

Overvåkning, personvern og sikkerhet

Hva mener du?

surprise
surveillance
privacy
security



«Dette prosjektet har mottatt støtte fra EUs syvende rammeprogram for forskning og teknologiutvikling, under kontrakt nummer 285492.».

Contents

1	Velkommen til SurPRISE.....	5
2	Sammendrag	6
3	Overvåkning, personvern og sikkerhet.....	8
3.1	Overvåkning	8
3.2	Personvern og datalagring – viktige utfordringer	8
3.3	Sikkerhet.....	9
4	Ny sikkerhetsteknologi.....	10
5	Smarte overvåkningskameraer	11
5.1	Hvorfor ble smarte overvåkningskameraer utviklet?.....	11
5.2	Hvordan brukes smarte overvåkningskameraer?.....	12
5.3	Økt sikkerhet.....	13
5.4	Utfordringer.....	13
6	Droner.....	14
6.1	Hvorfor ble droner utviklet?.....	14
6.2	Hvordan brukes droner?.....	15
6.3	Økt sikkerhet.....	16
6.4	Utfordringer.....	16
7	Pakkesniffing og overvåkning på internett.....	17
7.1	Hvorfor ble pakkesniffing utviklet?.....	18
7.2	Hvordan brukes pakkesniffing?	18
7.2.1	Kommersiell bruk.....	19
7.2.2	Sikkerhetsorientert bruk.....	19
7.3	Økt sikkerhet.....	19
7.4	Utfordringer.....	19
8	Sporing av smarttelefoner.....	21
8.1	Hvorfor ble sporing av smarttelefoner utviklet?.....	21
8.2	Hvordan brukes sporing av smarttelefoner?.....	22
8.2.1	Kommersiell bruk.....	22
8.2.2	Sikkerhetsorientert bruk.....	23
8.3	Økt sikkerhet.....	23
8.4	Utfordringer.....	23
9	Biometri	24
9.1	Hvorfor ble biometri utviklet?	24
9.2	Hvordan brukes biometri?	24
9.3	Økt sikkerhet.....	25
9.4	Utfordringer.....	25
10	Er overvåkningsteknologi den eneste løsningen?.....	27
10.1	Alternative sikkerhetstiltak: globalt og nasjonalt.....	27
10.2	Alternative sikkerhetstiltak: lokalt	27
11	Tilbake til deg.....	29
	Partnere.....	31

1 Velkommen til SurPRISE

SurPRISE er et europeisk forskningsprosjekt. Navnet SurPRISE står for overvåking, personvern og sikkerhet (Surveillance, Privacy and Security). Målet med prosjektet er å få vanlige folks syn på ny sikkerhetsteknologi. Mye av denne teknologien baserer seg på overvåkning av personer. Den blir brukt av politi eller sikkerhetspersonell for å følge med på hva som skjer, og for å oppdage og avverge kriminelle handlinger.

Når du skal ut på reise og bagasjen din skannes automatisk eller når du blir filmet av et overvåkningskamera på gaten, er du i kontakt med overvåknings- og sikkerhetsteknologi. SurPRISE har som mål at slik teknologi skal være effektiv og trygg, og ivareta menneskerettigheter og personvern. For å få til dette trenger vi din hjelp.

Vi har invitert deg til å delta i SurPRISE-prosjektet fordi EU-kommisjonen ønsker å komme i kontakt med innbyggere i hele Europa, og få vite hva de kan gjøre for at du skal føle deg trygg. Ved å delta i

workshopen får du mulighet til å dele dine meninger om sikkerhetsteknologi.

SurPRISE undersøker innbyggers syn på sikkerhetsteknologi i ni europeiske land: Østerrike, Danmark, Tyskland, Ungarn, Italia, Norge, Spania, Sveits og Storbritannia.

Dette heftet gir deg en innføring i temaene som skal diskuteres på den norske workshopen i juni 2014. Du får informasjon om ny sikkerhetsteknologi, men også mer generell informasjon om overvåkning, sikkerhet og personvern i Europa.

Nettopp fordi du ikke er ekspert på temaet, er din deltakelse i workshopen viktig. Vi har invitert vanlige innbyggere som blir påvirket av de beslutningene som tas av norske og europeiske politikere.

Det er politikere som utformer politikken, men du som innbygger må leve med disse beslutningene. Det gjør din mening viktig.

Vitenskapen gir oss informasjon, men forteller oss ikke hva vi skal gjøre. Valget er vårt. Si din mening!

2 Sammendrag

Mange mennesker kan ikke forestille seg et liv uten smarttelefoner, bankkort eller internett. Men de tenker kanskje ikke over hvor mange elektroniske spor slik teknologi etterlater seg i løpet av en dag. Disse sporene kan si hvor vi befinner oss på ulike tidspunkt og hva vi gjør. Banktransaksjoner, som for eksempel de som gjøres med et bankkort, kan fortelle hvor og hva vi handler. Dette er informasjon som oppbevares i bankenes databaser og som er synlig på kontoutskriften.

Flyselskapenes bestillingsinformasjon forteller om vi reiser til eller fra et høyrisiko-land. Mobildata kan fortelle hvor vi befinner oss, hvem vi snakker med og hvor ofte vi ringer dem. Teleselskapene oppbevarer denne typen informasjon i faktureringsdatabaser og derfor er det mulig å identifisere, lokalisere og spore de fleste av oss.

Andre kan også dra nytte av informasjonen fra denne typen teknologi. I kjølvannet av større terrorangrep i Europa og i verden, har myndighetene i mange land investert i avansert sikkerhetsteknologi. Lover har også blitt endret og vedtatt slik at myndighetene får tilgang til denne typen informasjon i sikkerhetsøyemed. Myndighetene har innsett at terrorister og kriminelle kan spores gjennom andre kilder enn de mer «tradisjonelle» etterretningskildene. Terrorister har også et hverdagsliv som er veldig likt alle andres; de har bankkontoer og identitetspapirer, og de bruker internett og mobiltelefoner. De bruker også offentlig transport, de ferdes på offentlige steder og kjøper varer og tjenester. Det kan hende at informasjon om denne typen aktiviteter kan være viktig for å spore opp kriminelle. Mange myndigheter tror også at denne typen informasjon kan gjøre det mulig å stanse terrorister og kriminelle før de handler. Fordi noen typer sikkerhetsteknologi bruker denne typen informasjon, blir de betegnet som «overvåknings- og sikkerhetsteknologi» i SurPRISE-prosjektet.

En sikkerhetsteknologi som baserer seg på overvåkning er:

«en type teknologi som bruker informasjon om befolkningen, innhentet fra forskjellige kilder og i

ulike sammenhenger, i den hensikt å løse en sikkerhetsutfordring.»

Slik teknologi analyserer informasjon fra innbyggernes hverdagsliv, for eksempel fra mobiltelefoner, internett eller fra «smart» teknologi som nye typer overvåkningskameraer som forsøker å identifisere kriminelle handlinger.

I dette informasjonsheftet vil vi se nærmere på fem slike teknologier:

- **Smarte overvåkningskameraer:** Overvåkningskameraer som gjør mer enn passivt å overvåke det offentlige rom. Smarte overvåkningskameraer består av digitale kameraer og programvare som kan gjenkjenne ansikter, analysere adferd og oppdage gjenstander.
- **Sivile droner:** Sivile droner er ubemannede luftfartøy for ikke-militær bruk. De kan bli brukt til en rekke ulike formål som involverer overvåkning. En drone kan bli utstyrt med kamera eller andre sensorer, og på mange måter er det en mobil versjon av overvåkningskameraet.
- **Overvåkning på nett ved pakkesniffing:** Ved bruk av spesifikke typer maskin – og programvare kan meldinger som blir sendt over internett bli lest, analysert og endret.
- **Sporing av smarttelefoner:** Ved å innhente posisjonsdata fra smarttelefoner, kan man analysere hvordan den som bruker telefonen beveger seg. Smarttelefonens posisjonsdata kan angis av GPS-systemer, trådløse nettverk og mobilmaster.
- **Biometri:** Ulike metoder kan brukes for å gjenkjenne individer basert på fysiske trekk eller adferdsmønstre. Et eksempel er biometriske pass som baserer seg på ansiktsgjenkjenning, finger- og/eller irisgjenkjenning.

Sikkerhetsteknologi kan bidra til å øke sikkerhet gjennom å identifisere mistenkte og kriminelle, og avdekke ulovlige aktiviteter. De kan også bidra til å gjøre livet enklere for folk. Men teknologien har også ulemper. Smarte overvåkningskameraer og droner fungerer kun under gitte forhold og kan utløse falske alarmer. Overvåkning på nett kan

bidra til at personvernet brytes ned. Sporing av smarttelefoner er vanskelig å begrense fordi mange applikasjoner sender posisjonsdata uten at brukeren vet det. Biometrisk informasjon på avveie kan føre til identitetstyveri. Manglende kontroll over innhenting og bruk av informasjon er en gjennomgående utfordring ved alle teknologiene vi skal se på.

Bruk av slik teknologi reiser problemstillinger rundt menneskerettigheter, personvern, regulering og tillit. Vanligvis samler og deler slik teknologi informasjon om individer uten at de vet om det. Data om uskyldige personer blir helt bevisst samlet inn og analysert. På grunn av dette er de potensielt svært personverninngrepene. Det kan også føre til at uskyldige mennesker blir feilaktig identifisert som kriminelle, noe som kan ha alvorlige konsekvenser.

Noen innbyggere er usikre på hvordan de skal forholde seg til at personopplysninger brukes i sikkerhetsteknologi. Dersom samfunnet blir tryggere kan det kanskje aksepteres, men hva om det også fører til at grunnleggende rettigheter brytes? Folks holdninger kan være avhengig av hvordan de forholder seg til andre spørsmål, som for eksempel:

- Fører bruken av sikkerhetsteknologi til et tryggere samfunn?
- Hvor problematisk og påtrengende er teknologien?
- Finnes det lovverk som regulerer bruken?
- Brukes teknologien i samsvar med lovverket?
- Har vi tillit til institusjonene som bruker teknologien?
- Er det klare retningslinjer for hvordan den innsamlede informasjonen kan brukes?
- Er institusjonene som bruker teknologien åpne om denne bruken? Kan de ble holdt ansvarlige hvis de bruker teknologien på en problematisk rolle?
- Hvem holder et øye med overvåkerne?
- Finnes det andre alternativer som ikke baserer seg på overvåkning?

Dette er noen av spørsmålene som vil bli diskutert på workshopen.

Mer kunnskap og tilgjengelig informasjon er blitt viktig for at innbyggere skal kunne delta i samfunnsdebatten når det kommer til temaer relatert til vitenskap og teknologi.

3 Overvåkning, personvern og sikkerhet

3.1 Overvåkning

Når vi tenker på overvåkning, dukker en rekke assosiasjoner opp. Kanskje du tenker på “Big Brother” – enten reality-programmet eller George Orwells bok “1984”. Derfor er det lett å knytte begrepet overvåkning til en uggen følelse av å bli iaktatt av en mektig, men ukjent organisasjon eller person.

Når vi snakker om overvåkning i SurPRISE-prosjektet, tenker vi på det som:

«å observere mennesker for å regulere eller styre deres adferd, til ulike formål».

Overvåkning kan iverksettes av sikkerhetshensyn. For eksempel kan politiet bruke overvåkingskameraer eller droner til å få øye på kriminelle. Overvåkning kan også brukes kommersielt. For eksempel kan en søkemotor overvåke nettbruk, analysere søkshistorikk og besøksmønstre for å forbedre tjenesten sin. Overvåkning kan altså brukes til å forhindre kriminalitet og finne kriminelle, men det kan også brukes til å tilby og forbedre produkter og tjenester.

Dersom overvåkning er så utbredt og integrert i samfunnet, lurar du kanskje på hva som kan være galt med dette? Nyhetsartikler om det som kalles «overvåkingssamfunnet» har ofte en dyster undertone. Å ha kontroll over overvåkningsteknologi medfører mye makt. Derfor er det viktig at de som har denne muligheten, for eksempel i politiet eller næringslivet, bruker makten i tråd med lovene og respekterer våre rettigheter.

Hvem som driver med overvåkning, hvorfor de gjør det og hva de leter etter, kan påvirke ditt syn på overvåkningen. Kanskje du mener at du ikke har noe å skjule, og at det derfor ikke er så nøye? Hvis noen plutselig bestemmer seg for å overvåke deg på grunn av din religion, etnisitet, kjønn eller politiske holdninger, forandrer du kanskje mening. Det er på grunn av slike ting at overdreven overvåkning kan ha negative konsekvenser for menneskerettighetene, som for eksempel ytringsfriheten. Det kan også svekke tilliten i samfunnet, fordi

folk kan bli redde for å være seg selv. Det er derfor en vanskelig balansegang å anvende ulike typer overvåkningsteknologi i sikkerhetsøyemed.

3.2 Personvern og datalagring – viktige utfordringer

En av de viktigste utfordringene handler om personvern og hvordan dataene som samles inn av sikkerhetsteknologi kan lagres på en sikker måte. Personvern kan bety forskjellig ting for forskjellige mennesker, men det er en viktig del av vårt hverdagsliv. Det kan være mye du ikke alltid vil dele med andre:

- Hva du gjør, tenker og føler
- Informasjon om intime forhold, hvor du befinner seg, hva du kommuniserer til andre og bilder av deg selv
- Hvor mye av kroppen din du viser, uønsket kroppsvisitering, og om du kan kontrollere hvordan ditt fingeravtrykk eller DNA blir brukt

Ville du vært fornøyd med at forsikringsselskapet ditt hadde ubegrenset tilgang til pasientjournalen din? Eller om politiet hadde anledning til å avlytte alle samtaler dine? Har du gardiner i huset ditt?

Om du svarer «nei» på de to første spørsmålene og «ja» på det siste, så er du likevel opptatt av personvern! Og du er ikke alene. Studier av unge menneskers nettvaner viser at de er veldig selektive med den informasjonen de legger ut på sosiale medier. Folk ønsker å dele informasjon, men innenfor visse grenser. Det er disse grensene som markerer hvor personvernet gjelder.

I SurPRISE definerer vi personvern som:

«et individs mulighet til å være utenfor offentlighetens søkelys, og individets kontroll over sin egen personlige informasjon».

Retten til personvern og beskyttelse av personopplysninger, er en grunnleggende rettighet i Europa. Alle har behov for personvern for å kunne handle fritt, møtes, diskutere og debattere i et demokratisk samfunn. Det er ikke mulig å utøve dine demo-

kratiske rettigheter hvis andre vet alt om dine tanker, intensjoner og handlinger. Personvernlovgivningen som utvikles i Europa nå, legger vekt på at personvern skal være tenkt inn i ny teknologi. Bedrifter som utvikler teknologi oppfordres til å ta hensyn til personvernet fra starten av. Denne nye tilnærmingen kalles «innebygd personvern».

3.3 Sikkerhet

I SurPRISE-prosjektet definerer vi sikkerhet som:

«en tilstand der en er beskyttet mot, eller ikke utsatt for, fare; en følelse av trygghet eller fravær av fare».

Sikkerhet handler ikke bare om beskyttelse av fysiske ting (som bygninger, informasjonssystemer, nasjonale grenser osv.), men også om menneskers trygghetsfølelse. I en ideell verden ville effektive sikkerhetstiltak ført til en sterkere trygghetsfølelse, men dette er ikke alltid tilfellet.

Siden ny sikkerhetsteknologi kan føre til brudd på personvernet, kan den paradoksalt nok ende opp med å få folk til å føle seg mindre trygge. Men denne følelsen deles ikke nødvendigvis av alle. Også sikkerhet kan bety forskjellige ting for forskjellige mennesker. Hver og en av oss har formeninger om hva vi betrakter som en trussel mot vår egen sikkerhet, og hvor langt vi er villige til å gå for å beskytte det som er viktig for oss.

Dette er også tilfellet for de som har ansvaret for samfunnets sikkerhet. De må identifisere og håndtere de mest alvorlige truslene med begrensede økonomiske, menneskelige og tekniske ressurser. Derfor må de gjøre prioriteringer. For EU er de viktigste prioriteringene å:

- Øke sikkerheten på internett for innbyggere og næringer i Europa
- Oppløse internasjonale kriminelle nettverk
- Forhindre terrorisme
- Styrke Europas evne til gjenoppbygging etter en krise eller katastrofe

Fordi gjenoppbygging er en av EUs prioriteringer, har sikkerhetsbegrepet blitt utvidet utover terror- og kriminalitetsforebygging. EU fokuserer også på trusler mot miljøet, naturressurser, infrastruktur, næring og helse. Sikkerhet er noe som inngår i nesten alle saksområder. Denne tilnærmingen finner man i mange europeiske land. Men er det i det hele tatt mulig å etterleve garantien om full sikkerhet og trygghet på alle samfunnsområder? Sikkerhetsindustrien er en ny og rask voksende industri under utvikling i Europa. Industrien inkluderer store produsenter knyttet til forsvar, men også mindre selskaper vokser fort. Nyere utvikling innen overvåkning- og sikkerhetsteknologi inkluderer blant annet:

- Smarte overvåkningskameraer, som fokuserer på å fange opp bilder av kjente kriminelle og å identifisere mistenkelig adferd før en kriminell handling blir begått
- Teknologi for overvåkning på nett som har til hensikt å oppdage virus, hackere eller identitetstyver
- Biometri som brukes for å hindre at uvedkommende får adgang til et territorium og for å effektivisere reisen for de som har blitt definert som «sikre» av myndighetene
- Droner, som fra luften kan filme farlige aktiviteter som ellers ikke er mulig å få øye på fra bakken
- Avansert innsamling av informasjon om flypassasjerer, med den hensikt å oppdage individer som kan utgjøre en trussel før de reiser inn eller ut av landet
- Sporingsteknologi som kan sikre transport og forsendelser, og spore opp mistenkte i kriminalsaker

4 Ny sikkerhetsteknologi

De fem teknologiene som diskuteres i SurPRISE-prosjektet er:

- Smarte overvåkningskameraer
- Droner
- Overvåkning på nett ved pakkesniffing
- Sporing av smarttelefoner
- Biometri

Disse sikkerhetsteknologiene er fortsatt under utvikling, og det er mulig å påvirke hvordan bruken av dem skal reguleres.

I de neste kapitlene beskriver vi hvordan teknologien fungerer, hvorfor den har blitt utviklet, hvem som bruker den og hvordan den brukes. Vi skal også beskrive hvordan den kan bidra til økt sik-

kerhet og hvilke utfordringer den medfører for personvernet.

Det er viktig for SurPRISE-prosjektet og for EU å forstå hvordan folk oppfatter sikkerhetsteknologi og om bruk av slik teknologi er noe befolkningen aksepterer. Derfor er din mening viktig. Det kan hende at du allerede har sterke meninger for eller mot sikkerhetsteknologi. På workshopen får du anledning til å si hva du mener, og vi ønsker spesielt at du skal tenke på følgende spørsmål:

Hva avgjør om du aksepterer eller ikke aksepterer ny sikkerhetsteknologi?

Er det:

- å ha kjennskap til teknologien, og hvordan den fungerer?
- å vite mer om institusjonene som benytter seg av teknologien, og hva slags type informasjon teknologien bidrar med?
- at bruken er regulert og kontrollert av et lovverk?
- å være bedre informert om de sikkerhetsutfordringene vi står overfor, og som teknologien er ment å løse?

Eller kanskje det handler om hvor sterkt teknologien utfordrer personvernet? For eksempel:

- setter den deg i forlegenhet på noen måte?
- bryter teknologien med grunnleggende menneskerettigheter?
- blir privat informasjon delt med tredjeparter uten ditt samtykke? Eller påvirker den privatlivet ditt på andre måter?

Kanskje er det et spørsmål om hvor effektiv teknologien er?

- forenkles hverdagen din?
- føler du deg tryggere?
- er den et effektivt redskap for å identifisere kriminelle?

Kanskje du kun tenker på sikkerhetsteknologi når du merker at den er i nærheten av deg, for eksempel på flyplasser, på gata, når du bruker en mobiltelefon eller er på internett. Kanskje du har et avslappet forhold til sikkerhetsteknologi nå, men er bekymret for hvordan dette kan brukes i fremtiden?

5 Smarte overvåkningskameraer

Et «tradisjonelt» overvåkningskamera-system består av flere kameraer som er montert i butikker og i det offentlige rom. Kameraene er tilkoblet et kontrollrom der sikkerhetspersonell overvåker et sett av videoskjermer. Det blir gjort opptak av bildene som deretter lagres og slettes etter en gitt frist. Systemet er «lukket» i den forstand at bildene ikke blir kringkastet, men kun overført til kontrollrommet. Dersom sikkerhetspersonellet legger merke til noe mistenkelig, kan de kontakte vektere eller politiet som kan undersøke situasjonen nærmere.

5.1 Hvorfor ble smarte overvåkningskameraer utviklet?

Overvåkningskameraer ble opprinnelig utviklet for å overvåke rakettutskytinger under andre verdenskrig, og for å kunne følge med på farlige industrielle prosesser på trygg avstand. Det var først i USA på 1950-tallet at de ble kommersialisert som sikkerhetsteknologi. Amerikansk politi startet å bruke dem på 60-tallet. I 2013 var bildene fra overvåkningskameraer sentrale for å få identifisert de skyldige etter bombingene av Boston Marathon.



Smarte overvåkningskameraer ble utviklet for å håndtere den svakheten som tradisjonelle systemer for kameraovervåkning alltid har hatt: sikkerhetspersonellets begrensede kapasitet til å få med seg hva som foregår på hver enkelt av de mange skjermene, til enhver tid. Smarte overvåkningskameraer er derfor koblet til hverandre, og til en programvare som analyserer bildene automatisk. Hvis analyseprogrammet oppdager noe mistenkelig, varsles sikkerhetspersonellet som deretter kan

vurdere hva som foregår på bildene. Varslene og de tilhørende bildene blir lagret og kan enkelt hentes ut eller deles.

Smarte overvåkningskameraer kan utføre en rekke oppdrag. Oftest går disse ut på:

- Identifisering av gjenstander, for eksempel biler, ved å lese av bilskilt og sammenlikne dem med informasjon fra en database
- Ansiktsgjenkjenning. Dette fungerer best mot en ensfarget, flat bakgrunn. Ansiktet sammenliknes deretter med en database av registrerte personer
- Identifisering av bagasje uten tilsyn. Dette fungerer kun dersom bagasjen er i et åpent og tomt område

Det arbeides med å tilpasse smarte overvåkningskameraer til stadig flere oppgaver. Dette inkluderer:

- Identifisering av enkeltpersoner i en folkemengde ut fra klærne de har på seg.
- Identifisering av mistenkelig adferd, eller adferd som er uvanlig sammenliknet med hva som kan forventes, for eksempel forspøling. Adferden sammenliknes med kjente adferdsmønstre i en database.

Alle smarte overvåkningskameraer er imidlertid ikke like. Hvor «smart» et system er, avhenger av hvor godt programvaren analyserer bildene og hva som skjer med bildene etter at de har blitt delt. Ulike systemer blir satt opp for ulike hensyn, og hvert enkelt system kan derfor ikke utføre alle oppgaver.

5.2 Hvordan brukes smarte overvåkningskameraer?

Smarte overvåkningskameraer er kommersielle produkter som selges av selskaper innenfor sikkerhet og forsvar. Det er allerede utviklet mange forskjellige systemer, og de viktigste brukerne finnes innenfor samferdsel slik som bomselskaper, flyplasser eller jernbane. Systemene brukes også av politi og myndigheter.

I 2012 tok politiet i Budapest i bruk smarte overvåkningskameraer for å overvåke kollektivfeltet på veiene. Politiet kan bruke informasjon fra disse kameraene for å straffe privatbilister som kjører i kollektivfeltet.

EU har finansiert 16 forskjellig prosjekter for å utvikle algoritmer og funksjoner for smarte overvåkningskameraer. Myndighetene i Roma, London, Paris, Brussel, Milano og Praha har nylig gjennomført prøveprosjekter for å teste smarte systemer rettet mot fotgjengere. Disse systemene varsler sikkerhetspersonell hvis noen etterlater seg mistenkelige pakker eller oppfører seg unormalt i menneskemengden. Dette er fortsatt under utprøving.

Den mest utbredte bruken av smarte overvåkningskameraer er identifisering av bilskilter. Informasjon som blir innhentet fra kameraene blir sammenliknet med bilregistre og databasene til forsikringsselskap og politiet. Slik kan systemene enkelt knytte individer til et spesifikt sted og til en gitt tid. Systemet kan også brukes til å identifisere stjålne biler, fartsovertredelser og biler som kjører uten forsikring.

Et viktig spørsmål er om alle former for kriminalitet eller dårlig oppførsel bør overvåkes på samme måte. Skal smarte overvåkningskameraer brukes for å avsløre alle former for kriminalitet, eller bare de mest alvorlige lovbruddene? I Europa er det ulike holdninger knyttet til dette. I Tyskland for eksempel, innskrenket høyesteretten politiets bruk av automatisk skiltgjenkjenning av hensyn til personvernet. Retten insisterte på at politiet kun skulle lagre digital informasjon fra de smarte kameraene dersom sammenlikninger opp mot andre databaser blir gjort umiddelbart. Skiltgjenkjenning blir også brukt ved bompasseringer, men også dette har blitt kritisert fordi det eksisterer mindre personvernkretnende teknologi som kan utføre samme oppgave.

Hvordan fungerer smarte overvåkningskameraer?

Smarte overvåkningskameraer benytter seg av spesielle algoritmer for å gjenkjenne forskjellige typer adferd. Adferd som skiller seg fra det som er vanlig, blir kalt triggerhandlinger. Dette kan for eksempel være en person som holder et våpen eller noen som står stille i en ellers bevegelig folkemengde. En algoritme er et sett med matematiske beregninger som leter gjennom informasjonen i et digitalt bilde. En intelligent algoritme lærer seg hva den bør lete etter, basert på tidligere analyser.

Algoritmene i smarte overvåkningskameraer er bygget for å etterligne hvordan øyet og hjernen fungerer. Programvaren bryter bilder ned i mindre deler, kalt piksler. Du kjenner sikkert igjen begrepet hvis du har et digitalt kamera eller en smarttelefon. Når et kamera har «3 megapiksler», består hvert bilde av 3 millioner piksler.

Algoritmen kan beregne mengden bevegelse for hver piksel, slik at programmet kan identifisere de aktive områdene i hvert bilde. Ut fra dette lærer den å gjenkjenne bevegelsesmønstre. Systemet kan identifisere og klassifisere hendelser etter hvilke mønstre den allerede kjenner til. Programvaren kan for eksempel skille mellom stillestående og hoppende tilskuere på en fotballkamp.

5.3 Økt sikkerhet

Smarte overvåkningskameraer kan øke sikkerheten på følgende måter:

Sikkerhetsutfordringer blir identifisert i sanntid:

- Systemet identifiserer ting som virker unormalt og varsler automatisk personalet. Dette gjør det enklere å følge med på bildene.
- Varslene gjør det mulig for operatøren å ta hurtige beslutninger, og vurdere om andre tiltak bør settes i gang.
- Algoritmene er i stand til å behandle langt større mengder informasjon enn personalet, og kan derfor fange opp detaljer som ellers ville blitt oversett.

Redusert frykt og styrket personvern:

- Når sikkerhetsteknologi fungerer optimalt, vil folk føle seg tryggere av at hendelser utenom det vanlige blir fanget opp av smarte overvåkningskameraer
- Smarte overvåkningskameraer kan fange opp mer detaljert informasjon enn de tradisjonelle overvåkningskameraene. Dette innebærer at færre kameraer kan overvåke større områder. Færre kameraer kan oppleves mindre krenkende på personvernet.
- Personvernet kan styrkes ved at de delene av kameraets synsvinkel som dekker privat eiendom kan «sladdes», slik at det forblir skjult for sikkerhetspersonalet.

5.4 Utfordringer

Det er flere ulemper ved smarte overvåkningskameraer som må vurderes:

Algoritmene som brukes i dag har flere svakheter. De kan utløse falske alarmer ved at en ellers ufarlig hendelse feilaktig blir registrert som en trussel. I verste fall kan dette føre til at uskyldige får status som mistenkte når ingen lovbrudd har blitt begått. Svakheterne til algoritmene består av følgende:

- Det er kun enkelte typer gjenstander som kan gjenkjennes med stor treffsikkerhet, for eksempel bilskilt eller bagasje uten tilsyn.

- Kameraenes evne til å identifisere adferdsmønstre og hendelser i folkemengder er begrenset.
- Skjult kriminalitet som lommetyveri, nasking og lignende er også vanskelig å identifisere
- Fordi det er mennesker som definerer hva som skal være normalt eller unormalt i systemet, kan algoritmene aldri bli helt nøytrale. Dermed er den fare for at systemet kan, enten bevisst eller ubevisst, rettes spesifikt mot minoriteter.
- Det er også enkelt for personer å unnsnippe de smarte overvåkningskameraene, for eksempel ved å skifte klær, da algoritmene identifiserer enkeltindivider blant annet ved klærne de bruker.
- Det høye antallet falske alarmer kan svekke tilliten operatørene har til systemet, og føre til at alarmer etter hvert ignoreres.

Smarte overvåkningskameraer er både mindre og kraftigere:

- De kan fange opp mer informasjon. Tersken for å bryte personvernet er dermed lavere. Dette skyldes at sannsynlighet er høy for at adferden til tilfeldig forbipasserende blir analysert og kanskje lagret.
- Kameraene er mindre synlige, slik at det er vanskeligere for folk å vite når og hvor de blir overvåket. Det blir dermed vanskeligere å unngå overvåkning.
- Ytringsfriheten kan bli utfordret dersom folk innser at deres adferd blir overvåket og analysert av programvare og sikkerhetspersonell.

Man trenger fortsatt mennesker til å styre systemene:

- Systemene kan identifisere hendelser utenom det vanlige, men de kan ikke forklare hvorfor de finner sted. Personalets analyse er en uunnværlig del av systemet.
- Det bør være strengt regulert hvordan institusjoner kan bruke smarte overvåkningskameraer slik at man forhindrer misbruk av informasjonen som blir samlet inn.

6 Droner

En drone er den flyvende delen av et ubemannet system. Den styres av en pilot som befinner seg på bakken, men den kan også fly autonomt ved hjelp av et datasystem. Bruken av droner har fått økende oppmerksomhet etter at USA startet å bruke dem i krigføring mot terrorisme i Afghanistan, Pakistan, Jemen og Somalia. De siste årene har mange europeiske land også innført droner i sine militære styrker.

Det er ikke bare militæret som bruker droner. Også politi og andre sikkerhetsmyndigheter bruker dem til overvåkning og rekognosering. Slike sivile droner blir i stor grad brukt som flyvende overvåkingskameraer. De kan overvåke offentlige rom med hensikt å avverge eller oppdage en rekke trusler mot samfunns-sikkerheten. Et annet viktig element er at droner kan overvåke områder som er farlige for mennesker og bevege seg i, for eksempel etter snøskred eller atomulykker. Etter ulykken på atomanlegget i Fukushima ble droner brukt til å overvåke tilstanden på atomanlegget og kontrollere strålingsnivået.

Sivile droner brukes også til formål som ikke er relatert til sikkerhet, for eksempel kartlegging av landområder, landskapsfotografi eller som rene leketøy.



I SurPRISE-prosjektet har vi valgt å fokusere på bruk av sivile droner til sikkerhetsøyemed.

6.1 Hvorfor ble droner utviklet?

Droner ble opprinnelig utviklet for rekognosering og målrettede angrep i militæret. Teknologien for å fjernstyre et ubemannet fly ble utviklet under første verdenskrig. Den første dronen ble lagd av den britiske professoren A. M. Low i 1916.

Selv om droner fortsatt i stor grad forbindes med militæret, øker stadig bruken av sivile droner hos myndigheter, private selskaper og privatpersoner.

Innenfor EU regulerer landene selv bruk av "små" droner som veier mindre enn 150 kg og all bruk for formål innen sikkerhet eller militæret. Bruk av større droner til kommersielle formål blir nå diskutert i Europakommisjonen, som har som mål å introdusere droner i sivil luftrom innen 2016. Innen 2028 skal droner være fullt integrert i EU's sivile luftrom.

Forskere jobber nå med å utvikle droner som er mindre avhengige av mennesker for å utføre oppgaver, og som kan fly forhåndsprogrammerte ruter på egenhånd. Masseproduksjon av mikro- og nanodroner er også under utvikling.

Produksjon av elektronikk og sensorer blir stadig billigere, noe som utvider mulighetene for bruk av droner. Hvilke oppgaver en drone kan løse, avhenger av størrelse, bæreevne og valg av sensorer til hver enkelt drone.

6.2 Hvordan brukes droner?

Droner kan være et effektivt supplement til eksisterende infrastruktur når det gjelder håndtering av krisesituasjoner, til grensekontroll, overvåkning av trafikk eller ved brann.

I flere land i Europa har politiet brukt droner til å overvåke store folkemengder som for eksempel på musikkfestivaler, demonstrasjoner eller sportsarrangementer. Dronene gir overblikk slik at man kan oppdage uventede hendelser i folkemengden. Dronene har også blitt brukt av politiet til åstedsundersøkelser og i søk etter ulovlig dyrking av narkotiske stoffer. Grensekontroll er et område hvor bruken av droner trolig vil øke i nærmeste fremtid.

Å bruke droner til å overvåke offentlige områder gir noen store fordeler. De kan overvåke store arealer, de er mobile og kan gi tilgang til flere synsvinkler sammenliknet med de tradisjonelle, statiske overvåkningskameraer.

Droner kan brukes til mange ulike kommersielle formål. Noen eksempler er inspeksjon av områder for landbruk og fiske, kraftlinjer og annen infrastruktur, kommunikasjon- og kringkasting, over-

våkning av naturressurser og naturområder.

Til tross for alle disse mulighetene er det fortsatt mange tekniske utfordringer knyttet til bruk av droner. Dette dreier seg om begrenset kapasitet når det kommer til høyde, fart og levetid på batteri eller drivstoff. Droner er også sårbare for mange værforhold, for eksempel tette skyer, vind og regn.

Hvordan fungerer droner?

Droner finnes i mange ulike varianter, og de kan utstyres på mange forskjellige måter. Droner fjernstyres som regel av en eller flere operatører på bakken som styrer dronen og følger med på for eksempel bildene fra dronens kamera. Man kan kontrollere droner både med smarttelefoner og nettbrett. I noen tilfeller er det mulig å programmere en drone til å fly en forhåndsbestemt rute. Sammenliknet med fjernstyring er slik autonom flyving fortsatt lite brukt, og er fortsatt i utviklings- og testfasen. Kommunikasjon mellom dronen og operatøren kan foregå på flere måter. Ved lange distanser brukes for eksempel satellitt-tilkoblinger for å overføre data mellom dronen og operatøren.

Et ubemannet system består av flere elementer:

- en drone
- kontrollenhet på bakken (for eksempel en smarttelefon eller en datamaskin)
- kommunikasjonslinje
- kamera, sensor eller annet utstyr

Størrelsen og utstyret på dronen varierer kraftig, og avhenger av dronens bruksområde. Dronen kan for eksempel utstyres med ulike typer kameraer, radar, sensorer som kan oppdage stråling eller kjemiske utslipp eller våpen.

Mye forskning fokuserer på utvikling av mikro- eller nanodroner, som ser ut som, og oppfører seg som insekter eller fugler. Dette kan føre til at overvåkingskapasiteten til droner vil vokse i fremtiden, selv om mange scenarioer fortsatt er begrenset av lovverket.

6.3 Økt sikkerhet

1. Droner gjør det enklere å oppdage sikkerhetsutfordringer

- Droner kan overvåke store og utilgjengelige områder, for eksempel i søk- og redningsaksjoner. Droner kan også overvåke store grenseområder for å oppdage ulovlige grenseovergang eller menneskehandel.
- Droner er mobile. Hvis de oppdager mistenkelige objekter eller individer, kan de følge etter disse hvis de beveger seg videre. Dronene har både større utholdenhet og er mindre synlige enn mennesker som kunne gjort den samme jobben.
- Droner er mindre synlige enn tradisjonelle overvåkningskameraer. Dette gjør at kriminelle har vanskeligheter med å oppdage at et område blir overvåket.

2. Frykten for kriminalitet vil bli redusert:

- Når man vet at et område blir overvåket av en drone vil det kanskje være betryggende å vite at hvis noe uvanlig hender vil dette raskt bli oppdaget av dronen.

6.4 Utfordringer

1. Droner er mindre synlige enn tradisjonelle overvåkningskameraer, noe som muliggjør overvåking uten at man er klar over det.

- Droner har mye større kapasitet til å samle inn informasjon enn overvåkningskameraer, siden de kan bevege seg i områder som er stengt for uvedkommende. I områder hvor det for eksempel er satt opp gjerder for å hindre innsyn, kan en drone enkelt fly over gjerdet. Slik kan dronene samle inn bilder og informasjon som ikke er tilgjengelig for tradisjonelle overvåkningskameraer.

- På samme måte som mange overvåkningsteknologier, muliggjør droner datainnsamling om store grupper mennesker. Slik masseovervåking av kan være negativt for samfunnet og demokratiet.

- Sammenliknet med overvåkningskameraer kan droner være vanskelige å få øye på. Dette gjør det vanskelig for folk å vite når de blir overvåket. At dronene er mobile gjør det også vanskelig å vite hvem som utfører overvåkingen, derfor er det lite man kan gjøre for å unngå overvåkingen.

- Når man ikke vet om man blir overvåket kan det føre til usikkerhet i befolkningen. Dette kan igjen føre til at de forandrer på egen oppførsel, i frykt for at noen følger med på hva de gjør. En slik effekt kan bli enda sterkere av at droner utstyres med smarte kameraer eller sensorer som gjør det mulig å identifisere individene som overvåkes.

- Bruk av droner i kombinasjon med overvåkningskameraer og sporings-teknologi gjør den overvåkingen total. Dette muliggjør innsamling av detaljert informasjon om et individs bevegelser, oppførsel og sosiale liv.

2. Droner som samler inn data ved hjelp av kamera eller sensorer kan være sårbare for hacking-angrep fra utenforstående.

3. Hvis droner brukes i tettbygde strøk er det utfordringer knyttet til sikkerhet

- Droner er oftere innblandet i ulykker enn bemannede fly. Dette er blant annet fordi de er mye mer sårbare for værforhold. Hvis operatøren mister kontrollen over en drone kan dette sette mennesker på bakken i fare.

7 Pakkesniffing og overvåkning på internett

Internettleverandører, teleselskaper og nettverksoperatører har alltid hatt mulighet til å overvåke sine nettverk. Å vite hvem som kommuniserer med hvem, hvilke nettsider som blir besøkt og hvilke tjenester som blir benyttet, legger grunnlaget for å kunne fakturere brukerne, forvalte nettverket og legge en markedsføringsstrategi. Teknologien som kalles pakkesniffing går enda lenger, og gjør det mulig for selskaper, sikkerhetstjenester og myndigheter å lese innholdet i kommunikasjon på internett. Som en sammenlikning kan man si at pakkesniffing tilsvarer en postmann som åpner og leser alle brev, og som kan endre eller slette inn-

holdet, eller la være å levere brevene til mottakeren.

Pakkesniffing kan overvåke alt av digital kommunikasjon: tekster du leser på nett, nettsidene du besøker, videoene du ser på, og hvem du kommuniserer med, enten det er via e-post, chat eller på sosiale medier. Teknologien åpner og analyserer meldinger mens de er på vei gjennom nettverket, og identifiserer de som kan utgjøre en risiko. Du trenger ikke være mistenkt for noe for å bli utsatt for pakkesniffing – hvis pakkesniffing først brukes, undersøkes all kommunikasjon som går via dette nettverket.

Hvordan fungerer pakkesniffing?

Når du sender eller mottar informasjon over internett, går informasjonen gjennom en svært kompleks prosess via mange forskjellige datamaskiner.

Datamaskinene bryter ned informasjonen du sender og mottar i mindre deler som kalles «pakker». Hensikten er å gjøre det enklere for informasjonen å reise gjennom internett. Hver pakke har en overskrift som beskriver hva pakken er, hvem den er fra og hvor den skal, akkurat som et brev i posten. Selve innholdet blir ikke beskrevet i overskriften. Når pakkene ankommer bestemmelsesstedet, settes de sammen til den opprinnelige meldingen.

Hver pakke består av flere lag som inneholder ulik informasjon om meldingen. Lagene ligger inni hverandre, på samme måte som en russisk dukke. Internettleverandørene må inspisere noen av pakkene for å kunne sende den videre. I de aller fleste tilfeller trenger de kun å se på overskriften, og ikke innholdet, for å sende meldingen videre. Pakkesniffing derimot, innebærer en grundigere undersøkelse av selve innholdet i samtlige pakker.

Ved pakkesniffing blir meldingene inspisert av et system som leter etter spesifikke typer data. I presentasjonen av smarte overvåkningskameraer beskrev vi programmer som sorterer og analyserer data. Slike programmer brukes også i pakkesniffing, men på en annen måte. I pakkesniffing blir algoritmene programmert til å søke etter nøkkelord, på samme måte som når du søker etter informasjon på Google eller en annen søkemotor. Typen data som det søkes etter bestemmes av de som leter. Nøkkelordene kan være knyttet til kriminelle eller mistenkelige aktiviteter, til et nytt datavirus, eller om et spesifikt produkt har blitt kjøpt.





7.1 Hvorfor ble pakkesniffing utviklet?

Pakkesniffing ble opprinnelig utviklet for å oppdage virus og ondsinnet programvare som kunne skade nettverkene. Ved å bruke pakkesniffing til å analysere innholdet i meldinger som sendes over nettet, kan også andre former for kriminalitet oppdages og stoppes.

Utstyret som brukes til pakkesniffing eies av internett-selskapene. Disse selskapene kan kontrollere hvordan internett fungerer lokalt, regionalt, nasjonalt og internasjonalt. Disse selskapene benytter seg av denne teknologien selv, men de kan også tjene penger på å selge teknologien til andre. Det finnes også andre selskaper som utvikler slik teknologi, noe som gjør at det etter hvert har blitt et marked for pakkesniffing.

7.2 Hvordan brukes pakkesniffing?

I Europa er bruk av pakkesniffing kun lovlig for å hindre spredning av virus og ondsinnet programvare. I tillegg kan internettleverandører bruke det til å håndtere trafikkflyten i nettverkene sine. Det blir også brukt til å oppdage spesifikke typer kriminalitet, som for eksempel spredningen av barnepornografi. Selv om dette er lovlig, er det fortsatt kontroversielt å utføre såpass detaljert pakkesniffing fordi de gjeldende EU-lovene som regulerer informasjonsinnhenting og kommunikasjon ble

opprettet før pakkesniffing ble utviklet. Myndighetene i EU har tolket nåværende lovverk slik at de kun regulerer overfladisk analyse av internettrafikk. Nye lover må utvikles før man kan regulere mer detaljert pakkesniffing på en ordentlig måte.

Et resultat av dette er at pakkesniffing i Europa ikke kan brukes til å identifisere brudd på opphavsrett, sensur av politiske meninger eller målrettet markedsføring, selv om teknologien kan utføre slike analyser. Det europeiske lovverket beskytter konfidensiell kommunikasjon. «Dypere» pakkesniffing ville også brutt med den europeiske menneskerettighetskonvensjonen fordi det innebærer ubegrunnet og vilkårlig masseovervåkning.

I USA er bildet litt annerledes: pakkesniffing er ikke regulert på samme måte, og mange selskaper bruker det for eksempel til målrettet markedsføring. Hvis du har en Yahoo- eller Gmail-adresse er det sannsynlig at epostene dine blir sendt via amerikanske servere, og dermed utsettes for pakkesniffing. Det ser også ut som at pakkesniffing ble brukt i forbindelse med de amerikanske (NSA) og britiske (GCHQ) etterretningstjenestenes masseovervåkningsprogram som ble avslørt sommeren 2013.

Hvordan pakkesniffing kan oppdages, begrenses, eller kontrolleres, er uklart. Teknologien utvikles så raskt at det er vanskelig å lage regelverk som holder følge. Det er også vanskelig å vite omfanget av pakkesniffing. Enhver melding du sender på nett kan reise jorda rundt før den kommer fram til adressaten, og kan dermed ha vært gjenstand for pakkesniffing hos hvilken som helst internettleverandør eller sikkerhetstjeneste. Det er nærmest umulig å avgjøre om det har funnet sted eller ikke. Uten regulering kan det bli «ville-vesten»-tilstander, der regjeringer, sikkerhetstjenester og private selskap utnytter gråsoner i regelverket.

Det vi kan fastslå, er at svært mange forskjellige institusjoner og selskap benytter seg av pakkesniffing, deriblant nettleverandører, markedsførings-selskap, politiet og sikkerhetsmyndigheter. Bortsett fra den omfattende overvåkingen som ble avslørt i USA i 2013, er det kun offentliggjort en håndfull saker hvor pakkesniffing har blitt brukt.

Dette inkluderer både kommersiell og sikkerhetsorientert bruk.

7.2.1 Kommersiell bruk

- *Nettverkssikkerhet:* Meldinger inspiseres for å være sikker på at de ikke inneholder virus, ondsinnet programvare eller feil.
- *Målrettet markedsføring:* Innsamlet informasjon blir brukt for å kartlegge avsenders produktpreferanser. Dette er ulovlig i Europa, men ønskes velkommen av enkelte forbrukere i USA. Det vektlegges at målrettet markedsføring gir forbrukerne enklere tilgang til produkter og tjenester som er tilpasset deres behov.
- Beskyttelse av opphavsrett: Meldinger inspiseres for å identifisere ulovlig fildeling og brudd på opphavsretten.

7.2.2 Sikkerhetsorientert bruk

Overvåkning av kriminell aktivitet: pakkesniffing har blitt foreslått som verktøy i etterforskning av visse typer forbrytelser, men dette er veldig kontroversielt (og kan være ulovlig). Eksempler på tilfeller der pakkesniffing kan benyttes inkluderer etterforskning av:

- angrep mot datasystemer eller der datamaskiner blir brukt for å utføre kriminelle handlinger (for eksempel spredning av barnepornografi)
- rasistiske trusler og ytringer
- oppfordringer til terror eller terrorplanlegging
- ytringer som støtter folkemord eller forbrytelser mot menneskeheten

Sensur: Det blir spekulert i om pakkesniffing har blitt brukt for å villedde opposisjonen i undertrykkende regimer over hele verden. Et amerikansk forsvarsselskap, NARUS (en underleverandør av Boeing), solgte teknologi for pakkesniffing til Libya som deretter ble brukt til å slå ned på opposisjonelle under den arabiske våren. Storbritannia derimot, trakk tilbake eksportlisenser for pakkesniffing til Egypt, Bahrain og Libya. Iran bruker pakkesniffing for å overvåke og sensurere internett, men også for å forandre på innhold på nett eller i eposter. Kina bruker pakkesniffing på samme måte.

Hvorvidt slik sensur også foregår i Europa, vet vi fortsatt ikke.

7.3 Økt sikkerhet

Pakkesniffing kan bedre sikkerhet ved å identifisere og blokkere skadelig og ulovlige meldinger, slik som det ble beskrevet i avsnittet over.

Pakkesniffing kan ikke forhindre kriminalitet, det kan kun oppdage at noe ulovlig skjer og eventuelt bidra med bevismateriale i rettsaker. Derimot kan pakkesniffing stoppe spredning av virus og annen ondsinnet programvare.

7.4 Utfordringer

Bruk av pakkesniffing medfører flere utfordringer:

1. Pakkesniffing fanger opp all informasjon:

- Pakkesniffing analyserer alle meldinger og alt innhold, noe som innebærer at elektronisk kommunikasjon aldri er garantert privat.
- Vissheten om at all kommunikasjon kan overvåkes, kan medføre en omfattende «chillingæ-effekt», som innebærer at folk blir redde for å kommunisere og uttrykke seg fritt.
- Pakkesniffing er svært inngripende, og det er behov for streng regulering av bruken.

2. Teknologi utvikler seg langt raskere enn regelverket:

- Det foreligger ikke tydelige regler om hva pakkesniffing kan og ikke kan brukes til. Bruken av pakkesniffing avhenger i dag av brukerens egne etiske vurderinger. Det kan brukes til alt fra identifisering av virus til politisk undertrykkelse.
- I stater der det er tette forbindelser mellom myndighetene og teleselskap, kan informasjon enkelt deles slik at staten får tilgang til samtlige innbyrgeres elektroniske kommunikasjon.

3. Det er vanskelig å kartlegge nøyaktig hvem som benytter seg av pakkesniffing, og hvorfor de gjør det:

- Fremtidig regulering av pakkesniffing bør være internasjonal
- Et tilsyn for pakkesniffing bør være et internasjonalt organ som har myndighet til å straffeforfølge de som bryter reglene.

4. Effektiviteten ved bruk av pakkesniffing er tvilsom:

- Maskinene identifiserer meldinger som potensielt kan være ulovlig eller farlige. Derfor kan det være et problem at maskinene tolker ting feil, og at uskyldige mennesker blir sett på som mistenkte.
- Noen eksperter mener at pakkesniffing ikke er særlig effektivt for å avdekke ulovlig forhold som fremgår av analyserte meldinger.

8 Sporing av smarttelefoner

Smarttelefonen har overtatt plassen til den sveitsiske lommekniven som det perfekte «alt-i-ett»-verktøyet. I Europa er det gjennomsnittlig 1,3 mobiltelefoner per innbygger, noe som er enormt mange når mobiltelefoner slik vi kjenner dem i dag ikke var i salg før 1990-tallet.

8.1 Hvorfor ble sporing av smarttelefoner utviklet?

Smarttelefoner er et relativt nytt produkt. De er veldig populære fordi de kan utføre svært mange oppgaver. På mange måter er de mer som små datamaskiner som også fungerer som telefoner. Som en vanlig datamaskin har hver smarttelefon et operativsystem som tilrettelegger for bruken av e-post, chat og surfing på nett. De kjører programvare som kan tilby tjenester som spill, kart og nettsider. De har også digitalkamera, medieavspillere og store, fargerike berørings-skjermer.

Mobiltelefonens historie går tilbake til andre verdenskrig. En mobiltelefon er først og fremst en trådløs radio som kan både sende og motta meldinger. Den første trådløse radioen, «walkie-talkien», ble først brukt for å hjelpe soldater å holde kontakten med hverandre på fronten. På 70- og 80-tallet muliggjorde utviklingen av mikroprosessorer de første håndholdte mobiltelefonene. Den første modellen var like stor og veide like mye som en murstein. Batteriet varte kun i 20 minutter. Tidene forandrer seg, og fra og med 80-tallet forbedret et stadig voksende mobilmast-nettverk både lokale og internasjonale telefonsignaler.

Mobilmaster er svært viktige for å lokalisere mobiltelefoner. En mast dekker et gitt geografisk område. For å kunne være tilknyttet et nettverk, må mobiltelefonen kobles til nærmeste mast. Dersom personen som bærer på telefonen forflytter seg inn i rekkevidden til en annen mast, vil telefonen tilkobles denne masten i stedet. På denne måten kan teleselskap lokalisere en person. Gjeldende lovgivning i EU krever at teleselskapene lagrer denne informasjon i minst seks måneder, og maksimalt tjuefire måneder. Selv om det siste EU direktivet ble avvist av Europadomstolen i april 2014, har ikke nasjonale regelverk blitt forandret enda.

Smarttelefoner kan også lokaliseres på andre måter, for eksempel ved å bruke GPS-funksjonen på telefonen, eller ved å koble seg til trådløse nettverk. Dette har ført til en enorm utvikling av tjenester som bruker posisjonsdata. Disse er vanligvis tilgjengelige som applikasjoner («apper») som kan installeres på telefonen. En app er en programvare som utfører gitte funksjoner eller tjenester. Posisjonsbaserte apper kan gjøre det enklere for en bruker å finne informasjon om nærliggende restauranter og butikker, eller til og med finne ut om venner befinner seg i nærheten. Det finnes også spill som bruker disse funksjonene. Tjenester basert på posisjonen til brukeren er trolig et marked som vil fortsett å vokse de neste årene.

Posisjonsbaserte tjenester tilbyr mange praktiske funksjoner. For noen personvern-forkjempere er det likevel bekymringsverdig at det kan innhentes så mye informasjon om hvor en person befinner seg.



Da den tyske politiker Malte Spitz fra De Grønne fikk utlevert data hans mobilselskap hadde lagret om han, så det ved første øyekast ut som en lang og meningsløs strøm av tall.

Men etter at en statistiker fikk sett på tallene, innså Spitz at tallene kunne gi en svært detaljert oversikt over livet hans. Sammen med den tyske avisen Die Zeit laget han en grafikk som anga nøyaktig hvor han hadde vært det siste halvåret, til enhver tid. Malte ble spesielt bekymret for hvor detaljert informasjon man kunne få ved å sammenstille posisjonsdataene fra telefonen med informasjon fra sosiale medier som Twitter og Facebook.

Den amerikanske høyesteretten konkluderte nylig at GPS-data kan gi svært detaljert informasjon om private ærend, som for eksempel «turer til psykologen, til en plastisk kirurg, en abortklinikk, til et AIDS-senter, en strippeklubb, forsvars-advokaten [...], fagforeningen, synagogen, moskéen eller kirken, homobaren osv».

8.2 Hvordan brukes sporing av smarttelefoner?

Det er både kommersielle og sikkerhetsmessige bruksområder for posisjonsdata fra smarttelefoner.

8.2.1 Kommersiell bruk

- Telefonregninger: Teleselskap trenger posisjonsdata og telefonens identifikasjonsnummer for å kunne fakturere kundene sine.
- Målrettet markedsføring: IT-utviklere som produserer applikasjoner som Twitter, AngryBirds eller CandyCrush, samler inn posisjonsdata og informasjon om kontaktlisten på telefoner for så å selge dem til markedsføringsselskap. Markedsførerne bruker deretter informasjon til å skreddersy reklame som er tilpasset vanene og interessene til forskjellige typer kundegrupper. Over 50 prosent av alle apper samler inn posisjonsdata selv om de ikke trenger det for å fungere.

- Byplanlegging: Posisjonsdata kan benyttes for å kartlegge bruken av byrom. Siden det er flere mobilmaster i byer enn på landet, er det også enklere å spore telefoner i byer. Dette litt merkelige bildet er et kart over hvordan mobiltelefoner brukes i Graz i Østerrike. Forskere ved Massachusetts Institute of Technology sporet opp mobiltelefoner anonymt for å kunne tegne et bilde av hvordan innbyggerne forflytter seg. Hensikten er å gi bedre bakgrunnsinformasjon til byplanleggere og transportmyndigheter om hvordan byen benyttes..



Hvordan fungerer sporing av smarttelefoner?

Både vanlige mobiltelefoner og smarttelefoner kan spores. Det finnes tre forskjellige måter å spore mobiltelefoner på: via mobilmaster, GPS og trådløse nettverk. Alle mobiltelefoner kan spores via mobilmaster, mens de to siste metodene gjelder kun for smarttelefoner.

Mobilmaster: alle telefoner registreres ved den nærmeste mobilmasten slik at anrop, tekstmeldinger og e-poster kan sendes og mottas via mobilnettet. Hver telefon bærer på et unikt referansenummer som knytter telefonen til en konto hos teleselskapet, og derfor også til brukeren. Dette gjør det mulig å tilpasse forskjellige løsninger og sende regninger til hver enkelt bruker. Hvis myndighetene eller sikkerhetstjenester forsøker å spore opp personer, kan de be teleselskapene å avgi denne type informasjon. Ved å samle informasjon om én telefon fra flere forskjellige master, vil brukeren være mulig å spore.

GPS: Smarttelefoner inneholder kart-programvare og applikasjoner som må være tilkoblet GPS for å fungere. Når funksjonaliteten for GPS er slått på, vil posisjonen beregnes ut fra avstanden til nærmeste GPS-satellitt. Telefonen kan ikke kobles til GPS-satellitten dersom denne funksjonen er avslått. Imidlertid finnes det applikasjoner som fjernstyrer denne funksjonen uten å informere brukere. Dette kan for eksempel være apper som kan lokalisere en stjålet telefon. Produsenter av applikasjoner innhenter posisjonsdata fra telefonene, og noen selger dem videre til markedsføringsselskap. Dersom myndigheter og sikkerhetstjenester ønsker å spore noen, kan de be teleselskap om GPS-data.

Trådløst nettverk: Smarttelefoner kan kobles til trådløse nettverk som virker innenfor et gitt område. Å koble telefonen til et slikt nettverk gjør det mulig å lokalisere den innenfor nettverkets rekkevidde. Dersom funksjonen slås av, er det ikke mulig å spore telefonen på denne måten. Et trådløst nettverk vil vanligvis ha en rekkevidde på 20 meter innendørs, og noe større rekkevidde utendørs.

Andre "smarte" mobile enheter, som nettbrett og bærbare datamaskiner kan spores på samme måte.

8.2.2 Sikkerhetsorientert bruk

- Finne savnede og skadede personer: I USA og Canada har nødnummer-tjenesten E-911 fullmakt til å benytte seg av GPS i mobiltelefoner, slik at brukerne skal kunne lokaliseres i nødsituasjoner. Omkring 60 til 70 prosent av de 180 millioner telefon-samtalene som gjøres i Europa hver dag, blir gjort fra mobiltelefoner. Telefonene avgir posisjonsdata til den felles europeiske nødnummeret 112. I motsetning til amerikanerne og canadierne, må ikke europeerne ha GPS-tjenestene påslått til enhver tid.
- Oppsporing av mistenkte forbrytere: Teleselskap må gi politi og sikkerhetstjenester tilgang til posisjonsdata etter rettskjennelse. I Europa blir denne type forespørsler vurdert ut fra personvernlovgivning. Når teleselskap først mottar en slik kjennelse, er de pålagt å levere all data som kan knyttes til den mistenkte. Sikkerhetstjenester har også andre metoder for å spore opp mistenktes mobiltelefoner.
- Sporing av familiemedlemmer: Enkeltpersoner kan også ha nytte av posisjonsdata. Dette kan for eksempel være foreldre som ønsker å vite hvor barna deres eller demente familiemedlemmer befinner seg.

Debattene om bruken av posisjonsdata og smarttelefoner

Under "Occupy Wall Street"-protestene i New York ble selskapet Twitter pålagt å avgi posisjonsdata til amerikanske myndigheter for å identifisere demonstrantene. Nylig lanserte Twitter en ny tjeneste, «Please Don't Stalk Me». Tjenesten brukes til å knytte feilaktig posisjonsdata til meldinger. Brukerne velger selv ut hvor de ønsker å gi inntrykk av å befinne seg via kartene til Google Maps. Det finnes også andre apper som tilbyr lignende tjenester, som «My Fake Location», «Fake GPS Location» og «GPS Cheat»..

8.3 Økt sikkerhet

Lokalisering av smarttelefoner bidrar til økt sikkerhet på flere måter:

- De som befinner seg i nødsituasjoner er enklere å spore opp og kan dermed få hjelp raskere

- Familier kan enklere vite hvor sårbare eller pleietrengende slektninger befinner seg
- Myndighetene kan bruke posisjonsdata for å knytte mistenkte til en forbrytelse, eller tvert i mot å utelukke dem fra etterforskningen.

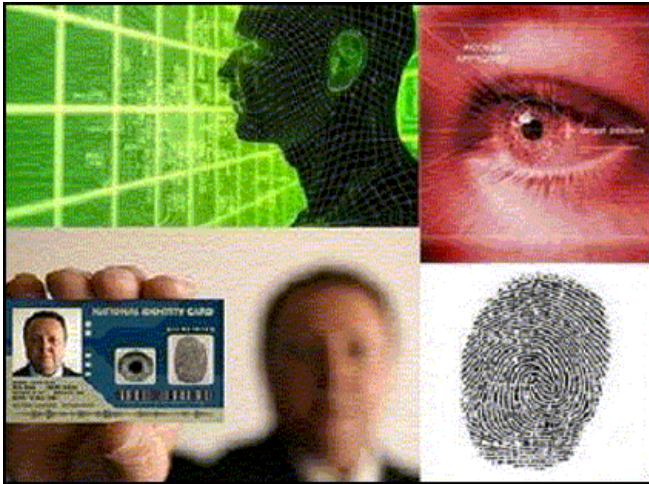
8.4 Utfordringer

Lokalisering av smarttelefoner skaper utfordringer knyttet til personvern, reguleringer og menneskerettigheter:

- Brukere har ikke kontroll over informasjonen som produseres og videresendes av smarttelefoner. Dette kan skape vansker for personer i utsatte situasjoner, for eksempel vitner, som ikke ønsker å dele sin posisjon, men likevel vil beholde fordelene ved mobilbruk. Noen telefoner lagrer posisjonsdata automatisk uten at denne funksjonen kan slås av.
- Mange apper lagrer posisjonsdata uten at dette er nødvendig for at appen skal fungere.
- Mange app-utviklere befinner seg utenfor Europa og er derfor ikke underlagt europeisk personvernlovgivning. Det er derfor vanskelig for EU å kreve at apper skal være mer personvernvennlige. En endring av ePrivacy-direktivet under-streker imidlertid at brukere må ha muligheten til å gi sitt samtykke til at apper behandler data fra telefonen, uansett hvor i verden utviklere befinner seg.
- I stater der det er et tett forhold mellom teleselskap og myndighetene kan informasjon deles slik at staten får oversikt over posisjonsdata til samtlige innbyggere.
- Siden lokasjonsdata har blitt brukt for å identifisere demonstranter, kan systematisk bruk føre til at folk ikke lenger ønsker å demonstrere eller utøve sine demokratiske rettigheter.

9 Biometri

Biometri er en samlebetegnelse på systemer som måler en persons fysiske kjennetegn, som fingeravtrykk, DNA, ansiktsstruktur, eller unike adferdsmønstre som analyse av ganglag eller stemme. Slike analyser har som regel det formål å identifisere eller bekrefte identiteten til en person.



Noen land registrerer innbyggernes fingeravtrykk eller andre biometriske kjennetegn, og lagrer disse i nasjonale ID-kort eller i en database. Slike databaser kalles biometriske systemer. Senere kan biometriske kjennetegn sammenliknes opp mot denne databasen for å identifisere personen. Store fremskritt innenfor dataprosessering har ført til automatiserte biometriske systemer, som kan gjennomføre et stort antall identifiseringsprosesser på få sekunder.

9.1 Hvorfor ble biometri utviklet?

På 1800-tallet utviklet mange land rettssystemer som krevde en mer formalisert måte å identifisere folk på enn man hadde hatt tidligere. Dette var for å kunne skille mellom førstegangsforbrytere og gjengangere hos politiet. I Frankrike utviklet Alphonse Bertillon en metode kalt "Bertillonage" eller antropometri, som er en metode for å identifisere personer basert på kroppsmål, som høyde, lengde på armene og bilder. Mot slutten av 1800-tallet fikk man en mer presis metode da Sir Francis Galton utviklet metoden for å identifisere personer basert på deres fingeravtrykk. I løpet av 1900-tallet ble stadig flere metoder utviklet. Dette

inkluderte identifisering basert på mønstre i iris og ansikts- og stemmegjenkjenning.

9.2 Hvordan brukes biometri?

Biometri har tradisjonelt vært brukt av politi og sikkerhetsmyndigheter til å identifisere kjente og ukjente kriminelle. Det er også vanlig for å godkjenne adkomst til spesielle områder, for eksempel regjeringsbygninger, lokalene til private foretak osv.

På 2000-tallet har biometri blitt mer og mer vanlig ved grenseoverganger. Når man ankommer en grenseovergang brukes biometri til å sjekke om personen tidligere har blitt nektet adgang, om han eller hun er en kjent trussel mot sikkerheten eller om man tidligere har brutt reglene for visum. Hvis man søker om et EU-visum, blir fingeravtrykk fra alle fingrene lagret, sammen med et bilde. Disse dataene lagres i VIS-databasen (Visa Information System). På samme måte har EU opprettet EURO-DAC, en stor database med fingeravtrykk fra asylsøkere og papirløse flyktninger.

I militær sammenheng har det amerikanske militæret tatt i bruk håndholdte apparater som kan brukes til for eksempel iris-skanning. Ettersøkte personer blir satt på en «watchlist», som gjør at soldater i felten kan identifisere for eksempel en mistenkt terrorist. Så langt har de lagret data om 209 000 personer over hele verden.

Selv om biometri opprinnelig ble utviklet for at man skulle identifisere personer av sikkerhetsgrunner, blir det stadig oftere bruk av kommersielle selskaper. Fordeler med dette er at i motsetning til PIN-koder og passord, er det svært vanskelig å miste eller glemme biometriske kjennetegn. De kan også være veldig vanskelig å kopiere. Derfor er det mange som anser biometri som mye sikrere enn PIN-koder eller passord.

For eksempel har Apples siste iPhone en fingeravtrykk-sensor, som kan skanne brukerens finger. Facebook bruker ansiktsgjenkjenning-teknologi for å kunne foreslå hvem som er avbildet. Facebooks forskningsprosjekt «DeepFace», kan med

97,25 % sikkerhet anslå om to bilder inneholder det samme ansiktet. Banker arbeider nå med å bruke stemmegjenkjenning, slik at kunder kan bruke kredittkort eller betale med mobilen ved å uttale et passord. Mange selskaper bruker også fingeravtrykk for å logge inn på bærbare maskiner. Reklamebyråer har også eksperimentert med å vise ulike reklame til ulike individer, basert på alder og kjønn.

I tillegg til identifisering, blir biometri i økende grad brukt for å analysere adferd. Mange treningsapper bruker biometriske kjennetegn, for eksempel hjerteslag og pustefrekvens for å gi skreddersydde anbefalinger til brukeren. I sikkerhetssammenheng kan biometri kobles med eksisterende systemer, noe som øker kapasiteten for overvåkning. Et eksempel er at teknologi for ansiktsgjenkjenning kan kobles med bilder fra overvåkningskameraer. Dette kan blant annet brukes til å lokalisere kriminelle hvis bilder fra overvåkningskameraet sammenliknes med politiets databaser. På denne måten kan man bruke biometrisk informasjon til å identifisere en person uten at personen selv er delaktig i prosessen.

9.3 Økt sikkerhet

Biometri kan bidra til økt sikkerhet på flere måter:

- Identifisering ved hjelp av biometri har blitt brukt i over 100 år av politi og sikkerhetsmyndigheter. Slik identifisering er for eksempel effektivt for å raskt avsløre identiteten til en ukjent person som er mistenkt for kriminelle handlinger.
- Innsamling av biometriske kjennetegn kan brukes til å øke sikkerheten ved spesifikke oppgaver. Man kan for eksempel sikre at bare autorisert personell har tilgang til maskiner som utfører visse oppgaver.

9.4 Utfordringer

Flere utfordringer må vurderes:

1. Biometriske data er ikke feilfrie.
 - Det sies at to biometriske prøver aldri er helt like. Ulikheter i utstyret som tar prøven eller forskjeller i lys eller temperatur kan føre til at man «godkjenner» feil person, eller at man avviser «riktig» person.
 - I tillegg vet man at biometriske kjennetegn kan forandres over tid. Alderdom,

Hvordan fungerer biometri?

Det første steget er å registrere et biometrisk «kjennetegn» fra et individ, for eksempel fingeravtrykk, iris-mønster eller mest typisk – et bilde. Disse kjennetegnene blir deretter lagret, enten som et bilde, eller som en digital gjenskapelse av mønsteret som brukes til i identifikasjonsprosessen. For å beskytte personvernet anbefales det å kun lagre mønsteret, og slette originalbildet.

Informasjonen kan lagres på ulike steder: lokalt på stedet prøven ble avlagt eller for eksempel i et identitetskort eller pass. Det kan også bli videresendt og lagret i en database.

Når man skal identifisere noen ved hjelp av biometri, blir personen bedt om avgi det aktuelle kjennetegnet. Deretter sammenliknes dette med bildet eller mønsteret som tidligere er samlet inn og lagret i databasen. Hvis sammenlikningen godkjennes blir personen akseptert.

Det vil alltid være en liten grad av usikkerhet knyttet til biometri. Visse fysiske kjennetegn forandres over tid. Det kan også oppstå små ulikheter mellom den opprinnelige prøven som er lagret i systemet, og prøven som avlegges ved identifikasjonsprosessen.

Biometri kan også brukes til kriminalitetsforebyggende arbeid, særlig når man bruker teknologi for å analysere adferd. Kombinert med for eksempel smarte overvåkningskameraer kan man prøve å identifisere en viss oppførsel som man antar vil være vanlig hos kriminelle. Dette kan for eksempel være en person som oppfører seg helt annerledes enn alle andre i en større folkemengde.

kirurgi eller ulykker kan føre til at systemet ikke lenger gjenkjenner personen.

- Det er mulig å forfalske biometriske data, som kan øke faren for identitets-tyveri.
- Det er fortsatt altfor lett å “lure” dagens teknologi. For eksempel man lure teknologi for ansiktsgjenkjenning ved å bruke briller, anlegge skjegg eller ny hårfrisyre.

2. Tidligere har bruk av biometri vært dyrt og tidkrevende, derfor har man klart å opprettholde personvernet knyttet til bruken. Nå blir dette utfordret av stadig billigere og mer effektiv teknologi. Hvis man utstyres overvåkningskameraer med ansiktsgjenkjenning koblet til sosiale nettverk er det enkelt å identifisere personer overalt hvor de ferdes.
3. I de fleste tilfeller må individet selv delta i prosessen ved å avlegge en prøve (for eksempel et fingeravtrykk). Nå finnes det stadig mer teknologi som kan registrere biometrisk informasjon uten at man er klar over det, for eksempel ved hjelp av bilder. Dette utfordrer konseptet om samtykke og ønsket om informasjon om slike prosesser.
4. Hvis den originale prøven blir ødelagt eller forandret vil det kunne føre til ubegrunnet stigmatisering av individer.

10 Er overvåkningsteknologi den eneste løsningen?

Du lurer kanskje på om overvåkning og sikkerhetsteknologi er den eneste løsningen. Til tider kan det virke som om sikkerhet kun handler om sporing og identifisering av mistenkte. Overvåkningsbasert sikkerhetsteknologi bygger på en antakelse om at å overvåke så mange som mulig, så detaljert som mulig er den beste måten å oppdage potensielle trusler og kriminelle. Når sikkerhetsteknologi blir implementert, inkluderer det nesten alltid overvåkning.

Dette bildet stemmer i en viss forstand, men viser ikke hele bildet. Selv om sikkerhetsteknologi kan brukes for å finne kriminelle og terrorister, og til og med få informasjon om hva de planlegger å gjøre, finnes det også tilnærminger som har som mål å øke sikkerheten med andre metoder. I dette kapitlet skal vi vise noen eksempler på slike alternative metoder.

Sikkerhet er et ganske vagt begrep som kan tolkes på mange ulike måter. Forhold knyttet til stabilitet i samfunnet, som for eksempel arbeidsmarked og sosiale ordninger er med på å avgjøre om folk kjenner seg trygge eller ikke.

10.1 Alternative sikkerhetstiltak: globalt og nasjonalt

EUs sikkerhetsprioriteringer, som vi så på tidligere, viser at sikkerhet er relevant på mange ulike samfunnsområder, og de omhandler ofte de «klassiske» sikkerhetsutfordringene som kriminalitet og terrorisme. De forrige kapitlene i dette heftet viser at det er mulig å bruke sikkerhetsteknologi for å finne og spore opp de som driver med slike aktiviteter. Men det er mange underliggende årsaker som fører til at slike sikkerhetsutfordringer oppstår, som for eksempel fattigdom, nasjonale eller internasjonale konflikter eller politiske og religiøse forskjeller. Sikkerhetsteknologi kan ikke brukes for å løse disse problemene.

Typiske sikkerhetsutfordringer for EU kan også være mat- og vannmangel, finanskriser, epidemier eller naturkatastrofer. Når vi tenker på sikkerhetsutfordringer i et mye bredere perspektiv, kan vi først se på noen global utfordringer.

Sikkerhetstiltak som har som mål å øke sikkerheten relatert til natur- og menneskeskapte katastrofer blir til en viss grad foreslått og implementert. Slike tiltak er ofte svært omfattende og langsiktige. Promotering av rettferdig handel, bistand og sletting av u-gjeld har som mål å bedre den økonomiske situasjonen, men også utfordringer knyttet til bedre utnyttelse av naturressurser, forurensning og klimaforandringer. Dette er på mange måter også utfordringer knyttet til sikkerhet. På samme måte er tiltak rettet mot lokal og nasjonal kriseberedskap, eller tiltak for å bedre infrastruktur og tilgang på mat og drikke noe som kan være med på å bedre sikkerheten.

Ulike måter å forstå sikkerhet på, og derfor ulike måter å jobbe for økt sikkerhet er utviklet både på globalt og nasjonalt/lokalt nivå.

Nasjonale og internasjonale løsninger:

- Promotering av rettferdig handel, bistand og sletting av u-gjeld.
- Økonomiske og sosiale tiltak som skal gi mer rettferdig fordeling av ressurser.
- Bedre ressursituasjon og infrastrukturen for krisehåndtering.
- Bruke bærekraftige og alternative energikilder i større grad.
- Forbedre informasjons- og kommunikasjonsstrukturer, samt mat- og vannforsyning i de deler av verden som trenger dette.

10.2 Alternative sikkerhetstiltak: lokalt

Det er flere alternative måter man kan prøve å oppnå økt lokal sikkerhet på. For eksempel kan man bruke sikkerhetsteknologi som ikke innebærer overvåkning. Metalldetektorer, lys med bevegelsessensorer, alarmer og til og med offentlige nødtelefoner er alle tiltak som kan bidra til økt sikkerhet uten å overvåke eller samle inn informasjon om befolkningen. Slike tiltak forsøker heller å bedre befolknings mulighet til å reagere slik at de kan beskytte seg selv og sine eiendeler. Teknologi som metalldetektorer identifiserer potensielle trusler ved å fokusere på kilden til trusselen (objektet i metall) istedenfor individet som kan utgjøre

re en trussel. De kan være svært effektive, men begrenser seg til det spesifikke området og tidspunktet de brukes. Samtidig utgjør de en liten trussel mot personvernet.

Tiltak for å forebygge kriminalitet og øke sikkerheten kan også gjøres gjennom byplanlegging og utforming av utemiljøer. Endring av utemiljøer slik at det blir færre «farlige områder» (for eksempel bakgater, torg eller parker som er vanskelig å ha oversikt over) – kan føre til økt trygghetsfølelse, og gjøre befolkningen mer bevisst på omgivelsene og hvilke trusler som kan oppstå.

Tiltak som ikke innebærer overvåkning eller datainnsamling:

- Fokus på teknologi som ikke innebærer overvåkning.
- Byplanlegging og utforming av utemiljøer som bidrar til økt trygghetsfølelse.

Det er også mulig å sette inn sikkerhetstiltak som innebærer overvåkning, men uten at det lagres store datamengder. Et typisk eksempel er å øke antall politipatruljer. Noen steder finnes det også vaktordninger i nabolag, hvor privatpersoner «patruljerer» nabolaget og tar kontakt med politiet dersom de oppdager noe mistenkelig. Gjestelister på utesteder og restauranter som kontrolleres av dørvakter er også et tiltak som baserer seg på overvåkning.

Tilnærminger som baserer seg på overvåkning uten datainnsamling:

- Tradisjonelle politipatruljer.
- Vaktordninger i nabolag.
- Dørvakter e.l.

En helt annen måte å takle sikkerhetsutfordringer på, er å se på de underliggende sosiale og økonomiske faktorene for vold, kriminalitet, rasisme og diskriminering. Dette er problemer som sikkerhetsteknologi ikke kan håndtere på en effektiv måte.

Det finnes flere eksempler på tiltak som går ut fra en slik bred tolkning av sikkerhetsbegrepet. Bedre kontakt mellom politi og lokalmiljø og involvering av religiøse eller andre samfunnsgrupper for å

styrke sosialt samhold er noen eksempler. Andre muligheter kan sees på som sikkerhetstiltak er sosial og økonomisk støtte for å få flere i arbeid og opplærings- og mentorordninger for personer som tilhører utsatte miljøer.

Frivillige organisasjoner for rehabilitering av rusmisbrukere og introduksjonssentre for innvandrere er andre tiltak som kan styrke sosialt samhold og samtidig øke sikkerheten i lokalsamfunnet.



Den grunnleggende ideen bak slike tiltak er todelt. På den ene siden handler det om få innbyggerne til å aktivt delta i å løse konflikter, og på den andre siden å hjelpe de som faller utenfor tilbake til samfunnet gjennom sosiale ordninger istedenfor fengselsstraff.

Aktiv opplæring rundt integrering, respekt og mangfold kan bidra til å redusere sosial, kulturell og økonomisk uro, og bidra til økt følelse av tilhørighet i lokalmiljøet og gjennom dette øke sikkerheten.

Langsiktige tiltak rettet mot sosiale forhold:

- Investere i sosiale midler, tiltak og personell.
- Oppmuntre befolkningen til aktiv deltakelse for å løse lokale utfordringer.
- Skape sterke bånd mellom lokale organisasjoner.
- Øke støtten til opplæring, utdanning o.l.
- Opprette velkomstsentre, nabolagsgrupper og sosiale møtepunkt.

I dette kapitlet har du fått en kort introduksjon til alternative løsninger på sikkerhetsutfordringer. Kanskje har du andre ideer til hvordan man kan øke sikkerheten?

11 Tilbake til deg...

Du har nå fått presentert de fem sikkerhetsteknologiene som skal diskuteres på workshopen. Vi har forklart hvordan de fungerer, hvordan de brukes, hvordan de bidrar til økt sikkerhet og hvilke utfordringer de medfører. Vi har også beskrevet i hvilken kontekst teknologiene har utviklet seg: i et Europa som er svært bekymret for sikkerhet og der sikkerhet blir en del av hverdagen. Personvern og overvåkning er også viktige tema, blant annet på grunn av mengden persondata som i dag benyttes i sikkerhetsøyemed. Avslutningsvis så vi på ikke-teknologiske tilnærminger for å øke sikkerheten i et samfunn.

Det er nå opp til deg å gjøre deg opp en mening om disse spørsmålene. Ville det vært akseptabelt om disse teknologiene ble benyttet rutinemessig? Kanskje tenker du at sikkerhetsteknologi utgjør et effektivt virkemiddel for å bekjempe kriminalitet? Eller at ikke-teknologiske løsninger er mer effektive? Er det bedre å bruke tradisjonelle etterforskningsmetoder enn nye overvåkningsbaserte teknologier? Eller kanskje du synes sikkerhetsutfordringene er overdrevet og vi ikke trenger å bekymre oss?

Noen mener at disse teknologiene er i trygge hender fordi de brukes av offentlige etater og myndigheter som må stå til ansvar for sine beslutninger og handlinger. Andre tviler på at disse myndighetene er i stand til å bruke slik teknologi på en kom-

petent og etisk måte, med befolkningens beste i tankene.

Kanskje synes du ikke at slik teknologi angår eller påvirker deg personlig: de er tross alt utviklet og rettet mot kriminelle og blir utplassert i områder der du vanligvis ikke ferdes. Likevel kan det hende at alle bør bekymre seg over mengden persondata som disse teknologiene behandler, og fordi de gjør alle og enhver til en mistenkt. Du er kanskje tilfreds med hvordan sikkerhetsteknologi brukes i dag, men bekymret for hvordan de kan brukes i fremtiden.

Å frasi seg deler av personvernet i bytte mot økt sikkerhet er uansett ingen enkel avveining. SurPRISE ønsker å forstå bredden av folks holdninger til nye sikkerhetsteknologier.

Vi ser fram til å møte deg på workshopen om noen uker. Dersom du vil vite mer om SurPRISE-prosjektet og dets partnere kan du besøke SurPRISE-nettsiden på <http://surprise-project.eu>

‘Utfordringer knyttet til personvern handler like mye om politikk- og samfunnsspørsmål som teknologi’

Colin J. Bennett, professor and sikkerhetsekspert ved Institutt for statsvitenskap,

University of Victoria, Canada

Om informasjonsheftet

Dette heftet er produsert for å gi informasjon til deltakere på workshoper i regi av SurPRISE-prosjektet. Heftet er distribuert til samtlige partnere i SurPRISE-samarbeidet av det Østerrikske Vitenskapsakademiets Institutt for Teknologivurdering (Strohgasse 45/5, A-1030 Wien). Les mer om prosjektet og partnerne på nettsiden <http://surprise-project.eu/>.

Informasjonen som fremgår av heftet er skrevet av SurPRISE-partnerne, basert på forskning og rapporter skrevet av politikere, forskere og teknologer fra hele verden.

Dette heftet er en bearbeidet versjon av informasjonsheftet skrevet av Dr Kirstie Ball (The Open University) i 2013 i forbindelse med folketoppmøtene som ble arrangert i ni land våren 2014.

- Forfattere: Dr Kirstie Ball, The Open University; Maria Grazia Porcedda and Mathias Vermeulen, EUI; Elvira Santiago and Vincenzo Pavone, CSIC; Regina Berglez, IRKS; Eva Schlehahn, ULD; Márta Szénay, Medián
- Scientific Advisory Board: Dr Monica Areñas Ramiro, Mr Robin Bayley, Professor Colin Bennett, Dr Gloria González Fuster, Dr Ben Hayes, Dr. Majtényi László, Mr Jean Marc Suchier, Ms Nina Tranø, Prof Ole Wæver
- Layout: by Zsolt Bartha, Medián, based on the first magazine prepared by Mr Peter Devine, Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University
- Bilder: Mr David Winter, Corporate Media Team, Learning and Teaching Solutions, The Open University. page 11: Vision Systems, <http://www.visionsystems.co.nz/assets/Video-Analytics1.jpg> page 14 Mat Wellington, "Police Use Quad-Copter – UK" March 23rd 2011, <http://multirotor-news.com/2011/03/23/police-use-quadcopter-uk> page 21 © iStockPhoto.com / alexsl, page 22 Senseable City Lab, Massachusetts Institute of Technology page 24 © KIVI NIRA DV, 2011
- Dette prosjektet har mottatt støtte fra EUs syvende rammeprogram for forskning og teknologiutvikling, under kontrakt nummer 285492
- Heftet er tilgjengelig på www.teknologiradet.no og <http://surprise-project.eu>

Partnere

- Institut für Technikfolgen-Abschätzung/Osterreichische Akademie der Wissenschaften,
- Coordinator, Austria (ITA/OEAW)
- Agencia de Protección de Datos de la Comunidad de Madrid*, Spain (APDCM)
- Instituto de Políticas y Bienes Públicos/Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain (CSIC)
- Teknologiradet - The Danish Board of Technology Foundation, Denmark (DBT)
- European University Institute, Italy (EUI)
- Verein für Rechts-und Kriminalsoziologie, Austria (IRKS)
- Median Opinion and Market Research Limited Company, Hungary (Median)
- Teknologiradet - The Norwegian Board of Technology, Norway (NBT)
- The Open University, United Kingdom (OU)
- TA-SWISS/Akademien der Wissenschaften Schweiz, Switzerland (TA-SWISS)
- Unabhängiges Landeszentrum für Datenschutz, Schleswig-Holstein/Germany (ULD)

* APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Dette prosjektet har mottatt støtte fra EUs syvende rammeprogram for forskning og teknologiutvikling, under kontrakt nummer 285492.

Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe.

