

Politiet øker innsatsen innen håndtering av elektroniske spor for å styrke bekjempelse av kriminalitet

Fungerende leder for Politiets datakripsenter, Rune Erlend Fløisbonn

ØKOKRIM bygger opp et datakripsenter i verdensklasse for å trappe opp bekjempelse av datakriminalitet og annen kriminalitet hvor ny teknologi benyttes.

Bakgrunn

Mørketallsundersøkelsen om datakriminalitet som ble gjennomført av NSO og ØKOKRIM i 2001 viser at mindre enn 1 % av datainnbrudd og mindre enn 0,1 % av forsøk på slike innbrudd blir anmeldt. Trusselvurderinger viser at det kan forventes en økning i antall saker både innen datakriminalitet og tradisjonell kriminalitet hvor ny teknologi tas i bruk. Uten dybdekunnskap og gode verktøy for å avdekke denne type kriminalitet blir det vanskeligere for politiet å etterforske slike saker. Tall fra utlandet viser at flere organiserte kriminelle grupper er avanserte brukere av internett og datateknologi. De opererer ofte på tvers av landegrensene og skjuler identitet og innhold i elektroniske spor.

Tendensen er at elektroniske spor blir en stadig viktigere informasjonskilde som politiet benytter i bevisføringen i straffesaker. Det er en klar tendens at elektroniske spor etterlates i forbindelse med alle typer kriminalitet. Spesielt utfordrende er det at dagens finansinstitusjoner, moderne industribedrifter og tjenesteytende næring produserer mer elektronisk informasjon enn papirinformasjon, og at etterforskning av slike større bedrifter ved mistanke om kriminalitet kan gi u håndterlige datamengder å undersøke. Den såkalte Finance Credit-saken illustrerer dette veldig klart. Det ble beslaglagt papirmengder i størrelsesorden 10 hyllemeter med papirinformasjon. I tillegg ble det gjort elektroniske beslag som utgjorde ca. 2 terabyte, eller to tusen milliarder tegn. Dette tilsva-

Rune Erlend Fløisbonn er utdannet siv.ing. innen datafag fra Norges teknisk naturvitenskapelig universitet (Trondheim) og har erfaring fra stillinger som forskningsleder, forskningssjef, IT-direktør og fakultetsdirektør ved Universitetet i Oslo. Han har de siste tre årene arbeidet ved ØKOKRIM og hatt stilling som spesialetterforsker, prosjektleder for etablering av Politiets datakripsenter og nestleder. Han leder for tiden datakripsenteret.

rer en 50 kilometer høy stabel av A4-dokumenter lagt oppå hverandre.

Når politiet skal etterforske kriminelle handlinger i større virksomheter, blir den elektroniske datamengden så stor at den er vanskelig å finne fram i uten datateknisk spesialistkompetanse og gode datatekniske hjelpemidler. Selv da kan det ta flere timer og dager å la en datamaskin søke gjennom hele datamengden for å finne treff på enkle søkeord.

Politisk besluttsomhet

Etter forslag fra ØKOKRIM besluttet Regjeringen i mars 2001 å etablere Politiets datakrimsententer. I St.meld. (2001–2002) nr. 17 Samfunnssikkerhet – veien til et mindre sårbart samfunn – pekte utvalget på at Norge må redusere IKT-sårbarheten, og at landet vil være godt rustet til å oppklare datakriminalitet ved etablering av et datakrimsententer.

Regjeringen og Politidirektoratet har i 2002 og 2003 fulgt opp med bevilgninger slik at senteret nå har flyttet inn i egnede lokaler på Bryn i Oslo og blitt prioritert med stillinger og utstyr slik at bemanningen i 2003 blir på 21 medarbeidere. Det vil også bli foreslått en videre opptrapping for å nå det planlagte nivået på 34 stillinger. Senteret ble offisielt åpnet 15. mai 2003.

Senterets oppgaver

Senteret skal være en kombinasjon av et nasjonalt polititjenestorgan for å forebygge, etterforske og påtale datakriminalitet, og et kompetanseorgan for utvikle nye kunnskaper om metoder og teknologi i kriminalitetsbekjempelsen. Senteret skal også bistå hele politietaten i sikring og analyse av elektroniske spor, spesielt i større og komplekse saker.

Senteret vil dessuten ha en nøkkelrolle i å drive opplæring av polititjenestemenn og jurister i distriktene for at politiet skal kunne håndtere elektroniske bevis på en god måte i alle straffesaker. En viktig oppgave i etterforskningsarbeidet er å utvikle taktiske og tekniske metoder for spaning og etterretning som kan avdekke kriminelle handlinger på internett og i «cyber space».

Visjoner om senterets posisjon

Senterets mål er å være en nasjonal ressurs, et Centre of Excellence på høyt internasjonalt nivå innen nettbasert etterforskning og elektroniske spor, og en drivkraft for utvikling av tverrfaglig kunnskap i grenseflaten mellom juss, politifag og datateknologi. Dette gir også en unik mulighet for å gi innspill til lovgiver i forbindelse med videre utvikling av norske lovbestemmelser i det elek-

troniske rom. Senteret skal ha et oppdatert datateknisk laboratorium med utstyr, datanettverk og personell som kan bistå politiet med å sikre og analysere elektroniske spor. De ansatte skal være under kontinuerlig opplæring, og få mulighet til å vedlikeholde kunnskaper slik at senteret klarer å følge med i den raske teknologiske utviklingen. For å nå målet om et høyt kompetansenivå, utvikles det et tett samarbeid med ledende norske og utenlandske politienheter, forskningsmiljøer og bedrifter.

En moderne politiorganisasjon

Senteret har en tverrfaglig stab av jurister, politifolk og dataspesialister med universitets- og høyskoleutdanning. For å sikre at senteret blir både en polititjenesteorganisasjon og en kunnskapsorganisasjon, skal det prøves ut en ny organisasjonsform hvor saksarbeidet utføres som prosjekter med personell fra disiplinbaserte faggrupper som hver for seg fordyper seg innen sine spesialistområder. Dette er en interessant modell som kan gi verdifullt bidrag til hvordan fremtidens politi kan organiseres.

Aktiviteter

Senteret etterforsket i 2002 19 egne saker innen datakriminalitet og bistod politidistriktene med etterforskning/teknisk bistand i 230 saker. I tillegg ble det utført en rekke utviklingsoppgaver, hospitantopplæring og undervisning av studenter ved Politihøgskolen. Det er et utstrakt samarbeid med KRIPOS innen etablering av nye datatekniske metoder for etterforskning av seksuelle overgrep mot barn ved besittelse og distribusjon av bilder på internett. Senteret har også et tett samarbeid med norske og utenlandske IT-miljøer og forskningsmiljøer når det gjelder utvikling av verktøy for sikring og analyse av elektroniske spor, matematisk modellering og intelligent søking på store datamengder. Senteret ønsker å knytte sine oppgaver og kunnskaper i nært samarbeid med politidistriktene og eksterne kunnskapsmiljøer. Det vil årlig være 10-15 hospitanter som får opplæring og trening i våre spesialistområder, og det vil i perioder være universitets- og høyskolestudenter tilstede som utfører diplom/hovedoppgave ved senteret.

Elektroniske spor

I dagens digitale samfunn blir elektroniske medier og tjenester stadig mer integrert i forretningslivet, i fritiden og i omgangen mellom mennesker. Alle elektroniske tjenester gir en eller annen form for «avtrykk» og spor. I politiets etterforskning kan disse sporene sikres og senere analyseres og tolkes. Utdringene knyttet til sporsikring er dels at sporene kan ligge synlig, usynlig,

gjemt, forvrengt, slettet eller ødelagt og dels at det hele tiden utvikles nye varianter av medier, tjenester og produkter som slike spor kan knyttes til.

Elektroniske spor er knyttet til fysiske eller trådløse medier. De vanligste fysiske medier er lagringsenheter som harddisker, pendisker, floppydisker, CD-rom/DVD, taper av ulike typer, flashcards, ROM/RAM brikker og ulike elektroniske kort. Disse mediene er knyttet opp mot systemer og tjenester i datamaskiner, nettverk og forbrukerelektronikk. I de fleste tilfeller er mediene bare deler av det vi kaller personlige datamaskiner, servere, store datamaskiner, operativsystemer, mobiltelefoner, faks, geografiske posisjonssystemer, elektroniske kort, meldingsterminaler, kopieringsmaskiner, videokameraer, video/DVD-maskiner, printere, telefonsentraler, kommunikasjons-systemer, trådløse og fysiske nett, internett, kabelTV-anlegg og elektroniske brannvegger.

Innholdet i sporene er gjerne knyttet til bruksanvendelser i dokumenter, databasesystemer og registre for administrasjon, økonomi, elektronisk post, datakonferanser, tale og videokonferansesystemer, telefoni, loggsystemer, posisjoneringssystemer, alarmsystemer, detektorer etc.

Den allmenne bruk av informasjonsteknologi i samfunnet og den raske teknologiske utvikling medvirker til at det årlig produseres et stort antall varianter av medier, og at de kommer ut med nye typer bruksanvendelser. Eksempler på dette er bl.a. intelligente kjøleskap og komfyrer, elektronisk styrte boliger, elektronikk i biler og elektronikk i klær.

Politiets håndtering av elektroniske spor

Politiets håndtering av elektroniske spor kan deles inn i følgende faser: 1) sikring (kopiering uten endring av original), 2) teknisk analyse (beskrive sporene teknisk og konvertere til lesbar form) og 3) innholdsanalyse (anvende innholdet i sporene til etterforskningen).

Sikring av elektroniske spor innebærer å kopiere det originale «fingeravtrykket» og sporinformasjonen, uten å endre originalen, og lagre kopien slik at den kan rekonstrueres for analyse. Det kreves innsikt i elektroniske medier og forståelse for bruk av riktige metoder i sikringsfasen for at ikke sporene skal ødelegges som bevis. Samtidig er det nødvendig å benytte flere typer metoder og retningslinjer for bevissikring, fordi det er mange varianter av medier som krever spesiell håndtering.

Ikke alle politidistriktene har foreløpig mulighet til å kartlegge og sikre elektroniske spor innen alle varianter av medier med tilstrekkelig kvalitet. Det er vanskelig å bygge opp stabile kompetansmiljøer lokalt, først og fremst på grunn av manglende prioritering av IT-faglig kompetanse og ressurser på området. Det er

imidlertidig ønskelig at politidistriktene skal kunne utføre sikring og analyse på de vanligst forekomne elektroniske spor. Større og mer kompliserte oppgaver bør kunne utføres ved Politiets datakripsenter hvor det finnes spisskompetanse og spesialutstyr.

Automatiserte operasjoner

Innsamling og lagring av elektroniske spor har tidligere foregått med manuelle operasjoner på lokale lagringsmedier. Politiet utvikler nå systemer som gjør at alle elektroniske spor i en sak samles i ett sentralt masselager, tilknyttet datamaskiner som utfører automatiserte rutiner for undersøkelser av beslagene.

Dette gir høyere kvalitet ved sikring av data, mer effektiv analyse av spor hvor data kan vaskes for tekster, bilder, transaksjoner og mistenkelige mønstre. Sammenlignet med manuelle menneskelig gjennomganger arbeider datamaskiner mye raskere når en leter etter mønstre og kobler informasjon fra flere kilder.

Norsk politi har med sine nye metoder og teknologiske konsept vakt internasjonal interesse. Dette skyldes først og fremst at en er tidlig ute med å etablere politiet som en kunnskapsorganisasjon hvor dataspesialister, jurister og politifolk finner gode løsninger sammen og at en har etablert et tett samarbeid med næringsliv og forskningsmiljøer innen viktige kunnskapsområder.

Økende internasjonale krav til håndtering av elektroniske bevis

I Europa er det en økende bekymring for utviklingen som viser at de organiserte kriminelle nettverkene er blant de mest avanserte brukerne av ny teknologi. De opererer ofte over landegrensene samtidig med at bruken av ny teknologi kompliserer politiets etterforskning. For at politiet skal kunne styrke sitt arbeid innen slike saker, bør det foreligge felles lovverk for elektroniske bevis, minstekrav til kvalitet og felles metoder for håndtering av elektroniske beslag over landegrenser.

Det er derfor under utvikling klare kompetanse- og kvalitetskrav for håndtering av elektroniske bevis både i Europa og på den internasjonale arena som Norge må forholde seg til. Disse kravene utvikles for tiden i ENFSI (European Network of Forensic Science Institutes), IOCE (International Organisation on Computer Evidence) og American Society of Crime Laboratory Directors i USA. Akkreditering av laboratorier er i gang i USA, selv om kun et fåtall foreløpig er godkjent. Kvalitetskrav settes til bygninger, lokaler, utstyr, metoder og kompetanse til dem som utfører oppgavene. Det kan ta 3-5 år før en lignende prosess kommer i gang i Europa.

Intelligent analyse av elektroniske spor – en avgjørende faktor for å kunne håndtere store datamengder

Vi erfarer at et økende antall straffesaker byr på mange uhåndterbare informasjonskilder med store mengder av data. Dette betyr at kompleksiteten blir høy langs flere akser og karakteriseres av følgende:

- Store mengder av data
- Mange ulike typer av data
- Data finnes i ulike typer inhomogene systemer
- Data er spredt over flere tidsintervaller
- Data finnes i flere organisasjoner og hos flere personer

Datakrimsenteret arbeider med å finne intelligente måter å granske store datamengder på ved bruk av regelbaserte systemer, automatisk/halvautomatisk ekstraksjon av mønstre og regler, vasking og deteksjon av mønstre og utvikling av modeller (prediktive og ikke-prediktive) som angir ulike sannsynlige former for kriminelle handlinger. De verktøyene som tas i bruk, har som formål å utføre datakvalitets-analyse ved å hente rådata fra kildesystemene, transformere og organisere dem slik at de enkelt kan benyttes til analyse og rapportering.

Prediktive modeller øker treffsikkerheten i etterforskningen. Reglene kan lett modifiseres fordi logikken bak er tilgjengelig. Reglene kan redefineres og prioriteres slik at de fremstår mer som modeller som angir en sannsynlig utvikling enn som bare rapportering av historisk informasjon.

Hensikten er å få sikrere og mer effektive analyser ved

- å konstruere mer komplette profiler av mistenkelig personer, transaksjoner, og kanaler fra alle kilder, med mulighet for vasking av data
- mer korrekt deteksjon og avvisning av falske positive av mistenkelige mønstre som øker sannsynligheten for at man etterforsker de riktige sakene. Dette fører til spart tid, penger og ressurser
- ad hoc analyser gjør det mulig å oppdage og utforske alternative scenarier
- rapportering og kvalitetssikring av prosesser som understøtter etterforskningen for påtaleansvarlige
- å ta vare på kunnskapen i organisasjonen på en strukturert måte
- å koble sammen informasjon fra mange registre for å finne sammenhenger som ikke kan ses ved kun å se på enkelte av kildedataene

- å utvikle en minnebasert resonnering der en kan gruppere og klassifisere ulike strukturerte dokumenter i ulike formater slik at dokumentene knyttes til meningsinnhold

Det vil på denne måten være mulig å avdekke kriminelle handlinger raskere. Ved å se på dataene i sammenheng vil man kunne finne mønstre i dataene som ikke ofte kan ses med tradisjonelle metoder. Ved å bringe sammen ekspertise fra flere deler av etterforskningen og i tillegg benytte avanserte dataverktøy, kan man effektivisere etterforskningen samtidig som man kan bygge opp regelsett basert på de erfaringer man har gjort. I tillegg kan man bruke modeller som avdekker allerede kjente former for kriminelle handlinger.

Mary-Ann Hedlund er lagdommer i Borgar lagmannsrett. Hun er advokat fra UiO 1979, og tidligere arbeidet som advokat, dommerfullmektig og politifullmektig og har vært leder/medarbeider av flere offentlige utvalg. Hun er medlem av menneskerettsutvalget Den Norske Dommerforening.