til «Rikets sikkerhet». Men Jørgen Kosmo sier: «Dagens oppfatning av Rikets sikkerhet kan synes for snevert. Vi må inkludere andre vitale samfunnsinteresser og forholdet til internasjonale organisasjoner i et utvidet sikkerhetsbegrep. Det nye forslaget innebærer dermed at flere tusen nye saker må sikkerhetsgraderes».
(Aftenposten 24.2.97).

- Er det dette Jagland mener med «en overvåkingstjeneste som kan møte framtidas utfordring»?

Stortinget positivt til romavlytting. Metodeutvalgets innstilling.
Påtalemakta skyver MC-miljøene og internasjonal kriminalitet foran seg for å utvide fullmaktene til avlytting. Resultatet kan bli et regelverk som åpner for lovlig allmenn avlytting av deg og meg. Det såkalte metodeutvalget (for etterforskningsmetoder i politiarbeidet) avleverte i begynnelsen av mars -97 en instilling til justisminister Gerd Liv Valla, som nå sender innstillinga ut på høring. Dette lovforslaget ligger an til å få flertall på stortinget. Hvis dette forslaget blir vedtatt, innebærer det at grensene for hva som lovhjemles av overvåkingsmetoder flyttes betraktelig. Det innebærer en dramatisk utvidelse av politiets fullmakter til å ta i bruk avlytting, og dermed betydelig en betydelig inngripen i personvern og rettssikkerhet. Bakgrunnen for forslaget er kriminalitetsbekjempelse, men det som er tilfelle er at det åpner for en ytterligere legalisering av metoder, som innebærer at skansene for personvern og rettsikkerhet uthules. Alle former for telefon- og datakommunikasjon skal kunne avlyttes. Hva dette kan brukes til i andre, politiske sammenhenger er det fullt mulig å forestille seg. Det vil bli mye enklere å avlytte vanlige norske borgere.

Fra Justisdepartementet hevdes det at Norge bør tilpasse seg regelverket i andre land. Hvis politiet i Norge skulle ha færre midler å ta i bruk enn i resten av Norden, kan vi lett se for oss at organisert kriminalitet ser på Norge som et nytt eldorado og flytter planlegginga av kriminaliteten hit.

Dette forslaget kommer parallellt med oppbygginga av et globalt teknisk regime for telefonavlytting. Allerede i november -95 inngikk representanter for regjeringa en overenskomst med EU om å samkjøre reglene for overvåking av telekommunikasjoner.

Forslaget går ut på følgende:
- Romavlytting tillates i saker med strafferamme på ti år eller mer. Det vil si narkotikasaker, trusler mot rikets sikkerhet, grov vold og drap. All overskuddsinformasjon (iformasjon man får ved avlytting, som man egentlig ikke var ute etter i utgangspunktet) som samles inn på denne måten skal kunne brukes som bevis i en rettssak.
- Telefonavlytting må tillates for alle fomer for kriminalitet som har en strafferamme på mer enn seks år. Her også tilnærmet fri bruk av overskuddsinformasjon.
- Telefonavlytting av personer som mistenkte «antas å ville ringe til».
- Politiet skal fortsatt måtte innhente rettens kjennelse, men så snart avlyttinga er i gang skal all informasjon politiet kommer over kunne benyttes. Det vil si at avlytting av telefonlinjer, leiligheter, parker, restauranter, datakommunikasjon i praksis kan brukes i alle former for etterforskning.
- Forbudet mot å bruke telefonavlytting som bevis fjernes, fordi den dømmende rett bør få sakene best mulig belyst.
- Avlytting av samtaler på offentlig sted tillates i saker med mer enn seks års strafferamme.
- Hemmelig ransaking må tillates.
- Elektroniske peilere må kunne påføres ikke bare biler, men også mistenktes bagasje og klær.

Våre politikere har den siste tida hatt en stygg historie i forhold til å hemmeligholde innhold i konvensjoner, avtaler og lovforslag, for ikke å skape for mye offentlighet rundt tiltak som folk flest vil oppleve som ubehagelige. Jamfør problematikken rundt Schengen-avtalen, som ble framstilt som om det dreide seg om glade nordmenn på sydenferie.

Aftenposten kunne 18. april i år melde: «Politiet vil honorere tystere». Dette kommer fra det samme Metodeutvalget, og er et forslag om at politiet skal bygge opp et tyster-register. Et slikt register skal finnes ved det enkelte politikammer, og sjøl om tysterne skal betales med 15 000 kroner for opplysninger, sier kripossjef Arne Huuse til avisa: «Det er på tide å legalisere tysterhonorarer, som også kan føre til økonomiske besparelser for politiet». Arne Huuse er med i utvalget. Man kan jo lure på hva denne offisielle tystervirksomheten kan drives til. Lederen av Bergen Forsvarerforening, Jostein Alvheim, rykker da også ut og hevder at dette forslaget er en fare for rettssikkerheten. Det er etterhvert mange saker som er en fare for rettssikkerheten. Schengen-avtalen er ikke minst et eksempel på det.

Om overvåkingssystemet innafor Schengen.
Høsten -96 var det en del diskusjoner om Schengen-avtalen i stortinget og til en viss grad media, spesiellt i Klassekampen, i forbindelse med at regjeringa hemmeligholder deler av avtalen. Daverende justisminister Anne Holt sa i stortinget at Schengen-samarbeidet ikke omfatter de hemmelige tjenestene, men er retta mot tradisjonell, alvorlig kriminalitet. Dette viser seg å være løgn.

Det dreier seg om den såkalte **Sirene-håndboka**, som har blitt offentliggjort både i Belgia og Danmark. I Sirene-håndboka går det fram at SIS, dvs det databaserte registret over blant annet ettersøkte, utviste utlendinger eller stjålne kjøretøyer, er kobla til et skjult informasjonssystem, som kan anvendes av de nasjonale etteretningstjenester i saker som vedrører rikets sikkerhet. Dessuten beskrives det i dette papiret detaljert hvordan et lands etteretningstjeneste f.eks. kan be kolleger i andre land om at det foretas overvåking.

I artikkel 93 i Schengen-konvensjonen heter det: «Formålet med Schengen-informasjonssystemet er, i samsvar med bestemmelsene i denne konvensjonen, å opprettholde den offentlige orden og sikkerhet, herunder statens sikkerhet, og anvende bestemmelsene om persontrafikk i denne konvensjonen på kovensjonspartenes territorium ved hjelp av opplysninger som formidles gjennom systemet».

Og i artikkel 46: «I særlige tilfeller kan hver konvensjonspart i samsvar med sin nasjonale lovgivning uoppfordret oversende den berørte konvensjonspart opplysninger som kan ha betydning for denne part som bistand i forbindelse med forfølging av framtidige lovovertredelser og forebygging av straffbare handlinger, **eller handlinger som utgjør en trussel mot offentlig orden og sikkerhet».**

I den belgiske regjeringas offisielle redegjørelse heter det at målet «er å garantere sikkerheten innen Schengen-landene, alle fremmede som skal forbys adgang innføres i Schengen Information System, såvel personer som er rapportert av statlige sikkerhetsmyndigheter».

En person ved det belgiske Sirene-kontoret sier at «den viktigste forskjellen mellom Interpol og Schengen er at Interpol dreier seg om et rent politisamarbeid, mens Schengen også omfatter sikkerhetspolitiet i medlemslanda. Interpol har som oppgave å bekjempe kriminalitet. SIS derimot har som målsetting å garantere sikkerheten innen Schengen-landa».

Den danske folketingsrepresentanten Keld Albrechtsen har fått tilgang til Sirene-håndboka. Han sier: «Her er det etablert et informasjonsutvekslingssystem så vel for data som for telefonkontakt mellom etteretningstjenestene. Sirene-systemet omfatter de tjenester som har ansvar for den offentlige orden og rikets sikkerhet. Vanligvis er det for slike saker etablert et direkte kontrollsystem i landene. Når det gjelder denne delen av Schengen Information System er det ikke mulig med noen parlamentarisk kontroll, her mangler kontrollsystem i det hele tatt. Denne registreringa av opplysninger gjelder for en stor del «anmodninger om diskret overvåking». Her kan man utveksle opplysninger om personer som ikke har begått noe ulovlig eller er mistenkt for alvorlige forbrytelser. Her kan man bli innrullert kun på mistanke om å være en trusel mot den offentlige orden. I dette systemet er det fare for politisk registrering i et helt annet omfang enn hva som har vært tilfelle i de nordiske landene. Vi anser denne delen av Schengen-samarbeidet som forstadiet til dannelsen av EU's etteretningstjeneste, som igjen blir en del av det samlede politisamarbeidet i EU».

Thomas Mathisen sier til Klassekampen 13. desember 1996: «Av de fire millionene innrapporteringer til SIS gjelder 1,3 millioner identitetspapirer, dvs grensekontroll. I tilleg er det hundre-tusenvis av saker som gjelder uønskede fremmede og asylsøkere som får avslag på opphold, og skal kastes ut. Schengens ansvar er altså å sørge for statens sikkerhet overfor alle fremmede som nektes adgang, samt for personer generellt som er rapportert av hensyn til statens sikkerhet. Det springene punktet er Sirene, som dreier seg om et teknisk system for gjensidig utveksling av tilleggsinformasjon mellom nasjonenes politimyndigheter. I EIS, utkastet til Konvensjonen om det europeiske informasjonssystemet, er det eneste stedet Sirene står omtalt. Her framgår det at det her dreier seg om opplysninger eller dokumenter av viktighet for «fortsettelse av aksjon». Det er snakk om en meget bred og omfattende informasjon. Ikke mindre enn enhver informasjon politiet finner interessant kan legges inn i det nettverket som Sirene representerer».

Du er registrert 500 ganger.
Det er en del saker den siste tida som har retta oppmerksomheten mot personvernet i disse registertider. Georg Apenes i Datatilsynet opplyser i Arbeiderbladet 22. mars -97 at 65 000 registre med personopplysninger har fått konsesjon siden Datatilsynet ble oppretta i 1980, og at en gjennomsnittsperson

må regne med å være registrert i 500 av dem. I 1996 ble det gitt konsesjon til å opprette 2713 nye personregistre, mot 1656 i 1994. «Vi er på full fart mot et gjennomsiktig samfunn», advarer han.

Økt bruk av teknologi har ført til at antallet konsesjonssøknader har økt kraftig i de seinere åra, og personvernhensyn ligger etter. Utenlandske undersøkelser viser med til dels dramatiske tall at folk i stigende grad er bekymra over at de i stadig grad legger etter seg elektroniske spor. Datatilsynet gjennomfører nå en tilsvarende undersøkelse i Norge.

Fri flyt av persondata i Europa.
Aftenposten kunne melde 14. mars 1997 at personopplysninger om nordmenn skal flyte fritt i EU. Innen høsten må Norge lage ny lovgivning om personregistrering som er tilpasset EU's direktiv, som også skal gjelde i EØS-området. Norge kan bli nødt til å fjerne dagens konsesjonsordning for personregistre, noe som vil gjøre det lettere å opprette registre med personlige opplysninger. Datatilsynet vil bli svekka, og det vil bare kunne komme inn i bildet hvis data skal selges til et tredje land, noe direktivet innebærer utstrakte muligheter til.

Folk skal selv kunne ha muligheten til å si nei til at opplysninger skal kunne brukes videre, for eksempel til markedsføring, men i praksis er det ikke mange som vil gjøre noe aktivt for å forhindre det.

«Reglene er lagt opp slik at det skal bli så lett som mulig å bruke personlige opplysninger i handel og vandel», sier professor Jon Bing.
«Det er ikke min oppfatning at Datatilsynet vil bli svekket», sier konserndirektør i DnB Arne Skauge, leder i Justisdepartementets utvalg som snart skal legge fram forslag til ny personregisterlov. Dette arbeidet skal etter planen avsluttes i begynnelsen av mai -97.

Ting skjer fort.
Det er mange saker i tida som må sees i sammenheng. F.eks ble det i mars foreslått at Oslo Kommune skulle opprette et register over alle byens innbyggere med oversikt over deres økonomiske situasjon. Et annet eksempel: Aftenposten 2. april 1997 melder at Finansdepartementet i april vil fremme et forslag til ny regnskapslov, virksom fra neste år, som innebærer at alle kontantkjøp over 10 000 kroner skal registreres med fullt navn, adresse og telefonnummer. Dem som handler med sjekk eller bankkort kan kontrolleres av myndighetene via bankutskrifter. Disse registrene skal oppbevares i hvert enkelt firma, og skal være tilgjengelig for kontrollmyndighetene. Begrunnelsen er bl.a. at dette er viktig for etterforskning av økonomisk kriminalitet, og som i andre lignende tiltak skyver man andre motiver foran seg for å øke kontrollen.

Et annet eksempel: Teknisk Ukeblad kunne i nr. 17 -97 melde at Statens institutt for folkehelse ikke har konsesjon for adgangskontrollsystemet sitt. Da to ansatte ble mistenkt for tyveri i vinter, forsynte Folkehelsas ledelse politiet med data fra kortleseranlegget sitt. - Ulovlig overvåking! hevder de ansatte. Et adgsngskontrollsystem som registrerer ansatte og dessuten lagrer tidspunktopplysninger er konsesjonspliktige. Når opplysninger da i tillegg blir overlevert politet, er dette ganske grovt. Hvor mange andre steder skjer det samme?

18. juni i år (1997) ble ennå et nytt personregister lansert gjennom Aftenposten. Sosial- og helsedepartementet vil opprette et personregister over absolutt alt legemeldt sykefravær. Det skal opprettes i Rikstrygdeverket, og inneholde opplysninger om den enkeltes fravær, diagnose, uføhetsgrad og yrkesskade. Informasjon om ferieperioder, arbeidskategori, og hvilken lege som sykemlder skal også stå i registeret. Formålet med registeret er "høyverdig" nok: Finne måter å forebygge sykefravær på, muliggjøre bedre kostnadsberegninger og lette forskning på området. "Vi trenger en samlet sykefraværsstatistikk, og skal den bli god nok trenger vi opplysninger helt ned på individnivå...Dette for å kunne finne bakenforliggende årsaker til fravær", sier Bjørn Halvorsen, ekspedisjonssjef i Sosial- og helsedepartementets trygdeacdeling. Men både Datatilsynet, Den norske legeforening og juridisk ekspertise er kritiske. "Det er vanskelig å skjønne hvorfor disse opplysningene må lagres på navn", sier Georg Apenes. "Jeg stiller meg uforstående til at de formål som dette registeret skal ha nødvendiggjør individopplysninger", sier Hans Petter Aarseth, president i den norske legeforening.

Det samme sier vi. All denne registreringa er betenkelig nok i seg sjøl, men sett i sammenheng med alt det andre som skjer, og kobla sammen med andre typer registre med andre typer personopplysninger, trår bildet av «storebror ser deg»-samfunnet ganske klart fram. Poenget er at ting skjer fort, og det skjer mange ting på en gang.

I løpet av våren skal stortinget ta stilling til s-loven, metodeutvalgets innstilling og Schengen-avtalen. Hver for seg gir disse forslaga POT og s-tjenesten fullmakter som savner sidestykke i norsk historie, men de har ikke

ført til stor offentlig debatt. De færreste stortingspolitikere har faktisk oversikt over konsekvensene av dagens utvikling.

Oppsmuldringa av personvernet er viser også en skremmende utvikling, og må sees i sammenheng med andre sikkerhets- og overvåkingstiltak. Personvernet er samfunnets regelverk for å sikre og beskytte den enkeltes private del av livet. Regelverket regulerer bruk av personopplysninger i offentlig forvaltning og privat virksomhet, og gir oss muligheter til å kontrollere hvordan opplysningene blir innhenta og brukt. Det skal finnes et vern mot urimelig kontroll og maktmisbruk. Det store antallet personregistre er et problem i seg sjøl, men oversikten blir helt borte når registrene blir kapital og kan omsettes fritt på et marked, her er et nytt marked for kjøp og salg, og store penger å tjene. Vi vil dessuten bevege oss i retning av et samfunn der alt som er avvikende blir mistenkelig og dermed gjenstand for registrering eller overvåking.

Det ser også ut som om politiet opptrer mer åpenlyst og hemningsløst. I demonstrasjonen mot nazi-huset på Alnabru/Oslo 1. mars i år ble alle demonstrantene leda gjennom en sluse på 1-2 meter. Slusa var plassert på ei bro over motorveien, ikke mulig å komme seg unna. Påskuddet var å renske demonstrasjonen for slag- og kastevåpen. Det som i tillegg skjedde var at et videokamera var oppstilt i slusa med en uniformert politi bak som trynefotograferte alle demonstrantene. På forespørsel fra en av våre folk om hva dette skulle brukes til, om det var til POT ol kom de sjølsagt ikke med noe svar.

Det er tydelig at et oppsving i den anti-facsistske kampen brukes som påskudd til å øke overvåkinga. Episoder som har vært våren -97, med angrep på nazihuset på Alnabru, angrep fra antirasister på et privathus hvor det var nazi-fest i Kristiansand, og slåsskamp i forbindelse med en nazi-marsj på Jessheim er med på å piske opp et generell stemning og et bilde av gjengkrig mellom ytterliggående grupper. Samtidig gir det politiet en legitimitet i offentligheten om at det er nødvendig å ta skjerpede tiltak.

7. Hva slags overvåkingsutstyr finnes på markedet, hvor finnes det, og hvem kan få tak i det?

Omfanget av metoder og utstyr i denne bransjen er omfattende og stadig i utvikling. Det finnes mange måter å avlytte på, f.eks. trådløse små radiosendere, båndopptakere, mikrofoner, kontaktmikrofoner, retningsmikrofoner, automatiske opptaksmaskiner som tar opp telefonsamtaler, fjernstyrte mikrofoner til både telefon- og romavlytting osv. Det nyeste på markedet er laserstråle-avlytting og infrarøde mikrofoner. Altså det meste. Det er omtrent bare fantasien som setter grenser.

Hvis du har penger, er det ingen sak å få tak i utstyr. Det finner flere, mer eller mindre seriøse firmaer som selger slikt utstyr, både i utlandet og i Norge. Og ikke sjokkerende, slike firmaer opplever stor interesse og pågang. «Vi kan dekke ethvert anti-tiltak og sikkerhetsbehov», står det i innledninga i katalogen til et norsk firma. Det sender ut varer pr. postoppkrav og kjører det gratis ut til kunder i Oslo. De har ikke noe butikklokale, men kan gjøre avtale om besøk pr. telefon.

I dette heftet skal vi ikke gi noen fullstendig oversikt over dette utstyret, men gi noen eksempler på hva det går an å skaffe seg, og til hvilke priser. Det skulle gi en ide og illustrere poenget ganske godt. (Teksten er henta fra reklamekatalog).

Anti-avlyttingsdetektor.
Et følsomt apparat som finner trådløse sendere. Den søker seg fram til lokale kilder for radiofrekvens på et bredt spekter, og finner alle former for mikrofoner som sender innafor frekvensområdet. Når du nærmer deg mikrofonen piper detektoren, eller det lyser en lampe. Du kan nemlig skru av lyden for ikke å alarmere fienden.
Pris kr. 4950.-

En enda mer følsom anti-avlyttingsdetektor, opplæring i bruk tar 10 minutter, vil ta inn de svakeste sendere, og gir deg muligheten til å høre hva den skjulte mikrofonen sender. Den vil lokalisere en sender på 0,5-2 meters avstand.
Og koster kr. 18 000.- (Hvis du vil opp en prisklasse til, har de en profesjonell detektor til kr. 35 000.-)

Videokameradetektor.
Kan avsløre kameraer skjult i vegger eller dagligdagse gjenstander.
Pris kr. 4950.-

Forskjellige typer stemme-scramblere eller telefon-scramblere; «som kan tilkobles ethvert telefonsystem, og liten nok til å passe inn i en standard attache-koffert, med plass til overs. Beskytter brukeren på kontoret, hjemme eller på reise».
Priser fra 34 995,- til 64 800,-

Fax-scrambler.
Beskytter all informasjon sendt mellom to parter, fax-linjer kan tappes uten avansert utstyr, ved å konvertere informasjon til et kodet format. Når det mottas i den andre enden blir teksten eller bildet automatisk dekodet og kommer ut i klartekst.
Pris kr. 19 000 pr. enhet.

Skjult kamera.
Film eller video, kan bygges inn i mange forskjellige dagligdagse gjenstander og gir glassklare bilder.
Pris kr. 19 588,-

Armbåndsur-kamera.
Miniatyrkamera bygd inn i et fungerende digitalt ur. Leveres med framkallingsutstyr og filmdisker, klart til bruk. Bare rett det mot objektet og knips.
Kr. 19 900,-

Videoovervåking, komplett pakke kr. 5900,-
Eller mer avansert video attache system, alt utstyr innebygd i en eksklusiv liten koffert, kr. 75 000,-
Eller mer diskret: Miniatyr slipsnål-videokamera, opereres via batteri i 3 timer, kr. 49 000,-
Du kan også få opptakssystem på størrelse med en sigarettpakke som tar videoopptak og tar opp hviskende lyd på 6 meter. For kr. 4900,-

I katalogen finnes videre 12 forskjellige modeller av utstyr til telefonavlytting og annet opptaksutstyr av forskjellig slag med forskjellige egenskaper, med samme prisnivå som effektene over. Med helautomatisk opptak, av alle inngående og utgående samtaler. En av dem på størrelse med en zippo lighter som kan ta opp 3 timers kontinuerlig samtale på en mikrokassett. En annen modell er innebygd i en koffert og starter opptaket ved berøring av kofferten, og tar opp i 90 minutter. En tredje modell monitorerer alle utgående samtaler med opplysninger om oppringt nummer, dato, tid på døgnet og samtalens varighet.

Videre en liten, hendig sender/mottaker som kan skjules og bæres hvorsomhelst på kroppen. En liten sender på størrelse med et kronestykke som kan plasseres på biler, båter, pakker, folk, som sender lydsignal som viser hvor gjenstanden befinner seg med en nøyaktighet på 50 meter.
Og forskjellige typer mikrofoner.
- For kr. 2900,- kan du få en avansert mikrofon innebygd i en penn.
- Kontaktmikrofoner som kan plasseres mot en overflate (vegg eller vindu), forsterker lyden og tilkobles en opptaker. Kr. 3900,-
- En sterkere type, et elektronisk stetoskop koster kr. 12 200,- og en feltopptakermikrofon, velegna for telefonkjosker og mobiltelefoner, koster bare kr. 250,-
- Gjennom en enkel montering i telefonapparatet eller langs linja kan man klart og tydelig høre hva som sagt av begge parter i en telefonsamtale. Ubegrenset sendetid, fordi den får strøm fra telefonsystemet. Bruker linja som antenne, som minsker muligheten for å bli oppdaga. Kr. 3800,-.
- En mikrofon forkledd som kalkulator med rekkevidde på 500 meter koster kr. 5000,-
- En mikrofon som kan kobles innvendig i de fleste telefonapparater eller i telefonkontakten, som når telefonen ikke er i bruk fanger opp all lyd eller samtale innafor 10 meter og sender dette trådløst opptil 500 meter. Kr. 6000,-
- Eller en jakkeslagsmikrofon, ubetydelig større enn 2 fyrstikkhoder, som lett kan skjules til kr. 1300,-

Lommenattkikkert.
Et «must» for mobile operasjoner. Inkluderer infrarød lyskilde for bruk i totalt mørke.
Kr 68 649,-

Så finnes det overvåkingskikkerter, infrarød markeringslampe (kan plasseres på biler, båter og personer og gir blinkende, infrarødt lys, usynlig for det blotte øyet), infrarøde lyskilder, infrarøde varmesøkere, periskop og nattkikkerter. Firmaet kan også levere komplette kjøretøyer for overvåking, pris ikke oppgitt.

Firmaet forhandler videre portable veisperringer, skuddsikre vester, T-skjorter og caps, digitale stemmefordreiere, løgndetektorer, spionpapir, og en video til 450 kroner som er som en lærebok i hvordan avlytting fungerer og hvordan den skal elimineres.

Dette sier vel kanskje noe om hva slags firma dette er, hvem det tenker seg å betjene og hvor seriøst det er. Og et åpent spørsmål er sjølsagt også om utstyret fungerer etter forventningene.

Men hovedhensikten med dette kapitlet har som sagt vært å gi en smakebit på hva som finnes på markedet. Og det finnes jo også seriøse firmaer, firmaer som betjener offentlige og statlige institusjoner. Overskrifta er i alle fall, som ellers i samfunnet: Har du penger, finnes det få grenser for hva som er mulig.

Hva må gjøres?

Dette er ikke noe utfyllende avsnitt, bare noen problemstillinger på tampen.

Vi har tidligere stilt krava "Vi vil se mappene våre" og "Nedlegg overvåkingspolitiet". Dette i forhold til den politiske overvåkinga av venstresida, en viktig side ved POT er at det har fungert som et politisk politi. Men stilt overfor den utviklinga av overvåkingssamfunnet som vi ser foran oss, og som vi har skissert i denne håndboka, er det også andre krav vi må stille.

Er det mulig for oss og våre allierte å bygge en front mot dette? Hvilke krav og paroler skal vi stille, på vegne av oss alle, og på vegne av partiet? Er vi i stand til å intensivere kampen og propagandaen mot Schengen? Og kamp mot oppsmuldringa av personvernet?

Er det mulig for oss å avsløre den borgerlige propagandaen, løgnene, fortielsene og fordreininga av virkeligheten? På nyhetene på TV 2 16. april blir det f.eks. trukket fram at det viktigste med den nye s-loven er at den sikrer folks rettigheter når de er i en prossess med personkontroll, det vil si sikkerhetsklarering.

Og når det gjelder den lokale jobbinga: Er det mulig å grave opp igjen gamle saker, mistanker vi hadde den gangen, folk vi tror spilte en rolle, eksempler som viser hva vi har vært utsatt for, nå når alt framstår i et nytt lys? Når det gjelder folk som har vært knytta til lyssky virksomhet i forbindelse med e-tjenesten og Stat Behind må vi stille kravet "De som vet må få lov til å snakke!"

Partiets oppgave er foruten å bygge fronten, å spre materiale og våre analyser. Har vi ikke både materialet og analysene?

Vi avslutter herved med formann Mao's ord: "Kvitt dere med bagasjen, og sett i gang maskineriet!"
