Et sårbart samfunn

Taler
Kåre Willoch

Dato
15 januar 2001

Sted
Oslo Militære Samfund

Omstendigheter
En redegjørelse for Sårbarhetsutvalgets innstilling

Som utgangspunkt for min redegjørelse vil jeg gjerne ta det godt kjente forhold at vår tid preges av uvanlig raske og dyptgående forandringer i vilkårene for styring av både offentlig og privat virksomhet. Ny teknologi har gitt et enormt potensial for rasjonalisering i nær sagt all virksomhet, og har medvirket til en uvanlig lang oppgangstid i store deler av verdensøkonomien.

Men som alltid før gir raske teknologiske fremskritt også både nye motiver og nye muligheter for dem som har vondt i sinne, og nytt potensiale for ulykker. Den teknologiske fremgangen, og den økonomiske veksten som den har forsterket, er i utilstrekkelig grad benyttet til å fjerne grunnlag for konflikter og voldsanvendelse. Samtidig påvirker menneskene naturen sterkere enn før. De ødelegger noen av naturens forsvarsverker mot dens egne destruktive krefter. Og utslipp av gasser forandrer atmosfærens sammensetning. Klimaet forandres, og man får mer ekstremt vær. Kort sagt: Menneskelig aktivitet medvirker til at risikoen for naturkatastrofer stiger. Samfunnet blir mer sårbart.

Dette bør man bli litt skremt av, men ikke til pessimisme, bare til handling. For samfunnet får også stadig nye midler til å beskytte seg og redusere sin sårbarhet til et akseptabelt nivå. Man kan høste fordelene av den nye teknologi og samtidig unngå de farligste skyggesidene ved den. Vanskelighetene med å få dette til, ligger blant annet i de populistiske fristelsene i politikken. Det er vanskelig å få øye på mange av de nye truslene før de har ført til skade. Politikere kan bli populære på å motsette seg statlige inngrep og bevilgninger for å hindre farer som mange ikke er oppmerksom på. Det er fristende å vente og se om det kommer noen ulykker, og derefter satse på å hindre at de gjentar seg. Politikken blir altfor lett reaktiv, i betydningen at den reagerer på efterskudd mot ulykker som har skjedd, i stedet for proaktiv, i betydningen å reagere på

forhånd på risiko for at noe vil skje.

Motstanden mot en effektiv klimapolitikk er langt det farligste eksempel på dette. Men et forholdsvis ferskt eksempel som ligger nærmere de militære omgivelser for dette arrangement, kan også belyse dette primitive reaktive politiske handlingsmønster: Norges for tiden nest største politiske parti ville stanse alle norske bevilgninger til å hindre atomulykker utenfor Norges grenser i nord. Så sank atomubåten "Kursk".

Først da ville denne bevegelse av skattemotstandere erkjenne en risiko som man må ha sett på forhånd, men som man neglisjerte fordi velgerne ikke hadde sett den. Efter dette vil også de være med på bevilgninger, for "nå er det skjedd noe".

Prisen for en slik "vente og se" holdning til tidens nye farer kan bli svært høy. Den kan føre til at man driver inn i flere katastrofer og de uhyggelige menneskelige lidelser og økonomiske tap som de vil føre med seg. Vilkåret for å hindre det er at vårt politiske system må reagere mot teoretisk risiko fremfor bare å handle efter drastiske erfaringer. Og man må ta tilbørlig hensyn til den lærdom som for over 2000 år siden ble beskrevet av Aristoteles: "Det er sannsynlig at det vil skje noe usannsynlig".

En særlig løfterik del av den teknologiske fremgang jeg nevnte er utvilsomt datateknologien. Potensialet for fortsatt fremgang er åpenbart også betydelig, for å si det forsiktig. For det er jo også en del av dagens virkelighet at flere enn noensinne før forsker på videreutvikling av denne teknologien. Og denne forskningen er selvforsterkende ved at den utvikler verktøy som gir enda raskere forskningsresultater. Jeg behøver ikke i denne forsamling dvele ved de teknologiske nyvinninger som det sannsynligvis vil føre til, og som raskt vil åpne enda mer enorme anvendelsesområder for IKT. Men jeg må understreke at datateknologien også er en særlig viktig bidragsyter til den mer omfattende nye risiko for samfunnet som det er mitt oppdrag å tale om nå.

Denne sterkt økte risiko har ikke vært tillagt rimelig vekt før ganske nylig. Den blir påtrengende på grunn av noe som vel må oppfattes som grunnleggende nytt i vår tids elektroniske revolusjon, i motsetning til den utvikling av elektronisk kommunikasjon som man opplevet fra slutten av 1800-tallet og i det meste av 1900-årene. Tidligere var det jo praktisk talt alltid mennesker mellom de elektroniske beskjedene og de handlinger de skulle utløse. Om beskjeden var

forfalsket eller ikke kom frem, var det likevel ikke for sent å hindre skadevirkningene. Med den nye teknologi kan et feilaktig elektronisk signal direkte utløse en katastrofal prosess på mottakersiden. Man har ikke lenger mennesket som kontrollør mellom det mottatte signal og den prosess det tok sikte på.

Sikkerhetsproblemene henger altså sammen med at det verdensomfattende nettet som formidler elektroniske signaler, også vil ta imot eventuelle signaler som sendes ut for å gjøre skade. Når man ser hva amatør-"hackere" kan få til, bør man bli bekymret over hva som kan skje dersom ressurssterke grupper eller stater vil lamme våre datasystemer. I tillegg til at det kan gjøres ved hjelp av elektroniske signaler gjennom systemene selv, kan lammelse oppnås ved elektromagnetisk stråling utenfra, eller ved enklere tekniske inngrep på kritiske punkter i infrastrukturen. Lammelse av datasystemer kan i verste fall bety stopp i store deler av transportvirksomheten, stans i livsviktige forsyninger, stans i betalinger med den lammelse av annen virksomhet som det efterhvert vil føre til, og lammelse av forsvaret mot militære og kriminelle angrep, med den risiko det innebærer for økonomi, helse og endog liv.

Direkte katastrofalt kan det bli hvis noen utenforstående ikke bare vil lamme, men lykkes med å forandre elektroniske styringssignaler til automatiserte prosesser, slik at farlig utstyr på mottakersiden begynner å gjøre skade på egen hånd. Og slike skadevoldende signaler kan sendes fra nær sagt et hvilket som helst sted på jorden. Kanskje kan man for eksempel sitte i Asia og skifte fra rødt til grønt signal ved en jernbanelinje i en norsk dal.

Selvfølgelig kan man beskytte seg mot slikt skadeverk gjennom datasystemer. Spørsmålet er om man gjør det godt nok, ikke bare mot dagens angrepsmuligheter, men også mot morgendagens? Dette er internasjonale problemstillinger av betydelig rekkevidde. Jeg velger å illustrere ved et sitat fra "Dagens Næringsliv" for 11.01 i fjor:

Det taiwanske forsvarsdepartementet tror at Kina kan vinne en krig ved hjelp av elektronisk krigføring. Taiwan har mobilisert programmerere til å utvikle farlige datavirus i håp om å lamme fiendens datasystemer i en konflikt.

At dette ikke er for fantasifullt illustreres ved en hendelse i 1999. Efter uttalelser av Taiwans president Lee Teng-hui, som Kina fant provoserende, reagerte Kina

ved å forandre en profil av presidenten på hans egen hjemmeside. (Samme kilde)

Man kan spørre om ikke eierne av elektroniske og andre utsatte systemer selv vil sørge for at de blir sikre nok. Men det er dessverre ikke så enkelt. Hard konkurranse betyr at eierne kan finne det umulig å bruke betydelige midler for å forebygge ulykker som mest sannsynlig ikke inntreffer, selvom de blir fryktelige hvis de kommer. Det gjelder generelt at når skaden ved et sammenbrudd, i data eller andre systemer, blir relativt større for samfunnet enn for eieren, kan det være behov for at staten stiller krav om større sikkerhet enn eierne finner forretningsmessig riktig. I andre tilfelle kan man måtte erkjenne at man ikke oppnår nødvendig soliditet i uunnværlig "infrastruktur" uten at staten betaler for sikringstiltak.

Omfattende utredninger har vist at Norges sikkerhet mot skadeverk gjennom datasystemer ikke er god nok. En slående illustrasjon på riktigheten av Sårbarhetsutvalgets advarsler fikk man så sent som i sommer ved et kabelbrudd i Kristiansand. Brudd på én kabel førte til langvarig stans i alle telekommunikasjoner, inklusive lammelse av informasjon til politi, brannvesen og annen redningstjeneste, helsevesen og flyledelse, i det meste av en landsdel. I dette tilfelle skyldtes bruddet et uhell, men det kunne åpenbart også vært besørget som ledd i en aksjon mot norske interesser. Det foruroligende er ikke at noen kan komme til å bryte en kabel, men at vårt fremdeles statseide teleselskap Telenor har innrettet seg slik at konsekvensene blir så drastiske. Begivenhetene, og bortforklaringene, viser tydelig at telebransjen trenger formyndere.

Mer datasikkerhet er bare en side av et mangfoldig bilde. Vi står også overfor mer konvensjonelle, men likevel farlige trusler fra aggressive stater, terroristgrupper og annen organisert kriminalitet. Endog svake stater kan bruke kraftige ødeleggelsesmidler mot mål som ligger meget lenger borte enn de fjerneste mål som de kunne ramme før. Og både terroristgrupper og annen organisert kriminalitet har enorme resursser, som de kan få fra stater, narkotikahandel eller annen kriminell aktivitet. Tenkelige virkemidler for sabotører, terrorister og andre kriminelle er sterkere sprengstoffer enn før, kjemiske og biologiske skadestoffer, og radioaktivt materiale.

Man kan likevel spørre: Er det nevneverdig risiko for at det lille og avsidesliggende Norge kan bli rammet av slikt? Svaret er ja, til tross for at

politiske motsetninger er blitt mindre i vår del av verden. En grunn er at Norge er blitt en betydelig eksportør av energi til land som kan komme i væpnet konflikt, eller som kan bli mål for voldelige pressgrupper. Våre kunders motstandere kan finne det hensiktsmessig å ramme dem ved å stanse energileveransene fra oss. Gassen er her særlig relevant, men også oljen.

Selvom det er et verdensmarked for olje, kan bortfall av norske leveranser få følelige negative virkninger for vestlige land i konflikt. Det kan motivere sabotasje mot vår produksjon og transport av olje og gass. Men slike motstandere kan også finne det enklest å stanse energieksporten ved å angripe andre deler av det norske samfunn, for at energieksporten skal falle bort som følge av lammelse i andre sektorer. Dessuten: Norges engasjement i andre deler av verden kan skape ikke bare venner, men også fiender, og vi kan bli truet av grupperinger med rene utpresningsformål eller uklare motiver.

"Sårbarhetsutvalget" har levert en omfattende beskrivelse av slike farer mot samfunnets sikkerhet som jeg nå har nevnt, og mange andre former for risiko. På alle punkter skisseres mottiltak, eller retningslinjer for videre utredning. Utvalget anbefaler at man beholder den grunnleggende retningslinje for sikkerhetsarbeidet som man har bygget på gjennom svært mange år nå, nemlig at den instans som har ansvaret for driften av en virksomhet, har også ansvaret for at sikkerheten er god nok. Men vi erkjenner at dette ikke alene kan bli godt nok, av særlig to grunner. Den ene er den normale tendens til at sikkerhetsarbeid altfor lett kan komme i bakgrunnen når tid eller økonomi er presset, hvis det ikke er noen utenfor vedkommende instans som passer på at man ikke forsømmer det. Den andre grunn til at man trenger en fornyelse av hele opplegget er det uvanlig høye tempo i de teknologiske og økonomiske forandringer.

Man må erkjenne at det ikke er mulig, i en tid med så rask teknologisk utvikling som nå, å finne beskyttelse som forblir effektiv i mer enn begrenset tid, nemlig inntil skadevoldere får nye virkemidler til å eliminere effekten av gamle forsvarstiltak. Derfor understreker vi at man må etablere institusjoner med høy motivasjon for å følge med og foreslå nye forsvarsmidler hver gang ny risiko oppstår. Samtidig må de gis en plassering i samfunnet som fører til at de ansvarlige for sikkerheten blir hørt, og vinner kampen mot den lettsindighet som altfor lett brer seg når forrige alvorlige angrep eller ulykke kommer på avstand.

Derfor går utvalget inn for at man langt mer enn i dag samler under ett departement den sivile del av den offentlige innsats for sikkerhet og beredskap. Opprettelse av et slikt departement vil bringe den norske departementsstrukturen mer på linje med det som er vanlig på dette saksområde i andre land. En realistisk vurdering av logikkens trange kår i politikken kan for øvrig gjøre det til et spørsmål av betydning hvilket navn man i tilfelle vil bruke på en slik nydannelse. Hvis man kaller tingen ved dens rette navn, nemlig sikkerhetsdepartementet, risikerer man at assosiasjoner med tidligere kommuniststater hemmer rasjonell tenkning om saken. Derfor ble utvalget stående ved den nokså intetsigende arbeidsbetegnelsen innenriksdepartementet.

I dag er statens sikkerhetsarbeidet spredt på en lang rekke ulike organer, med dårlig koordinering og ofte liten gjennomslagskraft. Et eget departement for større trygghet bør belastes minst mulig med arbeid som ikke har med sikkerhet å gjøre. Derved oppnår man at samfunnets sikkerhet blir kriterium for suksess for en politisk ledelse med tyngde i samfunnsstyringen, mens det i dag knapt er noen sentral leder som blir vurdert efter hva hun eller han gjør for beredskap, bortsett fra at forsvarsministeren blir tillagt ansvar for den militære del av samfunnets sikkerhet, som tross alt gjelder en mindre del av det totale trusselbilde enn før.

En annen viktig side av spørsmålet om et nytt departement er at det kan styrke grunnlaget for effektiv krisehåndtering. Når ett departement har ansvar for de fleste typer mulige krisesituasjoner, vil organisering og øvelse av det apparat som må ta ledelsen når kaos truer, bli vesentlig enklere. Dette vil også gjelde for den innsats som vil bli krevet av landets øverste politiske ledelse: Man vil ikke behøve å samle ledere fra mange departementer for å få tilstrekkelig oversikt, men vil kunne klare seg med et beslutningsorgan med ganske få deltakere. I en krisesituasjon uten normale kommunikasjoner, men med behov for uvanlig raske beslutninger, kan det bli en avgjørende fordel.

Man kan kanskje likevel undre seg over at utvalget kan finne på å foreslå enda et departement, når vi allerede har for mange. Svaret er at et slikt nytt departement for sikkerhet vil avlaste flere andre departementer for så mange oppgaver, at det blir mulig å slå sammen noen av dem og unngå at det samlede antall departementer blir større.

Personlig frykter jeg at det er en viktig mangel ved norsk arbeid for sikkerhet at man ikke er gode nok til å utnytte efterretningstjenestene, og at overvåkingstjenesten ligger langt tilbake i forhold til behovet. Sistnevnte forhold skyldes efter mitt skjønn særlig mangelen på realisme i Stortingets reaksjoner på beretninger om overvåkningen i den kalde krigens tid. Rapporten fra Lundkommisjonen, og særlig den såkalte Furre-saken, førte jo til et partipolitisert kontrollsystem for de hemmelige tjenestene som begrenser mulighetene for hemmelighold, og dermed også begrenser effektiviteten. Sårbarhetsutvalget er sikkert ikke enige om årsakene til at overvåkningstjenesten ikke er så god som den burde være, men kunne samle seg om forslag som vil forbedre situasjonen, nemlig at under et nytt departement for et tryggere samfunn, bør man legge bl.a. politiet, samt en nytt sekretariat for samordning og effektivisering av våre ulike organer for efterretning, overvåkning og sikkerhet.

En sidevirkning av Sårbarhetsutvalgets forslag til overordnet ledelse av sikkerhetsarbeidet, blir at politiet og domstolene vil ikke lenger vil ligge under samme departement. Mange vil vel mene at det vil bli en fordel for rettsstaten om politiet og domstolene ikke lenger får de samme overordnede, slik toppledere i justisdepartementet er i dag. Men dette er spørsmål om rettssikkerhet, ikke sikkerhet i annen forstand. Vanetenkning vil gjøre en slik forandring vanskelig.

Også Direktoratet for sivil beredskap og hovedredningssentralene, og fylkesmennenes og kommunenes beredskapsarbeid vil naturlig sortere under et nytt departement for sikkerhet. Utvalget sier at "Det må være et klart plassert ansvar for ett departement å påse at fylkesmennenes beredskapsarbeid blir tilfredsstillende ivaretatt". Samtidig blir oppgaven for fylkesmennene foreslått noe utvidet ved at flere av statens tilsynsfunksjoner overfor kommunene vedrørende sikkerhet og beredskap plasseres hos dem, og ved forslag om at kommunene pålegges arbeid med kriseplanlegging. Utvalget uttaler også at regelverket for samordning på regionalt nivå under krisesituasjoner bør gjennomgås.

En rekke organer for tilsyn med sikkerheten i ulike sektorer reiser også viktige organisasjonsspørsmål. Det er viktig poeng at tilsyn med sikkerheten, for eksempel ved transport på land, til sjøs og i luften og i telekommunikasjoner, må

bli uavhengige av de politiske lederne som har ansvar for den virksomheten som de skal føre kontroll med.

Det kan man oppnå ved å legge slike tilsyn til det nye departement for sikkerhet. Det er for eksempel ikke bra at jernbanetilsynet sorterer under samferdselsministeren, som samtidig har et ansvar for at jernbanedriften ikke blir for dyr. I et eget departement for sikkerhet vil slike tilsynsorganer også kunne gis bedre muligheter for å utvikle et felles sikkerhetsfaglig miljø. Et solid miljø kan også styrke kontrollorganenes uavhengighet av dem som naturlig vil sette lavest mulige utgifter som et høyt mål.

For sikring av datasystemene kan man få stor nytte av et uavhengig Senter for informasjonssikring, som utvalget foreslår å opprette efter sveitsisk og amerikansk mønster. Det må understrekes at utvalget ikke tenker seg at dette skal være noen statlig institusjon, men et uavhengig organ, gjerne en stiftelse, der offentlige og private deltar i samarbeid på like fot. Meningen er først og fremst å få en "kunnskapsbank", der virksomheter kunne melde inn angrep mot og ulykker med egne datasystemer. Derved kan de bidra til å oppdage nye trusler mot datasystemene, og motta råd om hvorledes sikkerhetsproblemer kan løses. Det er viktig at berørte kan ha kontakt med dette senteret uten risiko for at sensitiv informasjon om deres egen virksomhet lekker ut, til konkurrenter, offentlige myndigheter eller allmennheten.

Når offentlige myndigheter samtidig får kompetanse til å sette klare krav til sikkerhet ved drift av samfunnsviktige datasystemer, og hele tiden fører kravene ajour, mens et uavhengig tilsynsorgan passer på at sikkerhetskravene til enhver tid blir oppfylt, bør sikkerheten mot skadeverk mot norske datasystemer kunne bli god.

Datasikkerhet er også en del av sikkerhetsarbeidet for kraftforsyning og petroleumsvirksomheten. Men disse sektorene er blant dem som krever mer: Bedre fysisk sikring av oljeinstallasjonene og andre samfunnsviktige objekter krever bl.a. effektivisering av samarbeid mellom politi og forsvar. Efter mitt skjønn er gjeldende regelverk for samvirke mellom samfunnets sivile og militære maktorganer bedre egnet til å hindre en gjentakelse av Menstadslaget i 1931 enn til å sikre maksimal effektivitet under en eventuell konfrontasjon med betydelige grupper av terrorister eller sabotører.

Sikring av kraftforsyningen er blitt et større problem fordi mulige motstandere har fått farligere skademidler. Dette kan kreve spesielt omfattende tiltak i Norge, på grunn av risikoen for katastrofeflommer ved brudd på dammer tilknyttet vannkraftverk. Norske dammer ble bygget med meget solide sikkerhetsmarginer i sin tid, men kan likevel være for svake til å motså sabotasje eller missiler med de langt mer effektive sprengstoffer som finnes i dag.

Dessuten betyr det nye konkurransemarked for elektrisitet at man ikke lenger kan regne med at noen frivillig vil holde den reservekapasitet som trenges for å hindre sammenbrudd under særlige belastninger. Nettopp kraftforsyningen illustrerer godt hvorledes nye markedsøkonomiske prinsipper, som blant andre undertegnede er tilhenger av, reiser nye problemstillinger vedrørende sikkerhet: Vårt tidligere ganske dominerende statlige kraftselskap har koblet ut produksjonskapasitet som det normalt ikke er marked for. Men den kapasiteten som er eliminert, ville kunne hindre sammenbrudd i kraftforsyningen dersom man skulle få bortfall av annen kapasitet, eller uvanlig høy efterspørsel. Ved å sløyfe slik reservekapasitet har selskapet styrket sin egen lønnsomhet, men samtidig har man fått økt risiko for at det øvrige samfunn kan bli påført enorme tap ved bortfall av kraftforsyning. Samfunnsøkonomisk er dette ulønnsomt.

Dette er et eksempel på problemer som godt kan løses, men bare hvis ansvaret for at det blir gjort blir klart plassert.

Sikkerheten i oljevirksomheten reiser, i tillegg til den fysiske beskyttelse som jeg allerede har nevnt, også spørsmål om såvel arbeidsmiljø, sikring av det ytre miljø, kvalitet i tekniske installasjoner og øvelse i bruk av dem. Man kan antakelig slå fast at oljeindustrien nå er blitt så stor, med så vidt forgrenede nett av produksjonssteder og transportsystemer, at det er blitt ganske vanskelig å stanse avgjørende deler av leveransene, som ledd i maktbruk mot vårt land eller våre kunder. Likevel vil militære angrep eller sabotasje kunne volde enorm skade, både ved tap av menneskeliv, økonomisk og ikke minst for miljøet. Uten å gå i detalj må jeg kunne si at utvalget ble litt skremt av mangler ved fysisk sikring, og mangler ved forsvarets og politiets kapasitet til å møte mulige angrep med fysiske virkemidler. Risikoen for angrep gjennom datasystemer har jeg allerede nevnt i annen sammenheng. Også dette er områder der bedriftsøkonomiske kalkyler tilsier mindre innsats for sikkerhet enn samfunnet må kreve, med de konsekvenser denne naturlige interesseforskjell må få for regelverk og tilsyn.

Blant andre beskyttelsesbehov for det moderne samfunn behandler utvalget konsekvensene av at forsyningsberedskapen er kommet i en helt annen stilling enn før på grunn av overgang til hyppige leveranser og nedbygging av lagre i nær sagt alle slags virksomhet. Videre understrekes nye problemer i smittevernet, for matvaretryggheten, og i vannforsyningen. Andre typer risiko i utvikling er kjemiske og biologiske stridsmidler, radioaktivt nedfall og massetilstrømning av flyktninger dersom det skulle inntreffe en større atomkatastrofe eller annen forurensningsulykke i områder nær Norge.

Som nevnt omfatter Sårbarhetsutvalgets innstilling en svært lang rekke risiki som man både kan og bør redusere. Til slutt vil jeg bare sammendra det hele ved å understreke at nettopp klar plassering av ansvar, i organer med muligheter for å fylle det står sentralt i utvalgets konklusjoner.

Kilde
www.oslomilsamfund.no

Emner
Forskning, Forsvar, Forsvarspolitikk, Redegjørelse, Sikkerhetspolitikk, Sårbarhet, Teknologi

URI
https://www.virksommeord.no/tale/et-sarbart-samfunn