Fra rådet til tinget
TEKNOLOGIRÅDETS NYHEDSBREV TIL FOLKETINGET

Nr. 162 | oktober 2001

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

Kroppen som identifikation

Nye sikkerhedsteknologier kan beskytte det sårbare samfund, men hvad er prisen?

Nye sikkerhedstrusler fjerner grænsen mellem det civile og det militære >

Moderne samfund er sårbare på mange fronter >

Nye overvågningsteknikker hævdes at kunne have forhindret terrorangreb i USA >

Fornyet debat om overvågningssamfundet >

Sikkerhed er ikke længere et spørgsmål om stater og militær. Et nyt sikkerhedsbegreb er ved at tage form, og det indebærer en ophævelse af grænsen mellem civile og militære mål. Netværk båret af politiske eller økonomiske mål er kommet i forgrunden som fjendebilleder.
Terrorangrebene i USA den 11. september afslørede sårbarheden i det moderne samfund. Det sætter nyt fokus på mulighederne for at sikre offentlige bygninger mod terrorister, at sikre datasikkerheden og stiller spørgsmål, hvilken rolle militæret kan spille i den sammenhæng. Eksperter hævder i dag, at nye overvågnings-teknikker, der identificerer folk på baggrund af deres fysiske kendetegn – såkaldt biometrik – kunne have forhindret terrorangrebene i USA. Men teknologien er fortsat dyr, og i USA har den allerede affødt en fornyet debat om overvågning.

Dette Fra rådet til tinget behandler nye trusselsbilleder og overvågningsteknikker oven på terror-angrebene 11. september 2001

Sikkerhed er ikke længere et spørgsmål om militær styrke og oprustning, som det var tilfældet i industrisamfundet. Store dele af samfundet er afhængige af teknik, hvad enten det er elektricitet, Internet-opkobling eller vandforsyningen. Og samtidig er konfliktlinjerne i den globale politik skiftet fra den kolde krigs globale magtbalancesystem bygget op omkring de to superstater og støttet af stærke stater til en situation, hvor den største trussel mod staters sikkerhed stammer fra globalt organiserede netværk med økonomiske, ideologiske eller religiøse motiver som for eksempel fundamentalistiske terrorgrupper eller kriminelle organisationer.

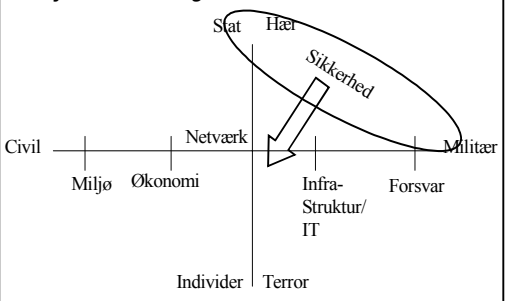
"Traditionelt har et militær med én ydre fjende at gøre. Her handler det om fjender, der danner netværk hen over landene. Og det betyder, at det ikke kun handler om installationer og infrastruktur. Det er også et spørgsmål om sociale, menneskelige og religiøse forskelle," fortæller Niels Johan Juhl-Nielsen, der er sektionsleder i Københavns Brandvæsens Beredskabssektionen.

Den nye sikkerhedstrussel betyder, at det moderne samfund er blevet sårbart, mener Mikkel Vedby Rasmussen, adjunkt og forsker i sikkerhedspolitik ved Institut for Statskundskab ved Københavns Universitet.
"I dag må vi tænke forsvar i meget brede sikkerhedsbegreber, der omfatter både civil og militær sikkerhed. Grænsen mellem civile og militære mål er ved at blive brudt ned. Det vil sige at vi står med nogle systemer (f.eks. vandforsyning, red.), der i udgangspunktet er lavet til at være civile systemer. Man har ikke forventet, at de skulle beskyttes som en militær institution. Hvis man under 2. verdenskrig forestillede sig, at et vandværk blev angrebet af fjenden, forestillede man sig, at det blev bombet.

Derfor er man ikke vant til at tænke over, at det er mindst lige så vigtigt at beskytte pumperne, der eksempelvis kan hackes eller ødelægges på anden vis. Mange institutioner, organisationer og virksomheder betragter overhovedet ikke sig selv som tænkelige mål, og derfor ser de ingen grund til skærpet sikkerhed. Men hvis en eller anden stiller alle trafiklysene på grønt, ødelægger fly-kontrollen og lukker alle vandværker ned, så er der alvorlige problemer," forklarer Mikkel Vedby Rasmussen, der har fået et toårigt stipendiat fra Statens Samfundsvidenskabelige Forskningsråd til et forskningsprojekt om nye sikkerhedspolitikker efter den kolde krig.

I Sverige og Norge har man forsøgt at klargøre sårbarheden i det teknologi-afhængige samfund. I Sverige besluttede forsvarsministeriet i 1999 at udpege en uafhængig komite, der kunne forske i sikkerheden. Det har ført til en sikkerheds- og sårbarhedsudredning, baseret på interviews, besøg og forskning ude i de forskellige institutioner og beredskaber. Rapporten eller betænkningen "Säkerhet i en ny tid" er udkommet i maj i år.
"De seneste år er der kommet mere opmærksomhed på sårbarheden i den tekniske infrastruktur. Elforsyningen, telekommunikationen og IT-sektoren er nok de mest risikofyldte områder, og mange mindre systemer afhænger af de tre. Sårbarheden findes både i fred- og krigstilstande eller under miljø- og naturkatastrofer," fortæller Åke Pettersson. Han er udpeget til "særlig undersøger" og ansvarlig for rapporten, Han er tidligere departementschef i det svenske socialministerium og stedfortrædende chef i Nordisk Råds parlamentariske sekretariat.

Et nyt sikkerhedsbegreb



Sikkerhedsbegrebet har fået et nyt og langt mere omfattende indhold. Hvor sikkerhed tidligere var et militært anliggende forvaltet af stater, er sikkerhed i dag relevant på en lang række militære og civile områder som infrastruktur, IT, økonomi og miljø. Samtidig er de relevante sikkerhedsorganisationer i dag ikke blot stater, men i lige så høj grad internationale netværk.

Nye teknikker kan forbedre sikkerhed

Med det nye trusselsbillede er det i dag blevet aktuelt med nye metoder til at højne sikkerheden omkring samfundets centrale institutioner og anlæg. Udover de traditionelle militære installationer kan det både være miljøinstallationer som vandværk, infrastruktur i form af lufthavne og broer, eller økonomiske strukturer som handelscentre. Terrorangrebet i USA var karakteriseret ved netop at gå efter både militære mål i form af Pentagon, økonomiske mål i form af World Trade Center og – ifølge spekulationer – politiske mål i form af præsidenten. Den store udfordring for sikkerhedssystemerne er, at truslerne ikke kan tilbagevises med militær styrke, men kun gennem indsamling af information, der gør det muligt at gå målrettet efter celler eller noder i terroristers og andre kriminelles netværk. Og den udfordring kan følges helt ned til det enkelte individ.

Der har været argumenter fremme om, at tragedien i USA kunne være afværget, hvis man havde brugt såkaldte biometriske teknologier til overvågning. Biometrik er egentlig et af de ældste redskaber til at identificere andre mennesker med. Begrebet dækker over, at man måler menneskelige karakteristika, såsom stemmen, øjnene eller kropslugten, og mennesker og dyr har altid brugt biometriske metoder til at genkende hinanden, ligesom der principielt set er tale om brug af biometrik, når tolderen sammenligner et ansigt med et pasfoto, eller en ekspedient sammenligner underskriften på dankortkvitteringen men underskriften på dankortet. Med nyere teknologi er det imidlertid muligt med minimalt besvær at indføre biometrisk data i computersystemer og dermed give mulighed for langt mere effektiv og omfattende kontrol. De seneste år er teknologien på området vokset enormt, og der findes nu adskillige velafprøvede metoder til at bruge kroppen som password.

De biometriske metoder finder anvendelse i situationer, hvor det er vigtigt at fastslå en persons identitet. Det kan være i politiet, i banksektoren, i sundhedssektoren, i lufthavnen, hos immigrationsmyndigheder, i computerskikkerhedssystemer og andre lignende situationer.

John Woodward arbejder i den uafhængige amerikanske analyseorganisation Rand Organisation. Organisationen forsker blandt andet i sikkerhed for det amerikanske militær og kan bedst beskrives som en tænketank. John Woodward har skrevet adskillige rapporter om Biometrik, og han er overbevist om, at de nye metoder ikke bare kan forebygge terror. De vil også blive meget anvendte af almindelige mennesker.
"Folk bruger ofte et password, de har nemt ved at huske. Det kan være navnet på deres barn, deres fødselsdato eller bryllupsdag. Den type passwords er nemme at bryde for en hacker. Man kan ikke bryde biometriske koder, så det ene argument for at bruge biometrikken, er, at det er mere sikkert. Et andet argument er, at det er nemmere for brugeren at vise sit øje end at skulle huske sit password. Man slipper

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

for en masse besvær." John Woodward er ikke i tvivl om, at biometrisk teknologi vil forbedre sikkerheden, hvis den bliver indført, fordi teknologien kan understøtte eksisterende sikkerhedsforanstaltninger. For et system er det muligt at sikre genkendelse på tre forskellige niveauer. Man kan have noget på sig, eksempelvis en nøgle eller et kort. Man kan kende noget, eksempelvis en PIN-kode eller et password. Og endelig kan det være noget, man er, altså en biometrik. Meget taler for, at en kombination af de forskellige niveauer vil give den største sikkerhed. "Man kan ikke sige, at biometrikken vil give os 100 procent sikkerhed. Men hvis man kombinerer biometrikken med redskaber som dem, vi kender i dag, må det jo betyde, at man øger sikkerheden. Eksempelvis kan man forestille sig, at medarbejderne i en lufthavn bærer et identifikationskort og samtidig skal lade deres hånd scanne for at få adgang til særlige områder," siger John Woodward.

Brug af biometrik i computersystemer er ikke en teknologisk nyskabelse, men hidtil har teknikkerne været relativt dyre at implementere. I løbet af de seneste år er biometriske metoder dog blevet testet og brugt i forskellige situationer, blandt andet ved store sportsbegivenheder, eksempelvis OL, grænseovergange mellem Israel og Palænstina og mellem USA og Mexico og i pengeautomater i den amerikanske Citibank. John Woodward er overrasket over, at vi ikke bruger biometriske metoder i endnu højere grad.
"Hvert år har jeg troet, at nu var det endelig biometrikkens år, og så er det alligevel ikke slået igennem. Det skyldes, at biometrikken har været utrolig dyr at investere i, men det er ved at ændre sig nu. Desuden er der også en tendens til, at virksomheder og organisationer accepterer det sikkerhedsniveau, de har. Det svarer til at man måske helst ville køre en Mercedes, men man er tilfreds med sin Volvo. Men jeg tror, det vil ændre sig, når priserne på teknologien falder," siger han. Det prisfald er allerede i gang, og ventes at fortsætte i de kommende år.

Ny debat om overvågning

Brugen af biometriske scanninger blandt andet ved store sportsbegivenheder i USA (se boks denne side) har pustet liv i debatten om overvågning. Biometriske metoder er potentielt særdeles effektive, fordi de kan kombinere masseovervågning med lynhurtig elektronisk søgning i databaser. Debatten er ikke uden begrundelse, men den er løjet kraftigt af efter den store tragedie i New York for nylig, mener John Woodward.
"Bigbrother- argumentet mistede meget af sin slagkraft efter det, der skete den 11. september i New York. Det er stadigvæk relevant at diskutere etik omkring overvågning i forhold til ansigtsgenkendelsesteknologien (se tekstboks) og man bliver nødt til at lave nogle fornuftige politikker og regler omkring det. En ansigtsscanner opfanger eksempelvis

Biometri i praksis
I dag findes der biometriske teknikker til at identificere personer ud fra følgende kendetegn:
Fingre og hænder bliver ofte brugt til at identificere mennesker med. Fingeraftrykket er den bedst kendte metode. I dag kan fingeraftryk imidlertid registreres og kontrolleres på et øjeblik gennem elektroniske scannere. I visse miljøer kan fingeraftrykket give problemer på grund af snavs og støv, og her er en måling af hånden eller fingrenes geometri meget anvendelig, eventuelt gennem brug af elektroniske scannere. Typisk bruges det som en nøgle til at åbne døre i eksempelvis bygningskomplekser, hospitaler eller på kontorer. Metoden blev blandt andet brugt ved sommer-OL i 1996 og er en af de mere udbredte metoder, som også bliver vel modtaget blandt brugerne.
Øjnene kan også identificere os. Ved en iris-scanning scannes den farvede ring omkring pupillen, og herved er det muligt at identificere personer med meget stor sikkerhed. Teknikken kræver et kamera, der tager et billede af øjet og foretager en aflæsning af mønsteret. Irisen indeholder 266 forskellige muligheder for måling. Da deltagerne i skiskydning ved vinterolympiaden i Nagano skulle have udleveret våben, brugte man irisscanninger til at identificere dem med. Det er også muligt at foretage biometriske målinger på nethinden, da blodårerne her danner et særligt mønster.
Ansigtet kan også måles og bruges til at fastslå identitet ved brug af algoritmer. Grundlaget for teknikken er måling af en række forskellige afstande og træk i ansigtet. I modsætning til irisscanning og øjenscanning kan det lade sig gøre at foretage målinger uden at den, der bliver målt, er opmærksom på det, fordi det kan foregå gennem et kamera. Samtidig er det muligt at måle mange mennesker på ganske kort tid. Problemet med ansigtsmålinger er, at dårlig belysning eller manglende samarbejdsvilje hos brugeren – hvis man eksempelvis vrænger ansigt – kan give et dårligere resultat. Metoden har været brugt i forsøg, hvor man har identificeret butikstyve i butikker eller kriminelle i udvalgte byområder. I Florida brugte man teknikken til den store Superbowl finale i amerikanske fodbold, der hvert år overværes af tusinder af tilskuere. For at beskytte mod terrorister foretog man scanninger af publikums ansigter og sammenligner med billeder i en database.
Stemmen kan nemt genkendes på digitale målinger. Typisk vil man bruge en password-sætning, men nogle systemer kan også genkende en stemme ud fra vilkårlige ord. En telefon eller en mikrofon kan bruges som sensor, og fordelen er, at teknikken er billig at implementere. Stemmegenkendelse har dog den svaghed, at stemmen kan ændre sig over tid, i forbindelse med sygdom eller den kan påvirkes af baggrundsstøj.
Underskriften kan genkendes på dynamikken i håndskriften eller i den rytme, en person taster sit navn på et computertastatur. Man kan måle, hvor hurtig der skrives, hvor hårdt der trykkes, retningen der skrives i og bogstavernes form. Målingen kan foretages gennem det underlag, der skrives på.

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

alle ansigterne i en lufthavn og sammenligner dem med billeder fra en database. Spørgsmålet er så hvis billeder, der ligger i databasen? Man skal jo ikke stoppes i lufthavnen, fordi man har glemt at aflevere sine biblioteksbøger," siger han. Dermed peger den biometriske teknologi på det bredere problem, at udvidelsen af sikkerhedsbegrebet medfører en udvidelse af de områder, hvor overvågning med henblik på forebyggelse af kriminalitet kan komme på tale.

Super Bowl - et eksempel

I den 35. Super Bowl turnering i Florida valgte myndighederne at bruge biometrisk ansigtsgenkendelse til at spore eventuelle balladem agere, kriminelle eller terrorister. Overvågningskameraerne blev sat til jævnligt at foretage scanninger af publikums ansigter og foretage geometriske målinger (se tekstboks). Resultatet er et såkaldt "faceprint", der kan køres gennem politiets databaser for at se, om der er nogle sammenfald med registrerede personer. Ansigtsgenkendelsesteknikkerne kan anvendes uden, at den der bliver undersøgt er opmærksom på det, og derfor skærper brugen af netop denne teknik overvågningsproblematikken. Brugen af teknikken til Super Bowl fik amerikanerne til at spørge, om det ikke var krænkende for privatlivet at bruge ansigtsscanninger til den type arrangementer. Kritikere af fremgangsmåden mener, man skal have en individuel, begrundet mistanke før man kan køre en persons ansigtstræk gennem det digitale forbryderalbum. Fortalerne argumenterer for, at oplysningerne hverken bliver gemt, givet videre eller kørt sammen men andre databaser end de aftalte. Og at privatlivet krænkes mindre, fordi ansigtsscanninger ikke i samme grad som en metaldetektor eller lignede forstyrrer den, der kontrolleres. Problemet er ifølge kritikerne, at det principielt er muligt for de offentlige instanser at udøve en ret høj grad af overvågning, især ved sammenkøring af flere forskellige registre. Og samtidig er det muligt gennem videooverv ågninger lagret på bånd efterfølgende at spore en bestemt persons færden. Det bedste argument for at benytte biometriske metoder som ansigtsgenkendelse er, at det kan forhindre terror og krisesituationer, fordi sikkerhedsniveauet forbedres. Overvågningskameraer (uden ansigtsgenkendelse) har beviseligt ført til en reduktion af kriminalitet, eksempelvis i Newham i England.

Københavns lufthavn venter

Efter terrorangrebene mod USA i september er opmærksomheden rettet mod sikkerheden i lufthavne verden over. I Københavns lufthavn ser sikkerhedschef Anders Maegaard dog ikke nogen umiddelbar metode til at skabe større sikkerhed. Luftavnen retter sig efter de regler, der bliver stukket ud af ICAO, international civil aviation organization, og som privat virksomhed er det ikke tilladt for lufthavnsselskaberne at udføre noget, der minder om politiarbejde. Derfor kan man heller ikke tjekke passagerne ved hjælp af biometriske metoder, idet man ikke har adgang til politiets databaser over forbrydere og terrorister.

"Biometriske metoder vil aldrig kunne bruges til at tjekke passagerer med. Det er fuldstændig urealistisk at lave en database, der er stor nok til at systemet ville være af nogen værdi. Som privat virksomhed har vi ikke adgang til politiets oplysninger, og der skal være fuldstændig vandtætte skotter imellem for at beskytte retssikkerheden. Og hvordan skulle vi bære os ad med at få oplysningerne fra resten af verden? Der er en meget tydelig distinktion mellem politi- og lufthavnsopgaver," siger Anders Maegaard. Det er dog ikke usandsynligt, at lufthavnen vil overveje at indføre biometriske teknikker som eksempelvis iris-scanninger på personaleområdet.

"I dag bliver der lavet et baggrundstjek af de ansatte hos politiet. Og for at få adgang benytter man et kort med en magnetstribe og et billede. Billedet kommer op på en skærm, og så tjekker sikkerhedspersonalet, at det er kortets ejer, der får adgang. Hvis prisen var mere overkommelig, kunne vi godt overveje at bruge iris-scanninger. Men dels har vi allerede et system, der virker tilfredsstillende og dels kan man jo ikke se, om en person har et våben i hånden, selv om man scanner deres øje. Derfor kræver de fleste situationer, at sikkerhedspersonalet er fysisk til stede," forklarer Anders Maegaard.

Fælles europæisk ID-kort?

Ian Smith, der er generalsekretær for den engelske Association of Biometrics, er ikke helt enig i, at man ikke kan lave store databaser. Ligesom andre af de eksperter Teknologirådet har talt med, mener han, at der er en generel tendens til, at borgerne er villige til at gå på kompromis med retten til totalt privatliv for at højne sikkerhedsniveauet. Det kan betyde, at der kommer mere fokus på, hvor man kan bruge biometriske metoder.

"Jeg har netop været til en konference, hvor vi så et videoklip af to af terroristerne fra angrebet mod World Trade Center, der gik ombord i flyvemaskinen. Eksperterne fastslog, at en ansigtscanner teknisk set kunne have stoppet de to terrorister, hvis

Amerikanere vil registreres efter terrorangreb
Fortalere for nationale identitetskort i USA og Storbritannien opfordrer nu til at indføre kort med indlagte biometriske data som for eksempel fingerscan eller facescans. Et sådant forslag ville i USA gøre det nødvendigt at tage fingeraftryk af millioner af amerikanere og oprette en national database, der kobler den enkelte borgers biometriske data med identifikationsinformation, straffeattest og andre oplysninger, som politiet vurderer, det er vigtigt at efterspore.
Kilde: Wired Magazine online: ID Cards Are de Rigueur Worldwide, 25. september

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

deres oplysninger fandtes i databasen. Den slags får en til at tænke, og på den måde tror jeg, tragedien i New York har fremskyndet udviklingen af biometrikken." Ian Smith mener, at der ligger et arbejde forude med at undersøge, hvilke biometriske metoder, der vil være mest relevante og sikre at anvende og i hvilke situationer, de skal bruges. Han peger på vigtigheden af internationale standarder og samarbejde.
"Man kan sammenligne det med, at man har forskellige radiofrekvenser i Europa, så man skal skifte kanal på sin bilradio, når man kører ned igennem landene. Den situation skal vi undgå, og derfor skal man bruge en ensartet teknik. Her har der været snak om at lave et fælles europæisk identitetskort, hvor eksempelvis en biometrisk fingeraftrykksteknik bliver brugt i alle lande," påpeger han.

Omstilling af beredskabet

Det er en vigtig pointe i den svenske sikkerhedsudredning, at de store forandringer på sikkerhedsområdet stiller nye og væsentlige krav til organiseringen af det moderne forsvar, blandt andet gennem omstilling af det traditionelle militær og forsvar til sikkerhedsopgaver. Eksempelvis for at sikre den nødvendige ekspertise til at rette op på en stor skade i et IT-system.
"I Sverige begyndte vi omstillingen af det militære forsvar for et år siden", fortæller Åke Pettersson.
"Tidligere har det civile og militære beredskab været meget klart adskilte, men nu skal der opstå et tættere samarbejde. I princippet skal alle, der er berørt af en eventuel hændelse, være i stand til at arbejde sammen, og derfor skal de også træne sammen. Det er vigtigere at fremme samarbejdet på lokalt niveau end at fremme overordnet ledelse og styring," forklarer han.
I forbindelse med udredningen har han dog erfaret, at det er svært at organisere og koordinere samarbejdet mellem det civile beredskab, militæret og andre spillere. "En væsentlig problemstilling er at få etableret samarbejde mellem de mange forskellige myndigheder, instanser og organisationer, der har hver deres kompetencer på forskellige områder. Hvis man skal kunne løse store kriser, er det nødvendigt med fælles planlægning og koordination, og et af de forslag, vi kommer med i rapporten går eksempelvis ud på at afvikle to af de statslige myndigheder, der eksisterer i dag og oprette en ny og mindre, der skal fokusere på IT-sikkerhed. Det er ikke altid lige populært at komme med den slags forslag," fortæller Åke Pettersson.

Mikkel Vedby Rasmussen fra Københavns Universitet forklarer, at vi vil opleve den samme problemstilling i Danmark. Hvor man tidligere har haft et meget klart skel mellem militære og civile opgaver, er der nu i høj grad et overlap. " For at matche de behov, der findes i dag, skal en hær være uddannet på alle mulige forskellige områder, og det militære forsvar skal integreres i det civile forsvar. Eksempelvis skal forsvaret kunne spille en rolle, hvis der sker et cyberangreb i en offentlig institution. Det bliver sværere at definere, hvor en politiopgave stopper og en opgave for forsvaret begynder."
Og ifølge Åke Pettersson er der ingen vej udenom. Det er nemlig ikke muligt at udelade den sårbare teknologi.
"Vi er meget afhængige af de tekniske systemer, og kan slet ikke klare os uden. Også i forsvaret bruger man mere og mere IT. Men der kan blive enorme skader, hvis nogen vælger at udnytte sårbarheden eksempelvis i form af en computervirus," siger han.

I Danmark har vi stadigvæk ikke gjort os så mange tanker om, hvilke nye sikkerhedstiltag det sårbare samfund kræver. Og det bliver vanskeligt at skaffe pengene til omstillingen, mener Mikkel Vedby Rasmussen. "Den største udfordring nu er at forstå den omstilling, der sker i forhold til sikkerheden og være opmærksom på forandringen og udviklingen. Det kræver utroligt store investeringer at omstille forsvaret til sikkerhedsopgaver, og det kan godt blive en vanskelighed. Det er nemmere at forhold sig til at bruge penge på kampvogne end på software og research," siger han.

Niels Johan Juhl-Nielsen, der er sektionsleder i Københavns Brandvæsens Beredskabssektionen, er fortaler for danske initiativer, der modsvarer de svenske og norske sårbarhedsudredninger. Terrorangrebet mod New York i september har åbnet op for mere forskning på området, mener Niels Johan Juhl-Nielsen.
"Man er nødt til at foretage nogle risikoanalyser, så man ved, hvordan man kan komme igennem en krise. Eksempelvis har Trondhjems tekniske universitet i Oslo kortlagt i alt 318 risici og delt dem op i 20 overordnede grupper. Herefter kan man så foretage øvelser, og få beredskabet til at matche sårbarheden, og på den måde kan vi mindske den. Efter orkanen forrige år lavede man en naturberedskabsplan, og det var en fejlfokusering. Vi har brug for et fleksibelt beredskab bygget op om en grundstruktur, der kan løse et væld af forskellige opgaver."

Men det bliver ikke nemt at lave omstillingen, for det er i lige så høj grad en menneskelig omstilling, mener Niels Johan Juhl-Nielsen.
"Omstillingen af militæret handler meget om kultur. Traditionelt har et militær med én ydre fjende at gøre. Her handler det om fjender, der danner netværk hen over landene. Og det betyder, at det ikke kun handler om installationer og infrastruktur. Det er også et spørgsmål om sociale, menneskelige og religiøse forskelle. Det handler altså ikke kun om materiel modstandskraft, men i lige så høj grad om dialog, demokrati og åbenhed. Hele miljøområdet har eksempelvis opnået stor opmærksomhed og er i flere henseender blevet væsentligt bedre og mere

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm

sikkert, fordi alle er blevet enige om, at de gerne vil passe på miljøet."

Og selvom det kan være svært at identificere truslen eller fjenden, mener Niels Johan Juhl-Nielsen, at det er muligt at skabe et vist niveau af forebyggelse. "Desværre skal der nok nogle flere katastrofer til, før man kan sige, hvad der skal til af forebyggelse. Men det er vigtigt også at lave øvelser ud fra en række scenarier og forestille sig, hvordan man ville reagere i forskellige situationer. Man kan gøre nogle konkrete ting, eksempelvis lave en række tekniske løsninger, som man har gjort på IT området for at gøre det mere robust. Og så er det meget vigtigt, at der bliver lavet risikoanalyser. Vi må gøre os klart, hvad det er for en beredskabskultur og sikkerhedskultur, der skal til. Her er vi på vej ind i noget helt nyt," siger han.

Kilder til faktabokse: www.biometrics.org, www.rand.org eksempelvis http://www.rand.org/publications/RB/RB3024/ eller http://www.rand.org/natsec_area/products/biometrics.html

Fra rådet til tinget udgives af Teknologirådets sekretariat. Dette nummer er skrevet af Torben Clausen og Maj Juni fra Konsulenthuset Wetware A/S

De seneste fem numre af Fra rådet til tinget er:
161: Open Source Software er ikke slået igennem
160: Styr på medicinsk udstyr?
159: Dyr biobrændsel til transport
158: Betal med Mobiltelefonen
157: GMO-debat i krydsild

Udgiver
Teknologirådet
Antonigade 4
DK - 1106 København K
Tel. 33 32 05 03
rtt@tekno.dk

Redaktion
Morten Jastrup (ansv.)
Mette Bom
Ida Leisner

Abonnement
Gratis pr. email
Tilmelding på:
rtt@tekno.dk
Tidligere nyheds-
breve findes på:
www.tekno.dk/rtt.htm