POLITIET
POLITIDIREKTORATET

Datakrimstrategien

Norge skal være
et av **foregangslandene**
i bekjempelse av **datakriminalitet** og
på denne måten bidra til en **trygg bruk** av
datasystemer for å sikre **verdiskapning**,
demokrati og velferd.

Politidirektoratets publikasjoner 2014

Strategi for informasjonssikkerhet for politiet 2014–2018.

Forebygge og bekjempe kriminalitet fra énprosentmiljøet og kriminelle MC-gjenger: håndbok for politi og kommunale myndigheter.

Tendenser i kriminaliteten: utfordringer i Norge 2014.

Report from the national coordinating unit for victims of trafficking 2010.

Report from the national coordinating unit for victims of trafficking 2011.

Ressursanalyse 2013: utgifter og bemanning i politi- og lensmannsetaten.

Rapport fra Koordineringsenheten for ofre for menneskehandel 2013.

Veileder – Risikovurderingsverktøyet SARA:SV. Det forebyggende sporet i partnervoldsaker.

IKT-begreper: versjon 1.0.

Etterretningsdoktrine for politiet: versjon 1.0.

Politiets bekymringssamtale: hva er det?

Politidirektoratets publikasjoner 2015

Overordnet IA-handlingsplan for politietaten.

Overordnet nasjonal strategi for bekjempelse av datakriminalitet (Datakrimstrategien)

Utredning fra en gruppe oppnevnt av Politidirektoratet etter oppdrag fra Justis- og beredskapsdepartementet i brev av 1. november 2013.
Avgitt til Justis- og beredskapsdepartementet 12. mai 2015.

Innhold

Del 1

Innledning

1. Sammendrag

Del 1: INNLEDNING

1.1. Oppdraget

Utredningen behandler datakrimtrusselen og hvordan bekjempelsen av datakriminalitet foregår i dag. Den gir en vurdering av om ansvar, roller og samarbeid fungerer tilfredsstillende, og foreslår en overordnet nasjonal strategi for bekjempelsen av slik kriminalitet.

Justisdepartementet (JD) utformet et mandat for utredningen i brev av 1. november 2013 og ba Politidirektoratet (POD) å utføre oppdraget. POD oppnevnte en arbeidsgruppe kalt Strategigruppen, som har vært sammensatt av representanter fra følgende organisasjoner:

- Politidirektoratet (POD), seniorrådgiver Rune Erlend Fløisbonn
- Politiets sikkerhetstjeneste (PST), seniorrådgiver Atle Tangen, erstattet av fagdirektør Jon Fitje Hoffmann. Ingen deltakelse i perioden juni 2014 til 19. januar 2015
- Kripos, avdelingsdirektør Eiliv Ofigsbø
- Nasjonal sikkerhetsmyndighet (NSM), underdirektør Anders Bjønnes
- Påtalemyndigheten, statsadvokat Carl Fredrik Fari
- Etterretningstjenesten (E-tjenesten), underdirektør Morten Groven. Ingen deltakelse i perioden november 2014 til 5. januar 2015
- Norsk senter for informasjonssikring (NorSIS), seniorrådgiver Vidar Sandland
- Næringslivets Sikkerhetsråd (NSR), seniorrådgiver Arne Røed Simonsen

Gruppen har vært ledet av professor dr.juris. Jon T. Johnsen, Institutt for offentlig rett, Universitetet i Oslo.

Sekretærer har vært:

- politiadvokat Knut Jostein Sætnan, Kripos
- rådgiver Simon Kiil, Nasjonal sikkerhetsmyndighet
- rådgiver André Nordbø, Politidirektoratet

I tillegg oppnevnte POD en styringsgruppe for arbeidet.

Kapittel 2 redegjør for mandatet, forståelsen av det samt oppbyggingen av strategirapporten, som er delt i tre hoveddeler:

Del 1: Innledning
Del 2: Utviklingstrekk ved det digitale samfunn og datakriminalitet samt dagens bekjempelse
Del 3: Overordnede strategier for bekjempelse av datakriminalitet

Til sammen dekker del 2 og 3 problemstillingene i mandatet.

DEL 2: UTVIKLINGSTREKK VED DET DIGITALE SAMFUNN OG DATAKRIMINALITET SAMT DAGENS BEKJEMPELSE

1.2. Databruk, datakriminalitet og trusselbildet

I kapittel 3 forklares først de sentrale begrepene 'trussel', 'risiko' og 'sårbarhet'. De som representerer truslene, kalles 'trusselaktører', og de som skal bekjempe dem, for 'sikkerhetsaktører'. Målet er å beskrive enkelte hovedtrekk ved dagens trusselbilde for datakriminalitet, inndele datakriminaliteten i hovedtyper og antyde mulige utviklingstrender. Utgangspunktet er den faktiske og ønskede databruken i samfunnet, fordi den også danner grunnlag for hvilke typer datakriminalitet som kan utvikle seg.

Utviklingen av det moderne digitale samfunnet har gått meget raskt de siste 20 årene og har ført til store samfunnsendringer. Den fysiske og digitale verden blir knyttet stadig tettere sammen: datamaskiner blir mindre, vi har dem med overalt, antall digitale sensorer øker, og maskinene tas i bruk i stadig større deler av våre liv; i arbeids- og næringsliv, samfunnsdeltakelse, hjemme og i helseoppfølging. Mengden data som samles inn, er overveldende, men gir samtidig store muligheter for å utvikle ny kunnskap. Teknologien sprenger stadig nye grenser og åpner for nye bruksmuligheter.

Dette benytter også de kriminelle seg av. Internett muliggjør deling av kriminell kunnskap, verktøy og metoder og innbyrdes kjøp og salg av kriminelle tjenester. Det utvikles dataverktøy for å utføre mange former for datakriminalitet som med minimal innsats kan tilpasses konkrete kriminelle handlinger.

Datakriminalitet er ikke noe ensartet begrep. Det kan dreie seg om datainnbrudd og datatyveri, sabotasje, ulovlig endring av data, avlytting eller avlesning av datakommunikasjon, spredning av skadevare, passordknekking, DDoS-angrep, spredning av overgrepsmateriale av barn, databedrageri, brudd på åndsverk- og opphavsrettslig beskyttelse, nettomsetning av narkotika og andre illegale produkter, trusler, rasistiske og hatefulle ytringer etc. Kapittelet gir en nærmere gjennomgang av dagens sentrale kriminalitetstyper.

Trusselaktørene favner vidt; fra enkeltpersoner til statlig finansierte grupperinger med store budsjetter og langsiktige mål. Vi finner organiserte kriminelle miljøer, aktivister og terrorister. Skadepotensialet er stort i form av tapt kritisk informasjon, sabotasje og lammelse av kritiske samfunnsfunksjoner.

Trusselaktørenes metoder er mange. De lurer inn skadevare, bruker sosiale manipulasjonsteknikker, skjuler seg ved anonymiseringsteknikker og kryptering. De bruker virtuelle betalingsformer, infiltrerer organisasjoner og produktleveransekjeder.

Informasjonssikkerhet har fremdeles lav prioritet i norske virksomheter. Stadig flere datatjenester blir kontrahert ut, ofte til aktører i andre land. Grensen mellom privatliv og jobb blir visket ut ved at vi bruker de samme digitale enhetene på tvers. Vi ser en økning i digitale identitetstyverier og etterfølgende misbruk av identitet. Det blir vanskeligere å beskytte personlig informasjon. Slik utviklingen er, med automatisering av helseprodukter, kjøretøy, hjemme og på jobb, må politiet være forberedt på å håndtere kriminalitet hvor dataangrep på norsk infrastruktur eller enkeltindivider fører til fysisk skade og dødsfall.

1.3. Dagens bekjempelse av datakriminalitet

I kapittel 4 gis en punktvis oversikt over hvilke oppgaver det samlede systemet av sikkerhetsaktører ivaretar:

- etterretning i form av innsamling av informasjon og analyse
- beskrivelse av trusselbildet (eller «utarbeidelse av trusselvurderinger»)
- forebyggende virksomhet
- oppdagelse og avdekking av datakriminalitet
- hendelseshåndtering med avverging og skadebegrensning
- etterforskning
- straffesaksbehandling

Hvilke oppgaver som ivaretas av de ulike sikkerhetsaktørene, varierer. Kapittelet gir derfor en kortfattet, men god oversikt over sikkerhetsaktørene her til lands, og over noen utvalgte utenlandske sikkerhetsaktører av særlig relevans for Norge. Her beskrives hva slags organisasjon det er tale om, og oppgavene deres. For de norske aktørene skilles det mellom offentlige og private aktører.

Til de offentlige aktørene hører *politiorganisasjonen* med Politidirektoratet som faglig leder, politidistriktene som den lokale komponenten og særorganer som Kripos og Økokrim. Politiorganisasjonen har oppgaver direkte knyttet til forebygging, avverging og straffeforfølgning av datakriminalitet. PST står i en særstilling ved å ha både en sentral enhet og lokale enheter i politidistriktene. PST er heller ikke underlagt Politidirektoratet, men sorterer direkte under Justis- og beredskapsdepartementet.

Også den høyere påtalemyndighet, ved Riksadvokaten og statsadvokatembetene, har straffeforfølgning av datakriminalitet som oppgave. Mens POD leder den forebyggende og avvergende virksomheten etter politiloven, er Riksadvokaten leder for straffeforfølgningen etter straffeprosessloven. POD sorterer under Justisdepartementet, mens Riksadvokaten har en selvstendig stilling.

Ingen av organisasjonsleddene i politiet eller Riksadvokaten har datakriminalitet som eneoppgave. Bekjempelsen må ivaretas som en del av den alminnelige kriminalitetsbekjempelsen og prioriteres sammen med annen kriminalitet. Vi har altså ikke noe eget «datapoliti» i Norge.

Av offentlige sikkerhetsaktører *utenfor politiet* og påtalemyndigheten har Nasjonal sikkerhetsmyndighet (NSM) et viktig sektorovergripende ansvar for datasikkerhet. Deres oppgaver er forebyggende sikkerhet ved skjermingsverdig informasjon og å koordinere håndteringen av forsvaret mot alvorlige dataangrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsinstitusjoner. NSM har derimot ikke noe spesifikt ansvar for å forebygge, avverge eller etterforske datakriminalitet.

Etterretningstjenesten i Forsvaret har et sektorovergripende ansvar for å innhente og analysere informasjon om fremmede stater, organisasjoner og personer som utgjør en sikkerhetstrussel mot samfunnskritiske datasystemer, og skal blant annet varsle om forstyrrelser, kompromittering og manipulering av datasystemer som kan ramme rikets selvstendighet, sikkerhet og andre nasjonale interesser utenfor rikets grenser.

Nasjonal kommunikasjonsmyndighet (tidligere Post- og teletilsynet) skal blant annet føre tilsyn med teleselskaper og telenett og forvalte frekvenser og nummerressurser inkludert IP-adresser, mens Datatilsynet skal ivareta personvernhensyn.

Av de *private* sikkerhetsaktørene er Næringslivets Sikkerhetsråd (NSR) en medlemsorganisasjon som skal forebygge kriminalitet mot næringslivet – også datakriminalitet – mens Norsk senter for informasjonssikring (NorSIS) arbeider for at alle skal kunne bruke datateknologi og Internett trygt på jobb og privat. NorSIS driver blant annet tjenestene Slett meg.no og IDtyveri.info.

Datakriminalitetens internasjonale karakter tilsier omfattende kontakt og utveksling med internasjonale sikkerhetsaktører og nasjonale aktører i andre land. Europol er EUs organisasjon for politisamarbeid og kriminaletterretning. De har inngått bilaterale samarbeidsavtaler med stater utenfor EU – deriblant Norge. EU opprettet nylig sitt eget datakrimsenter (European Cybercrime Center – EC3) ved Europol. Senteret skal styrke EUs kamp mot datakriminalitet. Interpol (International Criminal Police Organization) åpnet i 2015 et nytt datakrimsenter (IGCI) i Singapore. Også andre internasjonale tiltak nevnes kort.

En viktig oppgave for sikkerhetsaktørene er utarbeidelse av trusselvurderinger. Kapittel 4 avsluttes med en oversikt over dette.

DEL 3: OVERORDNEDE STRATEGIER FOR BEKJEMPELSE AV DATAKRIMINALITET

1.4. Utfordringene og strategier i andre land

Hovedmålet for strategigruppen har vært å identifisere utfordringene ved bekjempelse av datakriminalitet og foreslå hvordan de skal møtes. Kapittel 5 gir en oversikt over hva de sentrale sikkerhetsaktørene ser som de viktigste utfordringene, hvordan utfordringene har vært bedømt i tidligere utredninger, og hva slags strategiplaner andre land som er sentrale i bekjempelse av datakriminalitet, har utarbeidet. Denne gjennomgangen har vært et viktig utgangspunkt for gruppens egne strategivurderinger i kapittel 6–11.

Strategigruppen har innhentet egenvurderinger fra alle sentrale sikkerhetsaktører:

POD legger vekt på bedre samarbeid og koordinering sikkerhetsaktørene imellom og at rapporteringen av datakriminalitet må bedres, og mener en årlig nasjonal trusselvurdering bør vurderes. Oppdateringen av lovverket går for sakte. Metoder og teknologi foreldes raskt, og kunnskapsnivået og kapasiteten bør bedres. Politidistriktene har ikke tilstrekkelig bevissthet om datakriminalitet selv om den er økende, og bare et fåtall saker etterforskes. Kripos har bare kapasitet til to til fem saker per år. Politiet utfører i liten grad forebyggende arbeid og mangler systematiske metoder og verktøy for etterretning, etterforskning og straffeforfølgelse av større saker.

Kripos mener også det er behov for å styrke samarbeidet om bekjempelse av datakriminalitet nasjonalt og internasjonalt. Rapporteringssystemene er ikke spesielt tilpasset datakriminalitet, og det er vanskelig å få ut gode statistikker. Mørketallene er et problem. Alvorlig internasjonal datakriminalitet er vanskelig å etterforske og iretteføre, særlig når den

er knyttet til land som ikke prioriterer internasjonal bekjempelse av datakriminalitet.

PST vurderer trusselen fra fremmede stater og grupperinger med sterk statlig tilknytning som økende. Det samme gjelder annen alvorlig kriminalitet, radikalisering av muslimer og mellomstatlige konflikter. Utilstrekkelige lovhjemler for relevant metodebruk i det digitale rom svekker evnen til å beskytte nasjonale interesser og den enkelte borger. Internasjonalt og nasjonalt samarbeid må utvikles videre.

Påtalemyndigheten ønsker å styrke egen kompetanse og øke sakstilfanget. Samarbeidet nasjonalt og internasjonalt bør utvikles, spesielt med stater som er baser for internasjonal datakriminalitet.

NSM ønsker økt nasjonalt samarbeid – også med politiet – men påpeker at dette ikke må svekke et allerede etablert samarbeid mellom myndigheter og virksomheter (offentlige og private) som har ansvar for kritisk datainfrastruktur.

Datatilsynet er særlig opptatt av at de mest inngripende tiltakene i kriminalitetsbekjempelsen må ha hjemmel i lov, fastsatt av Stortinget, samt at sentrale prinsipper som proporsjonalitetsprinsippet og prinsippet om formålsbestemthet etterleves.

Etterretningstjenesten er i for stor grad avhengig av samarbeidende utenlandske tjenester, og har i for liten grad mulighet til å drive egen innsamling og analyse.

Cyberforsvaret mener Norge har et umodent planverk for håndtering av kriser knyttet til samfunnskritisk datateknologisk infrastruktur, og at en revisjon av nasjonalt beredskapssystem (NBS) trolig er nødvendig. Lovverk, praksis og nasjonal arbeidsdeling er ikke innrettet mot håndtering av flyktige og grensekryssende trusler. Myndighetsorganer og samfunnskritiske virksomheter mangler systemer og rutiner for formidling, behandling og oppbevaring av relevant, gradert informasjon.

NSR påpeker at 93 % av norske virksomheter har færre enn 10 ansatte, og særlig en del ledere synes å mangle kompetanse om informasjonssikkerhet og datakriminalitet[1]. Mange virksomheter tjenesteutsetter hele eller deler av IT-driften uten å stille krav om sikkerhet til leverandørene. Både NSR og NorSiS mener mulighetene for rapportering av datakriminalitet er mangelfulle og lite kjent i virksomhetene.

Gjennomgående gir vurderingene uttrykk for at etterforskning og straffesaksoppfølging i datakrimsaker er for hendelsesstyrt og for lite kunnskapsstyrt. Kapasiteten er under kritisk størrelse. Evnen til å utvikle og gå inn i større alvorlige saker er beskjeden.

Deretter oppsummerer kapittel 5 kort en rekke tidligere utredninger, som viser at mange av utfordringene som sikkerhetsaktørene påpeker, har vært kjent og påpekt helt siden årtusenskiftet, selv om de også har fått en mer alvorlig karakter.

Til slutt redegjøres det for strategier om datakriminalitet ('Cyber Crime Strategies') og datasikkerhet ('Cyber Security Strategies') fra Europarådet, EU, Nederland, Storbritannia, Finland og USA. Egne datakrimstrategier er uvanlig, men forekommer. De fleste landene inkluderer datakrimbekjempelse i sine datasikkerhetsstrategier. 'Public Private Partnership' går igjen i internasjonale strategier som et sentralt satsingsområde. Flere strategier erkjenner behovet for en mest mulig internasjonal og felles strategi mot datakriminalitet for å unngå at det oppstår kriminelle «frihavner», og for å legge et grunnlag for at flest mulig land samarbeider i internasjonale etterforskninger.

1.5. Visjon for bekjempelse av datakriminalitet

I kapittel 6 begrunnes forslaget om en visjon for den overordnede nasjonale strategien. Visjonen bør ta utgangspunkt i trusselens alvor. Hvor viktige er samfunnsinteressene som trues, og hva slags tilstand ønsker vi å ha for databruk? Datateknologiens enorme potensial for samfunnsutviklingen poengteres. Datakriminalitet truer vesentlige verdier. Visjonen bør angi den ønskede tilstanden for databrukerne og samfunnet, og være et mål for kriminalitetsbekjempelsen og for ivaretakelse av personvernet, rettssikkerheten og menneskerettighetene. Behovet for internasjonal bekjempelse er så viktig at det bør inngå i visjonen.

1 *NSR, Mørketallsundersøkelsen 2014.* http://www.nsr-org.no/moerketall/.

Visjonen for strategien er:

> *Norge skal være et av foregangslandene i bekjempelse av datakriminalitet og på denne måten bidra til en trygg bruk av datasystemer for å sikre verdiskapning, demokrati og velferd.*

Selv om den registrerte datakriminaliteten i Norge internasjonalt sett er lav, er mørketallene store. Kriminaliteten er økende og det fremtidige skadepotensialet stort. Dette bør være avgjørende for ambisjonsnivået. En vesentlig styrking av innsatsen må til for å redusere risikoen for en negativ utvikling.

En gjennomgang av visjonene i andre lands strategier for datasikkerhet og bekjempelse av datakriminalitet viser at et trygt digitalt rom prioriteres høyt. Dette «rommet» er i sin natur internasjonalt. Omfattende internasjonalt samarbeid er derfor vesentlig for å realisere en slik visjon.

Visjonen skal realiseres gjennom fem hovedstrategier for 1) analyse 2) kriminalisering 3) forebygging og avverging 4) straffeforfølgning og 5) kompetanseheving. To utfordringer er felles for alle strategiene, nemlig 1) ivaretakelse av personvern, rettssikkerhet og menneskerettigheter og 2) behovet for internasjonalt samarbeid. Strategier for disse to utfordringene er innarbeidet i hovedstrategiene.

Hovedstrategiene formuleres og behandles i separate kapitler (kapittel 7–11) med eksempler på tiltak inntatt på slutten av hvert kapittel.

I sammendragene av hovedstrategiene i det følgende sammenfattes først begrunnelsen for strategien. Så siteres hovedstrategien i sin helhet etterfulgt av et utvalg av de 55 foreslåtte tiltakene, kalt nøkkeltiltak. Dette er tiltak som strategigruppen mener er sentrale for gjennomføringen av strategien. De øvrige eksempeltiltakene vil bidra til å realisere hovedstrategiene på kort sikt. De er kalt eksempeltiltak fordi de ikke er ment å være uttømmende. Hovedstrategiene skal være overordnede og gi grunnlag for å utvikle stadig nye tiltak for å realisere visjonen.

1.6. Strategi for deteksjon og analyse

Den første hovedstrategien skal sikre oversikt over datakriminaliteten. God kunnskap om uønskede datahandlinger, trusselaktører og sårbarheter er en grunnpremiss for effektiv bekjempelse, enten det gjelder hva som bør være straffbart, relevante forebyggingstiltak, effektiv straffeforfølgning eller identifisering av forskningsbehov og videreutvikling av kompetanse hos sikkerhetsaktørene. Gode oversikter over datakriminaliteten eksisterer verken nasjonalt eller internasjonalt.

Personvernhensyn, rettssikkerhetshensyn og menneskerettigheter må ivaretas i all informasjonsbehandling – og som ledd i forslagene til tiltak under de øvrige hovedstrategiene.

Hovedstrategi for deteksjon og analyse. *Kapasiteten til å innhente data og analysere datakrimtrusselen må styrkes vesentlig, både nasjonalt og gjennom deltakelse i internasjonale satsinger for bekjempelse av datakriminalitet. Et nært samarbeid med forskere om utvikling av analysemetoder og analysekapasitet trengs. Politiet og PST må sikres et relevant og nødvendig informasjonsgrunnlag for planlegging av målrettet forebygging, avdekking og avverging av datakrimtrusler, samt for effektiv straffeforfølgning av begått datakriminalitet.*

Statistikk skal være et viktig instrument i planleggingen og ressursfordelingen. Ansvaret for en samlet og koordinert analyseinnsats bør ligge på sentralt nivå i politiet.

En effektiv og smidig informasjonsdeling mellom alle sikkerhetsaktørene er viktig. Det bør derfor etableres bedre/tettere partnerskap mellom politiet og offentlige og private virksomheter for å dele informasjon. Regelverket må ivareta det.

Konkrete trusler må så langt som mulig, avdekkes tidsnok til at de kan forebygges eller avverges. Alle viktige opplysningskilder må utnyttes. Etterretningsmål og -metoder må kontinuerlig oppdateres og utvikles i takt med trusselbildet. Bevis av verdi for en mulig etterforskning må sikres av preventive hensyn. Metodene må veies opp mot hensynet til individets rettsikkerhet, personvern og menneskerettigheter.

Systemene for tips og anmeldelse til politiet fra ofre og publikum må forenkles og bedres vesentlig. Ofrene må vite hvor de skal henvende seg for å få hjelp.

Til sammen foreslås tolv tiltak. Nøkkeltiltak er å

- øke politiets tilstedeværelse på Internett
- øke deltakelsen i relevante nasjonale og internasjonale fora for informasjonsdeling
- utarbeide en årlig nasjonal trusselvurdering
- legge til rette for utvidet lagring av eierskapet til IP-adresser, noe som også er viktig i etterforskning av datakriminalitet
- opprette et sentralt mottak for tips om og anmeldelser av datakriminalitet
- styrke kapasiteten for analyse av innhentet informasjon.

1.7. Strategi for kriminalisering

Den andre hovedstrategien gjelder hvordan uønskede datahandlinger skal kriminaliseres. Straffelovgivningen styrer kriminalitetsbekjempelsen. For det første angir den hvilke datahandlinger som anses som så samfunnsskadelige at de bør rammes av samfunnets strengeste reaksjonsform – straff. For det andre angir den hva slags straff som bør benyttes, og hvor streng den bør være. Bøter og frihetsstraff er de vanligste straffeformene.

Straffelovgivningen er derfor en sentral strategisk rammebetingelse når politiet og rettsvesenet skal bekjempe uønskede og samfunnsskadelige datahandlinger. Verken politiet, påtalemyndigheten eller domstolene har hjemmel til å bekjempe uønskede datahandlinger som ikke rammes av straffelovgivningen.

Politiet og påtalemyndigheten har ansvaret for å etterforske datakriminalitet. Måten handlingene er kriminalisert på, har innvirkning på hvor krevende det er å skaffe nødvendige bevis. Hvor streng straffen er, har betydning for hvor mye ressurser det er forsvarlig for politiet og påtalemyndigheten å bruke på etterforskning og iretteføring.

Etter strategigruppens syn er det et betydelig behov for å oppdatere den eksisterende straffelovgivningen mot datahandlinger i tråd med den teknologiske utviklingen. Straffebestemmelsene bør i langt større grad ta utgangspunkt i den virtuelle verdens egenart og avstå fra å forsøke å tilpasse eksisterende straffebestemmelser til datahandlinger. Særlig er det viktig å legge til rette for et effektivt internasjonalt samarbeid om straffeforfølgning av datakriminalitet.

Hovedstrategi for kriminalisering. *Straff skal brukes aktivt i utviklingen av normer mot uønsket og skadelig dataadferd i samfunnet. Sanksjonene må ligge på et nivå som gjør datakriminalitet ulønnsomt, og som forebygger at Norge blir en frihavn for internasjonal datakriminalitet.*

Norge trenger en straffelovgivning som oppdateres i takt med trusselen fra datakriminalitet, med anvendelige bevistemaer og avskrekkende strafferammer. Nye straffverdige datahandlinger bør kriminaliseres raskt og tydelig for å markere at de er uønskede, og for å sikre allmennprevensjonen.

Jurisdiksjonsreglene må legge til rette for effektiv straffeforfølgning uavhengig av landegrenser og for utstrakt internasjonalt samarbeid.

Til sammen foreslås sju tiltak. Nøkkeltiltak er å

- opprette et organ som løpende følger kriminalitetsutviklingen og tar initiativ til oppdatering av straffebestemmelsene
- vurdere strengere straffer
- gjennomgå reglene for den geografiske rekkevidden til bestemmelsene mot datakriminalitet og utvide denne vesentlig for å ramme den internasjonale datakriminaliteten bedre
- delta aktivt i arbeidet med å utvikle internasjonale regler mot datakriminalitet

1.8. Strategi for forebygging og avverging

Forebygging av kriminalitet er spesielt viktig i det digitale samfunn fordi antall ofre per gjerningsperson kan være svært høyt. De komplekse tekniske og juridiske problemstillingene som oppstår, kan noen ganger virke vanskelige å løse med tradisjonelle metoder. Forebygging av datakriminalitet må sees i et bredt perspektiv, og det fordrer et vidt spekter av metoder. Samarbeid mellom politiet og andre offentlige og private sikkerhetsaktører er sentralt og bør samordnes bedre.

Mye av ansvaret for forebyggingen må ligge lokalt hos virksomheter og privat, men også politiet har i dag et vidtrekkende ansvar for å forebygge og avverge datakriminalitet og kan bruke maktmidler både for å avverge og stanse lovbrudd. En rekke tilsyn og

kontrollorganer har avgrensede ansvarsområder knyttet til forebygging, avverging og krisehåndtering.

Forebygging kan skje gjennom en rekke ulike virkemidler som lovregulering med minimumskrav til informasjonssikkerhet, regulering av Internett-leverandørene, sårbarhetskartlegging, forbrukeres krav til informasjonssikkerhet, behov for bestillerkompetanse og sikker elektronisk identifisering (e-ID).

Straffeforfølgning vil i seg selv ha en forebyggende effekt, men for å være effektiv forutsettes det en god evne til å avdekke datakriminalitet. Aktuelle virkemidler er å forbedre politiets tilstedeværelse på Internett og samarbeid med andre virksomheter og interessegrupper. Mer omfattende datalagring vil ha en forebyggende effekt. Det er viktig å sikre digitale spor kontinuerlig, helst før datakriminaliteten finner sted.

Strategigruppen har vurdert det sektorovergripende forbyggende arbeidet, og spesielt mellom Forsvaret, NSM, PST og politiet. Utover tettere samarbeid anbefales ingen formelle endringer. Ansvarsprinsippene står seg også for det digitale samfunn.

Avverging og krisehåndtering henger sammen, og selv om krisehåndtering ikke er hovedmålet med denne rapporten, er det behov for å peke på noen problemstillinger: Datakriminalitet kan få store konsekvenser for samfunnet; millioner av mennesker kan få identiteten sin stjålet, digitale betalingsfunksjoner kan settes helt ut av spill, og manglende koordineringsevne kan sette produksjon og transport ut av funksjon.

Angrep som skader både den digitale og den fysiske verden, vil trolig øke som følge av økt kontakt mellom de to sfærene, og ansvaret for håndteringen av slike blandingskriser kan synes uklart. I det fremtidige arbeidet er det viktig å avklare begrepene knyttet til digitale kriser, revidere politiets beredskapssystem og fokusere mer på datakriminalitet ved nasjonale øvelser.

Hovedstrategi for forebygging og avverging. *Kriminalitetsforebyggende arbeid og avverging er de viktigste virkemidlene for å sikre at datakriminaliteten holdes lav. Sikkerhetsaktørene må arbeide for å øke evnen til selvbeskyttelse mot datakriminalitet i befolkningen og virksomhetene. Politiet må dele kunnskap med andre sikkerhetsaktører, potensielle ofre og publikum om pågående og forventede kriminelle aktiviteter og metoder for å avverge dem.*

Politiet må samarbeide med databransjen om strengere krav til regulering og tilsyn for å oppnå høyere innebygget sikkerhet i utvikling og leveranse av datatjenester, produkter og programvare. Minimumskrav og konsesjonskrav bør benyttes aktivt.

Politiet må styrke sin forebyggende virksomhet med tilstedeværelse og patruljering på Internett, og stadig utvikle metoder for å forebygge og avverge datakriminalitet. Politiets ansvar for krisehåndtering i det digitale rom må være like klart og bygge på de samme prinsippene som for den fysiske verden.

Til sammen foreslås tolv tiltak. Nøkkeltiltak er å

- gjennomføre et nasjonalt løft for å spre kunnskap om datakriminalitet og datasikkerhet, særlig til barn, ungdom og eldre
- skjerpe reguleringen av Internett-tilbydere
- stimulere forbruker-, bransje- og næringslivsorganisasjoner til å kreve et bedre sikkerhetsnivå
- på dataproduktene til produsenter og leverandører
- gjennomgå roller og ansvar ved håndtering av kriser som rammer både den digitale og den fysiske verden, og gjennomføre øvelser

1.9. Strategi for straffeforfølgning

Visjonen krever et effektivt vern mot datakriminalitet. En velfungerende straffeforfølgning er et vesentlig virkemiddel for å nå dette målet. Mens sikkerhetstiltak særlig kan avverge skadelige datahandlinger og bidra til å gjenopprette sikker tilstand, er straff et sentralt redskap for å hindre gjerningspersoner i gjentatte forsøk på å begå datakriminalitet, og for å innarbeide minimumskrav til akseptabel adferd for databruk i befolkningen.

Dagens straffeforfølgning oppfyller på langt nær visjonen, og det er behov for en langt bedre bekjempelse av datakriminalitet. Særlig politiets evne til å avdekke og etterforske denne typen kriminalitet må forbedres.

Datakriminalitet har noen særtrekk som skiller den fra annen kriminalitet:

- Den er sterkt teknologidrevet.
- Datamengden og sakskompleksiteten er gjennomgående svært høy.
- Tidsfaktoren er mer kritisk fordi de digitale sporene ofte har kortere levetid enn andre spor, anonymiseres, endres eller slettes oftere.
- Digitale spor kan være distribuert på en stor mengde e-kom- og tjenestetilbydere og private aktører som i liten grad ønsker eller kan gjøre kritiske, digitale bevis tilgjengelig for politiet – eller vet at de besitter slike.
- Datakriminaliteten er internasjonal. Det kan enkelt gjennomføres lovbrudd i Norge fra andre steder på jordkloden.
- Datakriminaliteten er dynamisk. Dagens trussel- og risikobilde viser at datakriminaliteten er sterkt økende både i omfang og kompleksitet. Økningen vil høyst sannsynlig fortsette. Bildet vil også endre seg ved at gjerningspersoner tar i bruk nye metoder. Parallelt vil eksisterende metoder miste effekt og benyttes mindre på grunn av beskyttelses- og bekjempelsestiltak.
- Datakriminaliteten dekker spesielle og nye kunnskapsområder der tverrfaglig tilnærming er viktig.
- Det kreves mer spesialistkompetanse i politiarbeid på nett og i bruk av digitale spor og bedre tilgang på teknologikompetanse i datatekniske undersøkelser og analyse.

Politiets kapasitet til å analysere store og komplekse datamengder er begrenset, og politiet er lite til stede i det digitale samfunn. Mesteparten av den lokale kapasiteten brukes for å sikre elektroniske spor for andre typer kriminalitet enn datakriminalitet, blant annet grunnet høyere strafferammer. Påtalemyndigheten har få saker knyttet til datakriminalitet. Dommere har også begrenset kjennskap til datateknologi.

Ofte er det behov for tvangsmidler for å innhente digitale bevis. Både kommunikasjonskontroll og dataavlesing vurderes. Det er viktig at politiet er i stand til å identifisere dem som skjuler seg bak IP-adresser, publiseringer og ytringer på Internett, og metodebruken bør standardiseres. IP-logger er nå underlagt et sletteregime på 21 dager og begrenser dermed sporingsmulighetene for politiet merkbart.

Organisering er viktig for en god balanse mellom lokal og sentral forfølgelse av datakriminalitet. Organiseringen av politiet er i støpeskjeen med en kraftig reduksjon av antall politidistrikter. Dagens modell med 27 desentraliserte fagmiljøer på området er lite gunstig for datakriminaliteten, og det er et stort behov for samarbeid på tvers av distriktsgrenser og med andre sikkerhetsaktører. Det er mange argumenter for en større grad av sentralisering på området.

Internasjonalt pekes det på tungrodde prosesser for utlevering av digitale bevis, noe som stadig blir viktigere ettersom mer data blir lagret i utenlandske skytjenester. Norge bør gå foran som et godt eksempel gjennom å tilrettelegge for at andre land effektivt kan innhente digitale bevis fra oss.

Hovedstrategi for straffeforfølgning. *Datakriminelles risiko for å bli oppdaget, straffeforfulgt og domfelt skal være høy. Norge bør være en pådriver i den internasjonale bekjempelsen av alvorlig datakriminalitet.*

Rettsvesenets evne til å forfølge denne typen kriminalitet må styrkes vesentlig og henleggelsesfrekvensen reduseres tilsvarende slik at tilliten fra publikum og ofre blir større.

Politiet trenger et vesentlig løft for å ha kapasitet, kompetanse og evne til å fange opp og etterforske datakriminalitet. Kapasiteten og metodene må kontinuerlig tilpasses nye former for lovbrudd og endret teknologibruk i samfunnet. Politi, påtalemyndighet og domstoler må også ha nødvendig kunnskap og erfaring for å vurdere, iretteføre og pådømme datakrimsaker.

Samarbeidet med andre sikkerhetsaktører må bedres. Spesielt må hindringer for et smidig og effektivt internasjonalt etterforskningssamarbeid fjernes.

Til sammen foreslås 16 tiltak. Nøkkeltiltak er å

- etablere et nasjonalt datakrimsenter som tillegges viktige oppgaver innen kompetanseutvikling og etterforskning av krevende former for datakriminalitet
- utrede skjulte etterforskningsmetoder

- sørge for en fleksibel arbeidsdeling mellom sentralt og lokalt nivå, med vekt på rask kompetanse- og kapasitetsøkning
- koble inn politiet raskere ved sikkerhetshendelser som håndteres av andre sikkerhetsaktører, for å sikre en kompetent vurdering av etterforskningsspørsmålet før bevis går tapt
- etablere permanent tilstedeværelse i viktige internasjonale samarbeidsorganer for bekjempelse av datakriminalitet
- effektivisere behandlingen av rettsanmodninger

1.10. Strategi for kompetanseheving

Det er behov for en betydelig og mer langsiktig satsing og bygging av større fagmiljøer som kan ta for seg temaer som er viktige for sikkerhetsaktørene. Det trengs insentiver som gir informasjonssikkerhet, datakriminalitet og digital adferd vesentlig større forskningsmessig oppmerksomhet enn i dag.

Justis-, sikkerhets- og beredskapssektoren bør i større grad sette langsiktige mål, forebygge hendelser og være godt forberedt til å ta i bruk nye metoder og teknikker etter hvert som de utvikles. Her trengs det en større nasjonal forskningsinnsats som forener både offentlig og privat tverrfaglig forskning. Forskningen må ha praktisk nytteverdi for politiet og andre sikkerhetsaktører. Tverrfaglige forskningsmiljøer vil kunne bidra til å gjøre dem mer attraktive som samarbeidspartnere internasjonalt.

Justis- og beredskapsdepartementet bør utforme en egen FoU-strategi som tar for seg sektorens langsiktige og kortsiktige behov.

Politiet trenger bedre basiskompetanse og spesialkompetanse innen digitalt politiarbeid. I tillegg er det behov for etterutdanning av påtalemyndigheten. På kort sikt har politiet et stort kunnskapsgap. Dette behovet bør dekkes både ved etterutdanning og ved å ansette sivil, teknisk kompetanse. Det er viktig at sivilt personell gis nødvendig politifaglig og juridisk kompetanse som kan gi grunnlag for politimyndighet.

Hovedstrategi for kompetanseheving. *Sikkerhetsaktørene må samlet ha tilstrekkelige teknologiske, juridiske, politifaglige og samfunnsvitenskapelige kunnskaper til å kunne bekjempe datakriminaliteten effektivt. For å oppnå dette trengs det en vesentlig oppgradering av forskning og utdanning og en systematisk opplæring på arbeidsplassen i kombinasjon med en løpende videreutvikling av kunnskapsbasen.*

Forskningen bør blant annet omfatte temaer som kriminalanalyse, forebygging, etterforskning, digitale kriser og personvern. Den bør også undersøke de store mørketallene for datakriminalitet.

Norge må delta aktivt i den internasjonale kunnskapsutviklingen og erfaringsutvekslingen. Ny kunnskap og nye erfaringer fra de beste kompetansemiljøene nasjonalt og internasjonalt må spres raskt til alle som deltar i bekjempelsen av datakriminalitet. Politiet må løpende vurdere sine forskningsbehov og formidle dem til forskningsinstitusjonene.

Utdanningen må gi nødvendig basiskompetanse til alle som deltar i bekjempelse av datakriminalitet. Den må også gi tilstrekkelig spesialkompetanse til å håndtere den mest komplekse datakriminaliteten. Sikkerhetsaktørene bør legge til rette for felles utdanning og kompetanseutveksling.

Politiet må også i større grad benytte seg av sivil utdanningskapasitet og rekruttere sivil kompetanse. Det må være enhetlige og tydelige kompetansekrav for oppgaveutføring i bekjempelsen av datakriminalitet.

Til sammen foreslås åtte tiltak. Nøkkeltiltak er å

- opprette en langsiktig FoU-strategi for viktige temaer innen bekjempelse av datakriminalitet
- innføre nasjonale kompetansekrav for digitalt politiarbeid i overensstemmelse med internasjonale krav
- rekruttere teknologer med høy datakompetanse og tilby dem nødvendig etterutdanning i politifag
- legge til rette for påbygning til master- og doktorgrad for politistudenter og politiansatte på kunnskapsområder av betydning for datakriminalitet

1.11. Hovedkonklusjoner

I et kort sluttkapittel oppsummeres strategiens svar på spørsmålene mandatet stiller om trusselbildet, og hvor godt dagens sikkerhetsaktører er rustet til

å møte truslene vi står ovenfor. Trusselen er betydelig, og trolig økende, og forbedringspotensialet for sikkerhetsaktørene stort. Til slutt oppsummeres strategigruppens viktigste forslag for å møte denne utfordringen.

2. Oppdraget

2.1. Strategigruppen og mandatet

Justis- og beredskapsdepartementet (JD) ba i 2013 Politidirektoratet (POD) om å utarbeide «en overordnet nasjonal strategi for å bekjempe og håndtere IKT-kriminalitet».[2]

JD viste til den nasjonale strategien for informasjonssikkerhet fra desember 2012, der en av de sju strategiske prioriteringene var å «sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet». JD har sagt at det foreliggende strategidokumentet vil legge rammene for det videre arbeidet med å bekjempe datakriminalitet.[3]

Mandatet har vært gjenstand for flere endringer. Gjeldende versjon er fra 28. juli 2014 og lyder slik:

Justis- og beredskapsdepartementet har besluttet at det skal utarbeides en overordnet Nasjonal strategi for å forebygge og bekjempe IKT-kriminalitet.

Med IKT-kriminalitet forstås kriminalitet som enten er rettet mot datasystemer og/eller datanettverk, eller der sentrale elementer av handlingsforløpet begås ved hjelp av datautstyr og/eller datanettverk. Definisjonen sammenfaller med Europarådets «Convention on Cyber Crime» (Budapestkonvensjonen) og den norske rapporten i Politidirektoratets rapport «Politiet i det digitale samfunnet». Det kan også vises til Nasjonal strategi for informasjonssikkerhet (Justis-, Forsvars-, Samferdsels- og Fornyings-, administrasjons- og kirkedepartementet desember 2012) der en strategisk prioritering er å sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet.

Departementet har besluttet at det skal nedsettes en bredt sammensatt arbeidsgruppe. Arbeidsgruppens rapport skal:

1. *Beskrive hvilken trussel og risiko IKT-kriminalitet utgjør i vårt land.*
2. *Redegjøre for hvilke etater som har ansvar for bekjempelse av IKT-krim, og hvilken myndighet og ressurser disse har. Vurdere i hvilken grad disse etatene oppfyller sitt ansvar, om de har tilstrekkelig ressurser, og hvordan de samarbeider.*
3. *Vurdere en nasjonal strategi for å forebygge og bekjempe IKT-kriminalitet med utgangspunkt i trussel- og risikobildet under punkt 1.*
4. *Vurdere om ansvar, roller og samarbeid på feltet er hensiktsmessig i dag og ved behov foreslå endringer.*

Arbeidsgruppen skal i sitt arbeid legge vekt på optimal bruk av de eksisterende ressurser, legge opp til samhandling og ta hensyn til personvern. Strategien skal omfatte både forebyggende og reaktive tiltak.

Arbeidsgruppen fikk opprinnelig det forholdsvis tunge navnet *Arbeidsgruppen til å utarbeide utkast til en overordnet nasjonal strategi for bekjempelse av IKT-kriminalitet*, men vedtok å heller benytte navnet *Strategigruppen for bekjempelse av datakriminalitet*. I resten av dokumentet vil vi benytte kortformen *strategigruppen*.

2.2. Hva er datakriminalitet?

2.2.1. Definisjonen av datakriminalitet

Begrepsapparatet rundt datakriminalitet er omfattende og komplekst, og det finnes ingen entydig og omforent definisjon av datakriminalitet internasjonalt. Andre begreper som brukes mer eller mindre synonymt med 'datakriminalitet', er 'IKT-kriminalitet', 'digital kriminalitet' og 'Internett-relatert kriminalitet'.

I mandatet brukes 'IKT-kriminalitet'. IKT er en forkortelse for 'informasjons- og kommunikasjonsteknologi' og omfatter teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon. I denne rapporten har vi konsekvent benyttet begrepet 'datakriminalitet', som trolig er det uttrykket som er lettest å forstå. Man vil likevel støte på de foregående begrepene der teksten er direkte sitater fra andre kilder.

I Stortingsmelding 7 (2010–2011) *Kampen mot organisert kriminalitet* er definisjonen av datakriminalitet todelt. Den første delen omfatter

2 Brev av 1. november 2013 fra JD til POD.
3 Skriv av 2. juni 2014 fra JD.

kriminalitet rettet mot datasystemer og den andre bruk av data eller datasystemer som redskap for å gjennomføre annen kriminalitet hvor disse er en vesentlig del av en kriminell handling.

Den første delen av definisjonen omfatter altså straffbare handlinger som har datasystemer som objekt. Gjerningspersonen har som mål å påvirke selve datasystemene på en eller annen måte, for eksempel ved å skaffe seg kontroll over dem, skade eller forandre dem eller bruke dem på andre måter enn rådighetshaveren ønsker.

Den andre delen omfatter straffbare handlinger hvor data eller datasystemer brukes som redskap eller verktøy for straffbare handlinger rettet mot andre goder enn datasystemer. Et eksempel er når en gjerningsperson skaffer seg tilgangsdata for å tappe en annen persons bankkonto for penger.

Det er imidlertid ingen klar grense mellom de to delene av definisjonen. Gjerningspersonen kan for eksempel endre et datasystem for å gjennomføre et databedrageri.

Kravet i definisjonen om at databruken skal være 'vesentlig', utelukker forhold der data eller datasystemer benyttes og avgir elektroniske spor under gjennomføring av ulike typer tradisjonell kriminalitet. Slike spor er viktige for å kunne forebygge, avdekke og bekjempe nær sagt alle former for kriminalitet.[4]

Det må brukes skjønn for å avgjøre hva som skal regnes som vesentlig bruk. Det er ikke nok at data og datasystemer har vært brukt og elektroniske spor avgitt i forbindelse med den straffbare handlingen; de må ha vært hovedredskapet. Mobildata kan for eksempel gi viktig informasjon om hvor en siktet befant seg under et ran, men ranet blir ikke datakriminalitet av den grunn.

Det skilles mellom de to formene for datakriminalitet også i mandatet. Her står det også at mandatets definisjon sammenfaller med Budapestkonvensjonen, der artikkel 2–10 omhandler en rekke datahandlinger som anses for å være straffverdige, og som statene forplikter seg til å kriminalisere.

Eksempler på straffbare handlinger som retter seg mot datasystemer, er å ulovlig avlytte, forstyrre, skaffe seg tilgang til eller modifisere informasjon på data- og kommunikasjonssystemer.

Eksempler på straffbare handlinger som benytter data eller datasystemer som et vesentlig redskap, er digital forfalskning og bedrageri, distribusjon av overgrepsmateriale og misbruk av opphavsretten. Kapittel 3 inneholder mer detaljerte beskrivelser av viktige former for datakriminalitet.

I utgangspunktet er altså den generelle definisjonen i mandatet meget vid, med stor variasjon i handlingstyper. Den fremstår som videre enn definisjonen i Budapestkonvensjonen, selv om handlingsbeskrivelsene i denne også er generelle og komplekse.

2.2.2. Avgrensning av oppdraget

Den vide definisjonen innebærer at rammene for strategigruppens utredning også kan bli svært vide, så det må prioriteres. Når det gjelder datakriminalitet hvor data og datasystemer brukes som redskap for å utføre en straffbar handling, må hva som er vesentlig, bero på gjerningsbeskrivelsen i det enkelte straffebudet og hvor viktig bruken av datasystemer er i den aktuelle handlingen. Siden formålet med utredningen er å foreslå en overordnet nasjonal strategi, er det ikke nødvendig med noen nærmere utdyping av skillet mellom vesentlig og mindre vesentlig bruk av data. Utredningen fokuserer på de viktigste formene for datakriminalitet.

Også elektroniske spor inkluderes gjerne i strategier mot datakriminalitet. Her dreier det seg dels om å bruke dataverktøy til å skaffe bevis og dels om å samle inn og analysere elektroniske data som kan kaste lys over forbrytelsen, uavhengig av om den straffbare handlingen som etterforskes, er rettet mot datasystemer eller er utført ved hjelp av dataverktøy.

Elektroniske spor i saker som ikke gjelder datakriminalitet, faller utenfor strategigruppens mandat og blir derfor ikke behandlet i sin fulle bredde. Strategien omhandler imidlertid dataverktøy som brukes til å etterforske datakriminalitet slik mandatet avgrenser begrepet. Mange av synspunktene her er også relevante for etterforskning av tradisjonell kriminalitet.

Denne prioriteringen betyr at elektroniske spor ikke er et eget tema i utredningen, men de nevnes når de er relevante for strategiene for bekjempelse av datakriminalitet. Mye av det som sies om elektroniske

4 *Justis- og beredskapsdepartementet, NOU 2007: 2 Lovtiltak mot datakriminalitet – Delutredning II,* pkt. 3.5, s. 30.

spor, kan også være relevant for andre former for kriminalitet.

2.3. Strategigruppens forståelse av mandatet

Strategigruppen ble bedt om å levere et forslag til en overordnet nasjonal strategi for bekjempelse av datakriminalitet.[5]

Med 'bekjempelse' forstår gruppen organiserte tiltak som kan redusere datakriminaliteten. Tilnærmingen skal være bred og omfatter ikke bare vanlig straffeforfølgning, men også tiltak som kan avdekke, forebygge og avverge datakriminalitet. Analysen av tiltak skal ikke begrenses til det politiet, påtalemyndigheten og domstolene kan bidra med, men skal trekke inn alle aktører som kan yte et betydelig bidrag.

Med 'strategi' forstår gruppen en langsiktig og omfattende plan som i vårt tilfelle skal sikre en god bekjempelse av datakriminalitet. En strategi bør ha et hovedmål eller en visjon om et resultat som skal virke retningsgivende på utformingen av enkeltaktivitetene, vurderingen av dagens virksomhet og ressursstyringen. Den skal sikre at pågående og nye aktiviteter er koordinerte og målrettede.

At strategien skal være 'nasjonal', betyr at det ikke inngår i gruppens oppdrag å utvikle mer desentraliserte strategier, for eksempel for det enkelte politidistrikt. Strategier for internasjonale tiltak er imidlertid en viktig del av utredningen, siden datakriminaliteten er internasjonal og må kunne slås ned på uavhengig av landegrenser.

At strategien skal være 'overordnet', innebærer dels at den bør være langsiktig. Når det gjelder datakriminalitet, innebærer dette noen særegne utfordringer, siden trusselbildet endrer seg raskt i takt med den teknologiske utviklingen. Strategien bør derfor søke å identifisere langsiktige trender i kriminalitetsutviklingen, gjerne i et fem- til tiårsperspektiv, og ellers foreslå mekanismer for hyppige oppdateringer av strategien.

Utfordringene bør også ses i et utviklingsperspektiv. Strategien bør inneholde tiltak for å sikre en god organisasjonsutvikling og en tilfredsstillende kompetanseoppbygning på sikt.

Strategien vil ikke gå i detalj og inneholder ikke noen uttømmende tiltaksliste. Derimot kan den brukes som et redskap for å utvikle stadig nye, konkrete tiltak for å realisere strategiens visjon eller hovedmål.

At strategien skal være overordnet, innebærer også at tilnærmingen bør være bred. Strategien bør gi en samlet plan for å bekjempe datakriminalitet i Norge. Den bør ikke bare omfatte straffesystemets rolle, men også andre sikkerhetsaktører som har eller bør ha oppgaver som har betydning for bekjempelsen av datakriminalitet.

Mandatet ber om en redegjørelse for trusselbildet når det gjelder datakriminalitet, og for hvordan apparatet for bekjempelse av datakriminalitet fungerer.

I denne rapporten benyttes utrykket 'trusselaktør' om personer, organisasjoner og stater som står bak datatrusler, mens 'sikkerhetsaktør' brukes om aktører som har til oppgave å motvirke datatrusler.

De ulike sikkerhetsaktørene tilnærmer seg bekjempelse av datakriminalitet på forskjellige måter. Noen er hendelsesorienterte og har som hovedmål å motvirke uønskede datahendelser og reparere skader etter dem uansett om de rammes av straffelovgivningen eller ikke, mens de som hører til straffesystemet, har som sin hovedoppgave å bekjempe kriminalitet gjennom å straffe utøvere av datalovbrudd. Selv om de ulike sikkerhetsaktørene har forskjellige hovedoppgaver, er det et betydelig interessefellesskap mellom dem, noe som har betydning for samarbeidsmulighetene. Dette vil bli grundig analysert senere i rapporten.

Det er en nær sammenheng mellom trussel- og risikovurdering og sårbarhetskartlegging. Mens 'trusler' gjelder trusselaktørenes kapasitet og motivasjon, beskriver 'sårbarheten' datasystemenes motstandsdyktighet mot trusler. Sårbarheten avhenger derfor ikke bare av truslenes karakter, men også av hvor effektivt sikkerhetsaktørene arbeider. Siden bekjempelsen av datakriminalitet omfatter både trusler og sårbarheter, er det ikke behov for noen omfattende analyse av forskjellen mellom disse begrepene i denne rapporten. Stort sett brukes uttrykket 'trussel'. Det vil normalt fremgå av sammenhengen om sårbarheter er inkludert.

5 Se mandatet i punkt 2.1.

Et hovedtrekk ved datakriminaliteten er at den er 'dynamisk'. Den forandrer seg stadig, og dermed må også strategiene for å bekjempe den være dynamiske. De må være i stand til å fange opp endringer og nye trender i trusselbildet og tilpasse bekjempelsen deretter. Strategien bør derfor være fleksibel.

2.4. Forholdet til Digitalt sårbarhetsutvalg (Sårbarhetsutvalget)

Den 20. juni 2014 oppnevnte regjeringen et utvalg for å kartlegge digitale sårbarheter (Sårbarhetsutvalget), i hovedsak som følge av den samme digitale utviklingen som førte til nedsettelsen av strategigruppen. Mandatene til de to utvalgene overlapper i stor grad, men Sårbarhetsutvalgets mandat er videre. Mens strategigruppens hovedfokus ligger på datakriminalitet, skal Sårbarhetsutvalget kartlegge alle viktige former for digital sårbarhet. Typisk vil rene digitale uhell falle utenfor det strafferettslige området, men innenfor en sårbarhetsanalyse.

Likevel vil de fleste av de uønskede hendelsene nevnt i Sårbarhetsutvalgets mandat kunne rammes av straffebestemmelser og således også være relevante for strategigruppen. De to utvalgene vil trolig i stor grad ha de samme utfordringene når det gjelder kriminalisering, straffeforfølgning, personvern, rettssikkerhet og samfunnssikkerhet. Begge mandatene ber om at det redegjøres for hvilke etater som har ansvar for å motvirke uønskede datahendelser, i hvilken grad disse etatene oppfyller sitt ansvar, om de har tilstrekkelig med ressurser, og om de samarbeider på en hensiktsmessig måte. Begge utvalgene skal foreslå endringer og tiltak når det gjelder kompetanse, teknologi og organisasjon.

Strategigruppens hovedfokus på kriminalitetsbekjempelse innebærer også noen forskjeller i forhold til Sårbarhetsutvalget. Uønskede datahendelser kan både være villede og ikke-villede. Eksempler på sistnevnte er uhell og hendelser som skyldes naturkatastrofer. Kriminalitetsbekjempelse har fokus på villede hendelser som utnyttes til kriminalitet, og sentrale oppgaver er avverging, sikring av digitale spor, etterforskning og ved behov krisehåndtering. Beskyttelsestiltak mot uønskede datahendelser i forkant og skadeutbedring i etterkant vil normalt falle utenfor strategigruppens mandat. Utvalgene overlapper når det gjelder forebygging, oppdagelse og avverging av straffbare handlinger. Her vil det være en oppgave for strategigruppen å foreslå strategier for en god rollefordeling mellom politiet og andre aktører og for hvordan et samarbeid bør legges opp. Enkelt forklart vil strategigruppen fokusere på aktører som vil skade oss, mens Sårbarhetsutvalget fokuserer på svakheter i samfunnet vårt, uavhengig av måten skaden inntreffer på. Begge utvalgene bes om å beskrive dilemmaer der man må velge mellom å løse sikkerhetsutfordringer og ivareta personvernet.

Den betydelige overlappingen mellom de to utvalgene kunne tale for å samordne arbeidet deres i en samlet analyse under Sårbarhetsutvalget. Strategigruppens tidsramme talte imidlertid mot dette, så strategigruppen fortsatte i hovedsak sitt arbeid som planlagt, uten spesiell tilpasning til Sårbarhetsutvalget.

Etter et møte ble lederne av utvalgene enige om at begge utvalgene burde kunne arbeide fritt ut fra sine mandater. Denne ordningen ble akseptert av Politidirektoratet.

2.5. Strategien – premisser og oppbygging

2.5.1. Hva slags strategi?

En strategi er et handlingsprogram for å forbedre nåsituasjonen. En strategi består av to deler: en visjon og hovedstrategier. *Visjonen* er et mål som tiltakene skal realisere. Visjonen skal angi hovedmålet for strategien og angi hva slags tilstand som ønskes oppnådd, i dette tilfellet når det gjelder datakriminalitet og reparasjon av skadene den medfører. Poenget er å peke ut hovedretningen for bekjempelse av datakriminalitet, angi de viktigste utfordringene og hvordan de kan løses, og spesifisere hvilke aktører som bør være sentrale i arbeidet.

Visjonen, den faktiske datakriminaliteten og den eksisterende kapasiteten til sikkerhetsaktørene vil bestemme hva slags *hovedstrategier* som trengs, og hvor krevende det vil være å gjennomføre dem.
Noen strategiplaner tar sikte på å samle *alle* aktiviteter som er nødvendige for å realisere planens visjon, både de som allerede pågår, og nye aktiviteter, mens andre først og fremst fokuserer på *nye* aktiviteter. Dette er den valgte metodikken, og det er da underforstått at aktiviteter som ikke uttrykkelig er foreslått opphevet, skal fortsette.

Strategigruppen foreslår et sett med hovedstrategier som samlet er ment å dekke alle viktige sider av en effektiv bekjempelse av datakriminalitet. Disse er først og fremst arbeidsprinsipper som må fylles ut med konkrete tiltak. Strategien inneholder også en del konkrete eksempler på slike tiltak basert på dagens situasjon, for å illustrere hva hovedstrategiene vil innebære. Hovedstrategiene skal i tillegg gi grunnlag for løpende å utvikle nye delstrategier så lenge den nasjonale strategien anses som politisk og administrativt relevant.

Strategien skal imidlertid være overordnet, så den kan ikke være for detaljert.

Det varierer hvor mye strategigruppen har arbeidet med de ulike eksemplene på tiltak. Noen er forholdsvis gjennomarbeidet, mens andre først og fremst identifiserer videre arbeidsoppgaver.

2.5.2. Oppbygging av rapporten

Denne rapporten er i tillegg til innledningen i del 1 delt i to hoveddeler.

Del 2 omhandler i hovedsak nåsituasjonen. Kapittel 3 tar for seg trusselen fra datakriminaliteten.

Analysen beskriver ikke bare dagens situasjon. Siden trusselen fra datakriminaliteten er dynamisk, prøver analysen også å peke på utviklingstrender som er relevante for en overordnet nasjonal strategi. Kapittel 4 tar for seg det eksisterende apparatet for bekjempelse av datakriminalitet.

Analysen i del 2 inneholder det empiriske utgangspunktet for strategidrøftelsene i del 3, som er rapportens hoveddel. Her behandles gruppens strategianalyser og strategiforslag.

Del 3 inneholder strategiforslagene. Strategigruppen har spurt de sentrale sikkerhetsaktørene om hva de mener om behovet for reformer og hvilke samarbeidsutfordringer som følger med håndteringen av datakriminalitet. De sentrale synspunktene sammenfattes i kapittel 5. Dette kapittelet omhandler også noen norske dokumenter som gir et grunnlag og et utgangspunkt for datakrimstrategien. Det gis også en oppsummering av noen strategier utarbeidet av internasjonale organisasjoner og andre stater som har særlig relevans for den nasjonale strategien.

Kapittel 6 tar for seg visjonen. Deretter beskriver kapittel 7–11 fem hovedstrategier som til sammen dekker de viktigste aspektene av visjonen.

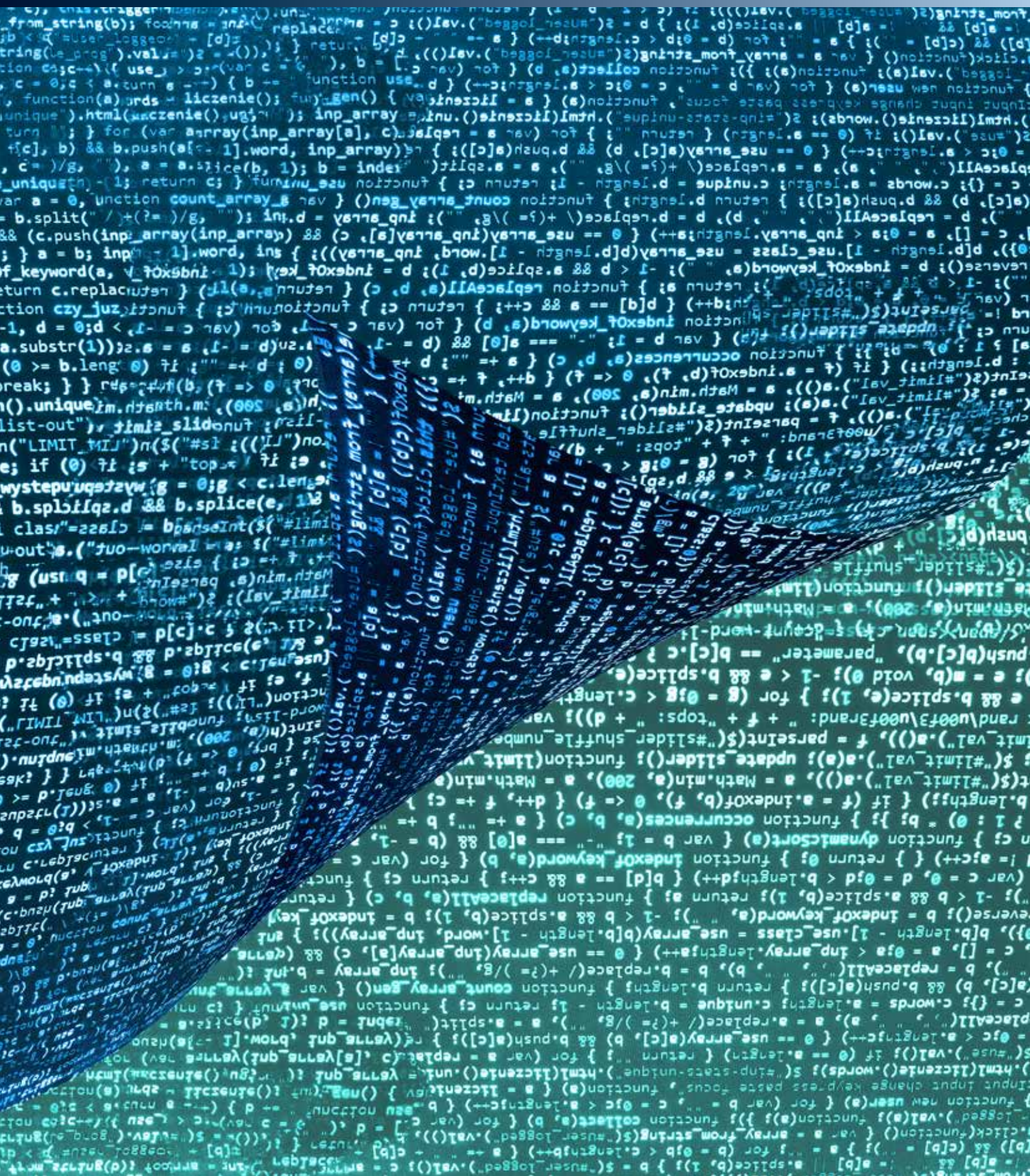
Strategigruppen har valgt å gi en forholdsvis omfattende begrunnelse for strategiforslagene. Den har sett det som viktig å tydeliggjøre tenkningen bak forslagene – også for å gi et grunnlag for å utvikle fremtidige tiltak for å realisere strategiene.

Visjonen, hovedstrategiene og eksempler på tiltak ble grundig gjennomgått av styringsgruppen[6] på et seminar i Oslo 5. og 6. februar 2015. Begrunnelsene ble derimot ikke behandlet. Styringsgruppas gjennomgang kan derfor ikke uten videre oppfattes som en tilslutning til disse.

6 Medlemmene i styringsgruppen er listet opp i vedlegg 1.

Del 2

Utviklingstrekk ved det digitale samfunn og datakriminalitet samt dagens bekjempelse



3. Databruk, datakriminalitet og trusselbilde

3.1. Innledning om trusler og risiko

En nasjonal strategi skal være basert på en bred forståelse av den risiko datakriminalitet representerer, og mandatet ber om en beskrivelse av hvilken trussel og risiko datakriminalitet utgjør i vårt land. I avanserte analyser og vurderinger av risikoen for uønskede villede hendelser er 'trussel', 'sårbarhet' og 'verdier' tre begreper med forskjellig betydning. 'Risiko' er altså det overgripende begrepet. Men de er alle knyttet til verdier vi ønsker å verne, og målet er å anslå risikoen for uønskede handlinger. Fokuset på datakriminalitet begrenser uønskede handlinger til de kriminelle forsettlige og uaktsomme handlingene.[7]

- Stikkordet er dermed uønskede handlinger og underforstått aktørene som står bak, her kalt 'trusselaktører', i motsetning til sikkerhetsaktørene, som bekjemper datakriminalitet. Det er vanlig å beskrive både trusselaktørers evne og intensjon.
- 'Sårbarhet' defineres som «manglende evne til å motstå en uønsket hendelse eller å opprette en ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning». Med andre ord i hvilken grad det som skal beskyttes, blir påvirket, slik at den potensielle risikoen går over i en konkret skade.

Dette kan illustreres med et eksempel. En tenkt verdi kan være en database med sensitive forsvarshemmeligheter. En ren sårbarhet kan være at databasen ligger på en eldre server med en kjent programmeringsfeil. Et reduserende tiltak kan være å blokkere tilgang til denne serveren fra utsiden. Sårbarheten er dermed mindre, men fortsatt til stede. Uten trusselaktører vil sårbarheten få ligge i fred, men hvis en trusselaktør skulle dukke opp, kan den beskrives med både evne og intensjon. Vi kan tenke oss en trusselaktør i form av et organisert kriminelt miljø. Forsvarshemmelighetene kan være mye verd på det svarte markedet, men miljøet mangler nødvendige ressurser og evne til å utnytte sårbarheten. Tilsvarende kan det være trusselaktører i form av fremmed etterretning som både har motivasjon og ressurser til å plassere en spion på innsiden for å skaffe seg uautorisert tilgang til informasjonen, og som dermed omgår beskyttelsesmekanismen.

Som avgrenset mot Sårbarhetsutvalget i kapittel 2 er ikke hensikten her å beskrive samfunnets sårbarheter knyttet til datakriminalitet, men heller å beskrive trusselen: trusselaktører, deres metoder samt konsekvensene av deres handlinger (skadepotensialet).

Alle vurderinger av fremtidige trusler er usikre. Trusselen fra datakriminalitet er særlig usikker på grunn av den raske og høyst uforutsigbare teknologiske utviklingen. I tillegg har vi relativt kort erfaring med disse truslene, og tilpasning til en stadig endring er krevende når en rekke hensyn må ivaretas. Dette er utgangspunktet i den overordnede strategien.

Utgangspunktet for strategigruppen har vært den eksisterende strafferettslige spesifiseringen av datakriminalitet, som alt i dag er svært detaljert, og de trussel- og risikovurderinger som foreligger fra nasjonale myndigheter og andre. Slike trussel- og risikovurderinger gjøres med ulike grader av presisjon og grundighet og med ulike grader av generalisering eller spesifisering. Strategigruppen ser det ikke som hensiktsmessig å knytte trusselvurderinger eller strategiforslag til det enkelte straffebud, men har samlet datakriminaliteten i en rekke hovedtyper som er hensiktsmessige i en overordnet strategianalyse.

3.2. Det moderne digitale samfunn

Begrepene 'Internett' og 'det digitale samfunn' ('cyberspace') benyttes om hverandre. Internett er den globale infrastrukturen der de ulike teknologiske komponentene kommuniserer med hverandre. Det digitale samfunnet omfatter alle brukere, bruksområder, anvendelser, Internett og alt som benytter denne teknologiske infrastrukturen.

Det begynte på 70–80-tallet. Datamaskiner, datanettverk og telekommunikasjonssystemer ble koblet sammen til et verdensomfattende datanettverk. Først for forskningsformål, og i 1989 som kommersiell tjeneste med navnet 'Internett'. Dette betraktes som en

7 *Norsk standard NS 5830: 2012, Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi.*

av de viktigste teknologiske innovasjonene i det 20. århundre.

Utviklingen har vært enorm, og det har gått ca. 20 år siden den første grafiske nettleseren ble lansert. Det var noe helt nytt å få tilgang til informasjon fra et verdensomspennende nettverk og mulighet til å sende meldinger til venner og familie på andre kontinenter. Senere har vi kunnet laste ned musikk, betale regninger i nettbank, handle aksjer på nettet og utnytte rask distribusjon av informasjon. Vi får tilgang til offentlige og private elektroniske tjenester, produserer digital kunnskap og samvirker med andre internasjonalt.

Antallet brukere og aktiviteten på Internett har økt voldsomt.[8] I 1995 var det ca. 30 millioner brukere. Nå nærmer vi oss 3 milliarder brukere, og antallet vokser kraftig. Grove overslag viser at det i dag kan være ca. 20 milliarder dataenheter av ulike typer i verden, hvorav ca. 10 milliarder datamaskiner, 7 milliarder smarttelefoner og 3 milliarder andre enheter tilkoblet Internett. Det har vært en voldsom vekst fra ett nettsted i 1991 til ca. 200 millioner i 2010 og mer enn én milliard i 2014. Det er ca. 3,8 milliarder e-postkontoer, og det sendes ca. 300 milliarder e-postmeldinger hver dag. Sosiale medier som YouTube og Facebook har hver ca. én milliard brukere.

Det digitale samfunnet har blitt en enorm informasjonskilde med stor kapasitet til lagring og transport av digital informasjon. *Digital Britain Report* angir at ca. 500 milliarder gigabyte ble transportert over kloden i 2009. Ifølge Cisco (2013) prognoseres det at den årlige IP-trafikken vil passere ca. 1000 milliarder gigabyte i 2015. Google har i 2013 anslått at de lagrer informasjon tilsvarende 10 milliarder gigabyte på disk. University of Southern California angir i 2011 at totalt lagret digital informasjon i verden er på mer enn 300 milliarder gigabyte.

Digital teknologi og Internett bidrar stort sett til alt vi har og bruker i samfunnet, og teknologien fører til endringer som påvirker våre daglige liv. Den påvirker også driften til private og offentlige virksomheter. Nye teknologiske løsninger gir stadig muligheter til økonomisk vekst og velferd og endrer nesten alle områder av menneskelivet, også den menneskelige adferden. Hver gang kundene endrer adferd, legges det press på private og offentlige virksomheter om å endre produkter og tjenester. Våre liv er blitt åpne og tilgjengelige i digitale kanaler. Det gir samtidig teknologiavhengighet og sårbarhet – og dermed en høyere risiko for alvorlige uønskede hendelser og digital kriminalitet.

Kriminelle handlinger og andre uønskede hendelser rammer det digitale samfunnet og får konsekvenser i den fysiske verden. Det antas å være store mørketall for det faktiske omfanget av datakriminalitet. Mange alvorlige angrep blir aldri oppdaget, og mange saker meldes heller ikke av ulike årsaker. Dette bekreftes av Næringslivets Sikkerhetsråds mørketallsundersøkelse[9] for 2014.

En rapport fra juli 2013 skrevet av Center for Strategic and International studies i USA angir at den globale økonomien taper ca. 300–800 milliarder dollar (0,4–4 % av brutto nasjonalprodukt) hvert år på grunn av datakriminalitet. Justert for befolkningstall ville det for Norge tilsi at datakriminalitet i 2013 forårsaket et tap på minst tolv milliarder kroner.

En vesentlig egenskap ved det digitale samfunnet er at det ikke har landegrenser og er gjenstand for lite offentlig regulering; det er vanskelig å iverksette nasjonale styresett, og det mangler utøvelse av overnasjonal suverenitet. Det betyr at hvert land må ha egne regler og tiltak for å unngå at noen tar seg for mye til rette. I motsatt fall kan man ende opp med anarki og militarisering eller tilrettelegging for kriminalitet, terrorisme eller spionasje. Forskjellige organer i FN har forsøkt å lage felles regler for en global styring av Internett, men resultatene er dårlige. Flere land ønsker stor frihet på nettet, uten hensyn til landegrenser. Argumentet for det er de grunnleggende menneskerettighetene. Andre lands myndigheter ønsker å forby adferd som truer politisk stabilitet og offentlig orden, eller aktiviteter som kan oppfattes som straffbare. Noen land mener at hver nasjon må ha rett til å kontrollere hva slags innhold som sendes og oppbevares på Internett, og derved føre omfattende kontroll av brukerne og tjenestetilbudet i det digitale samfunnet.

8 Basert på tall fra World Wide Web Consortium, Cisco Internet Business Solutions Group og The Radicati Group, Inc.

9 http://www.nsr-org.no/moerketall/.

3.3. Utviklingstrender i det digitale samfunn

3.3.1. Teknologibruk i samfunnet

Teknologibruken i samfunnet øker kraftig, og det moderne samfunnet er avhengig av datateknologi for å fungere. Ifølge Europol har ca. 39 % av jordens befolkning nå tilgang på Internett.[10] Den europeiske tilgangen er ca. 70 %, mens den er godt over 90 % i de nordiske landene. Afrika og Midtøsten er på full fart opp, særlig grunnet billige nettbrett og smarttelefoner.

Bølgen av digitale endringer som er over oss akkurat nå, er en konsekvens av raske bredbåndsnett, nye avanserte mobile enheter, sosiale medier og utnyttelse av stordata og skytjenester.

Vi ønsker å være på nett og være mobile. Det betyr at vi kjøper smarttelefoner og nettbrett i større grad enn tradisjonelle PC-er. Sensorer og annen elektronikk blir stadig billigere og integreres i blant annet kjøretøy, håndvesker og klær med tilkobling til Internett. Flere hundre millioner nye mobile enheter blir utviklet og tilpasset våre behov som forbrukere. Tingenes Internett ('Internet of Things') utvides slik at nesten alle typer gjenstander kan kommunisere over Internett.

Den enorme bruken av digitale kommunikasjonskanaler endrer måten vi oppfører oss på, hva vi forventer, og hvordan vi tenker. Vi sitter på tog og buss og surfer på nettet eller utfører digitale arbeidsoppgaver. Vi sjekker priser på alternative produkter i butikkene. Kaffekoppen har vi på sofaen sammen med nettbrettet mens vi ser på TV og småprater med våre kjære. Vi har mindre behov for fysiske bankfilialer (eller minibanker) til å utføre de fleste av våre pengetransaksjoner – det gjør vi i nettbanken. Vi forventer at Internett skal fungere til enhver tid.

Noen forskere har pekt på at den menneskelige hjerne, også i voksen alder, stadig tilpasser seg læring og endring. Derfor argumenteres det for at Internett endrer vår måte å tenke på. Noen hevder at vi blir mer overfladiske og lettere distrahert. Andre peker på at vi er i stand til både å tilegne oss breddekunnskap og dykke dypt i informasjon samt behandle og analysere informasjon mye bedre enn før.

Dagens unge er den første generasjonen som har hatt tilgang til Internett i hele sitt liv. De forventer stadig nye digitale tjenester. Norge er blant de øverste på listen over land som benytter og har tilgang til elektroniske tjenester: 95 % av befolkningen i Norge har PC. 90 % av befolkningen oppgir at de bruker Internett månedlig. 83 % benytter Internett daglig. Internett har nå passert både avisene, radioen og fjernsynet som vårt viktigste massemedium, ifølge *Norsk Medie-barometer 2012* fra SSB. Internett er noe vi bruker *hele tiden*, særlig den yngre generasjonen. Vi *går* ikke på Internett, vi *er* på Internett; vi logger oss eventuelt av og på tjenester. Det er ikke bare nettsurfing som er Internett. Det inkluderer også strømming av musikk og video, sending av direktemeldinger og nettspill, bare for å nevne noe.

3.3.2. Viktige digitale trender

Mangfold av teknologi og nye bruksmønster. En smarttelefon er nå en avansert datamaskin med trådløs kommunikasjon og mange typer anvendelser. Der vi før hadde egne dingser for å fotografere, sjekke lokasjon, ringe og spille av musikk, har vi nå én enhet som gjør alt sammen.

TV-signaler ble opprinnelig kringkastet fra egne radiotårn. Nå kan vi se TV på mobilen via nett-TV eller strømme våre yndlingsserier og filmer via strømmingstjenester. Distribusjonsrettigheter for immateriell innholdsproduksjon blir i dag ivaretatt innenfor landegrensene. Når TV-kanaler og annen innholdsproduksjon spres på Internett, er det vanskelig å begrense distribusjonen innenfor en landegrense. Brukerne kan gjennom bruk av tjenester for videresending synliggjøre seg med IP-adresser i det landet de ønsker, og får dermed overført innholdet hvor enn de måtte oppholde seg.

Skrivere har frem til nå skrevet ut todimensjonalt. Nå utvikles både enkle og avanserte 3D-skrivere. De enkle kan i dag produsere deler av enkeltmaterialer som for eksempel plast. De mest avanserte brukes blant annet til å forske på produksjon av reserveorganer. Konseptet vil kanskje i fremtiden sette hvem som helst i stand til å fremstille hvilke gjenstander som helst, når som helst. Mange typer drapsredskaper kommer til å finnes på nettet i fremtiden. Skytevåpen skrevet ut på 3D-skriver kan allerede i dag avfyre

10 https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta.

flere skudd. Det kan blant annet vanskeliggjøre kontroll med produksjon og spredning av våpen over landegrensene.

Near Field Communication (NFC), altså kontaktløs nærkommunikasjon, vil bli tatt i bruk av flere store tjenestetilbydere i år. DNB og Telenor har allerede prosjekter på dette området, og mange nye smarttelefoner leveres i dag med innebygget NFC-chip. Når vi får elektronisk lommebok, og samtidig kan benytte telefonen til både å kjøpe billetter og registrere oss inn uten å slå på skjermen, åpner dette også for at dersom noen stjeler telefonen, kan de tilegne seg eierens identitet og verdier ved hjelp av ulike antenner og lesere. En ny form for skimming vil vokse frem. Telefonen vil inneholde så mye personsensitiv og verdifull informasjon at den vil bli viktigere enn lommeboka.

Den fysiske og digitale verden blir tettere sammenknyttet. Datateknologi kan overvåke og styre fysiske systemer og industrielle prosesser. Slike systemer går ofte under begrepet SCADA[11] og innebærer industrielle kontrollsystemer blant annet for kritisk infrastruktur som vann, kloakk, trafikk og strøm.

Tingenes Internett ('Internet of Things'). Vi ser også den samme trenden i forbrukermarkedet. Utbredelse av Internett-dekningen har gjort at vi i dag kan kommunisere nesten hvor som helst, når som helst. Det nye er nå å kunne utveksle informasjon med nærmest hvilket som helst objekt eller gjenstand. Denne trenden kalles 'Tingenes Internett'. Her utnyttes ny teknologi som kombinerer avansert mikroelektronikk med nye materialer. Det betyr at alle ting kan inneholde en databrikke med regnekapasitet, lagringsmedium og kommunikasjon. Informatikken vil bli en integrert del av stort sett alle fysiske gjenstander. Tingene vil for eksempel kunne kommunisere trådløst og angi en geografisk lokasjon.

Det tilbys allerede slike funksjoner i noen få produkter i dag, blant annet i husholdningsprodukter, armbånd og klær ('wearables'). Nye biler har gått fra å være fullmekaniske fremkomstmidler til datamaskinstyrte maskiner. Det omfatter radiostyrte sentrallåssystemer, digital kontroll av drivstofftilgang og, snart, selvkjørende biler. Dette innebærer også at styring på vei, hastighet og brems vil kunne foregå digitalt. Smarte hus styrer oppvarming, musikk og lys, og garasjeporten åpnes automatisk.

Kroppsnær teknologi gir bedre helseoppfølging. Biosensorer og informatikk vil prege fremtidens helseoppfølging og pasientbehandling. Antall eldre øker i samfunnet, livsstilsykdommer øker og behovet for helsetjenester endres med mer fokus på behandling utenfor institusjonene. I en slik utvikling vil kroppsnær teknologi med biosensorer kunne overvåke pasienten og styre medisininntak og hjertefunksjoner og ha datateknisk kontroll med vitale funksjoner i menneskekroppen. Den første fasen er her allerede, med håndlenker og dataenheter som opereres inn i kroppen og som kan styre hjerterytme, insulinnivå og annen type medisinering. Disse små databrikkene har en datamaskin med høy regnekapasitet og lokal lagring. I tillegg kan den kommunisere over Internett mot en større database og holde orden på alle helsekritiske styringsdata som aktivitets- og sovemønster, blodtrykk og mye annet som bare fantasien kan begrense. Denne teknologien vil kunne overvåke store deler av vår kropp, varsle, forutse og gi meldinger etter hvert som hendelser inntrer.

Stordata ('big data') og intelligent analyse. 'Stordata' er et begrep som brukes om innsamling av veldig store mengder digital informasjon. Det er vanskelig å lagre, søke i og overføre informasjonen raskt nok. Grunnet volumet må dataene behandles på nye måter for å finne ønsket verdi eller innhold. Det er mange grunner til denne økte mengden med data. Lagringsplass blir billigere, det utplasseres flere sensorer, og vi utfører stadig flere handlinger digitalt. Det ser vi gjennom blant annet økt tilgang på metadata som tidspunkt, lokasjon, kommunikasjonspartner, IP-adresser, ordredata m.m.

Nye metoder utvikles for å kunne trekke ut kunnskap fra datamengden, for eksempel for å kunne anbefale deg en ny film eller låt. Dette gjøres ved mønstergjenkjenning, maskinlæring / kunstig intelligens (slik som klassifisering, gruppering), statistisk modellering og regresjonsanalyse. Datamaskiner kan analysere og presentere store mengder informasjon

11 'Supervisory Control and Data Acquisition'.

langt raskere enn vår menneskelige hjerne er i stand til. Datamaskiner begynner også etter hvert å kunne etterligne visse typer menneskelig adferd og kan utnyttes for sofistikert sosial manipulasjon og potensielt selvstendige handlinger som er vanskelig å kontrollere for mennesker. Det kan kanskje i fremtiden medføre at en datamaskin utfører lovbrudd uten at et menneske direkte har instruert den.

Skylagring og prosessering. Tilbake i den digitale tidsalders spede begynnelse var lagring og prosessering svært dyrt, og det var derfor vanlig med «dumme» terminaler koblet til stormaskiner, enten lokalt eller over telefonlinje. Teknologien ble billigere, og det ble populært med selvstendige datamaskiner en stund inntil vi innså at det er nyttig å ha tilgang til dataene våre uavhengig av hvor vi er og hvilke enheter vi jobber på. Trenden nå er derfor å plassere dataene tilbake i sentrale lager 'i skyene'. Disse skyene er selvsagt bare store maskinparker strategisk plassert på Internett. I tillegg til sentral lagring vil vi i fremtiden trolig også se mer til sentral prosessering av data. Det er i dag flere modeller: leie av dedikert infrastruktur (IaaS), leie av plattform (PaaS) og leie av tjeneste (SaaS).

Maskinlesbar web kan gi raskere informasjonsoversikt. En ny generasjon web som tolker sammenhenger og innhold ('semantisk web'), er under utvikling. 'World Wide Web', slik vi kjenner den i dag, er designet for å være lesbar av mennesker. Plassering av elementer som tekst og bilder gjør det lett for mennesker å lese og navigere. I neste generasjon web ønsker man å utnytte maskinlesbare elementer, slik at kunstig intelligens i datamaskinagenter skal kunne bistå med å søke opp, ta avgjørelser og handle på vegne av individer eller grupper basert på deres preferanser.

Økt utnyttelse av anonymisering og kryptering. Teknologi for anonymisering, kryptering og fjerning av digitale spor blir lettere tilgjengelig og tas allment i bruk. Det betyr at det blir vanskelig, og som oftest umulig, å tolke lagrede data og data i bevegelse. Kryptering gjør at innholdet ikke kan leses av andre enn dem som har tilgang til krypteringsnøklene. Slik teknologi er med på å beskytte vårt personvern og beskytte oss mot kriminalitet. Samtidig reduserer den også myndighetenes tilgang til digitale spor for å bekjempe lovbrudd.

3.3.3. Internett for organisert kriminalitet

Internett-basert kriminell tjenestearkitektur ('Crime-as-a-Service'[12]). Dagens datakriminalitet har i stor grad økonomisk vinning som motiv, og vinningsmotivet har utviklet seg sterkt gjennom utbredelse av Internett. Teknologien har gjort det enkelt å skaffe seg gode verktøy, få andre til å utføre deler av den kriminelle handlingen og skjule sine spor.

Internett brukes i økende grad i forbindelse med ran, narkotikahandel, våpensmugling, menneskesmugling mv. Politiet vil streve med å få innsyn i disse miljøene. Kjennetegnene på de avanserte kriminelle miljøene er at de er internasjonale, har mye ressurser og bruker den nyeste teknologien. Et marked for internasjonal kriminalitet vokser frem, med muligheter for hurtig kommunikasjon, skjermet for innsyn, uavhengig av landegrenser.

Utviklingen av datavirus og annen ondsinnet programvare domineres ikke lenger av ungdom som søker berømmelse og ære blant sine jevnaldrende. De fleste av dem er utviklet av profesjonelle kriminelle, som tjener millioner på nye måter å utføre datakriminalitet på.

Dette konseptet er basert på bakmenn med skjulte nettverk, en forretningsmodell som drives av svart økonomi med et bredt spekter av «kommersielle» tjenester som innbefatter alle typer datakriminalitet. Det kriminelle nettverket skaffer seg ekspertise som leies ut, og skreddersyr botnett, DDoS-angrep, skadevare, datatyveri, passordknekking m.m., eller bruker det til egne kriminelle handlinger. Man kan kjøpe skadevare, infrastruktur, stjålne data samt oversetter- og hvitvaskingstjenester. Kjøp og salg av disse tjenestene er organisert på samme måte som legitime tjenester ved oppbygging av renommé gjennom tilbakemeldinger.

De forskjellige stegene i nettkriminaliteten fordeles mellom aktører med hver sine spesialiseringer. Denne arbeidsfordelingen er basert på løse bekjentskap, i motsetning til hierarkiske organisasjoner som er vanlig i tradisjonell kriminalitet. Koordineringen

12 Ordspill med uttrykket 'as a service', http://en.wikipedia.org/wiki/Cloud_computing.

deres foregår via skjulte og separate nettverk, fora og markedsplasser. Anonymitetsteknologi gjør det vanskelig å kartlegge hele nettverk ved å spore opp enkeltpersoner, og aktørene kommer ofte fra forskjellige land. Nettverkene har internkontroll via administratorer og moderatorer. En anbefaling er ofte nødvendig for å kunne bli med. De økonomiske gevinstene fra slik virksomhet stimulerer kommersialisering av datakriminalitet med finansiering og utvikling av nye kriminelle metoder. Internett kan for kriminelle organiserte grupper bli et vesentlig redskap til å planlegge, organisere og gjennomføre narkotikahandel, korrupsjon, hvitvasking av penger og kommersiell sex.

3.4. Hovedtyper av datakriminalitet

Gjennom informasjonsteknologien knyttes kriminalitet og uønskede hendelser sammen i den digitale og den fysiske verden. De kriminelle får en ny arena med økt rekkevidde til å begå helt nye kriminelle handlinger, og kan samtidig gjennomføre tradisjonelle lovbrudd på nye måter. Lovbruddene vil være mer komplekse for politiet å oppdage, noe som stiller nye krav til politi og politimyndigheter.

Begrepet datakriminalitet er ikke definert entydig verken i Norge eller i andre land. Som introdusert i punkt 2.1 er det vanlig å dele kriminalitetsformen i to ulike kategorier. Den ene omfatter straffbare handlinger som har 'teknologi som mål', og den andre er 'teknologi som vesentlig verktøy'. Noen ganger er disse kategoriene knyttet sterkt sammen, andre ganger er de klart adskilte. Etter hvert som det meste styres av datateknologi, har det blitt mindre viktig å skille mellom disse kategoriene. Det viktigste er å oppdage denne typen kriminalitet, avdekke og hindre mer skade og sikre spor for videre oppfølging av lovbruddet handlingen medfører.

3.4.1. Kriminelle handlinger rettet mot datasystemer

Budapestkonvensjonen beskriver fire elementer ved datakriminalitet rettet mot data og kommunikasjonssystemer, samt en femte kategori som består i å utvikle og distribuere metoder for å utføre disse.

1. *Skaffe seg uautorisert tilgang til et datasystem*

Datainnbrudd er en stor trussel med etterfølgende uønskede handlinger som *informasjonstyveri* og *sabotasje*. *Informasjonstyveri* omfatter sensitiv og kritisk informasjon lagret i datasystemer. Til forskjell fra fysiske tyverier er det kopier som forsvinner, mens de originale dataene forblir intakte igjen. *Digital spionasje* er en form for informasjonstyveri.

Angrepsmåten har endret seg over tid og består i dag hovedsakelig av å lure inn en angrepskode i kjente dokumentformater via e-post (fisking med trojanere) eller ved utnyttelse av populære nettlesertillegg som automatisk aktiveres ved besøk på websider. For tilgang til de høyest sikrede nettverkene brukes ofte en kombinasjon av skadevare som sprer seg via flyttbare medier og angrep via underleverandører, og bruk av innsidere. Det er ikke noen forutsetning at sikkerhetsmekanismer må brytes. Utbredelse av botnett vil typisk falle inn under denne kategorien. Enkeltmaskiner samles da i større nettverk og kan samlet brukes for å utføre datakriminelle handlinger som distribuerte tjenestenektangrep, utvinning av virtuelle valutasystemer og utsendelse av store mengder søppelpost. Kompromitterte maskiner kan også brukes for lagring og distribusjon av uønskede og ulovlig ervervede data etter en informasjonstyverioperasjon.

2. *Hindre et datasystem i å fungere slik det er tiltenkt ('system interference')*

Gjennom *dataangrep* kan lagrings-, prosesserings- og kommunikasjonskapasitet misbrukes slik at tjenesteleveransen ikke lenger fungerer optimalt eller stopper helt opp. Distribuerte tjenestenektangrep er et kjent eksempel som bombarderer et nettverk med mer trafikk enn det klarer å håndtere, og dermed bruker opp kommunikasjonskapasiteten. Slike angrep kan være en brikke i en utpressingsoperasjon. En 17-årig norsk gutt ble siktet for grovt skadeverk med bakgrunn i et slikt angrep i 2014.

Langvarige målrettede *datainnbrudd* og *dataangrep* omtales gjerne som avanserte vedvarende trusler. Aktørene som står bak slike trusler, benytter seg av avanserte metoder som ofte er egenutviklede. De er godt organisert og har god finansiering. De legger vekt på å tilsløre egen aktivitet og identitet. Aktørene kan stamme fra alt fra fremmede staters

etterretnings- og sikkerhetstjenester eller militære spesialavdelinger til kommersielle aktører, terrorist- og ekstremistgrupper og mer eller mindre organiserte hackergrupper. Motivene omfatter idealisme, kriminell virksomhet, terrorisme, industrispionasje, økonomisk vinning og sikkerhetspolitiske målsettinger.

3. *Ødelegge, slette eller endre data uten autorisasjon ('data interference')*

Omhandler angrep på integriteten og tilgjengeligheten til innholdet på datasystemer. Ødelagte eller slettede data vil kunne hindre et datasystem i å fungere slik det er tiltenkt. Endring av data kan også være motivert i egen vinnings hensikt, som når skoleelever hacker seg inn i skolens databaser for å endre sine karakterer. Et annet eksempel er sverting av en motstander ved å innplassere falske digitale bevis. Sabotasjeaksjoner og terrorister kan endre styringsparametere i styringssystemer for kritisk infrastruktur for dermed å forårsake fysisk skade og i ytterste konsekvens død. Flere av disse angrepene kan stamme fra innsidere som ikke er avhengige av å bryte seg inn først.

4. *Avlytte kommunikasjon som ikke er offentlig ('illegal interception')*

Omhandler angrep på konfidensialiteten til digitalt overført informasjon når overføringen ikke er ment å være offentlig. Hva som er privat og offentlig, kan diskuteres. Lovverk kan derfor ha forutsetninger om at kommunikasjonen har et minimum av beskyttelse for å anses som privat, for eksempel bruk av kryptering.

Bruk av falske basestasjoner er et godt eksempel på hva denne kriminalitetsformen innebærer. Overgangen til et digitalt samfunn der de færreste forstår den bakenforliggende teknologien, har medført et stort gap mellom hva vi forstår som privat, og hva som teknisk sett er privat. En annen problemstilling er om avlyttet kommunikasjon kun dekker innholdet, eller om også metadata[13] skal ha beskyttelse. Det oppdages stadig svakheter i mobiltelefonsystemet som åpner opp for å spionere, ikke bare på innhold, men også på lokasjon[14], tidspunkt og hvem vi kommuniserer med.

5. *Utvikle, distribuere og besitte metoder for å utføre ovennevnte handlinger ('misuse of devices')*

Dette gjelder for eksempel utvikling av skadevare som virus, ormer og trojanere. Graden av kriminalisering varierer fra land til land, særlig knyttet til distribusjon og besittelse av slike metoder og verktøy. Budapestkonvensjonen inkluderer her også uautorisert adgang til tilgangsdata som passord og kryptografinøkler.

Besittelse, spredning og bruk av skadevare kan brukes til en rekke skadelige formål, blant annet misbruk av dataressurser, avlytting og modifikasjon av brukerens aktiviteter. EU har erkjent at nettverk av infiserte maskiner under ulovlig kontroll (botnett) er et stort problem, og har gjennom Europol/EC3 trappet opp kampen mot slik skadevare. Store kommersielle selskaper kjemper mot skadevare, både ved å utvikle antivirusløsninger og samarbeide med politiet for å ta ned kontrollsentre til skadevarenettverk. Det er også stort fokus på å skape løsninger hvor skadevare ikke får innpass, blant annet ved å kontrollere hvilke applikasjoner som tillates. Banker har gjort en stor innsats for å øke kunders sikkerhet, og seriøse Internett-leverandører tar tak i uønsket trafikk som går ut over andre kunder. Botnett kan brukes i distribuerte tjenestenektangrep og til målrettede angrep, for eksempel ved å sende fiskemeldinger på vegne av infiserte maskiner.

Alt dette skjer indirekte og skjuler de kriminelles identitet på Internett. Dette gjør etterforskningsarbeidet vesentlig mer komplisert.

Flere mistenkelige forsøk på digital spionasje og ulovlig informasjonsinnhenting mot mål i Norge og utlandet er avslørt de siste årene. Nedenfor angis eksempler som er kjent i mediene:

- Flere ledere i en større norsk bedrift ble utsatt for omfattende, organisert industrispionasje der datamaskinene ble tømt for informasjon ved hjelp av spionasjeprogramvare. En rapport har gått langt i å antyde at det er utenlandsk virksomhet som står bak.
- Det har vært flere alvorlige dataangrep mot selskaper i Norge. Aktørene har brukt 'spear phishing'-metoden – altså sendt ut e-post til ansatte i selskapene for å få dem til å klikke på en lenke. På denne måten kan det være mulig

13 Metadata som hvor du er, hvem du kommuniserer med, når og hvor lenge.
14 http://www.dn.no/magasinet/2015/02/13/2219/Teknologi/sirklet-inn-fra-utlandet (13.02.2015).

å undersøke hvilke sårbarheter som finnes i selskapenes datasystemer, og installere ondsinnet programvare.

- Et omfattende datainnbrudd i Belgia har vist hvordan datakriminalitet kan benyttes til å utvikle nye metoder for å begå tradisjonell kriminalitet. Et organisert kriminelt miljø skaffet seg tilgang og kontroll over datasystemene til en havn i Antwerpen for innførsel av større mengder narkotika. Etter å ha gjennomført datainnbrudd kunne kriminelle styre containertrafikken gjennom datasystemene og dermed hente ut containere som inneholdt store mengder narkotika, uten at det ble umiddelbart avdekket. Flere av de involverte var eksperter på sine felt; blant annet IT-sikkerhetseksperter med kontakter hos sikkerhetsbransjen, en teletilbyder og en person som drev en 'spy shop' og trolig skaffet en del av det tekniske utstyret til svindelen.
- Dansk politi har også informert om at et dansk politiregister med sensitiv informasjon er hacket. Registeret inneholder blant annet opplysninger om ettersøkte personer i Schengen-registeret (SIS).
- Ved et storstilt hackerangrep mot to britiske banker (Barclays og Santander) tok kriminelle kontroll over datasystemer og rakk å gjennomføre angrep som medførte at de klarte å stjele over tolv millioner kroner. Scotland Yard beskriver det som et av de mest sofistikerte angrepene noensinne, der hackerne opererte som en tredjepartsleverandørs IT-konsulenter.
- En undergruppe av Anonymous, OpLastResort, har blant annet stått bak tjenestenektangrep mot offentlige nettsteder i Storbritannia i protest mot behandlingen av en journalist i Snowden-saken.
- I november 2014 utførte Aftenposten en kartlegging av mobilovervåkingsutstyr i Oslo som indikerte at hemmelige, falske basestasjoner, såkalte IMSI-fangere, trolig var i bruk rundt flere sentrale bygninger i hovedstaden. Disse kan trolig overvåke bevegelsene til alle mobiltelefoner i og utenfor bygningene. Saken ga grunn til å frykte at de mulige overvåkerne fikk tilgang til informasjon om hvem som var i området, hvor de befant seg, hvem som snakket sammen, og hva som ble kommunisert. PSTs senere undersøkelser avdekket imidlertid ikke ulovlig overvåkningsaktivitet i området.

Det ventes at digital spionasje og ulovlig informasjonsinnhenting vil bli mer avansert, representere større skadepotensial og være vanskeligere å avdekke. Også sabotasje mot norske interesser, offentlige myndigheter og kritisk infrastruktur vurderes som en alvorlig trussel. Politiets sikkerhetstjeneste (PST) antar at avlytting og datanettverksbaserte etterretningsoperasjoner fra fremmede stater vil øke, se PSTs åpne trusselvurderinger.

Nasjonal sikkerhetsmyndighet (NSM) håndterte 88 alvorlige dataangrep mot Norge i 2014, kontra 51 i 2013, det vil si en økning på ca. 75 %. Flertallet av sakene dreier seg om forsøk på digital spionasje som potensielt kan føre til store skader. Det totale antall hendelser har økt fra 15 815 til 17 661 i perioden, og av disse økte andelen manuelt håndtert fra 3 901 til 5 067 saker. Denne hendelseshåndteringen innebærer blant annet varsling nasjonalt og internasjonalt, manuelle analyser og annen bistand. Vi ser en vekst både i antall angrep og kapasitet til å håndtere dem. NSM tror imidlertid at det er store mørketall, og at mange av de alvorlige angrepene aldri blir oppdaget.

I de årlige trusselvurderingene fra myndighetene blir det konstatert økt risiko for målrettede angrep på datainfrastruktur. Organiserte kriminelle miljøer og mange stater bygger opp etterretnings- og angrepsevne til bruk i og mot datainfrastruktur. Målet med aktivitetene kan være å skaffe seg tilgang til, manipulere eller fjerne kritisk forretningsinformasjon og sensitiv nasjonal informasjon. Norge må regne med at trusselen om datainnbrudd, dataangrep og datasabotasje er økende og kan rettes mot datasystemer som styrer privat og offentlig virksomhet, industriprosesser og kritisk infrastruktur.

3.4.2. Kriminelle handlinger med datateknologi som et vesentlig redskap

Elektronisk forfalskning og manipulering av digitale dokumenter ('computer-related forgery'). Elektronisk forfalskning er manipulering av digitale dokumenter. Det opprettes falske dokumenter som ser ut til å stamme fra en troverdig institusjon eller virksomhet. Det kan omfatte endring av regnskapstall eller manipulering av elektroniske bilder

eller tekstdokumenter. Ny teknologi har gjort det vanskeligere å oppdage forfalskningene.

Digitale bedragerier ('computer-related fraud'). Det finnes et stort antall falske nettsider på Internett hvor personer blir lurt til å gi fra seg både brukernavn, passord og kontoinformasjon til diverse nettjenester. Ved første øyekast ser nettsidene identiske ut med nettsider de pleier å besøke. Nettsidene som oftest forfalskes, er Facebook og Gmail, men vi ser også økt misbruk av lokale bedrifters nettsteder.

Nettbaserte markedsplasser benyttes i økende grad i Norge og utlandet, og nye typer nettsvindel har oppstått ved bruk av bankkort og varer som er falske eller ikke leveres. Slik virksomhet på Internett gjør gjerningspersoner i stand til å skjule sin virkelige identitet og sitt tilholdssted.

Ved gevinstbedrageri sendes det ut en e-post der en ber om mottakernes hjelp til å overføre store mengder elektronisk valuta til en tredjepart. Man lover dem en prosentandel hvis de godtar å behandle overføringen ved hjelp av sine personlige bankkonti. Så bes de om å overføre et lite beløp for å validere sine bankkontodata eller sende bankkontodata direkte. Når offeret har overført penger, hører vedkommende ikke mer fra lovbryterne.

Materiale som viser overgrep mot barn – både ekte og realistisk illustrert. Produksjon, tilgjengeliggjøring, overføring, fremskaffelse og besittelse av materiale som viser slike overgrep på Internett, er blitt en stor internasjonal aktivitet og trussel. Internett-teknologien gir mulighet for anonymisering av brukere, og innholdet kan spres i kanaler med lukkede brukergrupper. Lovbryterne bruker anonyme skyggenettverk for å dele slikt innhold, betalingen foregår anonymt og man bruker innholdsstrømming for å unngå å etterlate seg digitale spor på utstyr.

Misbruk av åndsverks- og opphavsrettslig beskyttet materiale. Piratkopiering og brudd på opphavsrett og åndsverksloven skjer ved nedlastning og bruk av digitalt innhold uten å betale for det. De vanligste bruddene på opphavsretten er ulovlig bruk og utveksling av opphavsrettslig beskyttet musikk, video, elektroniske bøker og programmer gjennom fildelingssystemer som omgår systemene som ivaretar rettighetseierne. Dagens fildelingssystemer kobler datamaskiner opp mot nettverksdistribuerte tjenester som utveksler opphavsrettslig materiale direkte mellom brukere og et mangfold av datamaskiner. Brudd på varemerkerettigheter er et velkjent aspekt ved global handel, med de samme utfordringer på nettet. Her brukes varemerker i kriminelle aktiviteter med sikte på villedende mål, krenkelser og falsk bruk av domener eller domenenavn i IP-verden.

Omsetning av narkotika og andre illegale produkter over Internett. Internett er en kanal som benyttes til omsetning av narkotika og illegale produkter. Det reklameres for slike produkter på nettet, og det er høy risiko med fare for liv og helse ved kjøp og bruk av falske eller ulovlige legemidler. Det er sannsynlig med en videre profesjonalisering av netthandelsløsninger som tilbyr narkotika. Betaling via anonyme betalingsløsninger er et stort problem her. Den mest kjente plassen for omsetning av narkotika, og andre ulovlige varer som våpen, er markedsplassen Silk Road, som har vært tatt ned av FBI flere ganger siden den dukket opp i 2011.

Brudd på ytringsfriheten og rasistiske og hatefulle ytringer på Internett. Krenkende uttalelser av rasistisk eller annen hatefull art skjer i dag ofte digitalt. Særlig kan oppfattelsen av å være anonym, dekket under falskt navn eller pseudonym, senke terskelen for dette. Krenkelser kan også ledsages av manipulerte foto eller misbrukt privat informasjon. Antall nettsteder som inneholder rasistiske og hatefulle ytringer, er i vekst.

Internett brukes som et *ledd i utpressing, krenkelser, mobbing og trolling*. Personer blir truet til å gi fra seg penger, utføre en uønsket handling eller holde tett om et forhold i frykt for at pinlig informasjon blir lekket eller offentliggjort. Aktivering av diverse kameraer over Internett eller lureri over videosamtaler er kilder til slik pinlig informasjon. Det har blitt vanlig at yngre mennesker deler personlige bildeopptak seg imellom, innhold som kan brukes til utpressing om det faller i feil hender. Et eksempel på dette er lekkasjen av private videoklipp og bilder fra Snapchat høsten 2014.[15] Opplevd anonymitet kan være en av hovedårsakene

15 http://www.aftenposten.no/article7749726.ece (18.10.2014).

til økt mobbing og krenkelser. Samfunnet har endret seg, og det er lettere å nå mange med sitt budskap. Vi har også sett mange eksempler på at personlig informasjon har kommet på avveie, særlig informasjon publisert i grupper på sosiale medier der man har hatt en uriktig antakelse om privatliv.

Radikalisering. Ekstreme grupper eller enkeltpersoner kan bruke datateknologi som et middel for å påvirke personer til å begå straffbare handlinger. Ofte vil dette være resultatet av en radikaliseringsprosess, der en person i økende grad aksepterer bruk av vold for å oppnå politiske, religiøse eller ideologiske mål.

Radikaliseringskampanjer og propaganda er ofte rettet mot et bredt publikum og vil i mange tilfeller omfattes av ytringsfriheten. Konkrete trusler eller oppfordringer til voldsbruk vil imidlertid kunne være straffbare. Norsk ungdom blir i dag eksponert for en mengde propaganda, hatefulle ytringer og trusler rettet mot Norge og det norske demokratiet. Ulike ekstreme grupper fremmer sitt syn gjennom propaganda på nettet, og søkende og sårbare personer kan bli fanget opp av de ekstreme gruppene. Hva som kan være avgjørende for at en person bestemmer seg for å begå en voldshandling, vil variere, men flere terrorgrupper forsøker å få sine sympatisører til å handle.

I mange tilfeller vil utstederen av voldspropaganda befinne seg i utlandet. Etterforskning og forsøk på straffeforfølgning vil i mange tilfeller være svært tid- og ressurskrevende, og i praksis ofte urealistisk. Mengden av propaganda og muligheten for videre spredning gjør det tilnærmet umulig å forsøke å stoppe slik virksomhet.

Trusler mot myndighetspersoner. De handlingene myndighetspersoner utsettes for, består for det aller meste av sjikane, trakassering og trusler. Hensikten kan være både å skremme og å uttrykke sterk misnøye. Ønske om oppmerksomhet, oppreisning eller hjelp er også vanlige motiv. Fellesnevneren er at svært mange ytringer og trusler kommer via ulike dataplattformer, og avsenderen er ofte ukjent.

3.5. Dagens trusselbilde

3.5.1. Trusselaktørene

I dagens trusselbilde kan det defineres ulike typer trusselaktører:

Ungdom med programmeringskunnskap ('script kiddies') kan være på jakt etter utfordringer. Noen ganger søkes uskyldig moro – andre ganger moro som innbefatter alvorlige lovbrudd. De gjør ofte bruk av lett tilgjengelige verktøy og teknikker. Uten erfaring og rettledning fra voksne kan denne aktiviteten forårsake datalovbrudd og skade. De kan lettere bli dratt med i mer alvorlige hendelser og involveres med trusselaktører som utfører organisert kriminalitet. Noen av disse ungdommene er svært kunnskapsrike, kan utvikle sine egne verktøy, gjennomføre målrettede angrep og avsløre sårbarheter.

Betrodde enkeltpersoner eller tidligere ansatte i virksomheter. Det kan dreie seg om faste medarbeidere, midlertidig ansatte, leverandører etc. som misbruker virksomhetens ressurser og informasjon.

Politisk motiverte enkeltpersoner og grupper ('hacktivister') kan utføre dataangrep for å støtte en bestemt politisk sak eller av idealistiske grunner. Angrepet kan komme fra bestemte navngitte grupper eller være anonymt. Disse aktørene får gjerne støtte fra andre trusselaktører som vil bidra med sine ferdigheter og råd til støtte for en sak.

Hacktivisme er en ny form for trusselutøvelse, der digitale verktøy benyttes for å true og påvirke private eller offentlige virksomheter eller for å oppnå politiske mål. Hacktivisme utøves i form av skadeverk og driftsstans på nettsteder, omdirigeringer av trafikk, tjenestenektangrep, informasjonstyveri, nettstedsparodier eller manipulering.

Virksomheter. Et særlig motiv vil være å få tilgang til viktig kunnskap og informasjon som kan gi konkurransefortrinn overfor andre virksomheter. Aktiviteter vil i hovedsak omfatte datainnbrudd, dataangrep og ulovlig innsamling av informasjon.

Organiserte kriminelle, enkeltpersoner eller grupper av mennesker kan utføre mer omfattende kriminell virksomhet. I det digitale samfunn inkluderer det aktiviteter som svindel, distribusjon av skadeverktøy og angrep på infrastruktur. Dette er en gruppe trusselaktører med betydelige ressurser og god evne til å skjule sin virksomhet. De besitter ofte spisskompetanse eller har lett tilgang til det gjennom tilkoblede kriminelle nettverk.

Terrorister kan bruke datateknologi som hjelpemiddel for å ramme personer, grupper eller samfunnsfunksjoner ved vold eller trusler om vold. Metodene kan omfatte manipulering av sosiale medier, inngrep med kritiske operasjoner i infrastruktur eller kommunikasjon og infiltrering av myndighetsorganer. Cyberterrorister skaffer seg tilgang til nødvendige ressurser og kunnskap for å ramme samfunnet.

I tillegg til at datateknologi benyttes som et hjelpemiddel for å utføre terrorisme, ser vi at terrorister i større grad bruker forskjellige varianter av datakriminalitet for å finansiere annen egen terrorvirksomhet. Transnasjonale terrorgrupper legger ut propaganda og oppfordringer til vold. Dette blir også gjort av nordmenn i utlandet, der avskrekking i form av trussel om straff ikke har noen effekt.

Andre stater og andre utenlandske aktører kan utføre innsamling av informasjon som er viktig for landet av politiske, økonomiske og militære grunner. Dataskadeverk og infiltrasjon vil ofte være målrettede og strategiske, avanserte og utført med betydelige ressurser. Man ønsker tilgang til hemmelig informasjon og tilgang inn i kritisk infrastruktur. Teknologiutviklingen er også så rask at Norge stadig trolig blir utsatt for dataangrep som ikke blir registrert.

3.5.2. Skadepotensial

Noen grupper er av erfaring mer utsatt for målrettede angrep enn andre. Det kan være for eksempel politikere, beslutningstakere og bedriftsledere, som alle besitter interessant informasjon; forsvarssektoren inkludert underleverandører og konsulenter; høyteknologiske selskaper som besitter informasjon som kan gi fortrinn til konkurrenter; samfunnskritiske funksjoner, menneskerettighetsorganisasjoner og advokater som besitter enten unik personsensitiv informasjon eller informasjon om politiske grupper. En stor del av trussel- og risikovurderingene gjelder uønskede handlinger rettet mot store enheter som stater, offentlige institusjoner og større næringslivsforetak. Men datakriminalitet rammer også vanlige databrukere i stort omfang. Noen ganger kan slike angrep også være veien inn til en virksomhet som er det egentlige målet.

Den enorme mengden personlig og sensitiv informasjon som ligger på nett, gjør det sannsynlig at trusler og utpressing mot enkeltpersoner, bedrifter og myndigheter blir enda vanligere.

Videre er skadepotensialet som økonomisk motivert nettkriminalitet kan medføre, av vesentlig omfang for norske virksomheter og privatpersoner. For næringsvirksomheter vil dette omfatte direkte tap, men også store skader som tapt omdømme og dermed indirekte tapt fortjeneste.

Etterretning fra fremmede stater og statsstøttede grupper. Statlig etterretningsvirksomhet utøves for å understøtte et lands politiske, økonomiske og militære interesser, og en rekke stater må antas å utøve etterretningsvirksomhet i Norge. Digitaliseringen av det norske samfunnet og internasjonaliseringen av forskning og næringsliv har gitt fremmede staters etterretningstjenester enklere arbeidsvilkår.

Nettverksoperasjoner kan brukes for å stjele enorme mengder gradert eller sensitiv informasjon. I tillegg kan slike operasjoner legge til rette for å skade eller lamme norsk kritisk infrastruktur på et senere tidspunkt. Nettverksoperasjoner kan også forberede for annen alvorlig sabotasje som kan bli iverksatt ved eventuelle fremtidige konflikter. Nettverksoperasjoner er derfor den etterretningsmetoden som kan ha de mest alvorlige og omfattende skadevirkningene på hele bredden av norske interesser. Nettverksoperasjoner kan også brukes for å stjele kunnskap, intellektuell eiendom og forretningshemmeligheter i kunnskapsbedrifter.

Avsløringene av nettverksbaserte etterretningsoperasjoner og avlytting i Norge de senere årene illustrerer hvor omfattende og kompleks etterretningsvirksomheten mellom stater er. En rekke forsøk mot norsk forsvars-, sikkerhets- og beredskapssektor, mot

politiske prosesser, mot norsk kritisk infrastruktur og mot virksomheter i energisektoren illustrerer dette. De brukes også til flyktningspionasje. Dette viser trolig langt fra det totale omfanget. Mange nettverksoperasjoner lar seg tilsløre eller skjule, og sikker attribuering vil i mange tilfeller ikke være mulig, selv om aktiviteten er oppdaget. I tillegg vil mange som utsettes for datarelatert etterretning, la være å melde fra om dette til sikkerhetsmyndighetene. Det kan enten skyldes at dataangrep ikke oppdages, eller at det å melde fra anses for å ha større negative enn positive effekter.

Store stater bruker enorme ressurser på å utvikle nye metoder for nettverksbaserte etterretningsoperasjoner, og den teknologiske utviklingen skjer raskt. Flere stater har ressurser og teknologi til å gjennomføre omfattende spionasje mot norske interesser og til å gjennomføre målrettede og ødeleggende dataangrep mot norsk data- og økonomiinfrastruktur. Trolig er norske sikkerhetsmyndigheters tekniske evne til å avdekke og hindre stadig mer avansert teknologisk etterretning ikke tilstrekkelig oppdatert.

Det er også en økende fare for såkalte forsyningskjedetrusler ('supply chain threats'), trusler mot distribusjonskjeden, hvor det i produksjonen av maskinvare og programvare bygges inn ondsinnet kode eller teknisk styrbare komponenter som kan aktiveres ved hjelp av Internett. Underleverandører angripes i større grad som et ledd i å kompromittere viktige samfunnsinteresser. Dette problemet er økende og vanskelig å kontrollere.

3.5.3. Metoder som benyttes

Bruken av ondsinnet kode ('skadevare') er vesentlig innen datakriminalitet. Ondsinnet kode har uønsket funksjonalitet sett fra offerets side, men må ikke blandes med programmeringsfeil, som er vanlig i all kodeutvikling. Intensjonen med skadevaren kan være så mangt:

- Gisseltaking av data for å presse eieren til å betale løsepenger, også kjent som *løsepengevirus ('ransomware')*. Et nylig eksempel er CryptoLocker, som krypterer datafiler og mapper, som kun kan dekrypteres når offeret gjør en nettbetaling til den ansvarlige svindleren og dermed får tilgang til dekrypteringsnøkkelen.
- Tyveri av penger / finansielle midler i form av *banktrojanere*.
- Informasjonstyveri. Spionasje og potensielt utpressing eller identitetstyveri basert på informasjon innhentet ved bruk av *spionprogramvare*. Det engelske uttrykket 'Remote Access Tool' (RAT) er mye brukt i denne sammenheng. Eksempler på sensitive opplysninger kan være brukernavn, passord, kredittkortnummer/CVC[16]-nummer og personnummer.
- Bygging av botnett for fremtidige *distribuerte tjenestenektangrep* og annen misbruk av dataressurser slik som utvinning av bitcoin og misbruk av annonsesystemer. Dette kan gjøres ved å automatisere klikk på reklameannonser.
- Andre eksempler er *reklamevare* som viser reklame til brukeren av enheten, og *logiske bomber* med den hensikt å utføre sabotasje på et senere tidspunkt.

Ondsinnet kode kan spres på mange måter. Angrepsmetodene er ofte en kombinasjon av

- utnyttelse av logiske sårbarheter ved bruk av *'exploit kits'* mot eksponerte tjenester og *vannhull* på populære nettsider for å nå mål bak brannmurer
- menneskelig manipulasjon ved utsending av e-postmeldinger eller direktemeldinger. Da ofte ved å forsøke å lure deg til å åpne tilsynelatende legitime e-postvedlegg, en såkalt *trojansk hest*, eller trykke på en lenke

Utplassering av lokke-USB-pinner er også en effektiv metode som utnytter sårbarheter i USB-protokollen for å starte skadevaren automatisk.

Når skadevaren, ofte en trojaner, har kommet inn på klienten, er den ofte i stand til å spre seg selv ('dataorm') fra én datamaskin til en annen ved å benytte kjente og ukjente sårbarheter i programvare på både servere og PC-er. Mange av de siste års trojanerangrep er basert på kjente kommersielle rammeverk som med en rekke utvidelser ('plug-ins') kan tilpasses etter behov og utbygges med den funksjonalitet som angriperen mener er mest

16 CVC: 'Card Verification Code' på betalingskort.

hensiktsmessig for å nå sitt mål. Utvikleren inkluderer ofte muligheten til å samle inn passord og fange opp tastetrykk, men skreddersydd funksjonalitet må utvikles av angriperen selv. For eksempel utvidelser for å stjele penger fra en konkret nettbank. Rammeverkene har også ulike former for egenbeskyttelse, deriblant kryptering av egen kommunikasjon samt teknologi for å skjule sin egen tilstedeværelse ved såkalt 'rootkit'-teknologi.

Det eksisterer et marked for tredjepartsutvidelser for de fleste av rammeverkene. Målrettede angrep fra aktører som ikke benytter denne type kommersiell skadevare, er ofte mer komplekse, men prinsippet om rammeverk som kan bygges ut med ulike egenskaper, er ofte det samme. Som et hovedprinsipp ser vi at alle angrepene er spesielt laget for det målet som angripes.

Sosial manipulering er en annen viktig metode. Sosial manipulering brukes for å lure inn ondsinnet kode som allerede nevnt, men har også helt andre aspekter. Sosial manipulering utføres via digital kommunikasjon og på sosiale arenaer, og kan være både målrettet og opportunistisk ved at man håper på at tilfeldige ofre biter på. 'Spear phishing' og 'whaling' er uttrykk som benyttes om målrettede e-postkampanjer. Tilsvarende begreper som 'smishing' og 'vishing' brukes når kommunikasjonen foregår via SMS eller oppringing. Søppelpost ('spam') er en vanlig metode for å komme i kontakt med tilfeldige naive personer.

Noen kjente taktikker innen sosial manipulasjon er fristelser, tiltrekning, sympati, tillit, autoritet, frykt og knapphet. For eksempel:

- tilby falske investeringsobjekter og lure deg til å betale inn et lite beløp i håp om å få utbetalt store premier. Ofte bes du om hjelp til å realisere formue *(fristelse)*
- rekruttere til hvitvaskingsoperasjoner der du får tilbud om å jobbe som «pengeoverfører». Også kjent som penge-muldyr ('money mule') (*fristelse*)
- selge falske eller ikke-eksisterende varer *(fristelse/knapphet)*
- utføre dating-svindel[17] ved å inngå falske kjærlighetsforhold i den hensikt å lure fra deg penger. Kjente metoder er å spille på vanskelige kår eller behov for medisinsk behandling og utgifter for å dekke reiser/besøk *(tiltrekning)*
- utgi seg for å være nære venner og familie i pengenød *(tillit)*
- gjennomføre skremselsaksjoner ved bruk av politilogo eller annen myndighetslogo. Ofte brukt på nettområder assosiert med ulovlig eller tabubelagt innhold *(autoritet/frykt)*
- søke bistand til uregistrerte/falske veldedighetsorganisasjoner *(sympati)*

Anonymisering, kryptering og virtuelle valutaer er nye digitale metoder som skaper store utfordringer i bekjempelsen av datakriminalitet. Det er helt legitimt for borgere å etablere personvernnettverk for å beskytte sine privatliv. Men verktøyene er også av stor interesse for kriminelle som misbruker slik anonymitet i stor skala for å skjule sine kriminelle handlinger. Et mye brukt anonymiseringsnettverk er TOR-nettverket, men stadig nye funksjoner og alternative nettverk vil bli tilbudt. Virtuelle penger og valuta samt anonyme betalingsmekanismer er nye metoder som benyttes for å kjøpe varer og tjenester i det globale nettsamfunnet, og som omgår myndighetenes kontroll. Valutaer som bitcoin og litecoin er slike nye elektroniske penger som veksles på Internett mot virkelige pengevalutaer. Det tilrettelegger for kriminalitet, ettersom valutaene tillater anonymt eierskap og anonyme overføringer av verdier. Denne type valuta vil høyst sannsynlig bli vanligere, og det vil komme ny teknologi og nye varianter som gjør det utfordrende for sentrale finansmyndigheter å regulere og kontrollere økonomiske transaksjoner. Det gir gode muligheter til å utføre hvitvasking av penger. Samfunnets kontrollinstanser og politiet vil da ikke lenger kunne følge pengestrømmer ved mistanke om ulovlige transaksjoner.

3.5.4. Trusselutviklingen mot samfunnet

Rundt tre milliarder mennesker over hele verden har tilgang til Internett. Vårt virtuelle samfunn vil fortsette å vokse og bli mer eksponert for digital kriminalitet. Folk som man normalt ikke tror kan stjele eller skade andres eiendom, oppfører seg annerledes når de er i aktivitet på Internett. De finnes over hele verden, og

17 Farene ved nettdating: http://www.online.no/trender/farene-ved-nettdating.jsp (26.12.2014).

lovbrytere kan få tilgang til ofre på nett med enkle metoder og til lave kostnader.

I det moderne samfunnet vil omtrent all kriminalitet avlegge elektroniske spor. Tradisjonell kriminalitet minsker i omfang i store deler av verden, og mange typer kriminalitet flyttes over til den digitale verden. I den fysiske verden trenger du bare å bekymre deg for de kriminelle som oppholder seg i ditt nærområde. I den digitale verden kan kriminalitet utføres over Internett fra andre steder på jordkloden, uten hensyn til landegrenser. Denne digitale kriminaliteten er dermed i stor grad internasjonal. Straffene er gjennomgående lavere enn ved annen type kriminalitet og virkningene større hvis en vil ramme mange og viktige samfunnsfunksjoner.

Økning i bruk av Internett, økt kunnskap om teknologiske muligheter kombinert med mangel på sikkerhetstiltak og sikkerhetskultur vil føre til mer kriminalitet via nettet. Det er sannsynlig at flere kriminelle utnytter mulighetene teknologien gir, og at det derfor dukker opp flere avanserte metoder.

En viktig strukturell sårbarhet er at informasjonssikkerheten har lav prioritet i mange norske statlige og private institusjoner og virksomheter. De tror sannsynligheten for å bli rammet av sikkerhetshendelser er lav, og tar derfor ikke trusselen på alvor. Lav sikkerhetskompetanse i kombinasjon med at stadig mer sensitiv informasjon legges ut på datasystemer tilknyttet Internett, medfører store sårbarheter. En særlig utfordring er at Norge har veldig mange små virksomheter, her definert som virksomheter med under ti ansatte. Det er vanskelig å ha god nok sikkerhetskompetanse hos små virksomheter, og som en konsekvens blir ofte hele eller deler av datadriften satt ut til eksterne parter.

Det avdekkes stadig flere tekniske sårbarheter, noe som gjør det mulig å hente ut sensitiv informasjon. En av de siste, en sårbarhet i programvaren OpenSSL som fikk tilnavnet Heartbleed, ble offentlig kjent i april 2014. Ved å utnytte denne kan angripere over tid snike til seg informasjon fra en sikker webserver, som i verste fall kan brukes til å avlytte kommunikasjon, stjele data direkte fra tjenestene og brukerne samt utgi seg for å være tjenester og brukere. Manglende sikkerhetsoppdateringer av operativsystemer og programvare gir ofte trusselaktører uautorisert tilgang til systemer. Nettverkskomponenter som brannmurer og rutere blir også oftere kompromittert på grunn av manglende sikkerhetsoppdateringer.

Det jobbes hardt for å oppdage og utnytte sårbarheter også i mobile enheter som mobiltelefoner og nettbrett. Den største risikoen i dag oppstår hvis man installerer programvare fra ukjente kilder utenfor de offisielle applikasjonsbutikkene. Det finnes hackerverktøy som innplasserer skadevare i legale programmer. Når brukere laster ned en piratversjon av for eksempel Angry Birds, vil spillet fungere som normalt, samtidig som hackeren tar kontroll over mobilen. Eldre mobiltelefoner som ikke er oppdatert, kan dessuten inneholde sårbarheter som kan utnyttes hvis de besøker ondsinnede nettsteder. En ny undersøkelse fra Telenor konkluderer med at én av to nordmenn ikke bruker automatlås på telefonen. I praksis betyr det at hvem som helst kan få tilgang til innholdet på disse telefonene hvis de blir stjålet eller kommer på avveier.

Skytjenester kan gi mange fordeler, men informasjonen lagres og behandles utenfor egen kontroll. Det blir mer komplisert å finne ut hvor dataene ligger, hvordan de sikres, og hvilken jurisdiksjon de fysisk oppbevares i. Små virksomheter har dessuten vanskelig for å stille tilstrekkelige krav til leverandører når det gjelder sikkerhet og hvor tjenesteproduksjonen foregår.

Jurisdiksjonsproblematikken skaper også store utfordringer for politi- og kontrollmyndigheter, ettersom informasjonen kan bli vanskelig å få tak i. Gjelder norsk lov? Hvordan håndteres uenigheter med underleverandører? Hvordan løser vi problemer med svindlere som har misbrukt norske bedrifters informasjon i utlandet, når dataene i praksis både er skapt, prosessert og lagret utenfor Norge? En utfordring i dag er at vi legger ut, lagrer og bearbeider veldig store mengder informasjon på tjenester i andre land, noe som gjør informasjonen særlig sårbar.

Fremmed etterretning trenger for eksempel ikke engang å bryte seg inn i systemene våre for å få tilgang til informasjonen vår. I USA er det en klar oppfatning om at suverenitet i det digitale rom ikke skal ta hensyn til hvor dataene blir lagret og behandlet, men kun hvilken nasjonalitet skyselskapet har. Amerikanske selskap har derfor utleveringsplikt selv om datasenteret er plassert utenfor amerikansk territorium.

Trenden 'Bring your own device' innebærer at skillet mellom datautstyr benyttet i jobbsammenheng og privat stadig reduseres. Arbeidstakere bruker samme enheter privat som på jobb, og enhetene er ofte eid av arbeidstaker. Utfordringen her er at sikkerhetsnivået på private nettverk ofte er mye lavere enn på arbeidsplassens nettverk.

Smarttelefoner og nettbrett er blitt attraktive mål for kriminelle utnyttelser. Vi har dem med oss overalt, vi gir dem utstrakt tilgang til tjenester vi bruker, vi betaler med dem, og de vet hvor vi er. De inneholder med andre ord veldig mye sensitiv informasjon. Varianter av ondsinnet programvare kan i økende grad rettes mot sårbarheter i mobile operativsystemer.

Siden forbrukerelektronikk ofte ikke har fokus på sikkerhet, men på funksjonalitet, ser vi at slike produkter stadig blir mer attraktive mål for trusselaktørene. Eksempler på enheter er overvåkningskameraer, babycaller og smart-TV-er. Hensikten er å fjernaktivere kamera og lydopptaksutstyr. Et stort antall av disse viser seg å være åpent tilgjengelig fra Internett grunnet feilkonfigureringer, manglende passord eller annen mangel på sikker angivelse av identitet.

Masseinnsamling av data og nye typer innsamlingsteknologi utnyttes i økende grad av både offentlig og privat virksomhet. Det omfatter søkemotorer, spesielle datafangere og analyseverktøy som målrettet fanger opp og analyserer informasjon om individer og private og offentlige virksomheter. Privat virksomhet som i særlig grad profilerer seg gjennom nye brukeranvendelser på Internett, vil samle inn informasjon om kundene og konkurrerende virksomhet. Slik informasjon vil kunne være persondatainngripende og utnyttes som overvåkningsinformasjon.

Den allerede eksisterende masseinnsamlingen av informasjon i dagens samfunn vil øke og inneholde større mengder og mer detaljert personrelatert informasjon, fordi digitale medier benyttes av de fleste borgerne til det meste. Politiet har spesiell hjemmel for innsamling av informasjon og for overvåking når det er nødvendig ved alvorlige kriminelle hendelser. Teknologien er blitt billig, brukervennlig og får omfattende bruksområder.

Økonomisystemer og betalingsteknologi misbrukes. En særlig utfordring ved betalingssystemet vi har i dag, både ved betalingssted og ved nettbank, er hvor lite som skal til for å autorisere overføring av penger. Finansinstitusjoner er koblet sammen internasjonalt i områder med liten kontroll med identiteten til kontoinnehaver, samt få muligheter for å reversere ulovlige overføringer. Bankvesenet har til nå gardert seg ved å ta ansvaret, men dytter samtidig kostnaden over på kundene gjennom høyere renter og gebyrer.

Nettbankbedrageri gjennomføres ved at nettbankkunder får innplassert en ondsinnet programvare i sine datamaskiner. Hensikten er å tappe bankkonti for penger. Penger blir ofte overført til bankkonti tilhørende personer som er rekruttert til å jobbe som «pengeformidlere». Utfordringen knyttet til nettbank er at banken ikke kan anta at datamaskinen benyttet for innlogging er til å stole på, med andre ord at maskinen ikke er kompromittert. Selv tofaktorautentisering[18] ved innlogging hjelper lite når en skadelig kode på innsiden kan manipulere og handle på vegne av kunden som bruker maskinen. Noen banker har derfor innført ekstra autentisering for hver overføring, eller for overføringer til usikre mottakere. Det benyttes i økende grad benyttet anomalideteksjon, slik at merkelige overføringer kan oppdages og stoppes på vegne av kunden.

Bankkort misbrukes. Magnetstripen kan lett kopieres. Europa har lenge brukt chip som en mer kopieringsmotstandsdyktig mekanisme for lagring av kontoopplysninger. Utfordringen her er at salgsstedet kan droppe å sjekke den personlige koden av tilgjengelighetshensyn, som for eksempel i situasjoner der kommunikasjon med banken ikke er mulig. Dette skjer blant annet på flere busser i Norge, og mange steder i utlandet. Noen ganger erstattes kodesjekken med krav om signatur, men signaturene blir i praksis aldri kontrollert. Betalingskort har innskrevet utløpsdato samt en autorisasjonskode med tre tegn på baksiden av kortet. Denne informasjonen er alt som skal til for å overføre penger (f.eks. via Internett/nettbutikker). Det har i den senere tid kommet

18 Noe du vet, noe du er, eller noe du har. Bruk av minst to slike faktorer for å bevise hvem du er, kalles 'sterk bekreftelse på identitet' (autentisering). Se https://norsis.no/leksikon/to-faktor-autentisering/.

løsninger for flerfaktorautentisering ved slik betaling, men det er ikke alltid påkrevet. Regionsperrer har vært et nyttig forebyggende tiltak. En ny utfordring vil være nye former for mobil og kontaktløs betaling samt betaling via applikasjoner med forhåndslagrede kontoopplysninger.

Elektronisk ID-tyveri og misbruk av digital identitet er når personinformasjon stjeles og utnyttes til bedrageri. Det skaffes tilgang til store mengder med personopplysninger som så selges videre eller benyttes i gjennomføringen av ulike former for alvorlig kriminalitet. Mangel på gode kompatible løsninger for sikker identifisering på Internett er en vesentlig kilde til mange av utfordringene vi har i det digitale samfunn, og særlig økningen i identitetstyverier og svindel. Identitet basert på statiske brukernavn og passord har lenge vært rådende. Flerfaktorautentisering ved bruk av tids- eller sekvensbaserte engangskoder levert via brikke eller SMS er et godt steg videre. Banknæringen har tatt grep ved introduksjon av BankID, som baserer seg på digitale sertifikater. Vi har også løsningen MinID for offentlige tjenester. Utfordringene ligger i at det er behov for identifisering på forskjellige sikkerhetsnivåer, alt fra å logge inn anonymt på en tilfeldig webside til å sende e-post for å signere viktige dokumenter elektronisk.

Mer og mer teknologi blir knyttet til det enkelte individ. Dette vil naturligvis medføre at det blir flere og mer avanserte teknologiske innretninger som vil inneholde personopplysninger, herunder også til dels sensitive personopplysninger. Der man i dag i hovedsak finner personopplysninger i diverse register, telefoner og datamaskiner, vil man i nær fremtid kunne få tilgang til personopplysninger fra nærmest alle dagligdagse ting. Nanoteknologi muliggjør for eksempel integrasjon av informasjonsteknologi, molekylærbiologi og medisin til nye anvendelser. Av praktiske anvendelser tenker man seg klær som tilpasser seg miljøet, byggematerialer og nanomaskiner med regelbaserte sensorer, og ikke minst sensorer og maskiner som bygges inn i kroppen. Slike sensorer/maskiner kan også settes opp for å utføre regelbaserte oppgaver, som automatisk registrering av for eksempel alkoholinntak hos yrkessjåfører eller automatisk medisinering av folk under tvungent psykisk helsevern. Nanoteknologien danner på mange måter en bro mellom den fysiske verden og den virtuelle verden, slik at disse går mer og mer over i hverandre. Elektroniske brikker og kort, ny sensorteknologi, biometri, trådløs kommunikasjon og lokaliseringssporing er alle teknologier som hyppigere vil bli tatt i bruk. Dette vil gjøre at alle individer til enhver tid går rundt med en enorm mengde opplysninger i og på kroppen. Disse er integrert i alle aktiviteter man utfører i løpet av dagen, og vil på den ene siden effektivisere den enkeltes hverdag, men på den andre siden gjøre individet sårbart, både gjennom en massiv form for overvåkning, men også på grunn av muligheten aktører med onde hensikter har til å få tak i store mengder personopplysninger.

Egenprodusert materiale og seksuell utnytting ('sextortion'). Det er et økende problem med «egenprodusert» materiale der barn og ungdom eksponerer seg selv foran et webkamera eller sender fra seg bilder der de er helt eller delvis nakne. Med dagens teknologi hvor barn er tilgjengelige på Internett til enhver tid, og spredningen av informasjon går svært raskt gjennom blant annet sosiale medier, er dette en langt større utfordring enn tidligere. Geotagging av bilder har blitt mer vanlig, og en stor ulempe er at lokasjonen på bildet kan røpe hvor bildet har blitt tatt, overfor potensielle overgripere.

Internasjonalt advares det mot fenomenet 'sextortion' (seksuell utnytting) hvor en utpresser lokker noen til å vise seg naken eller utføre seksuelle handlinger foran et webkamera, for deretter å presse fornærmede for penger med trusler om at bilder eller film publiseres på Internett. Også i Norge har det vært slike saker, og det forventes en økning fremover. At sensitive bilder eller filmer havner på avveie og for eksempel kobles til ulike pornografiske sider eller spres i vennekretsen, kan være svært belastende. I andre land har unge mennesker følt dette så belastende at de har tatt sitt eget liv.

Internasjonalt rapporteres det også om en bekymring over seksuelle overgrep mot barn via webkamera: Vestlige borgere betaler penger for å se barn gjøre seksuelle handlinger med seg selv eller andre på bestilling. Direktestrømming ('on-demand'-visning) vil trolig gi mer spredning av overgrepsbilder og -videoer av barn. Dette er nye former for seksuell utnyttelse av barn på nettet.

Det blir enda enklere å utføre målrettede dataangrep med ondsinnet programvare. Slike dataangrep kan rettes mot viktige samfunnsfunksjoner. Det er fullt mulig å stanse strømforsyningen som følge av infiltrasjon av datasystemer hos strømleverandører.

Industrielle kontroll- og styringssystemer (SCADA-systemer) er systemer med stort skadepotensial dersom de tilgjengeliggjøres og misbrukes over Internett. Vi kan se for oss stansing eller overbelastning av strømnett eller kloakksystemer og manipulering av signalering av offentlig transport. Utfordringen ligger i balansen mellom praktiske tilgjengelighetshensyn, som for eksempel å kunne fjernstyre systemene, og behovet for sikkerhet.

Flere samfunnssektorer vil være sårbare for sikkerhetsbrudd og digitale angrep. Et eksempel kan være helsesektoren. Når datamaskiner og elektronisk kommunikasjon får en så sentral rolle i overvåkning og styring av menneskekroppen, vil det gi mulighet for uønskede hendelser med drastiske konsekvenser for liv og helse, slik som manipulering av medisinske instrumenter, pasientidentitet og behandlingstiltak som kan føre til feilinngrep. Det er allerede påvist uautorisert styring og inntrengning i pacemakere, og tilsvarende handlinger i et mangfold av biosensorer kan medføre nye former for både tilsiktede og utilsiktede handlinger som dreper eller skader.

Økt fare for dataterrorisme. Enkeltpersoner eller organisasjoner som utøver terror, benytter Internett til ulike formål. Et slikt formål, som vil kunne få store konsekvenser, er nettbaserte angrep mot kritisk infrastruktur. Kritisk nasjonal infrastruktur omfatter kraftforsyning, luft og transport, telekommunikasjon, gass og olje, transport, bank og finans, vannforsyning og redningstjenester. Kritiske funksjoner er basert på datasystemer som kommuniserer med hverandre og utveksler informasjon. Selv korte avbrudd kan føre til store samfunnsmessige skader på militære, offentlige og markedsbaserte tjenester.

4. Dagens bekjempelse av datakriminalitet

4.1. Innledning

En rekke sikkerhetsaktører deltar i bekjempelsen av datakriminalitet, både offentlige og private. Blant de offentlige har vi dem som hører til politiet og påtalemyndigheten og andre offentlige organer. Det er også et utstrakt samarbeid med utenlandske sikkerhetsaktører. Oppgavene de norske sikkerhetsaktørene utfører, varierer, men er kort oppsummert:

- etterretning i form av innsamling av informasjon og analyse
- beskrivelse av trusselbildet (eller utarbeidelse av trusselvurderinger)
- forebyggende virksomhet
- oppdagelse og avdekking av datakriminalitet
- hendelseshåndtering med avverging og skadebegrensning
- etterforskning
- straffesaksbehandling

Dette kapittelet gir en oversikt over de viktigste sikkerhetsaktørene og deres rolle i bekjempelsen av datakriminalitet. Til slutt sies det litt om trusselvurderinger.

4.2. Sikkerhetsaktører i Norge

4.2.1. Straffeforfølgningen

Politidirektoratet (POD). Politidirektoratet leder og samordner politiet. Politiets ansvar for bekjempelse av kriminalitet er beskrevet i politiloven § 2 og innebærer blant annet å

- beskytte og verne lovlig virksomhet mot alt som truer den alminnelige tryggheten i samfunnet, og opprettholde den offentlige orden og sikkerhet
- forebygge kriminalitet og andre krenkelser av den offentlige orden og sikkerhet
- avdekke og stanse kriminell virksomhet
- etterforske og straffeforfølge lovbrudd

Politiet har derfor et klart ansvar for innsatsen mot datakriminalitet.

Politidirektoratet har ansvar for alle politidistriktene og politiets særorganer, med unntak av PST. POD har ansvar for faglig ledelse, styring, fordeling av ressurser, resultatoppfølging og utvikling av norsk politi. POD har i tillegg ansvar for å gjennomføre regjeringens politikk i henhold til tildelingsbrev, oppdragsbrev eller andre oppdrag gitt i styringsdialog mv. POD gir de overordnede rammebetingelsene og strategiene til de underliggende politienhetene på områdene økonomi, kompetanse, bemanning, verktøy og arbeidsdeling og for samarbeidet mellom ulike operative fagmiljøer i politiet. Det er de underliggende virksomhetene i politiet som utfører det operative politiarbeidet, det vil si forebygging, etterforskning og straffesaksbehandling av datakriminalitet.

POD er nasjonalt kontaktpunkt for internasjonalt samarbeid og ivaretar kontakten med Europarådet, FN, Europol og Interpol på et mer overordnet nivå samtidig som det også ivaretar nordisk og annet internasjonalt samarbeid. Kripos er nasjonalt kontaktpunkt for den operative og utøvende myndighetsrollen og bistandsfunksjonen.

Politidistriktene. Politi- og lensmannsetaten i Norge består av 27 politidistrikter, i tillegg til de nasjonale særorganene. Politidistriktene sorterer under Politidirektoratet, som har ansvar for faglig ledelse, styring og oppfølging. Hvert distrikt ledes av en politimester.

Innenfor hvert politidistrikt finnes det både politistasjoner og lensmannskontorer. Hver politistasjon ledes av en politistasjonssjef med geografisk ansvar for et politistasjonsdistrikt. Lovbrudd etterforskes og straffeforfølges som hovedregel av politidistriktet der lovbruddet ble begått. Det gjelder også datakriminalitet og innbefatter påtalemessig og politifaglig arbeid på nett, sikring av elektroniske spor ved beslag og etterfølgende datatekniske undersøkelser. En undersøkelse[19] hos politidistriktene i 2012 viste at de har fra null til tre dataetterforskere, med unntak av det største distriktet i undersøkelsen (Oslo politidistrikt), som hadde 14 dataetterforskere og planlegger å

19 Politidirektoratet. 2012. *Politiet i det digitale samfunnet* (2012).

utvide antallet til 20. Svært få distrikter har egen kompetanse på datakriminalitet rettet mot datasystemer.

Det mangler felles retningslinjer for sikring, forvaltning og behandling av digitale spor. Ofte er det opp til enkeltpersoner i distriktene å drifte egne løsninger for nødvendig dataverktøy. Særlig forvaltningen av sikrede spor, det vil si sikker og redundant lagring av digitale spor, er mangelfull. Både nødvendig utstyr og vedlikehold av kompetanse er kostbart, og på dette området er det derfor store effektiviseringsgevinster å hente.

Politidistriktene foretar i det daglige politiarbeidet datatekniske undersøkelser av datamaskiner, mobiltelefoner, lagringsmedier og andre elektroniske enheter. IKT benyttes i økende grad som verktøy ved lovbruddene man avdekker. Undersøkelsene kan foregå på åstedet for lovbruddet og vil kunne være avgjørende for oppklaring av saken. I noen tilfeller er de elektroniske sporene den eneste muligheten for å belyse en hendelse eller oppklare et straffbart forhold.

Politireformen vil trolig halvere antall politidistrikter, og dette vil kunne føre til større fagmiljøer for etterforskning av datakriminalitet i distriktene.

Økokrim er den sentrale enheten for etterforskning og påtale av økonomisk kriminalitet og miljøkriminalitet, et særorgan og et statsadvokatembete med nasjonal myndighet underlagt Riksadvokaten.

Politiets datakrimsenter ble opprettet under Økokrim i 2003 som et spesialorgan for å styrke politiets kompetanse og evne til å etterforske datakriminalitet. Enheten skulle ha egen påtalekompetanse til å etterforske og iretteføre egne datakrimsaker, samt sikre og analysere elektroniske spor. Det er etablert økoteam i politidistriktene for å ivareta etterforskningen av økonomisk kriminalitet og miljøkriminalitet lokalt, og disse brukes i mange tilfeller for å sikre digitale spor i datakrimsaker.

Politidirektoratet gjennomførte i perioden 2003–2004 en særorganutredning. Den anbefalte og førte også til en flytting av datakrimsatsingen til Kripos. Enkelte hensyn var avgjørende for flyttingen; Kripos skulle bli et sentralt bistandsorgan i utnyttelsen av elektroniske spor innen alle typer kriminalitet og etableres som et kompetansested i politiet for tilrettelegging av kommunikasjonskontroll.

Siden ett av hovedmotivene for datakriminalitet er økonomisk vinning, er det noen ganger uklart om saker skal etterforskes som økonomisk kriminalitet eller datakriminalitet. Kriminalitetsformene har det til felles at de innebærer bruk av digitale penge- og betalingssystemer, nettbankbedrageri, digitale former for hvitvasking og økonomisk digital utpressing. Økokrim har god evne og kapasitet til sikring og analyse av store mengder digitale spor og samarbeider også med andre finansinstitusjoner om felles kriminaletterretning, blant annet for å oppdage mistenkelige transaksjoner.

Allmennprevensjon er et sentralt mål for Økokrim. Gjennom arbeidet med konkrete straffesaker sender særorganet signaler til allmennheten om at man risikerer straff dersom man overtrer reglene. Som statsadvokatembete er Økokrim underlagt Riksadvokaten, mens det som sentralt politiorgan er administrativt og økonomisk underlagt Politidirektoratet.

Kripos er et nasjonalt særorgan og kompetansesenter underlagt Politidirektoratet. Formålet med Kripos er å bistå norsk politi i arbeidet med å forebygge og bekjempe organisert og annen alvorlig kriminalitet. Organet etterforsker og iretteforer komplekse og alvorlige straffesaker og yter taktisk og teknisk bistand til politidistriktene og andre enheter. Kripos er kontaktpunktet mellom norsk og utenlandsk politi og ivaretar oppgaver som følger av internasjonale konvensjoner og avtaler.

Den nasjonale satsingen på bekjempelse av datakriminalitet ble synliggjort da Politiets datakrimsenter ble etablert under Økokrim i 2003. Særorgansutredningen i 2004 medførte at virksomheten ble flyttet til Kripos i 2005 og omgjort til Datakrimavdelingen. Den nye avdelingen fikk blant annet ansvar for å avdekke, etterforske, utføre etterretning og føre datakrimsaker for retten og bistå politiet og påtalemyndigheten i straffesaksarbeidet. Et nasjonalt datateknisk laboratorium ble opprettet for å ivareta behovet for spesialutstyr og spisskompetanse. Gjennom flyttingen til Kripos ønsket politiet å styrke sin evne til å håndtere fremtidens kriminalitet og trusler – ikke minst gjennom tilstedeværelse på den digitale arenaen, kompetansehevende tiltak, rådgivning, forskning og utvikling på området.

Kripos har med begrensede ressurser utviklet spisskompetanse innen taktisk og teknisk datakrimetterforskning samt kriminaletterretning. Denne kompetansen benyttes i egne saker og ved bistand til politidistrikter og særorganer. Prioriterte områder har vært spesialisert bistand innen datatekniske undersøkelser, operativ kriminalanalyse, kommunikasjonskontroll, etterforskningsstøtte for spor på Internett, spaning, informantbehandling og vitnebeskyttelse.

Kripos har opparbeidet seg kompetanse, personell og utstyr til å utføre datatekniske undersøkelser på et høyt internasjonalt nivå. Undersøkelsene skal sikre at spor og bevis fra elektronisk utstyr, digitale lagringsmedier og Internett utføres med oppdaterte metoder som er mest mulig uangripelige i politiets straffesaksarbeid.

Bistanden til distriktene ytes etter anmodning og følger de ordinære bistandsformene i Kripos som *stedlig bistand, konsultativ bistand og bistand ved innsendt materiale*. Teknologien, verktøyene og metodene som benyttes, må stadig vedlikeholdes og videreutvikles. Derfor utfører Kripos egen metodeutvikling for å sikre og analysere data der kommersielle løsninger kommer til kort.

Kripos har de siste årene etablert støtte til politidistrikter og særorganer innen Internett-relatert etterforskning. Internett-relatert etterforskning innebærer hovedsakelig innhenting og sikring av informasjon fra ulike kilder på Internett. Dette kan foregå ved egenhendig sikring fra kilden direkte via Internett, utlevering fra tilbyder/besitter eller ved beslag hos tilbyder/besitter. Formålet kan være identifisering, lokalisering, dokumentasjon av handlinger, ytringer, kommunikasjon eller relasjoner eller andre operative, etterforskningsmessige eller etterretningsmessige formål.

Internett-tjenester kan ha betydning for politiets arbeid fordi de benyttes som:

- kommunikasjonsmiddel
- sted for publisering
- lagringsmedium/-plass
- hjelpemidler for å begå lovbrudd (for eksempel spredning av overgrepsbilder av barn, trusler, bedragerier, hvitvasking)
- objekt for en straffbar handling (for eksempel datainnbrudd og dataskadeverk)
- elektroniske spor, blant annet fra Internett, som kan inndeles i flere kategorier som abonnementsdata, lokaliseringsdata/posisjonsdata, trafikkdata og innholdsdata

Kripos er i ferd med å etablere en tjeneste for tilstedeværelse på Internett. Denne tjenesten eller enheten skal utarbeide et konsept for hvordan politiet i Norge bør være til stede på nett. Konseptet skal omfatte både skjult og åpen tilstedeværelse og skal, så vidt mulig, være anvendelig for politiet i alle ledd (forebygging, etterforskning, etterretning osv.).

Kripos har et overordnet nasjonalt ansvar for tilrettelegging av kommunikasjonskontroll for politiet i Norge. Det omfatter også et ansvar for å forvalte avtaler med teletilbyderne om tilretteleggingsplikten og politiets tilgang til informasjon etter kapittel 16 A i straffeprosessloven.

I tillegg til bistandsfunksjonen har Kripos ut fra definerte kriterier i påtaleinstruksen § 37 et riksdekkende ansvar som etterforsknings-, påtale- og bistandsenhet i saker som gjelder organisert og annen alvorlig kriminalitet. Dette inkluderer alvorlig datakriminalitet. I vurderingen av om en sak skal etterforskes ved Kripos, skal det blant annet legges særlig vekt på om saken er av prinsipiell karakter, om den krever utstrakt internasjonalt samarbeid eller hører naturlig inn under et politidistrikt, og/eller er særlig kompetanse- eller teknologikrevende.

Kripos er nasjonalt kontaktpunkt mot utlandet i datakrimsaker og har et tett samarbeid med både Europol og Interpol, som oppretter datakrimsentre som drivkrefter i bekjempelsen av datakriminalitet.

Politiets sikkerhetstjeneste (PST). PST er Norges innenlandske sikkerhets- og etterretningstjeneste og direkte underlagt Justis- og beredskapsdepartementet. PST er altså ikke underlagt POD slik distriktene og de andre særorganene er, men er tilsvarende underlagt Riksadvokaten i straffesakssporet. For PST er hovedmålet beskyttelse av demokratiet, borgerne og vitale samfunnsinteresser gjennom å avdekke spionasje, forebygge terror, hindre spredning av masseødeleggelsesvåpen og forebygge/forhindre trusler

mot norske myndighetspersoner[20]. Datakriminalitet er et viktig virkemiddel for trusselaktørene, alene eller i kombinasjon med andre virkemidler. Innenfor ansvarsområdet er PSTs oppgave å forebygge og etterforske straffbare handlinger i det digitale rom og i den fysiske verden.

Informasjonsinnhenting er bærebjelken både i forebyggings- og etterforskningsarbeidet. Sentralt står innsamling av informasjon om personer og grupper som kan utgjøre en trussel. Innsamlet informasjon brukes til utarbeidelse av analyser og trusselvurderinger. Hvilke metoder som kan benyttes for informasjonsinnhenting, avhenger av de konkrete sakene, og om det er forebygging eller etterforskning som er formålet.

Den høyere påtalemyndighet. Påtalemyndigheten er hierarkisk oppbygget og består av tre nivåer. Det høyeste nivået er Riksadvokatembetet, som har den overordnede ledelsen av påtalemyndigheten. Mellomnivået er statsadvokatembetene. Den høyere påtalemyndighet er en fellesbetegnelse for de ti statsadvokatregionene, Det nasjonale statsadvokatembetet, Økokrim og Riksadvokatembetet. Det tredje nivået er politiadvokatene som er integrert i politiet (se punkt 4.3.1.1), og som blant annet har ansvaret for å lede politiets etterforskning.

Riksadvokatembetet fastsetter i årlige rundskriv sentrale og landsdekkende prioriteringer for iverksettelse og gjennomføring av etterforskning. 'Alvorlig IKT-kriminalitet' har i flere år vært blant sakstypene Riksadvokaten har prioritert, jf. Rundskriv nr. 1/2014 punkt V1. Her har det vært pekt på at det sentralt kan føres saker som gjelder organisert og alvorlig kriminalitet, har internasjonale forgreninger, krever spesiell kompetanse og egnet verktøy eller er av prinsipiell karakter.

Det nasjonale statsadvokatembetet for organisert og annen alvorlige kriminalitet (NAST), underlagt Riksadvokaten, gjennomfører inspeksjoner for å kontrollere hvordan arbeidet med straffesaker innen datakriminalitet utføres ved Kripos. Inspeksjonene har de siste årene vektlagt saksutvelgelse, mengden av hendelsesstyrte saker og behovet for å prioriere kunnskapsstyrte saker.

20 'Myndighetspersoner' er definert som medlemmer av Kongehuset, Stortinget, Regjeringen, Høyesterett og representanter for andre land i Norge.

Påtalemyndighetens innsats mot datakriminalitet preges likevel av at det fortsatt er få saker som er gjenstand for straffeforfølgning, ikke minst 'alvorlig datakriminalitet'. De fleste datakrimsakene faller inn under politiets påtalekompetanse, og antall saker som behandles av Den høyere påtalemyndighet, er begrenset.

Det er kun politiadvokatene tilknyttet Kripos' Seksjon for datakriminalitet som har spesialisert kompetanse innen etterforskning av datakriminalitet. Hos Den høyere påtalemyndighet er det ingen med denne kompetansen. Statsadvokatene – i likhet med erfarne politiadvokater – har imidlertid betydelig erfaring med håndtering av elektroniske spor i ulike typer saker.

4.2.2. Andre offentlige sikkerhetsaktører

Nasjonal sikkerhetsmyndighet (NSM) er et direktorat med sektorovergripende oppgaver innen forebyggende sikkerhet, internasjonalt omtalt som 'protective security'. NSM er administrativt underlagt Forsvarsdepartementet, men rapporterer til Justis- og beredskapsdepartementet i saker som angår de sivile sektorene, og til Forsvarsdepartementet i saker som gjelder militær sektor, jf. Krpr.reg.res. av 4. juli 2003. Sjefen for NSM er Forsvarsministerens og Justis- og beredskapsministerens nærmeste rådgiver og utøver sin myndighet i spørsmål som angår forebyggende sikkerhet, blant annet datasikkerhet. Instruksen til sjefen for NSM ble gitt 9. desember 2014.

NSMs virksomhet er i hovedsak finansiert over forsvarsbudsjettet. Enkelte oppgaver, som NSM NorCERT- og VDI-funksjonen, er delfinansiert gjennom ulike former for brukerbetaling.

Forebyggende sikkerhet skal motvirke at sikkerhetstruende hendelser skader skjermingsverdig informasjon, IKT-systemer eller andre objekter. Dette kan omfatte sikkerhetstruende aktivitet som utføres med ondsinnede hensikter, inkludert datakriminalitet, gjennom utnyttelse av sårbarheter, men også ved teknisk eller menneskelig svikt eller andre tilfeldige hendelser som kan medføre lignende skadefølger. Det er det samlede risikobildet med hensyn til 'sikkerhetstruende hendelser' som legges til grunn for NSMs arbeid for å skape robusthet og håndteringsevne, ikke kriminaliteten alene. Fremmede stormakters evne til spionasje og sabotasje, samt

internasjonale terrorgruppers evne til anslag, vil være dimensjonerende for sikkerhetsarbeidet etter sikkerhetsloven og den nasjonale håndteringsberedskapen ved alvorlige datahendelser.

NSMs mest omfattende oppgave er å utøve fag- og tilsynsmyndighet overfor virksomhetene som er underlagt sikkerhetsloven. Loven regulerer beskyttelse av informasjon og objekter (blant annet datasystemer) av betydning for rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser mot spionasje, sabotasje og terrorhandlinger. Virksomhetene som omfattes av loven, er forvaltningsorganer i stat og kommune, private virksomheter som er leverandører av varer og tjenester til forvaltningen, og som i denne egenskap må ha tilgang til sikkerhetsgradert informasjon eller skjermingsverdige objekter, samt private rettssubjekter som av andre grunner er underlagt loven ved enkeltvedtak. Loven er under revisjon.

Den andre hovedoppgaven til NSM er funksjonen som nasjonal informasjonsdelings-, bistands- og koordineringsinstans for forebygging og håndtering av alvorlige dataangrep som kan ramme viktige samfunnsinteresser, den såkalte NSM NorCERT-funksjonen. NSMs rolle i konkrete hendelser vil variere etter alvorlighetsgraden, hvorvidt hendelsen favner bredt, virksomhetens egen evne til håndtering og det respektive, sektorvise responsmiljøets evne til å bistå og koordinere innenfor egen sektor. NSM oppfordrer generelt alle virksomheter som opplever hendelser som kan innebære kriminelle handlinger, til å anmelde forholdet til politiet.

Til NSM NorCERT-funksjonen ligger også forvaltningen av det nasjonale sensorsystemet Varslingssystem for digital infrastruktur (VDI). Hensikten med VDI-systemet er å gi sentrale myndigheter varsel om og mulighet for verifikasjon ved koordinerte og alvorlige dataangrep mot samfunnskritisk infrastruktur. Gjennom denne ordningen har NSM utplassert sensorer i et utvalg samfunnskritisk datainfrastruktur. Ordningen er basert på frivillighet og er regulert i egne avtaler mellom NSM og virksomhetene. Et bærende prinsipp er at disse virksomhetene 'eier' informasjon fra egne sensorer, og således har kontroll over hvordan den benyttes.

For at EOS-tjenestene skal være koordinert under håndteringen av alvorlige datahendelser, er det etablert en egen koordineringsgruppe – *Cyberkoordineringsgruppen* (CKG).

I forlengelsen av de ovennevnte oppgavene innen forebyggende sikkerhet og datasikkerhet har NSM også oppgaver og fullmakter i henhold til Nasjonalt beredskapssystem (NBS).

Forsvaret. De to avdelingene i Forsvaret som utfra sin primærfunksjon bidrar mest direkte i bekjempelsen av datakriminalitet, er Etterretningstjenesten og Cyberforsvaret.

Etterretningstjenesten er landets militære og sivile etterretningstjeneste og har et lovbestemt og sektorovergripende ansvar for å innhente og analysere informasjon om fremmede stater, organisasjoner og personer som utgjør, eller kan utgjøre, en sikkerhetstrussel for samfunnskritiske datasystemer. Etterretningstjenesten skal bidra til norske myndigheters evne til å forebygge, avverge og håndtere episoder, kriser og væpnet konflikt. Dette innebærer også ansvar for tidligst mulig varsling av forstyrrelser, kompromittering og manipulering av datasystemer som kan ramme rikets selvstendighet, sikkerhet og andre nasjonale interesser utenfor rikets grenser. Etterretningstjenesten følger primært fremmedstatlige aktører som utfører etterretningsoperasjoner, eller kan tenkes å bruke offensive nettressurser og -kompetanse i en sikkerhetspolitisk konflikt. Etterretningstjenestens ansvar er nedfelt i lov om Etterretningstjenesten av 20. mars 1998 nr. 11.

Cyberforsvaret har til oppgave å sikre, drifte og beskytte Forsvarets egne datasystemer og kommunikasjonsnettverk. I tillegg leverer Cyberforsvaret infrastruktur og tjenester til deler av statsforvaltningen, og til andre aktører med sikkerhets- og beredskapsbehov. Støtte til det sivile samfunn kan også innebære bruk av Forsvarets materiell og utstyr, personell og kompetanse i spesielle situasjoner hvor sivile myndigheters ressurser ikke strekker til, og hvor Forsvarets evne, kompetanse eller ressurser er relevante. Slik støtte vil eventuelt være regulert i *Instruks om Forsvarets bistand til politiet*. Det vises her til cyberretningslinjene for forsvarssektoren, hvor det blant annet fremgår at håndteringsbistand fra Forsvaret til det sivile samfunn i forbindelse med datahendelser, skal være koordinert med NSM. Cyberforsvarets oppgaver pålegges gjennom

stortingsvedtak og detaljeres gjennom Forsvarsdepartementets etatsstyring.

Ved håndtering av kriser knyttet til samfunnskritisk datainfrastruktur kan både Etterretningstjenesten og Cyberforsvaret få utvidede oppgaver i henhold til det nasjonale beredskapssystemet (NBS). Bestemmelser gitt i NBS vil i de tilfellene ha forrang foran bistandsinstruksen.

Nasjonal kommunikasjonsmyndighet (NKOM), kjent som Post- og teletilsynet før navneendringen i 2015, er underlagt Samferdselsdepartementet og driver tilsyn med tilbydere av post- og teletjenester. Tilsynet er i hovedsak finansiert gjennom gebyrer fra dem NKOM har tilsyn med, og ikke over statsbudsjettet.

NKOMs samfunnsoppdrag er å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester ved å legge til rette for bærekraftig konkurranse, stimulere til næringsutvikling og innovasjon samt å sikre et landsdekkende formidlingstilbud av postsendinger til rimelig pris og av god kvalitet. Dette er nedfelt i ekomloven og postloven.

NKOM skal sørge for at tjenestetilbydere får like konkurransevilkår. Markedet skal selv utvikle bærekraftig konkurranse der det er mulig, men det er også nødvendig med regulering. Hensikten er at alle som tilbyr tjenester, får konkurrere på like vilkår. I noen delmarkeder er det også nødvendig å stimulere til at små aktører skal få utvikle egen konkurransekraft.

For noen tiår siden var det svært liten konkurranse i det norske telemarkedet, mens det nå er over 200 tilbydere innen mobiltelefoni, bredbånd, fasttelefoni og så videre. Veksten har vært særlig sterk etter 2007. Telenor er, som den tidligere monopolisten i det norske telemarkedet, pålagt en rekke forpliktelser. Blant annet må Telenor slippe til konkurrenter som vil leie kapasitet i mobilnettet, og selskapet er forpliktet til å levere enkelte tjenester til alle husstander i Norge. Denne forpliktelsen er regulert i en egen avtale mellom staten og Telenor, og NKOM fører tilsyn med at Telenor oppfyller sine forpliktelser.

Oppgavene til NKOM er blant annet å

- føre tilsyn med at teleselskapene oppfyller sine forpliktelser, og sørge for at telenettene er best mulig sikret og kan stå imot både dataangrep og belastninger fra ekstremvær
- føre tilsyn etter e-signaturloven med utstedere av kvalifiserte sertifikater (fra 2001)
- føre tilsyn med sertifikatutstedere etter den frivillige selvdeklarasjonsordningen basert på kravspesifikasjonen for PKI i offentlig sektor (fra 2005)
- drive nettstedet www.nettvett.no, som gir informasjon, råd og veiledning om sikker bruk av Internett
- delta i omfattende øvingsvirksomhet for et sikrere samfunn og ha et tett samarbeid blant annet med Direktoratet for samfunnssikkerhet og beredskap (DSB)
- føre tilsyn med Posten og forvalte frekvenser og nummerressurser (inkludert IP-adresser)

Datatilsynet er både tilsyn og ombud. Datatilsynet skal medvirke til at den enkelte ikke blir krenket gjennom bruk av opplysninger som kan knyttes til ham eller henne.

Datatilsynet er et uavhengig forvaltningsorgan som er administrativt underlagt Kommunal- og moderniseringsdepartementet (KMD). Tilsynet ble opprettet 1. januar 1980. Datatilsynet har som hovedoppgave å

- kontrollere at lover og forskrifter for behandling av personopplysninger blir fulgt, og at feil og mangler blir rettet, blant annet gjennom tilsyn og saksbehandling
- holde seg orientert om nasjonal og internasjonal utvikling hva gjelder behandling av personopplysninger
- identifisere farer for personvernet og gi råd om hvordan farene kan unngås eller begrenses
- være høringsinstans i saker som berører personvern
- delta i råd og utvalg
- bistå bransjeorganisasjoner med råd og utarbeide adferdsnormer for å sikre personopplysninger i virksomhetene
- stimulere til opprettelse av personvernombud og bygge kompetanse hos ombudene
- ha en ombudsrolle overfor publikum og gi råd og informasjon, blant annet ved hjelp av nettsider, blogger og veiledere

- få viktige saker på dagsorden i media og bidra til samfunnsdebatt om personvern
- føre en offentlig fortegnelse over alle behandlinger av personopplysninger som er meldt inn til tilsynet, og behandle søknader om konsesjon

4.2.3. Private sikkerhetsaktører

Næringslivets Sikkerhetsråd er en medlemsforening uten profittformål etablert av de sentrale næringslivsorganisasjonene i Norge. Mandatet er å forebygge kriminalitet i og mot næringslivet. Bak NSR står Næringslivets hovedorganisasjon, Finans Norge, Virke, Arbeidsgiverforeningen Spekter og Norges Rederiforbund / Den Norske Krigsforsikring for Skib og Bedriftsforbundet. Virksomheten til NSR er finansiert gjennom medlemsavgift og har to fast ansatte. Foruten dette har virksomheten en rekke tillitsvalgte og deltagere i ulike utvalg, som er lønnet av egen virksomhet.

NSR representerer gjennom sine stifterorganisasjoner og medlemmer bredden i norsk næringsliv og fungerer som en samarbeidsarena for og et knutepunkt mellom næringslivet og myndighetene. Et overordnet mål for NSR er derfor å styrke bedriftenes evne til å ivareta datasikkerhet helhetlig og systematisk innenfor egen organisasjon. Søkelyset er rettet mot de grunnleggende tiltakene virksomhetene selv kan gjøre for å beskytte seg, heller enn på aktørene og risikobildet.

NSR er en privat organisasjon som ikke er tillagt myndighetsutøvelse, men som deltar i et forebyggende og utviklende arbeid og har et formalisert samarbeid med en rekke myndigheter. NSR arbeider i hovedsak med forebyggende rådgivning og veiledning til bedrifter i norsk næringsliv. Arbeidet utføres gjennom et aktivt nettverk som består av politiet og offentlige sikkerhetsmyndigheter. Hvert annet år utarbeider NSR en mørketallsundersøkelse som omfatter informasjonssikkerhet, personvern og datakriminalitet.

NSR gir både generelle og spesielle råd til næringslivet knyttet til alle former for datahendelser som kan ramme, eller som rammer, medlemsvirksomhetene. NSR veileder næringslivet generelt og medlemmene spesielt om hvor de bør henvende seg dersom de mistenker at de er utsatt for datakriminalitet.

Norsk senter for informasjonssikring (NorSIS). NorSIS arbeider for at alle skal kunne bruke Internett og data trygt på jobb og privat. Gjennom sin virksomhet er NorSIS både samarbeidspartner og pådriver overfor myndigheter og bedrifter.

NorSIS er et uavhengig tiltak som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen gjennom å

- bevisstgjøre om trusler og sårbarhet
- gi råd om sikkerhetstiltak gjennom nyheter, råd og veiledning
- påvirke til gode holdninger innen informasjonssikkerhet

NorSIS' målgrupper er innbyggerne og norske virksomheter i privat og offentlig sektor, med hovedvekt på små og mellomstore bedrifter. NorSIS samarbeider med en rekke virksomheter i informasjonsarbeidet, jobber aktivt med media, skaper møteplasser og er tilrettelegger av Nasjonal sikkerhetsmåned. Alle samfunnsgrupper og media skal kunne dra nytte av tjenestene.

En viktig del av virksomheten til NorSIS er Slettmeg.no, som er en gratis rådgivnings- og veiledningstjeneste for de som føler seg krenket på nett. Slettmeg.no har også en forebyggende rolle. Tjenesten er en aktiv deltaker i media og gir råd til barn, unge og foreldre om hvordan de best kan beskytte seg. Manglende kjennskap til lovverk er en av årsakene til at unge begår lovbrudd på nett. Manglende forståelse av konsekvensene er en annen. Her gir Slettmeg.no en direkte og aktiv hjelp som politiet, av flere grunner, ikke kan bidra med.

En annen viktig tjeneste er IDtyveri.info, som gir informasjon om hvordan man skal beskytte seg mot og hva man skal gjøre hvis man blir utsatt for ID-tyveri. Gjennom å informere om og anbefale tiltak mot ID-tyveri søker NorSIS spesielt å bidra til å begrense omfanget av svindel og krenkelser av personvernet.

NorSIS er tilrettelegger for gjennomføringen av Nasjonal sikkerhetsmåned i oktober hvert år. Hensikten med initiativet er å understøtte digitaliseringen av samfunnet. Nasjonal sikkerhetsmåned engasjerer norske virksomheter og innbyggere i tiltak for å gjøre

samfunnet mer robust mot alle former for datatrusler ved blant annet å tilby informasjon, seminarer og e-læring til offentlige og private virksomheter. I 2014 nådde NorSIS ut til 270 000 ansatte i norske virksomheter med e-læringspakken. Nasjonal sikkerhetsmåned er et viktig tiltak og verktøy for å fremme informasjonssikkerhet i Norge.

NorSIS har jevnlige møter med våre naboland via MSB[21] i Sverige, Digitaliseringsstyrelsen i Danmark og Kommunikationsverket i Finland. NorSIS samarbeider med EUs sikkerhetsorgan, ENISA[22], som koordinerer Nasjonal sikkerhetsmåned i EU. I USA har NorSIS samarbeid med Homeland Security og NCSAM. Samarbeidet vektlegger erfaringsutveksling og informasjon om gjennomføring av sikkerhetsmåneden.

Sektor-CERT. Samfunnet består av et stort antall offentlige og private virksomheter som hører inn under ulike sektorer og samfunnsområder. Disse er opprettet for å gi støtte og for å ha løpende dialog med viktige virksomheter i sektoren og NSM NorCERT. En sektor-CERT *kan* opprettes som en privat virksomhet, men ansvaret for at slike organer etableres, ligger i henhold til nasjonal strategi for informasjonssikkerhet hos det ansvarlige sektordepartementet. Det er et krav om at slike skal etableres. Hver sektor har sine leveranser, kompetansekjeder, behov og særegenheter. Etter beredskapsprinsippene om ansvar og nærhet er utgangspunktet at virksomhetene selv har ansvar for å identifisere sine verdier, ha oversikt over hendelser, foreta risikovurderinger og håndtere datasikkerhetshendelser.

For å ivareta sikkerheten er det avgjørende at alle virksomhetene sørger for tilstrekkelig teknisk og administrativ grunnsikring i henhold til gjeldende anbefalinger, blant annet gjennom styringssystemer for informasjonssikkerhet med klare ansvarsforhold og sikkerhetstiltak.

Enhver virksomhet er videre avhengig av et velfungerende samarbeid med både sektormyndigheter og nasjonale myndigheter for å beskytte seg mot alvorlige datatrusler, da kompleksiteten og avhengigheten er stor. En sektor-CERT skal bistå sin sektor med kompetanse innen datasikkerhet og ha god kjennskap til sektorens behov, verdier, infrastruktur og sårbarheter. Intensjonen er å være et ekspertorgan og et knutepunkt for informasjon og informasjonsflyt, både til og fra sektoren.

Hovedtrekk. For politiet og påtalemyndigheten, inklusive PST, utgjør datakriminalitet kun en begrenset del av den samlede kriminaliteten – riktignok av økende betydning. Mens kriminalitetsbekjempelse er en hovedoppgave for politiet og den helt dominerende oppgaven for Den høyere påtalemyndighet, utgjør den en mer avgrenset del av arbeidsfeltet til sikkerhetsaktørene som arbeider uavhengig av politiet og påtalemyndigheten. Etterretningstjenesten fremskaffer etterretning om alvorlige digitale trusler rettet mot norske myndigheter og virksomheter. NSM og NSR har datasikkerhet generelt som oppgave, hvor vern mot datakriminalitet er et viktig delaspekt.

NorSIS, derimot, er primært et spesialorgan med bekjempelse av utvalgte former for datakriminalitet som hovedoppgave. Ingen av de andre sikkerhetsaktørene har bekjempelse av datakriminalitet som hovedoppgave. Innledningsvis ble bekjempelse av datakriminalitet i likhet med annen kriminalitet delt i fire hovedoppgaver: forebygging, avdekking, stansing og straffeforfølgning. Det er bare politiet og påtalemyndigheten som arbeider med alle oppgavene. De andre sikkerhetsaktørene deltar i de tre første og kan også delta på etterforskningsstadiet under straffeforfølgning, men da i form av bistand. Påtaleavgjørelser og iretteføring er derimot politiets og påtalemyndighetens eneansvar.

4.3. Sikkerhetsaktører i utlandet

Det digitale samfunn og Internett er koblet sammen over landegrenser. Det betyr at geografisk avstand til andre land ikke er til hinder for utenlandske kriminelle som ønsker å målrette sin virksomhet mot norske ofre på nett. Politiet møter samtidig store utfordringer i straffeforfølgningen av kriminelle i andre land som utøver sin kriminelle virksomhet i Norge. Datakriminalitet er en internasjonal utfordring som krever et koordinert, internasjonalt samarbeid og informasjonsutveksling. Erfaringen viser at forskjeller i nasjonale lover, udefinerte nasjonale aktører, kapasiteter og

21 Myndigheten för samhällsskydd och beredskap https://www.msb.se/.
22 European Union Agency for Network and Information Security https://www.enisa.europa.eu/.

evne til å håndheve lovene over landegrenser skaper hindringer for effektiv straffesaksbehandling.

POD har undertegnet mange avtaler om internasjonalt samarbeid initiert på høyt politisk nivå eller i internasjonale politisjefmøter. I de neste avsnittene beskriver vi nærmere de internasjonale organisasjonene som er pådriverne i bekjempelsen av datakriminalitet.

4.3.1. Europol

Europol er EUs organisasjon for politisamarbeid innen kriminaletterretning. Den har som mål å sikre økt effektivitet og samarbeid mellom myndighetene i medlemsstatene med ansvar for å forebygge og bekjempe alvorlig internasjonal organisert kriminalitet og terrorisme. Europols oppgave er å yte et vesentlig bidrag til EUs innsats mot organisert kriminalitet og terrorisme, særlig mot kriminelle organisasjoner. Europol holder til i Haag i Nederland.

Europol skal hovedsakelig bistå politiet i medlemsstatene i arbeidet mot:

- ulovlig narkotikahandel
- nettverk for ulovlig innvandring
- terrorisme
- forfalskning av penger og andre betalingsmidler
- handel med mennesker, også seksuelle overgrepsbilder av barn
- ulovlig handel med kjøretøy
- hvitvasking av penger

Andre prioriteringer for Europol er straffbare handlinger rettet mot personer, økonomisk kriminalitet og Internett-kriminalitet hvor en organisert kriminell struktur er involvert, og to eller flere medlemsstater er berørt.

Europols bistand består i tilrettelegging av informasjonsutveksling mellom sambandspersoner – Europol Liaison Officers (ELO) – i samsvar med nasjonal lovgivning. Dette er personer som medlemsstatene har utstasjonert ved Europol, og som representerer sine ulike lands organer for rettshåndhevelse.

Europol utarbeider operative analyser til støtte for operasjoner, strategiske rapporter (trusselvurderinger) og kriminalanalyser på grunnlag av informasjon og etterretningsopplysninger gitt av medlemsstatene og tredjeland. Bistanden omfatter også ekspertrådgivning og teknisk støtte i forbindelse med etterforskning og operasjoner som gjennomføres i medlemsstatene under de berørte myndighetenes tilsyn og rettslige ansvar. Europol arbeider også aktivt med kriminalanalyse og harmonisering av etterforskningsmetoder i medlemsstatene.

Europol finansieres av medlemsstatene i henhold til deres brutto nasjonalinntekt.

Europol rapporterer til Rådet av justis- og innenriksministre i EU. Rådet har ansvar for rettlednings- og kontrollfunksjonene knyttet til Europol og utnevner direktøren og visedirektørene og vedtar budsjettet. Rådet er sammensatt av representanter for alle medlemsstatene. Kravet om at alle vedtak må være enstemmige, sikrer demokratisk kontroll med Europol. Europols styre, som består av en representant for hver medlemsstat, har som overordnet oppgave å overvåke organisasjonens virksomhet.

Ettersom internasjonal organisert kriminalitet ikke stopper ved grensene, har Europol også fremforhandlet bilaterale operative eller strategiske avtaler med andre stater utenfor EU, blant annet Norge og internasjonale organisasjoner.

Etter en studie utført av Rand Corporation Europe besluttet EU-kommisjonen å etablere et *europeisk datakrimsenter (EC3)* ved Europol. Senteret skal være navet i EUs kamp mot datakriminalitet og bidra til raskere reaksjoner ved lovbrudd på nett. Senteret skal dessuten støtte medlemsstatene og EUs institusjoner i å bygge operativ og analytisk kapasitet for undersøkelser og samarbeid med internasjonale partnere.

EC3 startet offisielt sin virksomhet 1. januar 2013. Mandatet var å bekjempe følgende områder innen datakriminalitet:

- kriminalitet begått av organiserte grupper for å generere stor kriminell fortjeneste, som for eksempel nettsvindel
- kriminalitet som forårsaker alvorlig skade på offeret, som seksuell utnytting av barn på nett
- alt som påvirker kritisk infrastruktur og informasjonssystemene i EU

Siden EC3 er underlagt Europol, kan de trekke veksler på Europols infrastruktur og nettverk for rettshåndhevelse. Senteret har på kort tid etablert seg som en

viktig aktør i bekjempelsen av datakriminalitet. Siden denne type kriminalitet ofte er grenseløs, er kompetente og effektive internasjonale organisasjoner som kan bidra i koordineringen av innsatsen, helt vesentlige. Senteret har fått stor oppslutning av EU-landene.

4.3.2. Interpol

Interpol (International Criminal Police Organization) er en internasjonal organisasjon som ble etablert i 1923 for å bidra til internasjonalt kriminalpolitisamarbeid.

Med 188 medlemsstater er Interpol verdens største internasjonale organisasjon etter De forente nasjoner. Interpol har sitt hovedkvarter i Lyon i Frankrike.

For å holde organisasjonen politisk nøytral er Interpol gjennom sin konstitusjon forhindret fra å engasjere seg i kriminalitet som ikke dekker flere land, og kriminalitet som gjelder politiske, militære, religiøse eller rasemessige forhold.

Organisasjonens arbeid er hovedsakelig rettet mot sikkerhet og terrorisme, organisert kriminalitet, narkotikaproduksjon og -handel, våpensmugling, menneskehandel, hvitvasking, overgrepsbilder av barn, økonomisk kriminalitet, høyteknologisk kriminalitet og korrupsjon.

I april 2015 åpner Interpols Interpol Global Complex for Innovation (IGCI). IGCI skal være Interpols nye satsing for å bekjempe datakriminalitet. Det skal etableres et 'Cyber Crime Center' der sentrale elementer er forskning og utvikling for identifisering av forbrytelser og forbrytere, innovativ trening, operativ støtte og partnerskap. IGCI er plassert i Singapore og forbedrer på den måten Interpols nærvær i Asia. Senteret blir etablert i splitter nye fasiliteter som sto ferdig i 2014.

Global Complex går utover den tradisjonelle, reaktive rettshåndhevelsesmodellen. Det nye senteret skal legge til rette for proaktiv forskning på nye områder og trening i de nyeste metodene. Målet er å gi politiet rundt om i verden både verktøyene og mulighetene for å møte de stadig smartere og mer sofistikerte tekniske utfordringene knyttet til bekjempelse av datakriminalitet.

Satsingsområdene er digital sikkerhet, opplæringsprogrammer og blant annet støtte til etterforskning og operasjoner gjennom å

- identifisere og analysere nye kriminalitetstrusler, for eksempel asiatisk organisert kriminalitet
- være en plattform for å identifisere ofre ved katastrofer
- utøve hendelseshåndtering og støtte ved store arrangementer
- fungere som operasjonsrom for ledelse og koordinering som forsterker operasjonsrommene som allerede er på plass i Lyon og i Buenos Aires. Tilstedeværelsen på tre kontinenter skal gi global operativ støtte til medlemslandene

4.3.3. Andre internasjonale fora

Av andre internasjonale fora kan nevnes:

- Nordisk samarbeid innen datarelatert etterforskning – *Nordisk forum* – som er en arbeidsgruppe som består av lederne eller stedfortrederne for de nasjonale datakrimenhetene i de respektive nordiske landene. Den skal blant annet utarbeide en strategisk plan for felles-nordiske aktiviteter innen datakrimetterforskning.

- ENFSI-gruppen *Forensic Information Technology,* som arrangerer årlige møter. Deltagelsen gir Norge tilgang til ressurspersoner og et bredt kontaktnett på det tekniske fagfeltet og til erfaringer og metoder fra Europa. Gruppen er også inngangsporten til tilsvarende tekniske grupper i Asia og USA.

- *Hardware Forensics* – internasjonal ekspertgruppe hvor en liten eksklusiv gruppe teknologer med spisskompetanse (uten politifaglig bakgrunn) møtes for å diskutere metodeutvikling i faget 'Hardware Forensics', som for eksempel metoder innen dypsikring av mobiltelefoner, GPS-er, knekking av passordbelagte harddisker/minnepinner, analyse av bilelektronikk og lignende. Dette er det viktigste forumet for Seksjon for elektroniske spor ved Kripos med henblikk på kompetanseheving og tilgang til verdensledende teknikker innen fagfeltet.

- ILETS – internasjonalt samarbeid om kommunikasjonskontroll og utnyttelse av elektroniske spor over landegrenser, hvor juridiske og teknologiske

utfordringer diskuteres. USA, Australia, Canada, Frankrike, Tyskland, Italia og Storbritannia deltar aktivt med representanter fra departementer og politiorganisasjoner som har ansvar for politi- og sikkerhetstjenester.

- Avtale med G8-land og Europarådet. Norge har inngått avtaler med G8-landene og Europarådet om bekjempelse av datakriminalitet gjennom Convention on Cyber Crime. Ratifiseringen av samarbeidet forplikter Norge til å følge opp avtalen. Kripos er blitt en sentral nasjonal aktør i arbeidet med å oppfylle avtalen om utnyttelse av elektroniske spor mellom Norge og andre land. I det praktiske etterforskningsarbeidet er det behov for å gå nærmere inn i de internasjonale avtalene og de politiske føringene for og tolkningene av disse for å vite hvordan vi skal opptre når Norge trenger internasjonal hjelp, og hvordan vi skal forholde oss når vi får henvendelser om bistand fra andre land.

4.4. Sikkerhetsaktørenes trusselvurderinger

Nasjonal sikkerhetsmyndighet (NSM) vurderer den nasjonale sikkerhetstilstanden og i den forbindelse de forebyggende tiltakene som sikkerhetsloven oppstiller. NSMs oppdrag innebærer å produsere et IKT-risikobilde. Fra og med 2014 skal NSM i henhold til sitt mandat rapportere om datarisikobildet for så vel statssikkerhet som for samfunns- og individsikkerhet.

Politidirektoratet (POD) vurderer fortløpende det samlede kriminalitetsbildet. Kripos står for utarbeidelsen av vurderingen.

I tillegg til offentlige myndigheters vurderinger utgir også en rekke private sikkerhetsfirmaer erfaringsbaserte vurderinger som er relevante for norske forhold.

Næringslivets Sikkerhetsråd (NSR) har dessuten i en årrekke gjennomført og publisert resultatene av den såkalte Mørketallsundersøkelsen. Den supplerer i stor grad de ovennevnte nasjonale myndighetenes og private firmaenes vurderinger.

Aktørenes metode og analysemåte varierer og baseres ikke alltid på unike og uavhengige analyser. Sikkerhetsaktører henter mye informasjon fra hverandre.

Vurderinger av trusler fra utenlandske aktører om handlinger som kan true vesentlige samfunnsinteresser, gjøres av Etterretningstjenesten. Totalvurderinger av sikkerhetstrusler som spionasje, sabotasje, terrorisme og så videre gjøres av Politiets sikkerhetstjeneste.

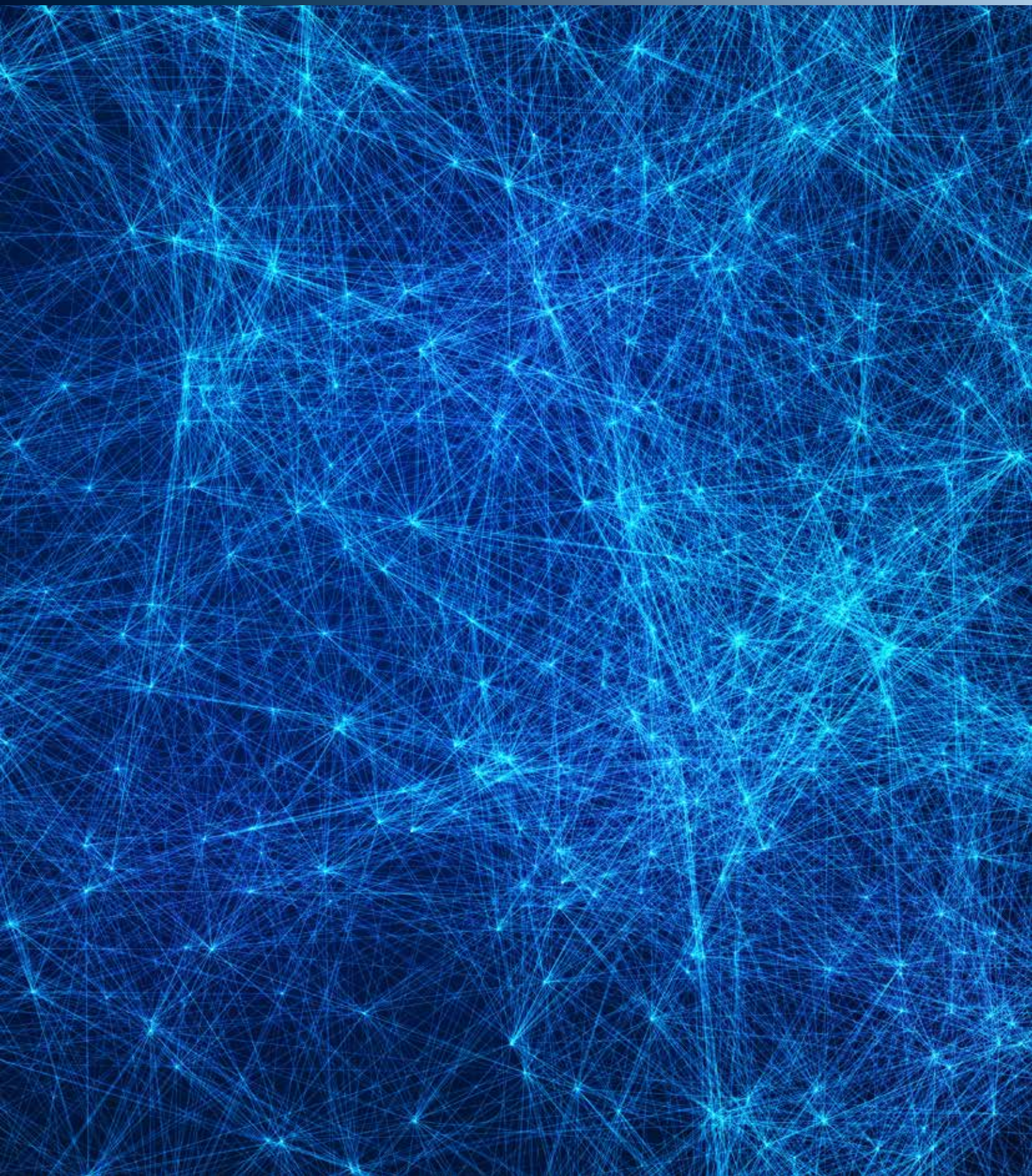
Kriminalitet er i økende grad et internasjonalt fenomen. Dette gjelder særlig datakriminalitet, hvor trusselaktørene og ofrene ofte befinner seg i ulike land, og hvor både de uønskede handlingene og virkningene av dem kan skje i en virtuell og grenseløs verden.

Hovedhensikten med en nasjonal trusselvurdering er å se truslene i sammenheng med det som kan ramme Norge. Siden datakriminalitet utøves uten landegrenser, er det grunn til å tro at kriminalitetsbildet på dataområdet internasjonalt ligner på situasjonen her, og at trusler som har fremkommet i andre land, også kan ramme Norge. Det kan derfor være høyst relevant å trekke inn tilgjengelige vurderinger gjort utenfor Norge.

I andre land gjøres trussel- og risikovurderinger med relevans for datakriminalitet av stort sett de samme organene som i Norge. Det eksisterer i tillegg en rekke internasjonale organer med særlig ansvar for sikkerhet og kriminalitetsbekjempelse som utgir vurderinger basert på grunnlagsinformasjon fra medlems- eller deltakerland. Norske myndigheter samarbeider i stor grad med så vel enkeltland som internasjonale organer, og deres/våre vurderinger vil derfor i mange tilfeller være influert av resultatene av dette samarbeidet.

Del 3

Overordnede strategier for bekjempelse av datakriminalitet



5. Utfordringene og strategier i andre land

5.1. Sikkerhetsaktørenes syn på utfordringene

5.1.1. Innledning

Hvilke utfordringer står man overfor i kampen mot datakriminalitet? Kapittel 3 redegjør for trusselen slik sikkerhetsaktørene oppfatter den i dag. I kapittel 4 har strategigruppen gitt en oversikt over sikkerhetsaktørene og deres oppgaver. Det sentrale spørsmålet ved utforming av en nasjonal strategi er imidlertid hvor godt det eksisterende apparatet av sikkerhetsaktører er i stand til å møte trusselbildet nå og i fremtiden. Hvilke utfordringer står Norge overfor?

Det er flere måter å besvare dette spørsmålet på. En viktig innfallsvinkel for strategigruppen har vært sikkerhetsaktørenes egne vurderinger av utfordringene; en annen hvordan utfordringene er blitt bedømt i tidligere utredninger. Datakriminalitetens internasjonale karakter betyr dessuten at mange andre land står overfor tilsvarende utfordringer som Norge, utfordringer som de har planlagt tiltak mot. Det pågår også et utstrakt internasjonalt samarbeid om bekjempelsen.

Slike erfaringer er nyttige utgangspunkter for strategigruppens egne vurderinger og forslag, og derfor redegjøres det for dem i dette kapittelet. I kapittel 6–11 analyseres og avveies dette materialet mot strategigruppens egne observasjoner fra en rekke studiebesøk og annen informasjon innhentet som grunnlag for forslagene til visjon og hovedstrategier. Her gis det også ytterligere informasjon om utfordringene som ledd i diskusjonen av hver enkelt strategi.

5.1.2. Sikkerhetsaktørenes vurderinger

Som ledd i utredningsarbeidet har strategigruppen innhentet egenvurderinger av utfordringene knyttet til bekjempelse av datakriminalitet fra de sentrale sikkerhetsaktørene. Egenvurderingene ble inngitt i et spørreskjema hvor respondentene ble bedt om å gi sitt syn på hva de anså som de viktigste utfordringene. Svarene oppsummeres i det følgende.

Politidirektoratet (POD). Utnyttelse av ny teknologi til kriminalitet, gjennom blant annet nettskyer og sosiale medieplattformer, anonyme nettverk og virtuelle valutaordninger, stiller nye krav til politiet. Kriminelle aktiviteter i dagens digitale samfunn er komplekse og krysser ofte landegrensene, i tillegg til at potensielle bevis har kort levetid og er spredt over flere jurisdiksjoner og land. Disse utfordringene krever et bredt nasjonalt og internasjonalt politisamarbeid samt partnerskap og engasjement mellom offentlig og privat sektor. Tradisjonelt og nytt, kunnskapsbasert politiarbeid med bruk av nye teknologiske verktøy og tekniske ferdigheter må kombineres.

Det er behov for et enda tettere samarbeid mellom politiet, PST, NSM og Forsvaret. I alvorlige hendelser og kriser må politiet og NSM iverksette raske og overstyrende tiltak rettet mot tjenestetilbydere og nasjonal kommunikasjonsinfrastruktur.

POD ønsker en bedre rolleavklaring og et tettere samarbeid med Nasjonal kommunikasjonsmyndighet (NKOM) for å kunne handle med nødvendig effektivitet og kvalitet i slike situasjoner. Samarbeidet mellom politiet, PST, NSM og Forsvaret vil møte utfordringer gjennom sikkerhetsloven og begrensninger knyttet til utveksling av taushetsbelagt informasjon. Hvis offentlige aktører ikke er seg sitt ansvar og sine oppgaver bevisst, gir det grobunn for usikkerhet og mer konkurranse i stedet for samarbeid i akutte situasjoner. Uklare og overlappende ansvarsområder i det digitale rom kan gjøre at offentlige aktører går «i beina på hverandre» og på den måten forstyrrer hverandre i arbeidet.

POD mener at det eksisterende samarbeidet mellom myndighetsorganer og andre aktører om bekjempelse av datakriminalitet stort sett er godt. Det eksisterer imidlertid en viss usikkerhet knyttet til politiets rolle ved alvorlige hendelser og kriser i den digitale verden. POD mener at politiet må utøve den samme rollen i både den digitale og den fysiske verden.

Ved en bedre samordning av den totale innsatsen er det fullt mulig å oppnå en bedre og mer effektiv bekjempelse av datakriminalitet. Dette gjelder både

for politiet og for andre offentlige og private aktører. POD mener man bør vurdere tydeligere sentraliserte funksjoner og en bedre arbeidsdeling mellom aktører og operative miljøer, slik flere land har gjort.

Rapporteringen av datakriminalitet er mangelfull, og det finnes ikke tilfredsstillende rapporteringssystemer for datakriminalitet, verken i politiet eller mellom de andre aktørene. POD ønsker derfor økt rapportering og at man eventuelt ser nærmere på muligheten for å pålegge ved lov at datakriminalitet av en viss alvorlighetsgrad skal rapporteres inn. EU vurderer nå å innføre et slikt lovpålegg.[23]

Årlig utarbeider POD trendrapporter for kriminalitet i Norge, også om trusler og utvikling tilknyttet datakriminalitet. Rapportene baserer seg på de operative trusselvurderingene fra Kripos. Det kan være behov for en samlet, årlig trusselvurdering der offentlige og private aktører kommer med innspill.

POD mener det er for lite nasjonal forskning, utdanning og kunnskapsutvikling knyttet til forebygging og bekjempelse av datakriminalitet, og at det er behov for økt innsats. Politiet bør i tillegg øke sin evne til innsamling, behandling og deling av informasjon som kan hindre alvorlige hendelser på dette feltet.

Den raske utviklingen innen datateknologi setter gjeldende lovverk under press. Nye handlinger som klart er uønskede, vil, blant annet på grunn av legalitetsprinsippet, verken kunne forebygges eller straffeforfølges fordi de ikke dekkes av gjeldende lovverk.

POD er bekymret for effektiviteten og kvaliteten på politiets arbeid mot datakriminalitet. Politiet har for liten kapasitet, mangelfull kompetanse samt for dårlig tilgang på teknologi, dataverktøy og metodikk.

På grunn av datakriminalitetens raske utvikling står politiet og påtalemyndigheten overfor svært komplekse og kompetansekrevende saker. Metoder og verktøy endres raskt, straffesaker vil ofte behandles ulikt, og datatekniske undersøkelser og elektroniske spor vil kunne tolkes på forskjellige måter.

POD har observert at politidistriktene i økende grad er opptatt av datakriminalitet og utnyttelse av elektroniske spor i alle typer kriminalitet. Bevisstheten om datakriminalitet er likevel lav, og bare et fåtall saker blir etterforsket. Det er i hovedsak Kripos som etterforsker og påtaler alvorlige saker samt saker med spesielle krav til kompetanse og verktøy. Kripos har kapasitet til å etterforske og iretteføre to til fem saker med alvorlig datakriminalitet årlig. Det dreier seg da om saker tilknyttet datainnbrudd, dataangrep og skadeverk samt bruk av datateknologi ved nettbankbedrageri. I tillegg tar Kripos inn saker som gjelder besittelse og formidling av seksuelle overgrepsbilder på Internett.

Politiet utfører i liten grad forebyggende arbeid og mangler systematiske metoder og verktøy for etterretningsarbeid som kan sette dem i stand til å avdekke, etterforske og straffeforfølge større saker. De vanligste formene for datakriminalitet som rammer mange Internett-brukere i det daglige, blir ofte henlagt fordi politiet ikke har ressurser til å prioritere dem. Det er ofte vanskelig å angi tapets størrelsesorden og hendelsens alvorlighetsgrad. Ofrene henvender seg derfor til andre aktører, enten før de anmelder saken til politiet, eller når den er henlagt. Datatilsynet og NorSIS er blant aktørene som hjelper i slike saker. De bistår med å hindre eller stoppe videre konsekvenser av uønskede hendelser på nettet (ubehagelige bilder, uriktig informasjon osv.).

Kripos foreslår å styrke samarbeidet om bekjempelse av datakriminalitet mellom relevante virksomheter både nasjonalt og internasjonalt. Særlige utfordringer i så måte er kapasitetsproblemer og manglende klargjøring og oversikt over hvem som har ansvar for hva. Kripos mener det er behov for en kartlegging av roller og ansvarsfordeling mellom myndighetsorganer og andre aktører på nasjonalt nivå.

Det er et problem at rapporteringssystemene ikke er spesielt tilpasset rapportering av datakriminalitet, og det er vanskelig å få ut gode statistikker. Kripos antar imidlertid at det er enklere for dem å rapportere om datakriminalitet enn for andre virksomheter.

En av hovedutfordringene er de presumptivt store mørketallene som er knyttet til datakriminalitet. Få saker anmeldes, og de sakene som anmeldes, er ofte av mindre alvorlig karakter. Datakriminalitet er i mange tilfeller ekstra vanskelig å etterforske og iretteføre, særlig internasjonalt og særlig når den er knyttet til land som ikke prioriterer internasjonal bekjempelse av datakriminalitet. Lovverk og rettstradisjoner er

23 EU-direktiv: Network and Information Security IP/13/94.

ulike, og samarbeidet mellom de forskjellige landene fungerer ikke alltid like godt.

En annen hovedutfordring er at mange virksomheter bekymrer seg for omdømme og økonomiske kostnader dersom de blir utsatt for datakriminalitet. Det kan i en del tilfeller knytte seg indirekte kostnader til det å anmelde en sak, og det hender gjenopprettelse av normal drift prioriteres før bevissikring. Kripos opplever ofte at virksomheter mangler ressurser til forebygging og bekjempelse av datakriminalitet.

Politiets sikkerhetstjeneste (PST). En oppsummering av datatrusler fra PSTs åpne trusselvurdering for 2015 viser en økning i avlytting og nettverksbaserte etterretningsoperasjoner fra fremmede stater eller grupperinger med sterk tilknytning til stater. Man ser også økt radikalisering over Internett, hvor mer lukkede fora og reduserte geografiske barrierer gir nye utfordringer. En rekke forsøk på nettverksbasert etterretning tilsier en økt trussel på dette området, både for stats- og bedriftshemmeligheter. Alle etterretningstjenester med globale ambisjoner gjennomfører omfattende digitale etterretningsoperasjoner. En rekke land har i løpet av de siste årene utviklet en svært omfattende etterretningskapasitet i det digitale rom, med vide juridiske og politiske fullmakter. Mange stater bruker store ressurser på etterretningstjenestene og lar informasjonen spille en vesentlig rolle i beslutningskjeden.

Vi finner samme type aktiviteter i den digitale som i den fysiske verden. Trusselbildet mot Norge og norske interesser inneholder digitale trusler i tillegg til tradisjonelle trusler. Ordinær kriminalitet, alvorlig kriminalitet samt mellomstatlige kriser og konflikter vil i fremtiden ha fremtredende digitale elementer.

PST ønsker å samle bevis og drive etterretning i det digitale rom som i det fysiske rom. I den fysiske verden har PST et bredt spekter av metoder for å hente inn informasjon for etterretningsformål; det samme gjelder bevisinnhenting når tjenesten driver etterforskning. I det digitale rom er ikke lovhjemlene for dette tilsvarende utviklet, og vår evne til å beskytte grunnleggende nasjonale interesser og den enkelte borger er langt svakere. Det må etableres et reelt og fungerende myndighetsnærvær i det digitale rom for å beskytte både nasjonen og borgerne. Fordi myndighetene har vært fraværende, har det vokst frem kommersielle aktører som håndterer trusler, men med begrenset kontakt med myndighetene.

Det digitale rommet er globalt og stiller særskilte krav til samarbeid og informasjonsutveksling. De aller fleste trusler og problemstillinger er transnasjonale og krever internasjonalt samarbeid i tillegg til betydelig samarbeid og koordinering nasjonalt. Det må utvikles nasjonale samarbeidsplattformer som er robuste nok til å støtte håndteringen av et bredt spekter av digitale trusler og situasjoner.

Påtalemyndigheten ønsker å styrke egen kompetanse innen behandling av datakriminalitet. Så langt har få slike saker vært gjenstand for straffeforfølgning. Det har nok vært flere saker der datateknologi brukes som redskap for tradisjonell kriminalitet (seksuell utnyttelse av barn på nett, ytringer med hatefullt eller voldelig innhold over nett mv.). De fleste sakene håndteres av påtalemyndigheten i politiet, slik at statsadvokatenes erfaring med datakriminalitet trolig er enda mer begrenset.

Behovet for økt kompetanse gjelder både for etterforskningsfasen og iretteføringen for domstolen, i tillegg til bedre kjennskap til gjeldende regelverk. Videre bør det utredes hvor hensiktsmessig og effektiv den gjeldende kriminaliseringen er, og hva som bør gjøres for at lovverket til enhver tid er tilpasset kriminalitetsutviklingen.

Det er behov for å styrke samarbeidet med sikkerhetsaktører både nasjonalt og internasjonalt. Erfaringen med datakriminalitet så langt – for eksempel fra Kripos' etterforskning av nettbankbedragerier – viser at det ofte dreier seg om grensekryssende virksomhet, der trusselaktørene gjerne opererer i land som det kan være krevende å oppnå et effektivt samarbeid med (blant annet Russland og Ukraina).

Nasjonal sikkerhetsmyndighet (NSM). Også NSM har behov for å samarbeide med andre for å løse sine oppgaver, dette gjelder særlig i randsonen av deres ansvar og i problemstillinger som engasjerer flere myndighetsaktører. NSMs oppgave er å være en nasjonal sektorovergripende aktør til støtte for en god forebyggende sikkerhet i virksomhetene. Sikkerhetstruende hendelser er ikke synonymt med kriminelle handlinger, men begrepet dekker også slike handlinger. I NSMs defensive sikkerhetsoppgaver er

det derfor berøringspunkter mot politiets forebygging og etterforskning av kriminalitet, og NSM kan betegnes som en viktig sikkerhetsaktør med betydning også på kriminalitetsområdet.

Berøringspunktene maner til strukturert samhandling. NSM har registrert et ønske fra politiet om mer informasjonsdeling og økt synergieffekt gjennom tettere samhandling. Det har NSM forståelse for, men påpeker behovet for å ta hensyn til det tette samarbeidet om sikkerhet som er bygget opp gjennom flere år mellom de nasjonale sikkerhetsmyndighetene, virksomheter med ansvar for kritisk datainfrastruktur og sektormyndigheter. NSM ser i den forbindelse at det kan oppstå konflikter mellom alminnelig forebygging og etterforskning. NSM NorCERTs samarbeid med offentlige og private aktører er basert på frivillighet og en forutsetning om en strengt formålsbegrenset bruk av den informasjonen som mottas. I denne konteksten kan en omfattende informasjonsdeling med politiet være problematisk, og vil ikke kunne utføres uten informasjonseierens generelle eller konkrete samtykke. Spørsmål om ressurser til NSM er en del av styringsdialogen med FD og JD. Finansieringsmodellen knyttet til NorCERT-funksjonen og VDI er under diskusjon – endringer vil kunne få betydning for kvaliteten på det nasjonale datasikkerhetsarbeidet og dermed også for NSMs evne til å motvirke datakriminalitet.

Datatilsynet avdekker gjennom sitt tilsynsarbeid manglende kjennskap til de pliktene som gjelder internkontroll og informasjonssikkerhet – noe som gjør både samfunnet som helhet og den enkelte av oss sårbare overfor trusler. Det bør derfor settes inn målrettede tiltak for å høyne beredskapen mot kompromittering av personopplysninger og andre beskyttelsesverdige opplysninger. Tiltak for å beskytte personopplysninger mot eksterne eller interne trusler vil som regel samtidig være å anse som gode personverntiltak. I dagens samfunn, med økt bruk av digitale løsninger og økt trusselnivå, er personvernet under press fra både trusselaktører og sikkerhetsaktører. Datatilsynet søker å finne balansen mellom personvern og kriminalitetsbekjempelse, som her stort sett er to sammenfallende interesser.

Noen tiltak for å forebygge og bekjempe kriminalitet vil innebære en økt overvåkning og kontroll fra myndighetenes side, noe som kan utfordre personvernet. Personvernet tar utgangspunkt i den enkeltes rett til å eie og kontrollere opplysninger om seg selv. Denne selvbestemmelsen er imidlertid ikke absolutt. Hensynet til samfunnets interesser vil i noen tilfeller veie tyngre enn hensynet til den enkeltes personvern. Dette er særlig tydelig innen justissektoren. Her står den enkeltes individuelle interesser ofte i sterk kontrast til tunge samfunnsinteresser, slik som kriminalitetsbekjempelse og samfunnssikkerhet.

Datatilsynet er særlig opptatt av at de mest inngripende tiltakene må ha hjemmel i lov fastsatt av Stortinget, samt at sentrale prinsipper som proporsjonalitetsprinsippet og prinsippet om formålsbestemthet etterleves.

Metodekontrollutvalget ble opprettet i 2008, og i NOU 2009: 15 gis det en bred og grundig gjennomgang av en lang rekke inngripende etterforskningsmetoder. Datatilsynet mener utvalgets forslag burde vært bedre fulgt opp av departementet. Evaluering av personverninngripende etterforskningstiltak er svært viktig, og alle metoder bør være målrettede slik at de virker etter sin hensikt. Dersom en metode ikke har den forventede effekt, bør den oppheves.

Etterretningstjenesten (E-tjenesten). E-tjenesten er i for stor grad avhengig av samarbeidende utenlandske tjenester, og har i for liten grad mulighet til å drive egen innsamling og analyse. Trusselaktørene må følges over lang tid. E-tjenestens fremste ambisjon bør være å bygge opp en tilstrekkelig evne til å jobbe selvstendig, for å styrke grunnlaget for samarbeid med andre lands tjenester og nasjonalt bidra til at generell og spesifikk trusselinformasjon kan distribueres og anvendes på en sikkerhetsmessig forsvarlig måte.

Cyberforsvaret har behov for bedre og raskere tilgang på relevant trusselinformasjon og signaturer som identifiserer skadevare. Lovverk, praksis og nasjonal arbeidsdeling er ikke innrettet mot håndtering av flyktige og grensekryssende trusler. Myndighetsorganer og samfunnskritiske virksomheter mangler systemer og rutiner for formidling, behandling og oppbevaring

av gradert informasjon som er aktuell i denne sammenhengen. Norge har et umodent planverk for håndtering av kriser knyttet til samfunnskritisk datainfrastruktur, og en revisjon av det nasjonale beredskapssystemet (NBS) er trolig nødvendig. Bruk av NBS er særlig aktuelt ved et koordineringsbehov på tvers av de normale ansvarslinjene, eller når det er behov for særlige hjemmelsgrunnlag for å iverksette tiltak.

Næringslivets Sikkerhetsråd (NSR). NSR arbeider for et forsterket privat-offentlig samarbeid for bedre å kunne forebygge og bekjempe datakriminalitet. Samarbeid vil gi økt læring og kompetanse, og samlet styrke den nasjonale kapasiteten i det forebyggende arbeidet gjennom en bedre utnyttelse av de samlede ressursene. Taushetsplikt og manglende lovhjemler for deling av informasjon er to av flere hovedutfordringer ved etablering av et tettere operativt samarbeid på tvers av både private og offentlige virksomheter.

Ut over dette er hovedutfordringene for NSRs arbeid knyttet til det faktum at 93 % av norske virksomheter har færre enn ti ansatte, og særlig en del ledere synes å mangle kompetanse innenfor informasjonssikkerhet og datakriminalitet. Funn i Mørketallsundersøkelsen[24] viser at over halvparten av de spurte virksomhetene tjenesteutsetter hele eller deler av datadriften uten å stille krav om sikkerhet til leverandørene. Mange virksomheter vet ikke om, eller på hvilken måte, de er utsatt for hendelser.

NSR er av den oppfatning at både myndighetene og virksomhetene i for stor grad har fokusert på trusselbildet, og for lite på gode og enkle tiltak. Virksomhetene vet i mange tilfeller heller ikke til hvem, og i hvilke tilfeller, de skal rapportere om mulige kriminelle handlinger. NSR har observert at mange i det private ønsker å kunne rapportere uønskede datahendelser til én enkelt aktør. De er imidlertid opptatt av at rapporteringen må være frivillig og basert på tillit mellom den som rapporterer, og den det rapporteres til. NSR får i dag utrettet mye med sine begrensede ressurser. Aktivtetsnivået de senere årene har imidlertid økt betydelig sett i forhold til bemanningen, blant annet kommer det flere forespørsler om privat-offentlig samarbeid innenfor informasjonssikkerhet.

Norsk senter for informasjonssikring (NorSIS). NorSIS mener at mulighetene for rapportering av datakriminalitet er mangelfulle og lite kjent i virksomhetene. De største utfordringene ved forebygging og bekjempelse av datakriminalitet er knyttet til at mange virksomheter ikke tar sikkerheten på alvor og ikke tror at sikkerhetshendelser vil ramme akkurat dem. NorSIS har erfart mangelfull kompetanse innen datasikkerhet i virksomhetene og generell lav kompetanse og stor naivitet i befolkningen.

NorSIS peker også på at politiet og påtalemyndigheten mangler kompetanse og teknologi for å kunne håndtere den økende mengden av datakrimsaker. NorSIS opplever også utfordringer ved utilstrekkelig eller manglende koordinering av nasjonale informasjonssikkerhetsressurser. I tillegg er det en ubalanse mellom de store ressursene enkelte av trusselaktørene disponerer, og de ressursene virksomheter og privatpersoner bruker for å beskytte seg mot truslene. NorSIS opplever at hovedårsaken til dette er manglende risikoerkjennelse hos ledelsen i virksomhetene. Informasjonssikkerhet når derfor ikke opp på agendaen. Befolkningen opplever på sin side at det er teknisk komplisert å beskytte seg.

For å kunne forebygge datakriminalitet mer effektivt peker NorSIS på viktigheten av at myndighetene bidrar i finansieringen av Slettmeg.no. Dette er en tjeneste som når bredt ut og som også kan øke innsatsen innen forebygging og veiledning. I dag finansieres denne tjenesten fullt ut av NorSIS selv.

NorSIS ser at antall identitetstyverier øker, og de får flere henvendelser fra brukere som har vært utsatt for forskjellige typer svindel på Internett. I tillegg innser flere virksomheter at de har behov for hjelp til å øke sin egen sikkerhet.

5.1.3. Noen andre utfordringer

Strategigruppen har også merket seg enkelte andre utfordringer blant sikkerhetsaktørene:

Endringer i kriminaliseringen. Et effektivt straffe-rettslig vern mot uønskede datahandlinger forutsetter

24 NSR. *Mørketallsundersøkelsen 2014:* http://www.nsr-org.no/moerketall/.

en oppdatert straffelovgivning. De siste årene har fremveksten av sosiale medier (Facebook, Twitter osv.), utbredelse av trådløse nett, bruk av apper på smarttelefoner og nettbrett og så videre gitt nye muligheter for kriminelle. Lagring av ulike typer digital informasjon i nettskyer hvor som helst på nettet, også utenfor landets grenser, gir økt risiko for uønskede datalekkasjer og spredningsmuligheter.

Dataverktøy og tvangsmidler i etterforskning av datakriminalitet. Politiet benytter i økende grad dataverktøy og tvangsmidler i etterforskningen. Mange dataverktøy er ikke spesielt utviklet mot datakriminalitet, selv om noen er det. På tilsvarende måte kan tvangsmidler være nødvendige redskaper i etterforskningen av datakriminalitet så vel som i etterforskning av andre former for kriminalitet. Et spørsmål her er om redskapene som hjemles av straffeprosesslovgivningen i dag, er tilstrekkelige for en effektiv bekjempelse av datakriminalitet, eller om det er behov for nye virkemidler. Dette gjelder også for elektroniske spor, som blir stadig viktigere i etterforskning av alle former for kriminalitet.

Datasikkerhet og datakriminalitet. Det er politiets og påtalemyndighetens ansvar å straffeforfølge datakriminalitet. Sikkerhetsaktører som ikke hører til politiet eller påtalemyndigheten, skal primært avdekke og stanse trusler mot datasikkerheten, fjerne sikkerhetshull og gjenopprette normal drift dersom en angriper lykkes i å trenge inn i eller skade datasystemer. Trusselen vil bli håndtert ut fra en vurdering av dens faktiske skadevirkninger. NSM vil imidlertid kunne gi støtte ved straffeforfølgning på anmodning fra PST og politiet. Sikkerhetsaktørene, herunder NSM, kan ikke på egen hånd initiere en etterforsking hos politiet. Dessuten vil straffeforfølgning i liten grad være en prioritert oppgave for sikkerhetsaktørene. For politi og påtalemyndighet vil det derimot ofte være mindre interessant å utrede uklare datatrusler der sikkerhetsaktørene ikke gir den nødvendige informasjonen som kan benyttes i straffeforfølgningen.

Gjennomgående gir vurderingene uttrykk for at etterforskning og straffesaksoppfølging i datakrimsaker i for stor grad er hendelsesstyrt og i for liten grad kunnskapsstyrt. Kapasiteten er under kritisk størrelse, og det er liten evne til å utvikle og gå inn i store og alvorlige saker. I dagens situasjon vil det være vanskelig å bistå NSM og foreta etterforskning ved større angrep på nasjonal infrastruktur. Politiets manglende tilstedeværelse på Internett påpekes.

5.2. Nasjonale rapporter av betydning for strategien mot datakriminalitet

5.2.1. NOU 2000: 24 (Willoch-utvalget) – Et sårbart samfunn

Willoch-utvalget så nærmere på utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet. Det ble også fokusert på utviklingen innen informasjons- og kommunikasjonsteknologi, med særlig vekt på at alle IKT-systemer er i konstant fare for å bli angrepet. Utvalget foreslo en overordnet målsetting for arbeidet med IKT-sårbarhet og kritisk infrastruktur. Det var behov for å *øke robustheten* i IKT-infrastrukturen til et nivå som gjør det helt usannsynlig at viktige samfunnsfunksjoner stanses i en normalsituasjon. I en krisesituasjon skal robustheten være tilstrekkelig til å opprettholde kritiske funksjoner.

Utvalget pekte på at det var stort behov for informasjonsutveksling mellom private og offentlige aktører, og at det i kritiske situasjoner er viktig med rask varsling og informasjonsutveksling mellom aktørene. Det ble påpekt behov for tiltak som skulle bedre rutinene for overvåking, varsling og håndtering av sikkerhetshendelser mellom virksomheter, og som på den måten ville øke varslingsevnen. Willoch-utvalget påpekte også at det var behov for økt satsing innen kompetanse, utdanning og forskning, og det anså det som en klar utfordring for myndighetene å utvikle relevante og slagkraftige juridiske rammeverk som står i forhold til det tempo i samfunnsutviklingen som datateknologien skaper.

For å realisere en «strategi for å redusere samfunnets IKT-sårbarhet» ble det foreslått følgende tiltak:

- etablering av Senter for informasjonssikring
- økt innsats på forskning og utvikling
- styrket utdanning og kompetanse

- risiko- og sårbarhetsanalyser
- gjennomgang av behovet for lover, regler og insentiver
- etablering av et IKT-tilsyn og styrking av sertifiseringsarbeidet

5.2.2. Meld. St. 7 (2010–2011) Kampen mot organisert kriminalitet – en felles innsats

Den organiserte kriminaliteten representerer store og til dels nye utfordringer, den ser ut til å være i vekst, og innsatsen mot organisert kriminalitet må derfor intensiveres. Ett av områdene i meldingen var knyttet til datakriminalitet som en del av den organiserte kriminaliteten. Der pekte en på at Internett og bruk av datateknologi generelt er et økende problem i kriminalitetsutviklingen. Den organiserte datakriminaliteten blir vanskeligere å avdekke, samtidig som kriminalitetsbekjempelsen forutsetter betydelig tilgang på teknologikunnskap og infrastruktur hos politiet. Organiserte kriminelle miljøers økende bruk av datatjenester omfatter stadig nye typer tjenester på Internett, ofte tilknyttet sosiale medier og nettverk. Den organiserte kriminaliteten foregår i det skjulte.

Elektroniske spor og digitale bevis vil således ha avgjørende betydning for etterforskningen. Bevisbildet har høy kompleksitet, og bevisene kan ofte være teknologisk utfordrende å fremskaffe, bearbeide og presentere. Etterforskningen kompliseres ytterligere av at mange kriminelle benytter krypteringstjenester. Politiet må, gjennom metodeutvikling, settes i stand til å håndtere denne formen for bevis på en tilfredsstillende måte. Mulighetene for å begå kriminalitet på Internett har ført til et klart behov for at politiet er til stede på nettet, både åpent og skjult, enten ved spaning eller infiltrasjon. Politiet mangler imidlertid de nødvendige tekniske løsningene for spaning og etterretning på Internett.

5.2.3. Nasjonal strategi for informasjonssikkerhet[25] med handlingsplan

Nasjonal strategi for informasjonssikkerhet ble lansert av regjeringen 17. desember 2012. Den er tverrfaglig og utpeker og klargjør ansvaret for IKT-sikkerhet i Norge på alle nivåer.

Strategien utpeker prioriteringer og angir målbeskrivelser for disse i tillegg til statusbeskrivelser og en redegjørelse for hvilke områder som skal vektlegges fremover. De overordnede målene som er satt av regjeringen, er:

1. Styrket samordning og felles situasjonsforståelse
2. Robust og sikker IKT-infrastruktur i hele samfunnet
3. Sterk evne til å håndtere uønskede datahendelser
4. Høy kompetanse og sikkerhetsbevissthet

Regjeringens overordnede mål for informasjonssikkerhetsarbeidet veier alle like tungt og må virke sammen for å oppnå den ønskede tilstanden.

De overordnede målene skal operasjonaliseres gjennom sju strategiske prioriteringer:

- ivaretagelse av informasjonssikkerheten på en mer helhetlig og systematisk måte
- styrking av IKT-infrastrukturen
- felles tilnærming til informasjonssikkerhet i statsforvaltningen
- sikring av samfunnets evne til å oppdage, varsle og håndtere alvorlige datahendelser
- sikring av samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet
- kontinuerlig innsats for bevisstgjøring og kompetanseheving
- høy kvalitet på nasjonal forskning og utvikling innenfor informasjons- og kommunikasjonssikkerhet

Strategigruppen for bekjempelse av datakriminalitet ble oppnevnt for å følge opp den femte strategiske prioriteringen, som skal sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet.

Hvordan regjeringen skal følge opp strategiens utvalgte områder, fremgår av en detaljert handlingsplan for informasjonssikkerhet.[26] Handlingsplanen er delt i to, med en utfyllende beskrivelse av sikkerhetsutfordringer og trender samt et utvalg

25 http://www.regjeringen.no/nb/dep/jd/dok/rapporter_planer/planer/2012/nasjonal-strategi-for-informasjonssikker.html?id=710469.

26 http://www.regjeringen.no/nb/dep/jd/dok/rapporter_planer/planer/2012/handlingsplan---nasjonal-strategi-for-in.html?id=710471.

av tiltak. Følgende temaer er relevante for strategigruppens arbeid og vil på flere punkter gjenspeiles i hovedstrategiene:

- 5.1 Om styrking av politiets arbeid med forebygging og bekjempelse av Internett-relatert kriminalitet
- 5.3 Om oppfølging av kartlegging vedrørende politiets håndtering av datakriminalitet
- 5.4 Om å forebygge og avdekke kriminalitet på Internett – utredning av tipstjeneste
- 5.6 Effektiv lokal forebygging av datakriminalitet

5.2.4. Politiet i det digitale samfunnet[27]

Politidirektoratet opprettet i samråd med Riksadvokaten i april 2011 en arbeidsgruppe for å kartlegge politiets arbeid med datakriminalitet, elektroniske spor og politioppgaver på nett, samt for å vurdere hvordan det skal arbeides med disse områdene fremover. I rapporten gjøres det rede for status i politidistrikter og særorgan, og det gis anbefalinger om hvordan politiet kan arbeide med elektroniske spor, datakriminalitet og politioppgaver på nett.

Arbeidsgruppen ble nedsatt fordi datakriminalitet utgjør en stadig større trussel. Det var ønske om større politinærvær på Internett, samt behov for å se på arbeidsfordelingen mellom politidistriktene og særorganene og hvilken kompetanse som trengs for å løse oppgavene.

Rapporten redegjør kort for den teknologiske utviklingen og bruken av Internett. Den forklarer også begrepet 'elektroniske spor' og sier litt om hvor ofte slike spor forekommer. I tillegg beskriver den utviklingen av datakriminalitet, politiets arbeid med disse områdene og politiets mulighet til å utnytte elektroniske spor, bekjempe datakriminalitet og utføre politiarbeid på Internett fremover.

Rapporten peker på en rekke utfordringer som strategigruppen søker å løse gjennom den nye strategien for bekjempelse og forebygging av datakriminalitet.

5.2.5. Meld. St. 21 (2012–2013) Terrorberedskap[28]

Stortingsmeldingen beskriver nasjonal krisehåndtering og forholdet til alvorlige datahendelser. Den kom som en oppfølging av *NOU 2012: 14 Rapport fra 22. juli-kommisjonen*. I meldingen legger regjeringen frem en overordnet strategi for å forebygge og håndtere terror i Norge og mot norske interesser og nordmenn i utlandet.

Trusselbildet på Internett beskrives ut fra en terror- og radikaliseringssynsvinkel. Internett er i dag en viktig arena for offentlige diskusjoner og ytringer. Internett brukes imidlertid også som verktøy av terrorister til å spre deres ideologi, ved bruk av nettsteder for å distribuere propaganda og rettferdiggjøre aktiviteter. Internett er derfor en viktig arena for kontakt mellom eksisterende medlemmer av terrorgrupper og deres bidragsytere, for rekruttering, radikalisering og forberedelse til terrorhandlinger. Den alvorligste trusselen i det digitale rom mot norske interesser kommer fra andre stater.

I Meld. St. 21 ønsker man å beskytte samfunnets IKT-sikkerhet gjennom oppfølging av Nasjonal strategi for informasjonssikkerhet og den tilhørende handlingsplanen. For å sikre håndteringen vil regjeringen forankre beredskapsinstruksen i en ny lov om Forsvarets bistand til politiet og forsterke innsatsen mot terrorangrep utført ved hjelp av IKT. Det kan også nevnes at etter 22. juli-kommisjonens rapport bør det bli en økt satsing på bruk av IKT i politiet og hos andre sentrale aktører innen samfunnssikkerhet og beredskap. For å avverge terror skal det arbeides med å videreutvikle samarbeidet mellom E-tjenesten, PST og NSM. Se også *Meld. St. 29 (2011–2012) Samfunnssikkerhet*.

5.2.6. NOU 2009: 15 Skjult informasjon – åpen kontroll[29]

Metodekontrollutvalgets utredning har to overordnede temaer: politiets bruk av skjulte tvangsmidler og behandling og beskyttelse av informasjon i straffesaker. Utvalget ble for det første bedt om å foreta en etterkontroll av reglene om nye etterforskningsmetoder, som ble innført i 1999. Utvalget ble også bedt om å foreta en bred vurdering av hvorvidt målene med innføringen av de skjulte tvangsmidlene er nådd, deres ressurskrav og samlede effekt, samt å vurdere om det er behov for endringer i kriteriene for bruk eller for å innføre ytterligere metoder.

27 https://www.politi.no/vedlegg/rapport/Vedlegg_1866.pdf.
28 http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2012-2013/meld-st-21-20122013.html?id=718216.
29 http://www.regjeringen.no/en/dep/jd/dok/nouer/2009/nou-2009-15.html?id=569379.

Ifølge mandatet skulle utvalget «utrede og foreslå regler som tillater politiet å ta i bruk dataavlesing som metode i etterforskningen». Slike regler er så langt ikke vedtatt.

5.2.7. PBS I – Politiets beredskapssystem del I – Retningslinjer for politiets beredskap[30]

Politiets beredskapssystem (PBS) er fundamentet for en enhetlig og effektiv håndtering av så vel ordinære som ekstraordinære hendelser og kriser. Systemet skal blant annet bidra til en koordinert planlegging og innsats. Den viktigste forutsetningen for å lykkes i felles oppgaveløsning er at beredskapsaktørene har god kunnskap om hverandres roller og ansvar.

Et viktig formål med PBS I, foruten å gi retningslinjer for politiets beredskapsarbeid, er å beskrive de forskjellige beredskapsaktørenes rolle og ansvar når kriser oppstår. Formålet er å ha en felles plattform for innsatsen som er gjenkjennelig uavhengig av hvilket politidistrikt som er involvert.

På samme måte er det lagt opp til et beredskapssamarbeid mellom politi, kommuner og andre aktører. Dette skal bidra til å klargjøre ansvarsområder og ansvarliggjøre aktørene med hensyn til type hendelse, hendelsesforløp og tiltak. Informasjonsutveksling og felles situasjonsforståelse er viktige premisser for god, felles oppgaveløsning. Også innenfor beredskapsfaget må det arbeides etter kunnskapsbaserte mønster.

Under PBS-ens punkt 2.3 er det oppsummert eksempler på hendelser som kan være ekstraordinære. I tillegg til opplagte hendelser som bombetrussel, terroranslag, gisselsituasjon og så videre er også «omfattende avbrudd i viktige funksjoner som elektrisitets- og vannforsyning, data og radio- og telekommunikasjon» nevnt som eksempler på mulige ekstraordinære hendelser.

Alt nasjonalt beredskapsarbeid bygger på de overordnede prinsippene om ansvar, likhet og nærhet.

5.3. Utvalgte strategidokumenter fra andre land

Norge har i stadig større grad utviklet seg mot en «kunnskapsøkonomi» der ideer, kreativitet og innovasjon må beskyttes. Lovgiverne ønsker å gjøre Internett til et så trygt sted som mulig og sørge for at folk kan benytte nettet for informasjonsdeling, kunnskapsdeling og ytringsfrihet, samtidig som man i størst mulig grad unnslipper skade og/eller fare.

Myndighetene i mange land har etter hvert erkjent at de har en plikt til å beskytte sine borgere og interesser mot datakriminalitet.[31]

Selv om spørsmål omkring informasjon, datateknologi og datakriminalitet har vært av interesse en tid, er det først de senere årene at nasjonale myndigheter har tatt inn over seg betydningen av datasikkerhet og gjort det til et politisk spørsmål. I denne sammenheng var angrepene mot Estland i 2007[32] av stor betydning og medførte at spørsmål tilknyttet datasikkerhet og datakriminalitet rykket høyt opp på de fleste lands politiske agenda. Som en følge av dette vedtok mange land datasikkerhetsstrategier, og det vises i denne sammenheng til oversikten som European Network of Information Security Agency (ENISA) har utarbeidet over National Cyber Security Strategies in the World[33].

5.3.1. Konsepter og strategier

Utgangspunktet for de fleste datasikkerhetsstrategier er at de setter politiske mål, foreslår tiltak og fordeler institusjonelt ansvar. Dette gjøres for å sikre konfidensialitet, integritet og tilgjengelighet til elektroniske data og datasystemer, og for å beskytte mot tilsiktede og ikke-tilsiktede hendelser og angrep. Ofte ser man at beskyttelse av kritisk informasjonsinfrastruktur prioriteres høyt.

Enkelte datasikkerhetsstrategier inneholder også tiltak mot datakriminalitet. Strategier og tiltak mot datakriminalitet er knyttet til kriminalitetsforebygging og kriminalpolitikk, og skal også bidra til rettssikkerhet og å fremme menneskerettighetene.

Det er ingen tvil om at strategier for datasikkerhet og datakriminalitet henger nøye sammen. De har overlappende interesser, men er ikke identiske – datasikkerhetsstrategier løser ikke alle datakrimproblemer, og en datakrimstrategi løser ikke alle datasikkerhetsproblemer. Det er derfor nødvendig

30 https://www.politi.no/vedlegg/rapport/Vedlegg_1690.pdf.

31 http://www.europarl.europa.eu/document/activities/cont/201210/20121016ATT53718/20121016ATT53718EN.pdf.

32 http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia: Angrepene mot Estland var en serie dataangrep som startet 27. april 2007 og hadde utgangspunkt i en uenighet mellom nasjonale estiske myndigheter og den russiske minoriteten i landet om flytting av en minnestatue fra 2. verdenskrig. De fleste angrepene som var merkbare for allmennheten, var såkalte tjenestenektangrep.

33 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

å utarbeide konkrete datakrimstrategier, enten som selvstendige strategier eller som deler av datasikkerhetsstrategier.[34]

Det er allmenn aksept for at dataangrep særlig rettet mot kritisk infrastruktur kan true viktige samfunnsfunksjoner og i verste fall rikets sikkerhet. Som en konsekvens av dette ser man at mange datasikkerhetsstrategier er knyttet til nasjonale sikkerhets- og forsvarsstrategier. Datasikkerhetsstrategiene prioriterer derfor også beskyttelse av kritisk informasjonsinfrastruktur og særlig offentlige datasystemer mot ikke-tilsiktede hendelser, samt robust beskyttelse mot målrettede angrep.

Det er de målrettede angrepene som synes å være den primære bekymringen, og det fokuseres ofte på tekniske, prosessuelle og institusjonelle tiltak for å forhindre og stanse slike angrep. Man ser også at politiet, påtalemyndigheten og domstolene sjelden nevnes i de ulike datasikkerhetsstrategiene. Tekniske virksomheter og løsninger har en tendens til å komme i forgrunnen.

Tiltak som ofte foreslås i strategier for å bekjempe datakriminalitet, omfatter for eksempel styrking av lovgivningen (blant annet global harmonisering), operativ politikapasitet, kompetanseheving innenfor politi og rettsvesen, tverrfaglig samarbeid, privat og offentlig samarbeid samt internasjonalt samarbeid.

5.3.2. Europarådet – Cyber Crime Strategies

Europarådet har i sitt arbeid med Global Project on Cyber Crime utgitt en rapport med fokus på 'Cyber Crime Strategies'.[35] Strategien skal følge opp en rekke temaområder som omfatter:

- implementering og videre utvikling av Budapestkonvensjonen om datakriminalitet[36]
- kapasitetsbygging og styrking av evne til å bekjempe datakriminalitet
- beskyttelse av barn mot utnyttelse av seksuelle overgrepsbilder på nett
- radikalisme på Internett
- standardiserte prosedyrer for å håndtere elektroniske bevis over landegrenser og internasjonalt samarbeid
- fokus på forebygging og bekjempelse av datakriminalitet vil synliggjøre riktige tiltak og virkemidler
- justismyndigheten og påtalemyndigheten bør ha en ledende rolle i utviklingen av datakriminalitetsstrategier

Budapestkonvensjonen er den første internasjonale avtalen som søker å løse problemstillinger knyttet til Internett-bruk og datakriminalitet ved harmonisering av nasjonale lover, bedre etterforskningsmetoder og økende samarbeid mellom nasjoner. Konvensjonen er også den første internasjonale traktaten vedrørende forbrytelser begått via Internett og andre datanettverk. Hovedformålet med konvensjonen er å arbeide for en felles kriminalpolitikk som tar sikte på å beskytte samfunnet mot nettkriminalitet, spesielt ved å vedta hensiktsmessig lovgivning og fremme internasjonalt samarbeid.

Konvensjonen ønsker økt harmonisering av straffe- og straffeprosessuell lovgivning om datakriminalitet og på denne måten legge grunnlaget for raskt og effektivt internasjonalt samarbeid. Artikkel 15 i Budapestkonvensjonen pålegger landene å finne en balanse mellom statens plikt til å beskytte folk mot kriminalitet, og behovet for å kontrollere og begrense rettshåndhevelsen. De grunnleggende rettsprinsippene i denne sammenheng er legalitetsprinsippet[37] (EMK art. 7 og SP art. 15), rettferdig rettergang og uskyldspresumsjonen (EMK art. 6 og SP art. 14). Enhver innblanding av myndighetene i borgernes rettigheter kan bare skje i den grad de samsvarer med lovgivningen og er nødvendige i offentlighetens interesse. Dette gjelder også forebygging av kriminalitet eller beskyttelse av andres rettigheter (EMK art. 8). I praksis må derfor undersøkende (etterforskende) tiltak fastsettes ved lov.

Forholdsmessighetsprinsippet krever at det skal være et rimelig forhold mellom et inngrep (og en eventuell straff), gjerningspersonens skyld og grovheten av den begåtte handlingen. Dette følger også av Budapestkonvensjonen artikkel 15 (3). Jo mer

34 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf.
35 http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf.
36 http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?CL=ENG&NT=185.
37 http://lovdata.no/dokument/NL/lov/1999-05-21-30/KAPITTEL_emkn-1#emkn/a6.

datasikkerhet anses som et spørsmål av nasjonal interesse, desto større er risikoen for at datasikkerhet fjernes fra den strafferettslige arena. Det er da fare for at fokuset på rettssikkerhet og menneskerettigheter blir svekket.

Konvensjonen drøftes nærmere i kapittel 8 om kriminaliseringsstrategi.[38]

5.3.3. EU Cyber Security Strategy

Et fritt og åpent Internett er kjernen i EU Cyber Security Strategy. Dette ønsket støttes av et lovforslag for å styrke informasjonssystemene i EU.

Hovedmålet med strategien er å komme med klare prioriteringer for EUs internasjonale politikk som omfatter det digitale samfunn, grunnleggende rettigheter og et fritt og åpent Internett. Lover, normer og EUs kjerneverdier skal gjelde i den digitale som i den fysiske verden, og ansvaret for et sikrere nettsamfunn ligger hos alle som deltar i det, fra individer til regjeringer. EU skal sammen med internasjonale samarbeidspartnere og organisasjoner, privat sektor og det sivile samfunn også bidra til å støtte global kapasitetsbygging i tredjeland. Det inkluderer å bedre tilgangen til informasjon og til et åpent Internett, samt å hindre datatrusler. Å bevare et åpent, fritt og trygt digitalt samfunn der frihet og grunnleggende rettigheter gjelder, er en global utfordring. EU ønsker å bidra til dette i samarbeid med relevante internasjonale samarbeidspartnere og organisasjoner, privat sektor og det sivile samfunn.

EU støtter arbeidet med å definere normer for oppførsel i det digitale samfunn. På samme måte som det forventes at borgerne respekterer sine samfunnsplikter, sosiale ansvar og lover på nettet, så må også statene overholde normer og gjeldende lover.

EU vil ikke støtte nye traktater og konvensjoner som vil kunne bidra til å begrense ytringsfriheten og tilgangen til informasjon. Ifølge EU inneholder Budapestkonvensjonen tilstrekkelige elementer til å støtte etterforskning, påtalemyndigheter og internasjonalt samarbeid i arbeidet mot datakriminalitet. EU bistår Europarådet med formidling av konvensjonen over hele verden.

EU vil bygge videre på sitt engasjement med internasjonale samarbeidspartnere og organisasjoner, privat sektor og det sivile samfunn for å støtte global kapasitetsbygging i tredjeland.

EU anser det å bevare det digitale samfunn åpent, fritt og trygt som en global utfordring, og vil samarbeide med de relevante internasjonale samarbeidspartnere og organisasjoner, privat sektor og det sivile samfunn for å oppnå dette. EU legger vekt på dialog med tredjeland og internasjonale organisasjoner, med et spesielt fokus på likesinnede partnere som deler EUs verdier. Bilateralt er samarbeidet med USA spesielt viktig, og det vil bli videreutviklet.

Når det gjelder EUs felles sikkerhets- og forsvarspolitikk, er Det europeiske forsvarsbyrået (EDA) støttet av EUs medlemsstater i å utvikle digitale forsvarsevner og teknologier i tillegg til å bedre den digitale forsvarstreningen og gjennomføre øvelser. Siden truslene har mange likheter, skal synergier mellom sivile og militære tilnærminger til beskyttelse av viktige digitale funksjoner styrkes. Dette arbeidet må støttes av forskning og utvikling, og tettere samarbeid mellom myndigheter, privat sektor og akademia i EU er nødvendig. EU vil også arbeide for å involvere industrien og akademia i utvikling av løsninger samt i å styrke Europas forsvarsindustribase og innovasjoner i både sivile og militære organisasjoner. Samarbeid mellom EU og NATO pågår kontinuerlig og skal sikre effektive forsvarsevner, identifisere områder for samarbeid og bidra til å unngå dobbeltarbeid.

5.3.4. Nederland

I Nederland er det nå Cyber Strategy 2 fra 2013 som gjelder. Denne følger opp den tidligere Netherlands' National Cyber Security Strategy fra 2011, noe som også er symbolisert ved at den første strategien hadde tittelen *From ignorance to awareness*, mens Cyber Strategy 2 har fått tittelen *From awareness to capability*.

Nederland har erkjent at arbeidet for datasikkerhet og mot datakriminalitet er et kontinuerlig arbeid, og strategiene må løpende oppdateres. Årlige fremdriftsrapporter skal derfor utarbeides.[39]

Når det gjelder bekjempelsen av datakriminalitet, legger Cyber Strategy 2 særlig vekt på offentlig og privat samarbeid, nettverks- og koalisjonsbygging,

38 Se punkt 8.2.3.

39 https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html

rolleavklaring, styring av kompetanse og kapasitet mv. Nederland har bygd opp en kombinert datakriminalitets- og datasikkerhetsstrategi som tilsynelatende er solid forankret og på kort tid har styrket evnen til bekjempelse av datakriminalitet. Nederland er langt bedre rustet enn Norge på dette området, og flere av hovedstrategiene som vil bli omtalt senere, er inspirert av de nederlandske strategiene.

Det kan i denne sammenhengen særlig nevnes at i den første strategien, fra 2011, var det særlig fokus på å intensivere etterforskning og straffeforfølgning av datakriminalitet. Den andre utgaven følger opp de strategier og tiltak som man startet med i 2011, og har økt fokus på å oppdatere internasjonalt juridisk rammeverk. Datakriminalitet er lagt inn på en nasjonal prioriteringsliste. Cyber Strategy 2 definerer også et mål for den nederlandske High Tech Crime Unit og de enkelte distriktene ved å stille krav om minimum 20 større etterforskninger per år ved hver enhet.

5.3.5. Storbritannia

Den britiske Cyber Security Strategy[40] skiller seg fra de fleste andre tilsvarende strategier. Frem til juni 2011 var Storbritannia ett av svært få land som ikke bare hadde en Cyber Security Strategy (fra 2009), men også en egen Cyber Crime Strategy (2009), slik Norge nå også legger opp til. Disse ble imidlertid erstattet av den nye strategien i november 2011 med tiltak både for datasikkerhet og mot datakriminalitet.

Strategiens visjon er at Storbritannia i 2015 skal utvikle store økonomiske og sosiale verdier fra et levende, spenstig og sikkert digitalt samfunn. Her skal tiltak ledet av kjerneverdier som frihet, rettferdighet, åpenhet, rettssikkerhet, forbedret velstand og nasjonal sikkerhet gi et sterkt samfunn.

Det er fire hovedmål som skal nås innen 2015. Storbritannia skal for det første håndtere nettkriminalitet og være ett av de sikreste stedene i verden å gjøre forretninger digitalt. For det andre skal Storbritannia bli mer motstandsdyktig mot dataangrep og bedre rustet til å beskytte sine interesser på nettet. For det tredje skal Storbritannia bidra til å utvikle et åpent, stabilt og levende digitalt samfunn som det britiske publikum kan bruke trygt, og for det fjerde skal Storbritannia utvikle tverrfaglig kunnskap og ferdigheter for å understøtte landets datasikkerhetsmål.

Det er utarbeidet til sammen 24 tiltak for å gjøre Storbritannia til ett av de sikreste stedene i verden å gjøre forretninger digitalt. Menneskerettigheter og rettssikkerhet vektlegges spesielt og skal ivaretas ved hjelp av eksplisitt angitte kriterier.

5.3.6. Finland

Finlands Cyber Security Strategy[41] angir de viktigste mål og retningslinjer som skal brukes for å svare på trusler mot det digitale samfunn, og for å sikre deres funksjoner.

Den finske datasikkerhetsstrategien er en del av den nasjonale sikkerhetsstrategien. Strategien vil dekke praktiske tiltak som danner grunnlaget for strategiske retningslinjer og gjennomføringen av disse. Dette gjelder også tverrgående tiltak i samfunnet.

Visjonen for Finlands datasikkerhet er å sikre vitale funksjoner mot datatrusler i alle situasjoner. Borgere, myndigheter og virksomheter skal effektivt kunne utnytte et trygt digitalt samfunn og den økte kompetansen som følger av datasikkerhetstiltak, både nasjonalt og internasjonalt. Finland skal innen 2016 være et foregangsland innen beredskap mot datatrusler og i håndtering av forstyrrelser forårsaket av disse truslene.

Oppfølgingen av Finlands datasikkerhet baserer seg på at regjeringen har hovedansvaret og at departementene har sektoransvar. Prinsippene fra samfunnssikkerhetsstrategien skal legges til grunn, og datasikkerheten er avhengig av at informasjonssikkerhet gjennomføres i hele samfunnet og bygger på et tverrsektorielt samarbeid. Implementering av datasikkerhet forutsetter gjensidig deling av informasjon. Dette krever også drift av et nasjonalt cybersikkerhetssenter med en døgnkontinuerlig sikkerhetsovervåkning. Myndighetenes mulighet for rask handling forutsetter at datasikkerhet anses som en del av nasjonal beredskap og øvelser. Det skal videre investeres i forskning, utdanning, utvikling og lovgivning som støtter oppunder sikkerhetsstrategien.

40 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

41 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf.

5.3.7. USA

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World[42] er utgitt av The Executive Office of the President (EOP)[43] og er første forsøk på å samle den amerikanske regjeringens visjon for det digitale samfunn i ett dokument. Strategien omfatter mål for forsvaret, diplomatiet og den internasjonale utviklingen. Strategien beskriver USAs samarbeid med internasjonale partnere for å finne løsninger på alle datateknologiske utfordringer, inkludert nettkriminalitet.

Den amerikanske regjeringens grunnprinsipper, grunnleggende friheter, personvern og fri flyt av informasjon gjenfinnes i strategien. Samtidig ønsker man å beskytte sikkerheten til nasjonale nettverk.

Istedenfor å innføre en global styringsstruktur, anbefaler strategien å skape internasjonale normer for adferd og styrke interoperabiliteten[44].

Strategien skisserer enkelte prinsipper som det fremheves at alle nasjoner bør støtte, hvorav den ene er beskyttelse mot kriminalitet. Det er en forventning om at andre nasjoner skal identifisere og straffeforfølge kriminelle og i praksis nekte kriminelle å ha frihavner. I tillegg bør landene samarbeide i internasjonal etterforskning.

Forebygging, etterforskning og rettsforfølgelse av nettkriminalitet skal forbedres gjennom samarbeid innenfor rettshåndhevelse og rettssikkerhet. For å oppnå dette skal USA delta i utviklingen av en internasjonal datakrimpolitikk, blant annet ved å oppfordre andre land til å ratifisere Budapestkonvensjonen, målrette datakrimlovgivningen mot bekjempelse av ulovlige aktiviteter istedenfor å begrense tilgangen til nettet samt hindre at Internett utnyttes av terrorister og kriminelle som ønsker å planlegge, finansiere eller utføre ondsinnede aktiviteter.

Det overordnede målet med strategien er å øke USAs nasjonale og multilaterale evne til å bekjempe datakriminalitet. Strategien tar for seg datakriminalitet i en bredere forståelse av begrepet 'datasikkerhet' ('Cyber Security').

5.4. Oppsummering: Hovedtrekk i andre lands strategier

'Offentlig-privat samarbeid' går igjen i internasjonale strategier og er et sentralt satsingsområde. Det legges vekt på å opprette effektive samarbeidsmodeller mellom offentlige myndigheter og andre aktører som arbeider for datasikkerhet både nasjonalt og internasjonalt. Deling av relevant informasjon synes å være svært nødvendig for å bekjempe datakriminalitet.

I motsetning til i for eksempel Russland og Kina er det i de land Norge samarbeider med, et mål å satse på å bekjempe kriminalitet heller enn å begrense tilgangen til nettet. Et annet sentralt moment i flere strategier er at man erkjenner behov for en internasjonal datakrimpolitikk for å forhindre kriminelle frihavner og legge grunnlag for at så mange land som mulig samarbeider i internasjonale etterforskninger.

På den forebyggende siden ser man et sterkt fokus på å øke den alminnelige forståelsen av datasikkerhet i befolkningen generelt, for å sikre en økt bevissthet om truslene som eksisterer.

Erkjennelsen av at de datateknologiske truslene og datakriminaliteten øker, har ført til at mange land ønsker å sørge for tilstrekkelig evne til å forebygge, avdekke og oppklare datakriminalitet. Dette gjelder ikke bare for politiet og påtalemyndigheten, men for alle relevante samfunnsaktører.

Gjennomgående ser man en klar internasjonal forståelse for, og erkjennelse av, at innførte strategier må følges opp og stadig fornyes i takt med kommende trusler og situasjoner. Videreutvikling av strategiene er derfor ofte et eget satsingspunkt.

Gjennomgang av ulike lands strategier avdekker enkelte hovedtrekk som ofte går igjen, og som også har vært etterlyst i Norge. Sammen med erfaringer fra studiebesøk i Nederland, Storbritannia og USA har dette gitt ideer til flere av strategiene og tiltakene som foreslås.

42 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
43 http://www.whitehouse.gov/administration/eop.
44 http://en.wikipedia.org/wiki/Interoperability – 'Interoperabilitet' er produkters, systemers eller forretningsprosessers evne til å arbeide sammen for å løse en felles oppgave. Termen kan defineres rent teknisk eller bredt, hvor man inkluderer sosiale, politiske og organisatoriske faktorer.

6. VISJON FOR BEKJEMPELSE AV DATAKRIMINALITET

6.1. Hvilke hensyn bør visjonen ivareta?

6.1.1. Visjon og trussel

En overordnet nasjonal strategi bør ha et mål – en visjon om en ønsket tilstand som strategien skal sikre. En visjon for bekjempelse av datakriminalitet bør ta utgangspunkt i trusselens alvor. Hvilke samfunnsinteresser trues, og hvor viktige er de? Og hva slags tilstand ønsker vi å ha for databruk?

Databruk involverer vesentlige verdier på nær sagt alle samfunnsområder – offentlig virksomhet, næringsliv, samfunnsliv, frivillig virksomhet og privatliv. Datateknologi innebærer også store muligheter for forbedring av kommunikasjonsprosesser og analyse på nær sagt alle livs- og samfunnsområder. Den skaper handlingsrom som gir muligheter for økonomisk vekst, større velstand og velferd både fra et samfunnsmessig og et individuelt perspektiv. Samfunnet bør derfor verne databruk og datautvikling mot uforsvarlig og destruktiv virksomhet.

Datakriminalitet representerer nettopp en slik trussel. Datakriminaliteten skader den eksisterende databruken. Den vil også redusere verdien av de *nye* handlingsrommene som skapes gjennom den digitale utviklingen, og kan hindre effektiv bruk av disse. Den kan også hemme selve innovasjonsprosessen fordi risikoen for misbruk kan redusere viljen til å investere kompetanse, tid og ressurser i å utvikle og forbedre dataverktøy.

Datautviklingen gir derfor ikke bare nye handlingsrom for *ønsket* aktivitet. Dataverktøy kan også benyttes til kriminalitet eller annen destruktiv virksomhet. Særlig organiserte kriminelle kan være interessert i dette for å begå både tradisjonell kriminalitet og datakriminalitet. Samfunnet bør aktivt motvirke denne typen 'kriminell innovasjon' og holde den på et nivå som ikke i vesentlig grad hindrer utnyttelsen av datateknologiens samfunnsnyttige sider.

6.1.2. Visjon og samfunnsverdier

Strategien bør ivareta samfunnsverdier som det er bred enighet om er viktige. Strategigruppen vil særlig peke på følgende:

Brukerne og samfunnsnytten. Visjonen bør knyttes til krav om trygg og sikker databruk – at alle brukere skal kunne utnytte datateknologien på lovlige måter uten å bli utsatt for skadelige datahandlinger. Risikoen for ulovlig tilegnelse av datahemmeligheter fra lovlige eiere og brukere samt bruk av data til uønskede og skadelige formål bør være så liten at den ikke bremser samfunnsutviklingen. Trygg bruk av data bør være et samfunnsgode på linje med goder som rett til helse, forbrukervern, å eie formue og eiendom og å drive næringsvirksomhet.

I slike brede risikovurderinger vil reduksjon av datakriminalitet bli ett av mange virkemidler mot uønskede datahandlinger, og bekjempelse av datakriminalitet må ses i forhold til hvor effektive andre virkemidler er – som teknologiske sikkerhetssystemer, offentlige krav til og kontroll av datasikkerhet, opplæring i selvbeskyttelse osv.

Visjonen kan inneholde elementer som ligner andre lands datakrimstrategier. I flere tilfeller er visjonene basert på ideen om at landets innbyggere, virksomheter og myndigheter i fremtiden skal ha tillit til at det finnes trygge, sikre og robuste datasystemer.

Redusert datakriminalitet. Visjonen kan også knyttes mer direkte til forekomsten og oppklaringen av

datakriminalitet. Datakriminaliteten bør ligge på et lavt nivå. Kriminalisering, forebygging, avverging, oppklaring og sanksjonering må sikre dette.

Visjonen og straffetrusselens preventive virkning må ses i nær sammenheng. Ingen skal kunne begå datakriminalitet uten betydelig risiko for straff. Men selv om effektiv straffeforfølgning er viktig for straffetrusselens troverdighet, er ikke nødvendigvis et høyt sanksjonsnivå et hovedmål. Forebygging og avverging bør være viktige deler av visjonen.

Straffesystemets aktører må samordne sin aktivitet med andre sikkerhetsaktører. Lovgivningen bør harmoneres i takt med utviklingen. Når datatrusselen endrer seg, bør straffebestemmelsene oppdateres.

Beskyttelse av kritisk infrastruktur. Beskyttelse av kritisk infrastruktur er først og fremst en utfordring for virksomhetene, dernest for sektormyndighetene og de øvrige sikkerhetsmyndighetene. Men slike angrep vil også være alvorlig datakriminalitet som bør straffeforfølges. Dette kan være krevende, og utfordringene er mange. Selv om hovedansvaret ligger hos sikkerhetsmyndighetene, bør politiet tidlig inn for å gjøre strafferettslige vurderinger av hendelsen og sikre relevante bevis.

Rettssikkerhet og menneskerettigheter. Mens en sikkerhetstilnærming først og fremst skal avverge trusler og reparere skader, vil en strafferettslig tilnærming ha som formål å påføre utøvere av datakriminalitet straff. Her må strafferettslige rettssikkerhetsgarantier ivaretas. For å sikre effektive sikkerhetstiltak og straffeforfølgning kan det oppstå behov for overvåkning, kontroll og andre inngrep i den enkeltes integritet og privatsfære som reiser viktige spørsmål om personvern og individets menneskerettsvern. Både utformingen og bruken av inngrepshjemlene må være gjenstand for demokratisk kontroll.

Internasjonal orientering. Nær sagt alle aktuelle former for datakriminalitet bygger på teknologi som er internasjonal. De straffbare handlingene er også internasjonale. Handlingsmønstrene er de samme i ulike land. De kan også ramme ofre i forskjellige land samtidig. Utøveren av handlingen befinner seg ikke nødvendigvis i samme jurisdiksjon som ofrene. Det samme kan gjelde for datautstyret som benyttes.

Datakrimstrategien må vektlegge kriminalitetens internasjonale karakter og erkjenne at effektiv bekjempelse bare er mulig med et omfattende, fleksibelt og nært samarbeid med alle land som kan bidra. Arbeidsgruppen ser en sterk internasjonal orientering som en grunnpremiss i en strategi for en bedre bekjempelse av datakriminalitet enn den vi har i dag.

6.2. Ambisjonsnivå

Et viktig spørsmål er hva slags ambisjonsnivå en strategi mot datakriminalitet bør ha.

Internasjonalt har Norge lav anmeldt datakriminalitet, og en kan derfor spørre seg om det er nødvendig med en større satsing. Det lave anmeldelsesnivået kunne tolkes som et tegn på at Norge ligger langt fremme innen bekjempelse, og at vi gjør det meste riktig slik datakriminaliteten fremstår i dag. I praksis tolereres noe kriminalitet på de fleste samfunnsområder. En mulig visjon kunne være å anse dagens situasjon som tilfredsstillende, nøye seg med tiltakene som allerede er iverksatt, og avvente utviklingen før en eventuelt setter i verk nye tiltak. Men få – om ingen – vestlige land har trukket en slik konklusjon. Det er skadepotensialet, trusselen, som er hovedbegrunnelsen for en omfattende satsing, se punkt 5.3. Visjonen for den norske satsingen bør også ta utgangspunkt i skadepotensialet. Norge antas å være blant de landene i verden som er mest utsatt for datakriminalitet. Vi råder over verdier som er fristende for kriminelle, og den utbredte bruken av data i befolkningen gir gode muligheter for å begå datalovbrudd. Mørketallene er store, se nærmere under punkt 7.3.1 om skjult kriminalitet. Ut fra analysene i del 2 må det antas at datakriminaliteten og skadevirkningene vil øke betydelig i tiden fremover om vi ikke iverksetter nye og mer effektive tiltak enn i dag.

En vesentlig styrking av innsatsen må til for å redusere risikoen for en negativ utvikling. Det bør ha betydning for strategiens ambisjonsnivå. Visjonen bør være realistisk, men også ambisiøs nok til fortsatt å holde kriminaliteten nede. Strategien må være gjennomtenkt og målrettet. Det hjelper lite om innsatsen økes, dersom tiltakene ikke er effektive.

Et Norge uten datakriminalitet er en utopi i overskuelig fremtid. Analysene i kapittel 3 viser at straffeforfølgningen av dagens datakriminalitet er lite effektiv. Et realistisk femårsperspektiv kunne kanskje være å få den opp på samme nivå som for tradisjonell kriminalitet. Oppklaringsprosenten for forskjellige typer tradisjonell kriminalitet varierer imidlertid betydelig. Viktige faktorer her er kriminalitetens kompleksitet og utbredelse og hvilke ressurser samfunnet velger å sette inn for å oppklare den. Disse faktorene gjelder også for datakriminalitet. Det er derfor vanskelig å konkretisere ambisjonsnivået i en visjon for en overordnet nasjonal strategi. Det kan være enklere å gi mer konkrete mål for ulike typer datakriminalitet.

6.3. Visjoner i andre lands datasikkerhetsstrategier

Vi skal kort se på visjonene i datasikkerhetsstrategiene til noen andre land for å få et inntrykk av hva de har valgt å vektlegge.

Storbritannia utarbeidet først en egen strategi mot datakriminalitet som i 2011 ble innarbeidet i en mer generell strategi for datasikkerhet. Visjonen for datasikkerhet er ambisiøs:

> *Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.*

Et livlig, pulserende, robust og sikkert digitalt samfunn vurderes som et sentralt virkemiddel for å skape betydelig økonomisk vekst og sosial fremgang. Aktiviteten i det digitale samfunn skal være styrt av viktige (britiske) samfunnsverdier som frihet, transparens, rettferdighet og rettssikkerhet, og den skal fremme velstand, nasjonal sikkerhet og et sterkt samfunn.

Men noen nærmere presisering av kravene til måloppnåelse gis ikke, med unntak av tidsfristen 2015 – det vil si en fire- til femårsperiode. Inntrykket fra strategigruppens London-besøk i november 2014 var nok at måloppnåelsen i 2015 ville variere atskillig. Bekjempelse av datakriminalitet er ett av fire hovedmål for å realisere visjonen. Storbritannia skal bli et av de sikreste stedene i verden for virksomhet i det digitale samfunn. Det andre hovedmålet er å gjøre Storbritannia mer motstandsdyktig mot dataangrep. Det tredje er å bidra til «… an open, stable and vibrant cyberspace which the UK public can use safely …». Det fjerde hovedmålet er å skaffe Storbritannia nødvendige tverrfaglige kunnskaper, ferdigheter og ressurser til å realisere alle de tre hovedmålene.

Storbritannia har altså integrert strategien for kriminalitetsbekjempelse i den generelle strategien for data- og informasjonssikkerhet. Fordelen er at virkemidlene for å bekjempe datakriminalitet og uønskede datasikkerhetshendelser generelt ses i sammenheng. Svært mange opplysninger og virkemidler er nyttige for begge aktivitetene, og det kan oppnås betydelige rasjonaliseringsgevinster i godt samarbeid. Et minus er at de spesielle utfordringene som kriminalitetsbekjempelsen skaper, ikke nødvendigvis blir like godt ivaretatt i en generell informasjonssikkerhetsstrategi som i en spesiell datakrimstrategi, slik Norge har lagt opp til. Men koordineringsutfordringene blir større i en strategi etter norsk modell.

Nederland følger samme modell som Storbritannia med en National Cyber Security Strategy hvor kriminalitetsbekjempelse er integrert:

> *Working with international partners, the Netherlands aims to create a secure and open digital domain, in which the opportunities for our society offered by digitalisation are used to the full, threats are countered effectively and fundamental rights and values are protected.*

Strategien inneholder forholdsvis lite om bekjempelse av datakriminalitet, men det poengteres at trusselen er økende, og at bekjempelsen må prioriteres gjennom å styrke politiet og påtalemyndigheten og å oppdatere lovverket. Et nært samarbeid mellom de forskjellige sikkerhetsaktørene både med hensyn til informasjonsdeling og operativ aktivitet er avgjørende. Nederland vil aktivt fremme internasjonale samarbeidsordninger for å understøtte en internasjonal holdning mot datakriminalitet.

Den finske strategien for Cyber Security Management har som visjon å sikre landet mot datatrusler i alle situasjoner slik at borgere, myndigheter og næringsliv fritt og trygt kan utnytte det digitale samfunn. Finland skal være et foregangsland i beskyttelsen mot datatrusler og håndteringen av uønskede datahendelser (se punkt 5.3.6).

Alle visjonene vektlegger et trygt digitalt rom. Dette «rommet» må nødvendigvis være internasjonalt. Omfattende internasjonalt samarbeid er derfor vesentlig for å realisere dem.

6.4. Visjon

Strategigruppen har valgt en kort og generell visjon, kombinert med fem hovedstrategier. Visjonen angir ambisjonsnivået for datakrimstrategien og hvilke samfunnsverdier den skal bidra til å beskytte:

> *Norge skal være et av foregangslandene i bekjempelse av datakriminalitet og på denne måten bidra til trygg bruk av datasystemer for å sikre verdiskapning, demokrati og velferd.*

6.5. Kort oversikt over hovedstrategiene

Strategigruppen foreslår fem hovedstrategier som samlet skal ivareta de viktigste aspektene ved visjonen.

Strategier mot datakriminalitet inneholder mer enn strafferettslige tiltak mot angrep på datasystemer. De skal også beskytte mot andre uønskede datahandlinger som økonomisk svindel, seksuell utnyttelse av barn og hetsing (sjikane, trolling, hatefulle ytringer), også i tilfeller hvor selve databruken ikke innebærer noen trussel mot datasikkerheten. Dette betyr dels at en datasikkerhetsstrategi vil favne bredere enn en datakriminalitetsstrategi fordi den også vil omfatte uønskede datahendelser som ikke skyldes handlinger som bør straffes, som teknologisk svikt, ulykker, naturbegivenheter osv., og som ikke utløser straffeansvar. Men det betyr også at en datakriminalitetsstrategi vil omfatte uønskede handlinger som ikke innebærer noen sikkerhetsrisiko, som distribusjon av overgrepsmateriale av barn.

Også såkalte elektroniske spor inkluderes gjerne i datakrimstrategier. Her dreier det seg dels om bruk av dataverktøy for å skaffe bevis, dels om innsamling og analyse av elektroniske data som kan kaste lys over forbrytelsen, uavhengig av om den straffbare handlingen som etterforskes, er rettet mot datasystemer eller er utført ved hjelp dataverktøy.

Behandling av elektroniske spor i saker som *ikke* gjelder datakriminalitet, faller utenfor arbeidsgruppens mandat, og blir derfor ikke behandlet i sin fulle bredde. Men strategien behandler dataverktøy som er viktige for å etterforske datakriminalitet slik mandatet avgrenser begrepet. Mange av synspunktene her er også relevante for etterforskningen av tradisjonell kriminalitet.

Hovedstrategiene behandles i egne kapitler (kapittel 7–11). Hvert kapittel begrunner en langsiktig hovedstrategi og drøfter eksempler på tiltak som kan bidra til å realisere hovedstrategien, se punkt 2.5. Selve hovedstrategiformuleringen med eksempler på tiltak er inntatt i slutten av hvert kapittel. For å tydeliggjøre helhetsbildet skal vi kort angi hva de fem kapitlene handler om:

Effektiv bekjempelse av datakriminalitet må være tuftet på en kvalitetsmessig god analyse av trusselbildet og sikkerhetssystemets kapasitet, samt etterretningsdata om pågående datakriminalitet. Internasjonalt samarbeid er viktig. *Hovedstrategi for deteksjon og analyse* behandles i kapittel 7.

En forutsetning for å bruke ressurser på å bekjempe datakriminalitet må være at kriminaliseringen av det som anses som uønskede og skadelige datahandlinger, er relevant for trusselbildet. Dersom handlinger som ofre og samfunn opplever som alvorlige og belastende, ikke er straffbare, eller straffetrusselen oppfattes som beskjeden, vil en anmeldelse fort fremstå som lite meningsfylt. Politiet har heller ikke noe grunnlag for å forfølge uønskede datahandlinger som ikke straffbare. Handlinger med lav strafferamme vil normalt ikke bli prioritert av politiet og påtalemyndigheten. Siden datakriminaliteten endrer seg raskt, bør kriminaliseringen også holde tritt med utviklingen. *Hovedstrategi for kriminalisering* behandles i kapittel 8.

Effektiv straffeforfølgning kan kanskje fremstå som det beste virkemiddelet mot brudd på straffelovgivningen. Men forebygging, stansing og gjenoppretting

er i praksis vel så viktige virkemidler. Ikke bare politiet, men også andre instanser kan bidra i dette arbeidet. Behovet for egne tiltak ved ekstraordinære datahendelser og kriser som truer kritisk infrastruktur eller andre vitale interesser, behandles også. *Hovedstrategi for forebygging og avverging* behandles i kapittel 9.

Selv om mye gjøres for å forhindre datakriminalitet, er det ikke realistisk at den vil forsvinne. Til nå har den tvert imot utgjort et økende problem. Effektiv straffeforfølgning er et viktig virkemiddel for å synliggjøre hvilke datahandlinger som er forbudt, og hindre lovbrytere fra å fortsette sin kriminelle virksomhet. Straff kan også virke avskrekkende på potensielle lovbrytere. I dette kapittelet vil også forholdet mellom etterretning og etterforskning i datakrimsaker bli vurdert. *Hovedstrategi for straffeforfølgning* behandles i kapittel 10.

I likhet med bekjempelse av økonomisk kriminalitet stiller mye av datakriminaliteten betydelige krav til kompetanse hos sikkerhetsaktørene. Teknologisk, politifaglig, samfunnsvitenskapelig og juridisk kompetanse er spesielt relevant for å kunne håndtere datakriminalitet. Behovet for kompetanseheving er så påtrengende at de viktigste tiltakene er blitt samlet i en egen *Hovedstrategi for kompetanseheving,* som behandles i kapittel 11.

Hovedstrategiene blir konkretisert gjennom en rekke eksempler på tiltak basert på nåsituasjonen. Men hovedstrategiene er langsiktige. Eksemplene skal også gi ideer om hvordan hovedstrategiene kan følges opp gjennom nye tiltak. Eksemplene er nettopp eksempler. Strategigruppen har ikke hatt noen ambisjon om å lage en tilnærmet fullstendig katalog over nødvendige tiltak.

Tre viktige utfordringer ved visjonen melder seg under nær sagt alle hovedstrategiene og egner seg derfor ikke for behandling i egne kapitler, men heller som en del av alle hovedstrategiene.

Det første spørsmålet gjelder *beskyttelse av personer og foretak* mot integritetskrenkelser og avsløring av forretningshemmeligheter og annen informasjon underlagt taushetsplikt. Et viktig element ved mange datalovbrudd er ulovlig innhenting og misbruk av personinformasjon. I etterretnings- og etterforskningsarbeidet er det sikkerhetsaktørene som har behov for personinformasjon og annen beskyttelsesverdig informasjon. Strategigruppens hovedsynspunkter er her samlet i punkt 7.6.

Det andre gjennomgående spørsmålet gjelder *behovet for en internasjonal orientering* i bekjempelsen av datakriminalitet. Også her er drøftelsene og forslagene plassert i tiltakene under hver enkelt hovedstrategi.

Det tredje spørsmålet gjelder de raske endringene i trusselbildet. Datakrimstrategien må være dynamisk og kunne oppdatere virkemidlene løpende for å tilpasse seg disse endringene. Dette aspektet er også omtalt en rekke steder i strategikapitlene.

7. STRATEGI FOR DETEKSJON OG ANALYSE

7.1. Informasjonsbehov og mørketall

Mest mulig presis og omfattende informasjon om uønskede datahandlinger og datakriminalitet er en grunnpremiss for hele datakriminalitetsbekjempelsen. Bevilgende og styrende myndigheter, politiet og andre virksomheter trenger beslutningsstøtte i form av god kunnskap om farer som truer de verdiene man skal verne. Analysene må gi kunnskap så vel om truslene og trusselaktørene som om eksisterende sikkerhetstilstand, og omfatte sårbarheter i så vel virksomheter som ellers i befolkningen. God forståelse av kunnskapsbehovet er grunnlaget for gode beslutninger når det gjelder å

- utføre målrettet forebygging for å unngå datakriminalitet i fremtiden
- raskt å avklare hvilke avvergende tiltak som kan settes inn mens datakriminalitet pågår
- vurdere behovet for straffeforfølgning i etterkant av datakriminalitet. Når en uønsket datahandling blir oppdaget, må det avklares så tidlig som mulig om det er tilstrekkelig mistanke om datakriminalitet (eller annen kriminalitet) til at det bør startes etterforskning for å sikre spor og bevis
- vurdere behovet for endringer i kriminaliseringen av uønskede datahandlinger
- vurdere behovet for forskning
- vurdere behovet for å heve kompetansen hos sikkerhetsaktørene – spesielt hos straffeforfølgende myndigheter: politi, påtalemyndighet og domstoler

Innsamling og analyse av informasjon om datakriminalitet kan ikke helt løsrives fra formålene den samles inn for. Innsamlingen kan i seg selv virke forebyggende, blant annet fordi potensielle lovovertredere frykter at den kan utløse forebyggende og avvergende tiltak, eller at innsamlede data vil bli brukt under straffeforfølgning. Det kan også være naturlig å kombinere innsamling av data med rådgivning og hjelp til informantene.

Det finnes ingen god oversikt over dagens situasjon eller av datakriminalitetens løpende utvikling. Opplysninger fra andre land og etterretningsrapporter fra Europol viser også at vi mangler tilstrekkelig kunnskap til å gi noe fullverdig bilde av dagens situasjon. Det trengs derfor bedre analyse- og rapporteringsordninger. Datakriminalitetens internasjonale karakter krever internasjonalt og tverrfaglig samarbeid om innsamling av data og analyse.

Analysene i kapittel 3 viser store mørketall når det gjelder datakriminalitet. Rapporteringen av datakriminalitet til politiet er svært lav. Få oppdager hendelser og rapporterer disse. Dette fremgår også av Mørketallsundersøkelsen, som omtales nedenfor i punkt 7.3.1 om statistikk.

7.2. Deteksjon og innsamling

Nåsituasjonen. Datakriminalitet utøves mot mange i dagens samfunn og oppdages også av mange ulike aktører. Både individer, kommersielle virksomheter og statlige aktører kan bli rammet selv eller være vitne til at andre rammes. Det varierer hvor lett den lar seg detektere, fra lett observerbar skade, som for eksempel en tømt bankkonto, til datainnbrudd der

inntrengeren har ligget skjult i årevis. En grunnleggende forutsetning er derfor deteksjonskapasitet. Ofte vil offeret, enten det er et individ eller en organisasjon, ha evne til å oppdage datakriminaliteten selv, men i noen tilfeller må myndighetene ta denne rollen – særlig hvor det dreier seg om ressurssvake ofre.

Datateknologi fjerner mange geografiske barrierer mellom ofre og gjerningspersoner. Mange av datakriminalitetens metoder kan automatiseres og gjenbrukes mot nye ofre. Når politiet er organisert etter prinsippet om geografisk nærhet, sier det seg selv at samme hendelse vil kunne føre til duplisert innsats i mange distrikter.

Og denne trenden øker. Ikke bare opererer innbruddstyver på tvers av politidistrikter, men de kriminelle splitter også opp sine aktiviteter ved hjelp av løs organisering, og oppgavene fordeles på personer i et fritt undergrunnsmarked, som beskrevet i kapittel 3. Kunnskap om angrepsmetoder mot mine digitale verdier vil derfor i stor grad kunne forbygge et angrep på dine. Dette taler for at man i større grad bør sentralisere analysen av innrapporterte hendelser.

Siden datakriminalitet baserer seg på de samme metodene, er det synergier i å dele kunnskap om både datainnbrudd, angrep og metoder for å utføre annen datakriminalitet, slik at andre kan iverksette nødvendige forbyggende tiltak. Tilsvarende effekt kan oppnås gjennom sentralisering. Kripos er et svar på bekjempelse av organisert kriminalitet der man ser klare gevinster ved å samle nasjonal og internasjonal bekjempelse på et sted.

Noen virksomheter er underlagt tilsyn og har rapporteringsplikt. Den samfunnsinitierte koordineringen av hendelser utøves gjennom NSM NorCERT, og i økende grad også av aktiviteten i sektor-CERT-ene. Imidlertid vil størstedelen av norske virksomheter ikke regnes som kritisk infrastruktur eller kritiske samfunnsfunksjoner, og omfattes ikke av sikkerhetstiltakene det offentlige har etablert. Det legges her til grunn at en samfunnsfunksjon skal defineres som kritisk hvis bortfall av den truer samfunnets og befolkningens grunnleggende behov. Infrastrukturenes kritikalitet er knyttet til deres betydning for de kritiske samfunnsfunksjonene. Over 90 % av norske virksomheter fyller imidlertid ikke vilkårene for å defineres som kritisk infrastruktur, og omfattes vanligvis ikke av sikkerhetstiltakene staten har etablert gjennom disse organene. Kildene til informasjon om digitale kriminelle forhold er spredd på mange aktører med varierende roller i bekjempelsen.

7.2.1. Tips og anmeldelser fra individer og virksomheter til politiet

Begrenset rapportering. Det trengs enklere rutiner for rapportering fra ofrene og bedre nasjonale statistikker for datakriminalitet. Erfaringene fra besøk i Nederland, Storbritannia og USA viser at nettkriminalitet i liten grad rapporteres uten spesielle tiltak. De som utsettes for nettkriminalitet og alvorlige hendelser på nettet, trenger å vite hvor de skal rapportere, og hvor de får hjelp. Dessuten må man i dialogen mellom offer og offentlig myndighet få avklart omdømmetap, tap av viktig informasjon og andre former for tap som kan være årsaken til at ofrene ikke rapporterer datakriminalitet. Denne manglende rapporteringen begrenser ofte vår evne til å forstå datakriminalitet. Som i de ovennevnte landene rapporteres det også i Norge altfor lite om datakriminalitet. Det som er rapportert inn, er blitt spredd over flertydige kriminalitetskategorier hos politiet, noe som gir et dårlig grunnlag for videre systematisk rapportering til myndighetene.

Når tradisjonell kriminalitet er begått, er det ofte lett å forstå at noe kriminelt har skjedd, og folk finner det naturlig å varsle politiet. Situasjonen er annerledes for datakriminalitet. Når vi har vært utsatt for angrep mot nettbank og digitale betalingssystemer, henvender vi oss til banken. Vi klager til teleoperatøren når urimelige utgifter blir belastet våre telefonregninger, og vi henvender oss til e-postleverandøren om mottatt søppelpost med svindelforsøk. Antivirusselskaper samler inn statistikk om skadelig programkode oppdaget på datamaskinene våre. Mange virksomheter varsler til private sikkerhetsselskaper, som deretter går inn og rydder opp i datasystemene deres.

Årsakene til denne mangeartede rapporteringen kan skyldes at

- man ikke innser at unormale eller uønskede datahendelser kan være tegn på kriminalitet
- man føler seg usikker på politiets evne til å håndtere datakriminalitet og hvorvidt anmeldelse og etterforskning vil føre frem

- politiets førstelinje ikke forstår godt nok hva datakriminalitet er
- områdene håndteres av flere myndighetsorganer, og man er usikker på hvilket som skal kontaktes
- prosessen rundt rapportering er tungvint. Eksempelvis er det krav om fysisk oppmøte for å anmelde et straffbart forhold. Kanskje ønsker ikke offeret noe mer enn å rapportere at noe uønsket har skjedd

Felles portal. Det er åpenbart at politiet ikke kan være tilstede overalt på Internett. Politiet må tilrettelegge for at publikum på en brukervennlig måte kan tipse om og anmelde datakriminalitet. Slik tilfellet er for tradisjonell kriminalitetsbekjempelse, er politiet avhengig av at publikum også varsler om ulovligheter på nettet.

Terskelen for å varsle politiet må være lav. Dagens organisering av politiet er bygget på prinsippet om at det er lettest for publikum å kontakte politiet på et lokalt politikontor. Erfaringer tilsier imidlertid at særlig de yngre heller kontakter det offentlige via nettet enn ved personlig oppmøte eller per telefon. Det er derfor grunn til å tro at politiet vil få flere henvendelser hvis det er mulig å kontakte dem via nettet.

Enkeltindivider og virksomheter har et klart behov for enkle, klare prosedyrer for hvordan datakriminalitet skal rapporteres, uten å måtte ta stilling til om det er det lokale politidistriktet, Kripos, Økokrim eller PST som til slutt bør ende opp med informasjonen. For disse sikkerhetsaktørene er det selvsagt viktig at de får den riktige informasjonen raskt, men av hensyn til borgeren vil det være fornuftig at sorteringen skjer internt i politiet. Det må være unntak, slik som for virksomheter underlagt særskilt tilsynsmyndighet, men som hovedordning vil det være hensiktsmessig med et sentralt mottak for mistanke om datakriminalitet.

En slik felles portal må legge til rette for innrapportering gjennom den kommunikasjonsformen befolkningen føler seg komfortabel med, om det så er telefon, direktemeldinger eller et digitalt skjema. Den som rapporterer, bør kunne velge om det er snakk om et rent tips eller en anmeldelse, og eventuelt få hjelp til å avgjøre dette spørsmålet. Portalen bør favne alle politiets ansvarsområder, og ha funksjonalitet for oppfølging av den som rapporterer, i den grad dette er hensiktsmessig.

Tips. Det er nyttig å skille mellom anmeldelse og tips. Politiet kan alltid starte en etterforskning basert på en begrunnet mistanke om en straffbar handling, om den så stammer fra anonyme tips. Det er derfor svært nyttig for bekjempelsen av datakriminalitet å kunne samle inn eksempler på skadevare, mistenkelige nettsider, mistenkelig e-post og annen mistenkelig kommunikasjon uten at informanten behøver å begjære etterforskning i form av en anmeldelse.

«Rød knapp» ble iverksatt som et av tiltakene for å forhindre spredning av overgrepsmateriale av barn. Tjenesten ble lansert av Kripos i 2008, og gikk ut på at nettsider rettet mot barn skulle tilby en lenke til Kripos' tipslinje.[45] Tjenesten mottok i 2012 nesten 3000 tips, men antallet har siden falt til under 2000, og antall saker har vært få, 4–5 per år. Å håndtere reelle tips er ressurskrevende, det samme gjelder useriøse tips og tips som skyldes psykiske problemer.

Både teknologien og måten informasjon deles på, har endret seg etter at Rød knapp ble utviklet. Satsingen er nylig evaluert, med forslag til nye tiltak. Kripos har også vurdert muligheten for en «panikkapplikasjon» som sikrer all kontaktinformasjon på telefon, nettbrett og PC, lagrer aktive vinduer, IP-adresser koblet til enheten osv. for å lette politiets etterforskning i etterkant.

Mottak av tips og anmeldelser. Det bør legges til rette for nettbasert anmeldelse av datakriminalitet til politiet. Informasjon om hvordan man kan inngi tips og anmeldelser, bør annonseres på politiets nettside og gjøres kjent i ulike typer nettsamfunn. Tjenesten bør sørge for både sikker identifisering av anmelder ved anmeldelse, og ha løsere krav til identifisering ved tips, slik at terskelen for å tipse om straffbarheter blir så lav som mulig. Et eksempel på en sikker identifisering vil være å benytte Bank-ID eller MinID for å autentisere den som inngir anmeldelse.

Viderebehandling av tips. Tipsmottak og håndtering av tips vil generere arbeid og forutsetter en baktroppfunksjon som kan følge opp tipsene slik at de ikke blir

45 http://tips.kripos.no – for tips om seksuelle overgrep mot barn, menneskehandel og rasistiske ytringer på Internett.

liggende ubehandlet lenge. Politiet kan risikere å bli overveldet av tips, og erfaringsmessig tar det noe tid å få overført tips fra tipstjenestene til den som kan ta saken. Trolig er effektiviseringspotensialet stort hvis man automatiserer også bearbeidingen og videreformidlingen av innkomne tips og anmeldelser. Dette er områder med behov for forskning og utvikling, se kapittel 11.

Konklusjon. Det bør opprettes en sentral innrapporteringsfunksjon for tips og anmeldelser til politiet av datakriminalitet på den kommunikasjonsformen som er best tilpasset befolkningens behov, og med løsninger for sikker identifikasjon. Funksjonen må ha kapasitet til å veilede melderen og videreformidle informasjonen til riktig myndighetsorgan for videre oppfølging der dette er nødvendig.

Forslagene her vil også være viktige i forebygging og etterforskning.

7.2.2. Politiet og PST må øke sin tilstedeværelse i det digitale samfunn

Det er behov for økt tilstedeværelse og innsamling av informasjon på Internett, ikke bare i politiet generelt, men også hos PST. For sistnevnte synes en slik tilstedeværelse å være et sentralt virkemiddel for å motvirke radikalisering og en viktig kanal for informasjon om datakriminalitet og annen kriminalitet som faller inn under deres ansvarsområde etter politiloven § 17b.

Slik tilstedeværelse reiser viktige spørsmål rundt egensikkerhet og eksponering, søksmetodikk, korrekt opptreden på et «digitalt åsted» og de mer sammensatte utfordringene knyttet til bruk av skjulte etterforskningsmetoder på Internett.

Kripos er i ferd med å utarbeide og beskrive et konsept for hvordan politiets tilstedeværelse i det digitale samfunn bør organiseres og gjennomføres. Dette skal gjøres ved kompetanseoverføring, bistand og metodeutvikling. Tilstedeværelsen innebærer både «åpen» og «skjult» tilstedeværelse.

Den åpne, *uniformerte* tilstedeværelsen skal være et nødvendig supplement til politiets øvrige tilstedeværelse, med hovedvekt på forebygging, der det primære målet er synlighet og å høyne oppdagelsesrisikoen. Dette kan gjøres ved bruk av offisielle informasjonssider – en «politistasjon på nett» – for generell informasjon, kampanjer og «tipstjenester» for registrering av hendelser samt mer interaktivitet med politipersonell som kan besvare og respondere på henvendelser og gi informasjon.

Tilstedeværelsen kan også innebære aktiv deltakelse – «patruljering på nett» – med registrerte brukere på relevante sosiale medier som klart tilkjennegir seg med politiets logo og identitet.

Den *skjulte* tilstedeværelsen er nødvendig for å oppdage brukere som ikke ønsker å rette seg etter det som måtte være gjeldende lov på den norske delen av Internett. Den skal bryte opp nettverk og strukturer som genererer eller understøtter kriminell aktivitet, eksempelvis ved tilstedeværelse i fora der rekruttering til kriminell aktivitet forekommer, digital spaning, infiltrasjon og provokasjon. Disse metodene skal utgjøre et nødvendig supplement til øvrig skjult metodebruk, og bør kunne benyttes til informasjonsinnhenting for forebygging og etterforskning. Dette stiller høye krav, ikke bare til utstyr, tilrettelegging og metodikk, men også til personellets kunnskaper og ferdigheter.

Funksjonen bør

- ha kapasitet til målrettet informasjonsinnhenting
- ha evne til å analysere store mengder data
- legge til rette for rekruttering av kilder og informanter
- være et verktøy for kunnskap om trender, miljøer, arenaer
- gjennomføre skjult metodebruk på ulike stadier av etterforskningen

Slik innsats har allerede gitt gode resultater. Et eksempel er SnapSave-saken[46] der tidlig deteksjon etterfulgt av straffeforfølgning og avskrekkende operasjoner ble benyttet parallelt for å roe ned massiv distribusjon og sammenstilling av svært privat bilde- og videomateriale som hadde kommet på avveie. Politiets rolle var å informere om alvorligheten ved handlingene som ble begått, kombinert med å vise handleevne ved å gjennomføre ransaking hos to siktede for å begrense

46 Kripos-aksjon mot spredning av stjålne SnapChat-bilder av unge. Se nettlenke av 18.10.14: http://www.aftenposten.no/article7749726.ece.

omfanget av lovbrudd som medførte meget alvorlige inngrep i mange enkeltpersoners privatliv.

Tilstedeværelsen skal være uavhengig av kriminalitetsform, basert på prinsippet om «ett politi». Konseptet skal i størst mulig grad bygge på at *formålet* med tilstedeværelse på Internett ikke skiller seg vesentlig fra politiets øvrige virksomhet i samfunnet. Den skal ivareta politiets oppdrag etter politiloven – fremme lov og orden – også på Internett.

Tiltaket kan knyttes til det arbeidet som allerede pågår ved Kripos. Det vurderes som forholdsvis enkelt å igangsette, men vil kreve en del mannskap – litt avhengig av hvilket ambisjonsnivå man legger seg på. Man må regne med at aktivitetene vil kunne generere en rekke saker og identifisere hendelser som krever operativ oppfølging fra politiet eller andre. Dette må kartlegges grundig, og man må lage konkrete planer for å håndtere slike hendelser og forsikre seg om at slik oppfølging er mulig.

Tilstedeværelsen på nett kan gi mer tilgang på tilfeldig informasjon, og det åpner seg nye muligheter for innhenting av målrettet informasjon. Slik informasjon om hendelser vil i økende grad måtte registreres, og da er det viktig med en høy bevissthet om hjemmelsgrunnlaget for registrering, og man må vite om innhentet informasjon skal benyttes til forebygging, avverging eller etterforskning. Sikkerhetsaktørene har her forskjellige hjemmelsgrunnlag alt etter oppgavene som skal løses.

Konklusjon. Politiet og PST må øke sin tilstedeværelse på Internett, både i form av åpen og skjult tilstedeværelse. Politiet må, helt ned på enhetsnivå, bygge kompetanse og kapasitet til å benytte Internett for å sikre trygghet, lov og orden. En slik tilstedeværelse må kunne gi informasjon og gå i dialog med publikum samt avdekke og analysere store mengder innhentet informasjon. Tilstedeværelsen må understøtte politiets arbeid og ha en lokal forankring.

7.2.3. Behov for digitale varslingssystemer

Varslingssystem for digital instrastruktur (VDI). Gode prosedyrer og tekniske sikkerhetstiltak for å redusere sårbarheter kan erfaringsmessig ikke forebygge alle uønskede hendelser, særlig ikke de mest avanserte eller ukjente trusselmetodene. Det er denne restrisikoen NSM NorCERT[47] jobber med å håndtere på nasjonalt nivå, blant annet ved hjelp av varslingssystemet for digital infrastruktur (VDI). Systemet består av et nettverk av digitale sensorer, plassert i et utvalg samfunnsviktige IKT-infrastrukturer i sektorene. Sensorene vil blant annet kunne oppdage og varsle om alvorlige datatrusler, som digital spionasje og sabotasje, og angrep som favner bredt. Systemet kan også benyttes som verifikasjonssystem og til å bedømme skadeomfang ved hendelser. Sensornettverket ser etter angrepsformer basert på kjente deteksjonssignaturer. Utplasseringen av sensorene er basert på frivillighet ved avtale. Virksomhetene bekoster selv egne sensorer, men sentralutrustningen bekostes av det offentlige. Signaturbaserte systemer vil alltid være på etterskudd, og det blir stadig vanskeligere å utvikle gode signaturer. Etterretning er en vesentlig kilde til signaturer, og det er gode grunner til å hemmeligholde disse.

Resultater fra VDI- systemet er et viktig informasjonsunderlag for IKT-risikobildet som NSM har et ansvar for å vedlikeholde. Indirekte vil informasjon som fremskaffes fra systemet kunne underbygge politiets vurderinger av den trusselen som datakriminalitet representerer.

Frivillighet. Det arbeides med å lovfeste VDI-systemet i den eksisterende sikkerhetsloven. Regjeringen har dessuten nylig nedsatt et offentlig utvalg for å videreutvikle sikkerhetslovgivningen.

Det er viktig at deltakelsen i VDI understøtter formålet best mulig. Muligheten til å pålegge virksomheter deltakelse bør derfor vurderes i dette lovarbeidet. Andre virksomheter med viktige støttefunksjoner overfor kritisk infrastruktur kan også være aktuelle i VDI-samarbeidet. En åpen og rask deling med partene som deltar i samarbeidet, er viktig for en adekvat reaksjon og for å kunne forebygge nye datainnbrudd og dataangrep.

VDI finansieres med både private og offentlige midler. Selve finansieringsmodellen har vist seg å være en utfordring for videreutviklingen av systemet,

47 CERT (Computer Emergency Response Team) er et av flere begreper som brukes om miljøer som håndterer uønskede hendelser i datanettverk. NSM NorCERT er det øverste nivået og dermed vårt nasjonale CERT, som har en mer koordinerende enn håndterende rolle. Et annet begrep er CSIRT (Computer Security Incident Response Team).

og den kan komplisere NSMs myndighetsrolle. I den nevnte lovrevisjonen bør man derfor også vurdere en sterkere statlig finansiering. Argumenter for å beholde dagens finansieringsmodell er at det skaper et større engasjement fra dem som deltar. På den annen side er det viktig å unngå at VDI blir sett på som et sikkerhetsnett som anskaffes for den enkelte virksomhet, og som fratar disse ansvaret for egen sikring. Ulempen med dagens frivillige medlemskap og delvis private finansiering er at viktige aktører kan velge å ikke bli med om de ikke føler de får tilstrekkelig igjen for samarbeidet. Et slikt valg vil kunne undergrave en viktig sikkerhetsinfrastruktur i samfunnet som i neste omgang vil påvirke informasjonsunderlaget for trusselbildet når det gjelder datakriminalitet.

PSTs behov. For å kunne avdekke og bidra til håndtering av de alvorligste truslene mot rikets sikkerhet i det digitale rom, er det nødvendig å etablere en statlig etterretningsevne til å avdekke trusler i elektronisk kommunikasjon som går til og fra Norge, særlig med tanke på andre staters etterretningsvirksomhet og eventuell forberedelse til sabotasje. Det pågår allerede en prosess for å avklare spørsmålet om utvidede fullmakter og bygge opp en slik evne.

7.3. Registrering og analyse av informasjonen

7.3.1. Statistikk

En felles tips- og anmeldelsesportal vil være rettet mot publikums behov, men i bakkant må man ha et effektivt system for registrering og intern deling av hendelser detektert av politiet, og informasjon som kommer direkte fra andre sikkerhetsaktører.

Politiets registrering av datakriminalitet må forbedres. Mottatt informasjon må registreres i et databasesystem med gode muligheter for å kategorisere informasjonen slik at den lett kan behandles og søkes opp på tvers av geografiske politidistrikter. Presis registrering er også en forutsetning for å kunne trekke ut målrettet statistikk som igjen kan brukes ved beslutninger på strategisk nivå.

STRASAK. I dag benytter politiet et elektronisk straffesakssystem som heter STRASAK, som ikke er tilrettelagt for å registrere datakriminalitet som egen kategori. Det er imidlertid viktig å kunne se hvordan kriminaliteten utvikler seg i det digitale rom.

Statistikken som genereres fra STRASAK, deler sakene inn i to hovedkategorier:

- hva slags type kriminalitet som er begått, eller hvilket straffebud som er overtrådt (statistikkgrupper)
- måten den er gjennomført på (modusgrupper)

Innenfor begge kategorier har man overordnede og underordnede nivåer (kriminalitetsformer, modusgrupper, undergrupper osv.).

Kodeverket (kategoriene) i STRASAK er blitt til over lang tid, er svært sammensatt og komplisert, og mangler en helhetlig struktur. Det tar i svært varierende grad høyde for en enhetlig oppdatering etter hvert som kriminalitetstyper og modus endrer seg. Det er for lite tilpasset dagens kriminalitetstrender, og det evner ikke å gjenspeile endringer i kriminalitetsbildet. Stor valgfrihet for den som skal registrere opplysninger i systemet, fører til inkonsekvent, manglende eller feil registrering, noe som i neste omgang gjør statistikkene upålitelige og i verste fall verdiløse. STRASAK egner seg derfor i liten grad til å trekke ut statistikk som kan vise trender i datakriminaliteten som følge av teknologiutviklingen.

Gjennom besøk i utlandet har strategigruppen fått innblikk i ulike løsninger på dette problemet. I USA har FBI et eget nettverk mellom de statlige kontorene med mulighet for å registrere informasjon på høyt sikkerhetsgradert nivå via nettskjema. Databasen kan så brukes for avanserte søk på tvers av kontorer og for generering av statistikk. Dette systemet har også et lavgradert grensesnitt mot andre politistyrker (e-Guardian) og industripartnere (iGuardian). Individer og andre bedrifter kan rapportere inn og få informasjon om nettbaserte hendelser via IC3[48].

Politiets kriminalstatistikk inneholder i dag for mange begrensninger til å kunne si noe presist om hvor omfattende datakriminaliteten er, og hvordan den fordeler seg på ulike sektorer og bransjer, typer av lovbrudd, gjerningspersoner, geografi, saksbehandling, modus, teknologi, oppklaring osv.

48 www.ic3.gov.

Konklusjon. Det bør gjøres en grundig gjennomgang av kodeverket og registreringspraksisen i STRASAK for å bedre statistikkgrunnlaget om datakriminalitet. Strategigruppen anbefaler å se dette arbeidet i sammenheng med behovet for en felles rapporteringsportal og registrering av observasjoner fra politiets tilstedeværelse på Internett.

Det må produseres gode årlige statistikker over vesentlig datakriminalitet. Statistikkverktøyene må forbedres slik at man får et tilstrekkelig presist bilde av datakriminaliteten for aktuelle formål. Det må utvikles hensiktsmessige statistikkategorier for datakriminalitet.

Skjult kriminalitet. Mørketallsundersøkelsen er enestående i sitt slag i Norge som kilde til opplevd datakriminalitet i norske virksomheter og verktøy for å fange opp nye trender i kriminalitetsutviklingen. Finansieringen har vært ustabil, noe som har påvirket kvaliteten av undersøkelsene, blant annet ved en varierende svarprosent. Trenden er synkende, fra 39 % i 2006 til 15 % i 2014, og den har vært enda lavere enn dette. En god svarprosent er viktig for at undersøkelsen skal gi et pålitelig bilde.

Et hovedproblem med få respondenter er særlig at kartleggingen av hendelser blir upålitelig. Med et større utvalg ville undersøkelsen kunne omfatte flere observasjoner på dette området. Den svake kriminalstatistikken gjør undersøkelsen særdeles viktig for en god planlegging av bekjempelsen av datakriminalitet. Ikke minst gjelder dette for kapasiteten og kompetansen til politi, påtalemyndighet og domstoler. Strategigruppen mener det er av stor interesse å utvide Mørketallsundersøkelsen med flere spørsmål om datakriminalitet.

Konklusjon. Mørketallsundersøkelsen bør sikres stabil finansiering, slik at de mest effektive metodene benyttes for å oppnå en høy svarprosent. Det bør også iverksettes tiltak som sikrer at spørsmålene belyser datakriminaliteten bredt og grundig – gjerne i form av en separat undersøkelse. En tilsvarende undersøkelse rettet mot privatpersoner bør også gjennomføres.

7.3.2. Operativ analyse

Politiet. Norsk politi har begrenset erfaring med operativ analyse i datakrimsaker, blant annet fordi få av dem etterforskes. I utgangspunktet analyseres slike saker i dag ut fra de samme kriteriene som ved analyse av andre typer kriminalitet. Men datakrimsaker inneholder veldig ofte andre typer informasjon enn tradisjonelle etterforskningssaker. Utfordringene består i hovedsak i at man får inn mye ustrukturerte data i ukjent format som er tidkrevende å bearbeide, samt at strukturerte data ofte ikke passer inn i eksisterende maler for analyse. Informasjonsmengden er ofte stor og kildene mange.

Kapasiteten til kriminalanalyse i politiet varierer, fra politidistrikter som har liten eller ingen reell analysekompetanse utover analyse av hverdagskriminalitet, til de sterkeste analysemiljøene, som er hos Kripos og i Oslo politidistrikt. Politidistriktene må sikres en god analyseevne bestående av personell med god kompetanse som kan ta ansvar for større, alvorlige straffe- og informasjonsinnhentingssaker.

Samordning. Situasjonsforståelsen må bedres hos flere aktører, uavhengig av hvor tips, varslinger og anmeldelser kommer inn. Sikkerhetsaktørene har gjerne ulike perspektiver, og fokuserer dermed også gjerne på forskjellige aspekter ved datakriminaliteten. For politiet vil stikkordene være verktøy og metoder for å kunne sammenstille observasjoner og se fellestrekk.

For å få til en god samordning må alle som mottar tips og anmeldelser i politiet, registrere dem. På lokalt nivå igangsettes ofte en etterforskning med å sikre spor osv., deretter sammenstilles observasjonene slik at de kan ses i sammenheng med andre saker i andre distrikter osv. I datakrimsaker vil en ofte se at elektroniske spor berører flere saker, gjerne også flere distrikter, og kan spores til utlandet. Det er derfor viktig å ha en god samordning mellom Kripos og distriktene for å få en effektiv bruk av ressurser og spesialkompetanse på området, se punkt 10.5.1.

Politiets etterretningsdoktrine. Etterretning er en formålsstyrt aktivitet med innsamling, analyse og vurdering av informasjon om utfordringene som politiet og samfunnet står overfor. En vesentlig del av arbeidet

er innhenting av etterretningsinformasjon for å bygge opp et faglig beslutningsgrunnlag for dem som skal foreta prioriteringer i politiets innsats. Dette omfatter innhenting av opplysninger om personer, grupper og fenomener som skaper eller kan skape kriminalitet, samt uønskede eller ekstraordinære hendelser[49]

Etterretningsproduktene skal bidra til et bedre beslutningsgrunnlag. Grunnpilarene i etterretningsarbeidet er data, som er «rå informasjon» uten kontekst. Når data bearbeides og settes i en sammenheng, blir dette til informasjon. Informasjon fra flere kilder danner grunnlaget for analyser som sammenholdes med eksisterende kunnskap og på den måten omdannes til etterretning.

I politiet er det innført en etterretningsdoktrine[50] som skal gi en bredere forståelse av begrepet 'etterretning' og fungere som en dreiebok for alt etterretningsarbeid i politiet – også etterretning om datakriminalitet. Funksjonene som bygges opp for å innhente og bearbeide informasjon om datakriminalitet, må derfor tilpasses doktrinen og gjeldende regelverk. Doktrinen skal også kunne benyttes når politiet samler inn informasjon fra andre sikkerhetsaktører.

Doktrinen omfatter hele etterretningsprosessen med ledelse, innhenting, analyse og formidling. Kildegrunnlaget vil ofte ha direkte innvirkning på graden av sikkerhet, og det er derfor ønskelig med en bred innsamling av data.[51]

En helhetlig ledelse er en forutsetning for å sikre at arbeidet er målrettet og ressursbruken optimal. I arbeidet med datatrusler vil man ha korte tidsfaktorer, og truslene endrer seg raskt. Prosessen må derfor gå raskere og bli mindre stringent enn for klassisk etterretningsarbeid for å få et oppdatert bilde av situasjonen.

Ved dataangrep rettet mot datasystemer vil et godt situasjonsbilde basert på innsamlet informasjon og analyse gjøre NSM NorCERT og politiet i stand til å iverksette beskyttende tiltak og korte ned reaksjonstiden ved å dele på kunnskap om angrepet så langt det er mulig. Dette er uavhengig av om man velger å iverksette forebyggende og avvergende tiltak eller etterforskning.

Som et ledd i etterforskningen sikrer politiet store mengder elektroniske spor som kan bli avgjørende bevis i straffesaker eller benyttes i forebyggende arbeid for å hindre alvorlige trusler. De siste årene har mengden innsamlede data fra beslag økt voldsomt som følge av teknologibruk i det moderne samfunnet. Dataene har svært ulik form og struktur. Dagens metoder strekker ikke til. Det er behov for nye verktøy som kan trekke ut, knytte sammen og presentere relevant informasjon fra enormt store mengder innsamlede data.

PST har en bred tilnærming til datakriminalitet. Innenfor deres ansvarsområder kan digitale angrep i noen tilfeller indikere en ulovlig etterretningsoperasjon, sabotasje eller lignende. Andre ganger ser vi at digitale verktøy eller annen informasjonsteknologi benyttes til å fremsette trusler mot myndighetspersoner og oppfordre til terrorhandlinger. Datakriminalitet må bekjempes på ulike måter, også gjennom forebyggende arbeid. Ettersom PST også har et ansvar for å etterforske nærmere angitte overtredelser, vil det være en av deres oppgaver å møte datakriminalitet gjennom en adekvat og effektiv etterforskning. En etterforskning som evner å avdekke og oppklare denne typen kriminalitet, må også ses som et viktig forebyggende tiltak. PST må også skille klart mellom etterforskning og etterretning i sin innhenting av informasjon fra datasystemer. I tråd med PSTs lovpålagte oppgaver har deres etterretningsarbeid som hovedformål å *forebygge* at fremtidige straffbare og skadelige handlinger skjer. Etterforskningen tar sikte på å *avdekke* mulige straffbare forhold og *eventuelt straffeforfølge* disse. PST har en egen etterretningsdoktrine, og politiets doktrine er delvis inspirert av denne.

Mye av informasjonstilfanget til PST kommer fra kilder som ikke uten videre kan brukes i en straffesak. Informasjonen vil ofte forbli uverifisert, men kan likevel være viktig for å få gjort andre undersøkelser og dermed få bekreftet eller avkreftet en mistanke. I tillegg vil informasjonen i en sak ofte være gradert. Opplysninger fra saken kan derfor i mange tilfeller ikke offentliggjøres i en straffesak.

Digital etterretning utført av fremmede stater vil som regel være vanskelig å straffeforfølge. Selv om

49 Politidirektoratet. PBS I. *Politiets beredskapssystem del I*. s. 25.
50 Politidirektoratet. *Etterretningsdoktrine for politiet VERSJON 1.0*, august 2014.
51 Politidirektoratet. *Etterretningsdoktrine for politiet VERSJON 1.0*, august 2014, Figur 4 Etterretningsprosessen.

tekniske undersøkelser gir klare indikasjoner på hvilket land en ondsinnet programvare kommer fra, vil det være svært utfordrende å finne en konkret mistenkt. Det viktigste virkemiddelet vil derfor være å informere aktørene som er utsatt for ondsinnet etterretning, om hva de står overfor, og hvordan de kan redusere sin egen sårbarhet. Et annet virkemiddel kan være politiske reaksjoner, men dette vil oftest ha liten effekt.

NSM legger en egen etterretningsdoktrine til grunn for sitt arbeid når de kartlegger ulike aktører. Doktrinen settes inn i en større sammenheng i en risikoanalyse slik denne kommer til uttrykk i Norsk Standard 5830. Øvrig prosessmetodikk som brukes i NSM NorCERT-funksjonen, er bygget på mønsterpraksis fra FIRST[52], men med noe begrepsbruk fra ITIL[53]-rammeverket.

Konklusjon. En sentral enhet i politiet bør ha ansvar for å se innsatsen mot datakriminalitet i sammenheng på tvers av alle distrikter, og ha som oppgave å informere og koordinere felles innsats. PST bør samarbeide tett med en slik enhet, men må samtidig ha tilstrekkelig kapasitet til å dekke eget ansvarsområde.

7.4. Deling av informasjon

7.4.1. Politiets tilgang på informasjon om datakriminalitet i sikkerhetssporet

Politiets tilgang på hendelsesinformasjon. Hendelsene NSM NorCERT håndterer, vil i mange tilfeller falle inn under straffbar datakriminalitet. Det eksisterer allerede et samarbeid (CKG-gruppen) mellom de hemmelige tjenestene PST, E-tjenesten og NSM for deling av informasjon om alvorlige hendelser, men hensynet til rikets sikkerhet gjør at denne informasjonen fort blir sikkerhetsgradert. Det begrenser deling og spredning av slik informasjon.

Kripos er ukentlig representert ved en liaison hos NSM NorCERT, som får informasjon om trusselbildet, pågående alarmer og saker som kan bli anmeldt, men vurderer ikke denne informasjonskanalen som så viktig at de ønsker permanent tilstedeværelse.

NSM NorCERTs primæroppgave er forebyggende arbeid i «sikkerhetssporet». Det er utfordrende å kombinere dette med politiets «etterforskningsspor», hvor man forsøker å ta de ansvarlige. Utfordringene er knyttet til mandatet for hvordan informasjonen samles inn, sikkerhetsgradering, og krav til innsyn i etterforskningsmaterialet ved straffeforfølgning i retten. Dette kan løses gjennom tilstrekkelig klarering og autorisasjon av personellet, men det blir ofte vanskelig å etablere slike ordninger og få det til å fungere i praksis. Politiet har hovedansvaret for etterforskning og har adgang til å benytte tvangsmidler som NSM ikke har, for eksempel for avverging. PST påpeker at det ofte er statlige eller statsfinansierte trusselaktører som står bak datainnbrudd, og at straffeforfølgning ikke vil føre noen vei.

Virksomheter som faller utenfor. NSM NorCERT retter sin aktivitet mot kritisk infrastruktur og kritiske samfunnsfunksjoner. Etableringen av sektorvise CERT skal bistå så vel NSM NorCERT som virksomhetene i sektorene, samt understøtte sektordepartementenes konstitusjonelle ansvar for sikkerhetsarbeidet i sektoren.

Sensornettverket som forvaltes av NSM NorCert, er basert på et utvalg av virksomheter. Imidlertid er det slik at størstedelen av norske virksomheter ikke deltar i dette sensornettverket og ikke er en del av kritisk infrastruktur og kritiske samfunnsfunksjoner. Disse virksomhetene er i betydelig grad utsatt for datakriminalitet.

Over 90 % av norske virksomheter faller utenfor definisjonen av kritisk infrastruktur. Samtidig er disse virksomhetene i betydelig grad utsatt for datakriminalitet som går utover behovet for å oppdage dataangrep. For å avlaste NSM pågår det en utrulling av et system for sektorvise CERT-miljøer som skal vektlegge sektorens særegenheter og krav.

Konklusjon. Eksisterende regler og barrierer mot informasjonsdeling mellom politiet og NSM bør gjennomgås for å vurdere hvor hensiktsmessige de er.

For å sikre informasjon til kriminalitetsbekjempelse bør politiet rette oppmerksomheten mot andre samarbeidsfora og drive oppsøkende aktivitet overfor offentlige og private virksomheter for å få

52 https://www.first.org/about.
53 http://no.wikipedia.org/wiki/ITIL.

informasjon om truslene og hendelsene. I tillegg bør de støtte disse virksomhetene med avverging og etterforskning med de metoder bare politiet har tilgang på. Det bør forskes mer på metoder for å oppdage avanserte datatekniske innbrudd.

7.4.2. Politiets privat-offentlige samarbeid

NSM NorCERT samler inn store mengder informasjon om hendelser. Hvorvidt slike hendelser skal anmeldes, avgjøres i all hovedsak av ofrene, og informasjon videreformidles ikke automatisk til politiet. Dette har vært et viktig og nødvendig prinsipp for å skape tillit mellom virksomhetene og NSM NorCERT.

Politiet trenger imidlertid slik informasjon, og det er derfor behov for å se nærmere på hvordan politiet aktivt kan vise sin støtte til virksomheter som per i dag ikke anmelder datakriminalitet de har vært utsatt for. En politiliaison ved NSM NorCERT kunne veilede og oppmuntre ofrene til å anmelde. En kan her trekke frem Telenor som har stått frem som et godt eksempel og pekt på betydningen av anmeldelse i en datatyverisak mot ledelsen i 2013.

Det er mange typer datakriminalitet som ikke oppdages av individer og virksomheter fordi man ikke selv har systemer som kan oppdage datakriminalitet eller er tilknyttet et sensornettverk. Dette gjelder for eksempel økonomisk motiverte bedragerier og utpressingsaktivitet mot bankkunder og beskyttelse av merkevare, sporing av falske varer og økonomikjeden rundt dette.

Som et alternativ til å endre på et allerede velfungerende CERT-samarbeid kan vi peke på en løsning strategigruppen fikk presentert under sitt besøk i Pittsburgh i USA[54] Konseptet er et samarbeidsforum mellom politiet som vertskap, virksomheter og akademia. Samarbeidet legger stor vekt på felles innsats innen etterforskning av datakriminalitet ved å bygge saker og støtte etterforskningsprosessen.

Oppmerksomheten rettes mot nettverkene av aktører bak kriminaliteten, i motsetning til den tekniske, akutte håndteringen i CERT-miljøene. Forebygging og avverging er også viktige mål som søkes oppnådd ved informasjonsdeling.

For at et slikt samarbeid skal fungere kan vi peke på et par forutsetninger. Samarbeidet må være basert på virksomhetenes behov, være sektoruavhengig og foregå under rammevilkår som ikke begrenser bruken av eget teknisk utstyr og egne metoder. Man må for eksempel kunne jobbe på eget elektronisk utstyr og nettverk. Arbeidet bør altså skje i et nøytralt miljø, i motsetning til arenaer der personlig utstyr må legges igjen i resepsjonen.

Den amerikanske modellen innebærer at politiet har en ledende rolle, men en norsk utgave av et slikt samarbeid for informasjonsdeling og tverrfaglig innsats mot datakriminalitet bør også vurdere andre aktører, for eksempel NorSIS og Næringslivets Sikkerhetsråd. NorSIS' rolle som uavhengig ekspertorgan vil for eksempel være viktig for å skape legitimitet, tillit og effektivt samarbeid. Naturlige deltakere vil være aktører fra databransjen, datasikkerhetsbransjen og sektorCERT-miljøene. Eksisterende samarbeidsformer mellom finanssektoren og Kripos vil være et naturlig utgangspunkt for et slikt samarbeid, og kan for eksempel ses i sammenheng med datakrimsenteret som foreslås opprettet (se punkt 10.5.2).

Konklusjon. Det bør opprettes, eventuelt videreføres, en arena for samarbeid mellom politi og privat sektor der fokuset er forebygging og etterforskning rettet mot «hverdagsdatakriminelle». Dette initiativet skal ikke erstatte, men supplere det eksisterende samarbeidet mellom NSM NorCERT og virksomhetene. Denne modellen har et sentralisert preg og må ses i sammenheng med behovet for lokal kontakt mellom politi og virksomheter (se punkt 9.5.2 og 10.5.4).

7.4.3. Nasjonal trussel- og risikovurdering av datakriminalitet

I trussel- og risikovurderinger er det sannsynligheten og muligheten for fremtidige hendelser som vurderes, og de kan også inneholde vurderinger av potensielle aktørers evne og vilje til å utføre for eksempel datakriminalitet. Vurderingen omfatter altså både slagkraft, ulike typer hendelser og sannsynligheten for at hendelser vil inntreffe.

Strategigruppen har observert et klart behov for løpende nasjonale trusselvurderinger av datakriminalitet som oppdateres etter hvert som trusselbildet endrer seg. Mye av informasjonen som trengs, vil være av felles interesse for kriminalitetsbekjempelse

54 National Cyber-Forensics & Training Alliance (NCFTA), http://www.ncfta.net/.

og andre former for datasikkerhetsarbeid. Også med tanke på beredskap og krisehåndtering vil gode trusselvurderinger være vesentlige for en god planlegging av hvilke øvelser man skal ha, og for at myndighetene skal kunne innrette sine satsinger på en hensiktsmessig måte.

Strategigruppen har observert at både metoder og analysemåter varierer mellom de ulike sikkerhetsaktørene, og begreper som 'trussel', 'risiko' og 'sårbarhet' tillegges ulik betydning. Videre synes man å ha ulike målsetninger med å utarbeide trussel- og risikoanalyser, noe som igjen kan gjøre arbeidet med en løpende nasjonal oversikt over hvilken trussel og risiko datakriminalitet utgjør i vårt land, vanskelig og tidkrevende.

Det er i hovedsak sikkerhetsaktører tilknyttet politiet og påtalemyndigheten som først og fremst fokuserer på datakriminalitet. De øvrige sikkerhetsaktørene retter, i tråd med sine mandater, sitt fokus mot uønskede datahendelser og deres skadepotensial uavhengig av om handlingene er straffbare.

Mange av sikkerhetsaktørene baserer seg på trussel- og risikoinformasjon fra hverandre. At sikkerhetsaktørene er enige om en trusselvurdering betyr derfor ikke uten videre at vurderingene er basert på uavhengige analyser. En effektiv bruk av trussel- og risikovurderinger og adekvate og effektive mottiltak er viktige oppgaver for sikkerhetsaktørene, men også for sentrale myndigheter. Gode analyser er til liten hjelp dersom de ikke blir utnyttet!

Strategigruppen mener det er behov for en nasjonal koordinering av de ulike sikkerhetsaktørenes trusselvurderinger om datakriminalitet, og anbefaler derfor et løpende arbeid for å få satt sammen de ulike elementene til en felles vurdering. En slik nasjonal trusselvurdering vil kunne støtte sentrale myndigheter i deres strategiske arbeid og bidra til å tegne et løpende og helhetlig bilde av trusselsituasjonen for Norge. Det vil gi sentrale myndigheter et vesentlig bedre beslutningsgrunnlag. Beslutningsstøtten vil gi økt faktakunnskap om uoversiktlige problemstillinger med for eksempel store mengder data og et komplisert situasjonsbilde. Målet er at støtten skal redusere sjansen for feil beslutninger på strategisk nivå.

Strategigruppen ser for seg at oppgaven kan løses på flere måter. Hvor ofte slike trusselvurderinger bør utarbeides, bør vurderes ut fra departementets behov – gjerne etter en fast vurdering av oppdateringsbehovet i sist utførte trusselvurdering. Det sentrale er at det ikke blir opp til tilfeldige adhocutvalg, som denne strategigruppen, å foreta slike vurderinger, men at man får en systematisk gjennomgang og oppdatering av den nasjonale trusselvurderingen om datakriminalitet i takt med endringene i trusselbildet.

Forslaget til en nasjonal trussel- og risikovurdering medfører ingen endringer for de eksisterende ordningene, og sikkerhetsaktørene som i dag utarbeider egne trussel- og risikovurderinger, bør fortsette som før innenfor sine ansvarsområder. Strategigruppens oppfatning er at spesifikke trusselvurderinger må utarbeides i sammenheng med innhenting av data slik at opplysningene kan benyttes på en troverdig måte. En nasjonal trussel- og risikovurdering bør, slik strategigruppen ser det, tegne et mer overordnet trusselbilde enn de spesifikke trusselvurderingene.

Når det gjelder spesifikt datakriminalitet, er det naturlig at politiet leder arbeidet og utarbeider nasjonale trusselvurderinger. Innspill bør kunne gis fra andre sikkerhetsaktørers hendelsesrapportering og vurderinger av trusselsituasjonen. Et slikt ansvar har ikke vært vurdert tidligere for NSM. Svakheten ved en slik løsning er at de involverte kan bli sittende med sin «egen hatt på hodet» og bære med seg både ansvar og retning fra den enheten de representerer. Dette vil også kunne medføre at ordlyden og kvaliteten på trusselvurderingen i for stor grad påvirkes av dette perspektivet. Tilsvarende problemer vil kunne melde seg hvis sikkerhetsaktørene sammen skal utarbeide trusselvurderingen.

Man kan også vurdere å oppnevne et særskilt utvalg som får i oppdrag å utarbeide en helhetlig nasjonal trusselvurdering som et supplement til vurderingene aktørene selv lager. Metodisk er det å anta at et slikt utvalg har behov for å innhente informasjon fra sikkerhetsaktørene som arbeider innenfor feltet datakriminalitet. Strategigruppen antar at en slik gruppe vil kunne levere både en åpen og en begrenset trusselvurdering som kan dekke ulike behov.

Arbeidets organisering må vurderes nærmere. Aktuelle alternativer kan være:

- Trusselvurderingen utarbeides av et uavhengig oppnevnt organ.

- Trusselvurderingen utarbeides av en sentral sikkerhetsaktør, som Kripos eller NSM, i dialog med de øvrige sikkerhetsaktørene.

Konklusjon. Det bør utarbeides en årlig, nasjonal trusselvurdering om datakriminalitet. Vurderingen utarbeides etter innspill fra politiet, PST, NSM, Forsvaret og andre aktuelle offentlige og private sikkerhetsaktører.

7.4.4. Internasjonalt samarbeid

Et særlig trekk ved datakriminalitet er at denne typen kriminalitet utøves over landegrenser. Sakene har ofte både mistenkte og ofre i forskjellige deler av verden, noe som er en utfordring for innhentingen av informasjon, som må skje på tvers av landegrenser gjennom aktivt politisamarbeid. Store internasjonale operasjoner er vanskelige å håndtere for nasjonale politistyrker alene.

Våre analyser av datakrimtrusselen bør ha høy kvalitet og være på nivå med analyser fra land som er toneangivende i bekjempelsen av datakriminalitet. Norge bør være et interessant land å utveksle trusselvurderinger med. Vi er langt fra et slikt mål.

Europol/EC3 er et nytt EU-tiltak, og virksomheten har som oppgave å være den sentrale drivkraften i EU i bekjempelse av datakriminalitet (se punkt 4.3.1). Målet er å gi raskere reaksjoner ved dataangrep og bistå EUs medlemsstater og samarbeidspartnere i å bygge operativitet og analysekapasitet i det forbyggende arbeidet og i etterforskning. Det er behov for å etablere en norsk tilstedeværelse i Europol/EC3 som kan gi raskere bistand og kunnskap om hendelser som kan ha eller få virkning i Norge.

Interpols nye Cyber Crime Centre i Singapore samler og analyserer informasjon om datakriminalitet over hele verden, men fokuserer i særlig grad på de asiatiske landene (se punkt 4.3.2). Interpol vil dessuten satse sterkt på kunnskapsutvikling. Dette gjøres i samarbeid med kunnskapsinstitusjoner og privat sektor slik at politiorganisasjoner kan få raskere tilgang til ny teknologi og anvende denne til å bekjempe datakriminalitet. Innsamling og analyse av store datamengder er et av satsingsområdene som også er interessant for Norge. Det er behov for å etablere en norsk tilstedeværelse i Interpol.

PST mottar store mengder informasjon fra samarbeidende tjenester i utlandet. Noen av disse har påtalemyndighet, men de aller fleste er sivile etterretningstjenester, og informasjon derfra vil dermed være et resultat av ulike etterretningsmetoder. I utgangspunktet vil slik informasjon være klausulert av informasjonseier. Det betyr at informasjonen kun er ment for etterretningsformål, og ikke for offentliggjøring eller til bruk i straffesak. Hvis norske myndigheter ønsker å bruke slik informasjon i en sttraffesak, vil man måtte innhente tillatelse til dette på forhånd, og i mange tilfeller vil en slik tillatelse ikke bli gitt. Årsaken er at etterretningsopplysninger ofte kommer fra sensitive kilder som ikke må avsløres, eller de kan avsløre funksjoner og prioriteringer som må holdes skjult. Det samme vil gjelde for PSTs egeninnsamling av etterretning og etterretning som kommer fra norske samarbeidende tjenester.

Alt etterretnings- og sikkerhetstjenestearbeid er avhengig av et tett og forpliktende samarbeid, både nasjonalt og internasjonalt. Både trusselaktørene og deres bruk av datateknologi er transnasjonale utfordringer som Norge ikke klarer å løse alene. Å styrke det internasjonale samarbeidet er derfor en nødvendig forutsetning for å kunne løse også våre hjemlige utfordringer.

Konklusjon. Politiet må styrke sin deltakelse i internasjonale fora for bekjempelse av datakriminalitet. Det er behov for etablering av en norsk tilstedeværelse i Europol/EC3. Norsk politi bør også ha en tilstedeværelse i Interpols Cyber Crime Centre i Singapore.

7.5. Reguleringsspørsmål

7.5.1. Metodehjemler

Monitorering. Når det gjelder PSTs behov omtalt i punkt 7.2.3 om en statlig etterretningsfokusert evne til å avdekke trusler i elektronisk kommunikasjon som går til og fra Norge, må spørsmålet om lovhjemler og rettsikkerhetsgarantier også utredes, se punkt 7.6. Det

samme gjelder om det etableres andre VDI-systemer for å avdekke datakriminalitet.

Dataavlesning. I visse situasjoner kan politiet og PST gjennomføre kommunikasjonskontroll, dvs. avlytting, av personers bruk av IKT. For å bruke denne metoden må det i hvert enkelt tilfelle innhentes en rettslig kjennelse, og bruken av kommunikasjonskontroll vil være gjenstand for etterfølgende kontroll.

Den teknologiske utviklingen er slik at stadig mer av den databaserte kommunikasjonen er umulig å avlytte med tradisjonelle midler. I praksis betyr dette at kommunikasjonskontroll får mindre og mindre anvendelse, og blir stadig mindre relevant som informasjonskilde. For å bøte på denne situasjonen, og for å kunne utvikle en mer effektiv metode er det foreslått å bruke dataavlesning, som vil gi tilgang til informasjonen ved inntastingen, før den blir kryptert.

Behovet for metoder må imidlertid vurderes kontinuerlig. Ny teknologi utvikles og anvendes raskt, og det stiller oss overfor stadig nye utfordringer. Skal myndighetene kunne forebygge og etterforske datakriminalitet må også de tekniske forutsetningene og hjemmelsgrunnlagene være til stede. Særlig for PST trengs en gjennomgang av hjemmelsgrunnlaget for å kunne følge med på oppfordringer til og trusler om vold som blir lagt ut og delt på lukkede fora. Det vil være viktig, ikke bare for å kunne vurdere ulovlige ytringer, men også for å forstå hva slags propaganda som florerer, og i hvilken grad det er mulig eller formålstjenlig å møte dette med «mot-narrativer». Det samme gjelder for bruk av stordata, der formålet vil være å forstå trender og utviklingstrekk for i neste omgang å kunne forebygge en uheldig utvikling.

For det alminnelige politiet er dette et spørsmål om hvilke hjemler politiet skal ha tilgang til for å kunne utøve sin forebyggende rolle etter politiloven § 2 nr. 2 i den digitale verden.

Konklusjon. Myndighetene bør vurdere om PST og politiet har de nødvendige hjemler til å registrere og lagre ytringer som ligger på åpne kilder.

7.5.2. Tilsynsregulering og rapportering

Det eksisterer en rekke rapporteringsordninger knyttet til forskjellige lover, forskrifter og instrukser når det gjelder trusler, sårbarheter og hendelser som kan true datasystemers sikkerhet. I sivil sektor er tilsynsmyndigheter ofte mottakerne av slike rapporter. De utnytter materialet i sine løpende og periodevise vurderinger og i sitt utviklingsarbeid, og ved umiddelbar håndtering av enkeltsaker med behov for gjenopprettelse av sikkerhet.

Tilsynsmyndighetene følger opp sine sektorer på en rekke områder. Energisektoren har energiloven, Nasjonal kommunikasjonsmyndighet følger opp ekomloven, og finanssektoren er regulert ved IKT-forskriften for finanssektoren. Vi har også sektorovergripende tilsyn slik som Datatilsynet (personopplysningsloven), NSM (sikkerhetsloven) og Difi (eForvaltningsforskriften).

Disse regelverkene er utarbeidet på forskjellige tidspunkter for å dekke ulike behov for håndtering av informasjon som er oppstått som følge av ny infrastruktur.

Resultatet er et lappeteppe av ordninger uten noen sektorovergripende og fremtidsrettet plan eller enhetlig utforming. Eksempelvis inneholder enkelte regelverk bestemmelser om rapportering til politiet, mens andre ikke gjør det. Det er ingen som ser samtlige innrapporterte hendelser i sammenheng for å få en helhetlig situasjonsforståelse. For øvrig er ikke alle virksomheter underlagt noe konkret rapporteringsregime. Det svekker også muligheten for et helhetlig situasjonsbilde.

Når en trussel, sårbarhet eller sikkerhetshendelse er oppstått, er det viktig at man i etterkant sørger for helhetlig læring og forståelse av hvilke konsekvenser disse kan få for samfunnet. Forståelsen må også omfatte det forebyggende arbeidet mot datakriminalitet for å se hvilke virkninger det har på samfunnet.

For å sikre en slik helhetlig forståelse, foreslår strategigruppen at man utarbeider én felles instruks for alle sivile sektorers tilsynsmyndigheter og andre. Den skal sikre at hendelser som kan true datasystemers sikkerhet, enhetlig rapporteres til NSM.

Datakriminalitet må varsles videre til politiet eller PST for straffesaksoppfølgning såfremt det ikke foreligger restriksjoner eller klausuleringer som gjør at slike opplysninger ikke kan formidles til politiet.

Gjennom et nært samarbeid mellom NSM og Kripos vil helhetlig informasjon om slike hendelser

også kunne tilflyte politiet sentralt. Strategigruppen antar at Justis- og beredskapsdepartementet, som har et nasjonalt ansvar for sivil datasikkerhet, kan ta de nødvendige skritt for å få på plass en slik rapporteringsordning. Kommunesektoren bør involveres i dette arbeidet. Detaljene i ordningen foreslås utredet av Kripos og NSM i fellesskap i den utstrekning de ikke fanges opp av pågående utredningsarbeid. Forslaget vil supplere tiltaket i Handlingsplan til nasjonal strategi for informasjonssikkerhet, som innebærer en økt rapportering til NSM fra de sektorvise responsmiljøene som bygges opp (sektor-CSIRT-er).

Konklusjon. For å sikre en helhetlig forståelse, foreslår strategigruppen en gjennomgang av eksisterende regler og barrierer som kan hindre informasjonsdeling mellom sikkerhetsaktører, og en vurdering av om disse er hensiktsmessige. Det bør vurderes å utarbeide en instruks for samtlige sivile departementer om videreraportering til NSM eller et annet sentralt organ fra tilsynsmyndigheter eller tilsvarende av trusler, sårbarheter og hendelser som kan true datasystemers sikkerhet. Her bør muligheter og begrensninger for videreraportering til politiet behandles. Viktige kriterier er hvilke konsekvenser dette kan ha for det nasjonale sikkerhetsarbeidet og for virksomhetene det gjelder.

De eksisterende rapporteringsordningene må også harmoniseres som et ledd i arbeidet. Kommunesektoren bør anmodes om å bidra til rapporteringen.

7.5.3. Datalagring

Behovet for datalagring i et digitalt samfunn. Det finnes mange typer data som lagres i dagens samfunn, og de samles inn av mange aktører og lagres på forskjellige steder som hos teleoperatører, Internett-leverandører, banker med flere. Datateknologiens utvikling endrer også samfunnets kommunikasjonsmønstre, som beskrevet i punkt 3.3. Talekommunikasjon har beveget seg fra analog teknologi over på digital teknologi med Internett-tjenester basert på såkalt datatrafikk ved hjelp av IP-adresser. IP-adresser brukes for å angi sender og mottaker av datapakker over et nettverk, og kan grovt sammenlignes med telefonnumre. Dette skjer også med annen kommunikasjon, som i stadig større grad flyttes over på nettbaserte tjenester. Kommunikasjonen knyttes dermed i mindre grad til telefonnumre, og i økende grad til IP-adresser. Digitale spor i elektronisk utstyr påvirkes av mange ytre faktorer og har ofte kort levetid.

Politiet, flere sikkerhetsaktører og sentrale næringslivsaktører peker på at lovgivers krav om kort lagringstid for logger over IP-adresser – såkalte IP-logger – er en viktig enkeltårsak til at det er vanskelig å oppklare datakriminalitet. Politiet får for eksempel vite at en IP-adresse har vært involvert i distribusjon av overgrepsmateriale eller i et dataangrep mot en virksomhets database. Da trenger de å vite hvem som brukte IP-adressen på det aktuelle tidspunktet. Tilsvarende er politiet ved sporing av pengeoverføringer avhengig av at bankene holder oversikt over hvem som eier bankkontoer, og at teletilbydere holder oversikt over hvem som eier telefonnumre. Ved bortføring, drap og overfallssaker har man også behov for å skaffe en oversikt over hvem som befant seg i et område, ved å utnytte lokasjonsinformasjon i mobilnettverkene våre.

Forskjellige typer lagring av data. Vi må skille mellom allmenn datalagring og målrettet lagring for spesifikke formål. En allmenn datalagring innebærer innsamling uavhengig av mistanke om kriminelle forhold. Målrettet innhenting og registrering skjer blant annet hos sikkerhetsaktørene. PST har behov for å holde oversikt over ekstreme miljøer og enkeltpersoner, for eksempel ved registrering av ekstreme ytringer. Telenor oppbevarer logger over skadelig trafikk, som botnett. NSM holder oversikt over domener og IP-adresser tilknyttet angrep på samfunnskritiske datasystemer. Private aktører samler også inn store mengder informasjon om databruk på Internett til kommersielle formål.

Datalagring handler om den allmenne datalagringen. For å kunne diskutere lagringsbehovet er det nyttig å se på ulike typer av data som lagres:

- Identifikasjonsdata er koblingen mellom nettverksidentitet og faktisk identitet, for eksempel ved IP-adresser og telefonnumre. For telefonnumre har vi telefonkataloger hvor vi kan slå opp hvem som ringer. Noe tilsvarende finnes

ikke for IP-adresser. En kontrollert tilgang til denne koblingen handler rett og slett om ansvarliggjøring. En bruker kan i løpet av en dag bruke et titalls ulike IP-adresser – over mobilnett samt åpne og lukkede, offentlige, trådløse nett. Bruk av nettverksadresseoversettelse (NAT) skaper igjen nye utfordringer ved at flere brukere deler samme IP-adresse på det globale nettverket. I tillegg vil bruk av mellomtjenere kunne skjule den faktiske IP-adressen.

- Metadata er «data som beskriver andre data», det vil si data om bruken av en tjeneste. For telekommunikasjon vil informasjon om tidspunkt, samtalelengde og partene (representert ved telefonnumrene) klart være metadata. Samtalens budskap vil være innholdet, en samtale på et menneskelig språk. Det samme gjelder for SMS, e-post, Facebook-meldinger og Skype-anrop. Metadata for integrerte tjenester som SMS og telefonoppringninger kan lett loggføres. Verre er det med alle de nye IP-baserte tjenestene som ikke er standardiserte, og som ligger utenfor nettverkstilbyderens kontroll. Disse nye tjenestene er ofte kryptert, og det er mange av dem. Teknisk er det mulig å estimere geografisk lokasjon for en abonnent tilknyttet et kommunikasjonsnettverk basert på triangulering og signalstyrke. Denne informasjonen kan også – hvis den loggføres – være viktig i en etterforskning for å avklare alibi eller finne potensielle kilder til mer informasjon i en sak.

- Innholdsdata er det som blir sagt eller skrevet. Det er ikke alltid noe klart skille mellom hva som bør kalles metadata, og hva som er selve innholdet, og det blir ofte et spørsmål om innfallsvinkel. Det gjelder eksempelvis oppslag av domenenavn (DNS). For nettleverandøren er dette helt klart innholdsdata, men for nettleseren er det hovedsakelig metadata.

Jo lengre ned på denne «stigen» man kommer, desto mer usikkerhet kan knyttes til den tekniske evnen til å loggføre heldekkende uten at metoden lett kan omgås. Behovet for lagringsplass øker også drastisk ved loggføring av bruk av tjenester, og det er praktisk umulig å loggføre alle innholdsdata.

Logging av IP-adresser handler om identifikasjon av brukere og IP-adresser på nettverk og kan grovt deles i to hovedkategorier:

- Koblingen mellom IP-adresse og juridisk eier. Denne koblingen gjøres hos Internett-leverandøren.
- Koblingen av IP-adresser mot ulike tjenester på Internett. Dette innebærer en kobling mellom adresse, tid, tjeneste og eventuelle utførte handlinger, som å skrive et leserinnlegg på et forum, sende en e-post eller besøke et nettsted. Det er i utgangspunktet ingen kobling mot den juridiske eieren av IP-adressen. Loggføringen kan skje overalt i det digitale samfunn, også hos Internett-leverandøren, som i utgangspunktet ser alt en abonnent sender og mottar.

Lagring av disse to kategoriene opplysninger representerer utfordringer som må vurderes separat.

Hva bør lagres. Det etterlates digitale spor overalt. I forbrukerutstyr som mobiltelefoner, nettbrett og datamaskiner. Hos leverandører av tjenester på Internett, i betalingssystemer og kommunikasjonssystemer. Det dreier seg om både metadata og innholdsdata. Særlig er IP-adressene betydningsfulle for etterforskningen av datakriminalitet.

Som tidligere nevnt er en IP-adresse en unik identifikator eller adresse som tildeles en dataenhet som er koblet opp og kommuniserer i et Internett-basert nettverk. Alle dataenheter må ha en egen IP-adresse for å kunne kommunisere med andre enheter på Internett. Dette gir en entydig adresse til riktig mottakende dataenhet, uavhengig av om vi identifiserer oss på andre måter.

IP-adresser identifiserer maskinenheten man benytter, og har kobling til brukeren og dennes handlinger, men IP-adressen angir ikke annet enn en unik kommuniserende dataenhet. Den gir ingen sikker informasjon om hvilken person som bruker den. IP-adressen legges igjen og lagres hos ulike tjenestetilbydere ved bruk av Internett. I en etterforskning kan koblingen av en IP-adresse til en abonnent

eller bruker være helt avgjørende for å identifisere en bruker. Et viktig spørsmål er da hvor lenge en IP-adresse og koblingen til en bruker skal kunne lagres slik at politiet kan identifisere hvem som fremstår som bruker. Innlogging med en offentlig elektronisk ID eller identifisering via en sosial nettverksprofil vil være en mye sterkere indikasjon på at det er du, og ikke en maskin du eier, som utfører en handling.

For at slike data skal kunne brukes i bekjempelse av datakriminalitet, må de kunne gjenfinnes. I dag er det ingen lagringsplikt, bare en sletteplikt etter 21 dager. Vi bør også definere en lagringsplikt som minimum tar vare på koblingen mellom tildelte IP-adresser og juridisk eier. Den bør gå utover Internett-leverandørenes 21-dagers sletteplikt, som da også må endres. Norge er i ferd med å bli et fristed for datakriminalitet grunnet manglende oppslagsevne, og vi klarer heller ikke å oppfylle forpliktelser knyttet til samarbeid med andre land.

Koblingen mellom juridisk eier og IP-adresse bør beholdes i minst 2 år. Lang deteksjonstid, internasjonale etterforskninger og vanskeligheter knyttet til å «jobbe seg bakover» gjør at det kan ta lang tid fra en kriminell hendelse inntreffer til en IP-adresse er identifisert. Utlevering bør kun skje til justissektoren og kreve skjellig grunn til mistanke om at en straffbar handling er begått (se også punkt 10.4.4).

Lokasjonsdata fra mobile nettverk er en annen elementær type informasjon, men som er langt mer overgripende. For at mobilnettverkene i det hele tatt skal fungere, slik at innkomne anrop når deg uansett hvor du er i verden, blir det ført en kontinuerlig oversikt over hvor mobilutstyret befinner seg. Nøyaktigheten vil variere. Lagring over tid har helt klart store utfordringer knyttet til personvern, men behovet for å oppklare svært alvorlige forbrytelser tilsier at det bør vurderes å arkivere slike data.

For lokasjonsdata om mobile enheter i telenettverket vil lagringsbehovet typisk være noen uker. Utlevering må være basert på streng kontroll, godkjent av en dommer, med mindre det handler om en krise eller nødssituasjoner hvor politiet har utvidede fullmakter.

Oppbevaringssted, oppbevaringstid og utleveringsrutiner. Det er prinsipielt to steder man kan utføre slik preventiv datalagring. Lokalt hos datakilden, og sentralt. Det er fordeler og ulemper ved begge alternativer. Det er enklere å gjøre oppslag sentralt fordi færre ledd må involveres. Økonomisk er det mer kostbart å opprette et sentralt lager, kanskje statlig finansiert, men lokal oppbevaring hos kommersielle aktører vil også innebære en kostnad. I et sikkerhetsperspektiv vil det være større risiko å putte «alle eggene i samme kurv» om dataene skulle lekke eller misbrukes. På den annen side er det lettere å påvirke og få prioritert gode sikkerhetsløsninger på et sentralt sted. Norge har mange små Internett-leverandører som ikke har de samme forutsetningene for å passe på slike data som de største. Det er også lettere å føre tilsyn med både sikkerhet og bruk knyttet til dataene om de ligger sentralt. Lagringen må skje i Norge.

Datalagringsdirektivet (DLD). En av utfordringene med datalagringsdirektivet var at det omfattet lagring av store mengder data om abonnement, trafikk og tjenester. Kritikerne stilte spørsmål til sikker oppbevaring, politiets tilgang og eventuell senere utvidelse av hvem som skal ha tilgang til dataene. I april 2014 fastslo EU-domstolen[55] at direktivet ville utgjøre et inngrep i den enkeltes krav på privatliv og personvern. Formålet for innsamling var saklig, men drøftelser knyttet til forholdsmessighet og proporsjonalitet samt sikker lagring medførte at direktivet ble vurdert som ugyldig. Mange av svakhetene domstolen påpekte, ble i Norge tatt hensyn til i gjennomføringslovgivningen. Situasjonen i dag er derfor at vi ikke har noe effektivt datalagringsregime. I mangel av en straffeprosessuell hjemmel som DLD skulle ivareta, men som nå er satt på vent, har vi nå en særnorsk praksis der koblingen mellom IP-adresser og eier slettes innen 21 dager. Datatilsynet har i et brev av 13. mai 2009 til IKT-Norge lagt til grunn at denne knytningen skal slettes når virksomhetenes formål med behandlingen er oppfylt. Det formelle grunnlaget er personopplysningsloven § 28[56], som setter forbud mot lagring av unødvendige opplysninger. Hovedregelen er at personopplysninger skal slettes når formålet med behandlingen er oppfylt.

55 http://www.scribd.com/doc/216980523/Judgment-of-the-ECJ-in-Digital-Rights-Ireland-data-retention-challenge.
56 https://lovdata.no/dokument/NL/lov/2000-04-14-31/KAPITTEL_4#§28.

De norske gjennomføringsreglene for DLD har objektive kriterier og prosessuelle vilkår for tilgang og bruk samt kriterier for vurdering av forholdsmessighet. Det er i datalagringsforskriften[57] stilt krav til informasjonssikkerhet, herunder dataintegritet og sporbarhet, og krav om taushetsplikt for personer med tjenstlig behov og autorisasjon av disse. Ny straffeprosesslov §§ 210 b og 210c[58] setter krav til mistanke, kriminalitetstyper og alvorlighetsgrad, til datanes betydning i etterforskningen, til saksbehandling, beslutningskompetanse og at hele prosessen er underlagt domstolskontroll.

Konklusjon. Norske borgere og virksomheter bør ansvarliggjøres for sine digitale handlinger. Det er behov for lagring av data om eierskap til IP-adresser på Internett. Det bør opprettes et pålegg om slik datalagring over en periode som er tilstrekkelig for effektiv straffeforfølgning. For en kortere periode bør også lokasjonsinformasjon fra nettverk med mobilteknologi bli arkivert, slik at politiet ved alvorlig kriminalitet og nødsituasjoner kan benytte denne informasjonen. Plikten til lagring i et gitt tidsrom må hjemles i lov. Mye av grunnlaget for en slik hjemmel er allerede lagt i forbindelse med arbeidet med innføringen av datalagringsdirektivet. Dette bør kunne videreføres og nyanseres i lys av dagens trusler.
Se også punkt 10.4.4 om datalagring.

7.6. Rettssikkerhet og personvern

Innsamling og lagring av informasjon som ledd i kriminalitetsbekjempelse har mange utfordringer. Det eksisterer restriksjoner på *hva slags* informasjon som kan samles inn, og *hva slags metoder* som kan brukes. *Lagring* av informasjon er også regulert. Det samme gjelder bruken av informasjonen og hvem den kan spres til.

7.6.1. Hemmelighold av informasjon

Hensynet til en effektiv forebygging og straffeforfølgning tilsier at politiet trenger en omfattende innsikt i datakriminalitet; trusselaktører, modus, ofre, skadevirkninger osv. Sikkerhetsaktører utenfor politiet er ofte i besittelse av relevant informasjon. De offentlige sikkerhetsaktørene – inklusive politiet – har i utgangspunktet taushetsplikt, men det er mange unntak.

Under straffeforfølgning er unntakene vidtrekkende. Etter straffeprosessloven har både den straffeforfulgte, forsvareren, ofrene og bistandsadvokaten krav på en vidtgående innsikt i bevismaterialet i straffesaken. Domstolene følger offentlighetsprinsippet som gjør at alle bevis som hovedregel skal legges frem for domstolen i full offentlighet.

Etterforskning kan åpnes dersom det er mistanke om en straffbar handling. Fra da av trer straffeprosesslovens bestemmelser om tilgang til informasjon i kraft. Mistanken behøver ikke være rettet mot noen bestemt person. Siktede har dessuten et omfattende menneskerettsvern mot ufrivillig selvinkriminering som også omfatter forklaringer avgitt *før* etterforskningen ble iverksatt.

Datakriminalitetens internasjonale karakter innebærer at informasjon fra andre jurisdiksjoner ofte er viktig. Norsk politi/PST har sjelden kapasitet eller tilstrekkelig juridisk adgang til selv å innhente denne, og er derfor avhengig av internasjonalt samarbeid om informasjonsinnhenting og informasjonsdeling. En betingelse for å overlevere slik informasjon kan være at den ikke må bli offentlig kjent, og i hvert fall at kildene ikke avdekkes slik at de risikerer represalier.

For å holde tritt med de kriminelles bruk av moderne teknologi er politiet avhengig av å kunne benytte hensiktsmessige innsamlings- og etterforskningsmetoder. Noen av metodene som det kan være aktuelt å benytte, er inngripende og reiser rettssikkerhetsproblemer. I strafferett og straffeprosess gjelder et strengt legalitetsprinsipp. Inngripende metoder krever derfor en klar lovhjemmel. De utfordrer også personvernhensyn og kan være problematiske for menneskerettsvernet og ytringsfriheten.

Strategigruppen har som oppgave å foreslå overordnede, langsiktige strategier for bekjempelse av datakriminalitet. Et stort antall eksempler på tiltak drøftes kortfattet for å belyse strategiene. De fleste av dem gjelder informasjon. Det er derfor ikke rom for noen detaljert diskusjon av gjeldende restriksjoner for informasjonshåndtering for hvert enket tiltak. Slike konkrete analyser må gjøres dersom det blir aktuelt å gjennomføre dem.

57 https://lovdata.no/dokument/SF/forskrift/2013-05-14-484.
58 https://lovdata.no/dokument/NL/lov/1981-05-22-25/KAPITTEL_4-6#§210.

7.6.2. Personvern

Det fremgår av mandatet at strategigruppen skal ta hensyn til personvernet i sine vurderinger. Flere problemstillinger vedrørende personvernutfordringer og nye kriminalitetsformer har vært utredet ved flere anledninger, blant annet i *NOU 2009:15 Skjult informasjon – åpen kontroll* og *NOU 2007:2 Lovtiltak mot datakriminalitet*. Strategigruppen viser til disse utredningene, hvor det er gjort et godt arbeid.

I mai 2014 ble den personlige integriteten grunnlovsfestet i en ny paragraf 102 som lyder:

> *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller. Statens myndigheter skal sikre et vern om den personlige integritet.*

Politiets behandling av personopplysninger er regulert i flere lover, forskrifter og instrukser. Som utgangspunkt regulerer personopplysningsloven også behandling av personopplysninger der politiet er ansvarlig. En viktig begrensning følger imidlertid av personopplysningsforskriften § 1-3 som gir unntak fra personopplysningslovens virkeområde for saker som behandles eller avgjøres i medhold av rettspleielovene, herunder straffeprosessloven. Det er imidlertid ikke gitt at denne begrensningen gjelder behandling av opplysninger utenfor en konkret straffesak, for eksempel nedtegnelse av opplysninger i sentrale og lokale registre som brukes i politiets saksbehandling.

Det finnes en rekke hensyn som må tas for å sikre at personvernet ivaretas på en tilfredsstillende måte. Datatilsynet har overfor strategigruppen angitt flere tiltak for å sikre dette.[59] Blant dem er flere krav til *utredning* av konsekvensene for rettssikkerhet og personvern ved innføring eller utvidelse av inngripende etterforskningsmetoder. Problemstillingene som må vurderes, er sammensatte og knyttes både til etterforskningsmetoder og beskyttelse av samfunnet.

Strategigruppen forutsetter at alle hensyn, utredningskrav og prinsipper for personvern blir ivaretatt og vektet av dem som skal utrede gruppens anbefalte tiltak videre, og at beslutningstakerne på et senere tidspunkt følger opp at disse hensynene ivaretas på en adekvat måte før man går til det skritt å innføre metoder og tiltak som kan få konsekvenser for personvernet.

Det er utfordrende, men også svært viktig å beskrive så presist som mulig hva man ønsker å oppnå, og hva man faktisk forsøker å beskytte. I beskrivelsen må man gi argumenter for at det man ønsker å oppnå, kun kan oppnås ved innføring eller bruk av inngripende metoder. I tillegg må man belyse at de interessene man ønsker å beskytte, faktisk er utsatt for alvorlige og overhengende farer eller trusler. Metodene og virkemidlene som vurderes, må begrunnes i en sannsynlighet for at de er effektive, og faktisk vil bidra til å redusere risiko eller øke muligheten til å hindre og bekjempe kriminelle handlinger, samtidig som kostnadene tiltakene vil medføre, kan rettferdiggjøres.

Et helt sentralt vurderingskriterium er om metoden er proporsjonal med hensyn til krenking av individets frihet og personlige integritet. Metoder og virkemidler må også ses i lys av det eventuelle skadepotensialet de kan ha. Blant annet må man vurdere hvorvidt innføringen av en metode eller et tiltak faktisk kan skade befolkningens tillit til myndighetene, fremfor å øke tryggheten i befolkningen.

Det anbefales at metoder som kan synes inngripende, vurderes etter anerkjente kriterier. Særlig ved innhenting og analyse eller behandling av store informasjonsmengder kan det være hensiktsmessig å vurdere metodens inngripen i privatlivet gjennom en PIA-vurdering ('Privacy Impact Assessment') der man i tillegg til å ta for seg de sentrale problemstillingene som er skissert over, også svarer på:

- Hvem skal samle informasjon om hvem?
- Hvem skal ha tilgang til opplysningene?
- Hvor lenge skal opplysningene lagres?
- Skal det gis informasjon til dem som blir eller har blitt overvåket, som et kompenserende tiltak?

Strategigruppen har fortløpende i denne fremstillingen poengtert at personvernet må ivaretas. Kriteriene som må oppfylles for at personvernet anses ivaretatt,

59 Se *Datatilsynets innspill til Arbeidsgruppe om digitale sikkerhetsutfordringer og personvernspørsmål*. Redigert versjon 7. januar 2015 – kapittel V tatt ut. Justeringene i notatet ble gjort som følge av strategigruppens spørsmål til møtet 17. desember 2014.

kan med utgangspunkt i personopplysningsloven kort oppsummeres som:

- behovet for en lovhjemmel
- et klart definert formål
- en berettiget interesse
- sikring av eventuelle opplysninger
- behovet for et visst tilsyn og oppfølging

Hvor målrettet metoden er, kan fremheves. Dersom den innebærer at politiet får kjennskap til en stor mengde data som er irrelevant for forebygging og straffeforfølgning, taler det mot å tillate metoden.

Tilsvarende gjelder for sensitiviteten av opplysningene. Metadata i små mengder – om hvem som kommuniserer med hvem – anses normalt som mindre sensitive enn innholdsdata. Dette er annerledes ved innsamling av store mengder metadata. Etablering av strenge informasjonssikkerhetstiltak vil derfor ikke automatisk innebærer et godt personvern.

Konklusjon. Når strategigruppen fremmer forslag om tiltak for å forbedre informasjons- og etterforskningsmetodene, forutsetter den at Datatilsynets utredningskrav og prinsipper for personvern blir ivaretatt som ledd i utredningsprosessen. Politiet må ha mulighet til å behandle personopplysninger i nødvendig utstrekning for å bekjempe datakriminalitet.

Regelverket er i dag uoversiktlig. Det trengs en gjennomgang av bestemmelser som regulerer politiets behandling av personopplysninger, samt en vurdering av lovverk som regulerer andre behandleres lagring eller sletting av opplysninger med relevans for bekjempelsen av datakriminalitet. Det har aldri vært gjennomført noen bred evaluering av personvernets kår i justissektoren, slik det ble gjort for de fleste andre sektorers del av Personvernkommisjonen[60]. Spesielt i forbindelse med bekjempelse av datakriminalitet er det behov for å nedsette en personvernkommisjon som kan se alle personvernutfordringene i sammenheng.

60 Kommunal- og moderniseringsdepartementet, *NOU 2009: 1 – Individ og integritet. Personvern i det digitale samfunnet*.

7.7. Hovedstrategi for deteksjon og analyse

Kapasiteten til å innhente data og analysere datakrimtrusselen må styrkes vesentlig, både nasjonalt og gjennom deltakelse i internasjonale ordninger for bekjempelse av datakriminalitet. Et nært samarbeid med forskere om utvikling av analysemetoder og analysekapasitet trengs. Politiet og PST må sikres et relevant og nødvendig informasjonsgrunnlag for planlegging av målrettet forebygging, avdekking og avverging av datakrimtrusler, samt for effektiv straffeforfølgning av begått datakriminalitet.

Statistikk skal være et viktig instrument i planleggingen og ressursfordelingen. Ansvaret for en samlet og koordinert analyseinnsats bør ligge på sentralt nivå i politiet.

En effektiv og smidig informasjonsdeling mellom alle sikkerhetsaktørene er viktig. Det bør derfor etableres mer partnerskap mellom politiet og andre offentlige og private virksomheter for å dele informasjon. Regelverket må ivareta det.

Konkrete trusler må så langt som mulig avdekkes tidsnok til at de kan forebygges eller avverges. Alle viktige opplysningskilder må utnyttes. Etterretningsmål og -metoder må kontinuerlig oppdateres og utvikles i takt med trusselbildet. Bevis av verdi for en mulig etterforskning må preventivt søkes sikret. Metodene må veies mot hensynet til individets rettsikkerhet, personvern og menneskerettigheter.

Systemene for tips og anmeldelse til politiet fra ofre og publikum må forenkles og bedres vesentlig. Ofrene må få vite hvor de skal henvende seg for å få hjelp.

Anbefalte tiltak:

NB: Nummereringen av de anbefalte tiltakene nedenfor angir ikke prioriteringer.

7.1 *Gjennomgå oppgavefordelingen mellom lokalt og sentralt nivå i politiet knyttet til informasjonsinnhenting og analyse*. Se punkt 7.2.2 og 7.3.2.

7.2 *Øke PST og politiets tilstedeværelse på Internett, både i form av åpen og skjult tilstedeværelse, med kapasitet til å gå i dialog, avdekke kriminelle forhold og innhente annen relevant informasjon*. Se punkt 7.2.2, 7.5.1 og 9.5.1.

7.3 *Etablere en norsk tilstedeværelse i relevante multilaterale og bilaterale fora og ordninger*. Tilstedeværelse i Europol/EC3 og Interpols nye Cyber Crime Centre bør sikres. Se punkt 7.4.4.

7.4 *Videreutvikle spørreundersøkelser for å kartlegge skjult datakriminalitet, slik som Mørketallsundersøkelsen*. Se punkt 7.3.1.

7.5 *Revidere i detalj dagens registreringspraksis og kodeverket for registrering av datakriminalitet for å øke kvaliteten på statistikkgrunnlaget*. Det bør utarbeides en årlig statistikk over viktig datakriminalitet. Se punkt 7.3.1.

7.6 *Gjennomgå eksisterende regler og barrierer mot informasjonsdeling mellom sikkerhetsaktører, og vurdere om de er hensiktsmessige*. Se punkt 7.4.1.

7.7 *Utarbeide en årlig nasjonal trusselvurdering av datakriminaliteten i Norge*. Se punkt 7.4.3.

7.8 *Videreutvikle en arena for samarbeid mellom politi og privat sektor med fokus på forebygging og etterforskning*, som et supplement til eksisterende samarbeidsordninger. Se punkt 7.4.2.

7.9 *Iverksette forskningsprosjekter om stordataanalyse for å effektivisere utnyttelsen av politiets informasjon og kartlegge mulighetene for automatisk oppdagelse av datakriminalitet*. Se punkt 7.3.2, 11.1.2 og 11.2.1.

7.10 *Legge til rette for betydelig utvidet lagring av informasjon om kobling mellom IP-adresser og juridisk eier*. Se punkt 7.5.3.

7.11 *Utrede personvernkonsekvenser av alle tiltak for å forbedre informasjons- og etterforskningsmetodene i overenstemmelse med anerkjente personvernprinsipper*. Se punkt 7.6.

7.12 *Opprette et sentralt mottak i politiet for tips om datakriminalitet med god tilgjengelighet*. Funksjonen bør ha kapasitet til veiledning og videreformidling for oppfølging. Se punkt 7.2.1.

8. STRATEGI FOR KRIMINALISERING

8.1. Kriminaliseringens grunnleggende betydning i bekjempelsen av datakriminalitet

Straffelovgivningen styrer kriminalitetsbekjempelsen. For det første angir den hvilke datahandlinger som anses som så samfunnsskadelige at de bør rammes av samfunnets strengeste reaksjonsform – straff. For det andre angir den hva slags straffer som bør benyttes, og hvor strenge de bør være. Bøter og frihetsstraff er de vanligste straffeformene.

Straffelovgivningen er derfor en sentral strategisk rammebetingelse når politiet og rettsvesenet skal bekjempe uønskede og samfunnsskadelige datahandlinger. Verken politiet, påtalemyndigheten eller domstolene har hjemmel til å bekjempe uønskede datahandlinger som ikke rammes av straffelovgivningen.

Politiet og påtalemyndigheten har ansvaret for å etterforske datakriminalitet. Måten handlingene er kriminalisert på, har innvirkning på hvor krevende det er å skaffe nødvendige bevis. Hvor streng straffen er, har betydning for hvor mye ressurser det er forsvarlig for politiet og påtalemyndigheten å bruke på etterforskning og iretteføring.[61]

Mens alle sikkerhetsaktører kan innhente informasjon de har behov for, også om straffbare datahandlinger, er det bare politiet, påtalemyndigheten og domstolene som har myndighet til å bruke denne informasjonen til å behandle og avgjøre straffesaker. Finner de ikke grunnlag for å fremme noe straffekrav, er avgjørelsen bindende for alle andre sikkerhetsaktører, selv om handlingene det er snakk om, har stor skadevirkning.

Etter politiloven § 2 (2) og (3) er politiet også tillagt viktige oppgaver med å forebygge, avdekke og stanse straffbare datahandlinger.[62] Måten kriminaliseringen skjer på, har derfor også betydning for denne siden av politiets virksomhet. Hvis det er stor grad av samsvar mellom de datahandlingene sikkerhetsaktørene ønsker å forebygge, og de som er kriminalisert, er det også et godt faglig grunnlag for et omfattende samarbeid mellom politiet og andre sikkerhetsaktører om å forebygge, avdekke og stanse datakriminalitet.

Kapittel 3 omhandler kriminalitetsutviklingen. Etter strategigruppens syn er det et betydelig behov for å modernisere den eksisterende straffelovgivningen mot datahandlinger i tråd med utviklingen.

8.2. Nåværende kriminalisering

8.2.1. Rettsutviklingen

Straffebestemmelsene mot datakriminalitet ble omfattende, og for første gang helhetlig, utredet i forbindelse med vedtakelsen av straffeloven 2005. Utredningen resulterte i lovens kapittel 21 om vern av informasjon og informasjonsutveksling, og noen enkeltbestemmelser rettet mot datakriminalitet ble inntatt i andre kapitler i loven, blant annet § 351 annet ledd (dataskadeverk) og § 371 bokstav b (databedrageri). De nye bestemmelsene ble tilføyd ved lov 19. juni 2009 nr. 74.

Utredningsarbeidet foregikk rundt midten av 2000-tallet. I datasammenheng – hvor endringene i kriminalitetsbildet skjer raskt – er det derfor gått lang tid siden regelverket mot datakriminalitet ble utredet i tilnærmet full bredde. Justis- og beredskapsdepartementet har varslet at straffeloven 2005 vil tre i kraft

61 Etterforskning og iretteføring av datakriminalitet behandles i kapittel 10.

62 Forebygging og avverging av datakriminalitet behandles i kapittel 9.

i løpet av 2015, men iverksettelsen av flesteparten av bestemmelsene i kapittel 21 har blitt forskuttert ved at tilsvarende bestemmelser er inntatt i den gjeldende straffeloven.

Straffeloven 1902 inneholder ikke noe eget kapittel som beskytter retten til informasjon og informasjonsutveksling, som bestemmelser mot datakriminalitet. Over tid, og særlig ved forskutteringen av de nye bestemmelsene i straffeloven 2005, har det tilkommet enkeltbestemmelser mot datakriminalitet, blant annet disse:

- § 145 annet ledd (uberettiget adgang til data eller programutrustning)
- § 145b (uberettiget befatning med tilgangsdata, dataprogram mv.)
- §§ 145c og 294a (identiske bestemmelser om fare for driftshindring)
- § 190a (identitetskrenkelse)
- § 270 nr. 2 (databedrageri)

Det har altså vært en viss revisjonsvirksomhet, men ellers anvendes generelle bestemmelser mot tyveri, underslag, utroskap, skadeverk, ulovlig bruk og lignende også mot skadelige handlinger knyttet til datateknologi.

8.2.2. Datakrimutvalgets forslag og straffeloven 2005 kapittel 21

Straffelovkommisjonen foreslo i 2002[63] et eget kapittel i straffeloven om vern av informasjon og informasjonsutveksling. Det skulle inneholde bestemmelser mot datakriminalitet, men også om vern av informasjon og informasjonsutveksling som ikke knytter seg til datateknologi.

Datakrimutvalget. Regjeringen opprettet 11. januar 2002 et eget utvalg som skulle utrede lovtiltak mot datakriminalitet: Datakrimutvalget. Utvalget avga to utredninger.

Den første delutredningen[64] gjaldt gjennomføringen av Europarådets konvensjon av 8. november 2001 om bekjempelse av datakriminalitet (Budapestkonvensjonen). Utredningen ble fulgt opp med at Norge ratifiserte konvensjonen, i tillegg til at det blant annet ble tilføyd en ny § 145b i straffeloven 1902 (uberettiget befatning med tilgangsdata, dataprogram mv.), som senere ble endret ved lov 8. april 2005.

Formålet med den neste delutredningen[65] var å utarbeide forslag til straffebestemmelser mot datakriminalitet som kunne inngå i departementets arbeid med straffeloven 2005.

Av denne utredningen fremgår det at Datakrimutvalget fant at «dagens regler om datakriminalitet er utilstrekkelige, og at det foreligger et reelt behov for presiseringer og en viss nykriminalisering».[66] Blant forslagene til sistnevnte var å kriminalisere elektronisk kartlegging av datasystemer, ulovlig anbringelse av utstyr som kan påvirke databehandling, identitetstyveri, bruk av uriktig identitet og masseutsendelse av elektroniske meldinger.

Datakrimutvalget foreslo også en rekke endringer av strukturell karakter som er av særlig interesse for kriminaliseringsstrategien. Det drøftet prinsippene for kriminalisering av uønskede datahandlinger og gikk inn for ordninger som avviker til dels betydelig fra dagens system. Det foreslo blant annet

- et eget kapittel i straffeloven om datakriminalitet utelukkende bestående av dataspesifikke bestemmelser
- en egen bestemmelse med legaldefinisjoner
- gradering av straffebudene i liten, vanlig og grov overtredelse
- kriminalisering av grov uaktsomhet for visse overtredelser
- markant høyere strafferammer
- en presisering av straffeloven 2005 § 7 om straffelovens jurisdiksjon

Justis- og politidepartementet. I Ot.prp. nr. 22 ga departementet Datakrimutvalgets ulike forslag begrenset tilslutning, men det hadde et annet syn på behovet for nykriminalisering. Det fant at Datakrimutvalget «fremmer forslag om en rekke bestemmelser som utvider området for det straffbare».[67] I proposisjonen står det om kapittel 21 i

63 Justis- og beredskapsdepartementet, *NOU 2002: 4 Ny straffelov – Straffelovkommisjonens delutredning VII*.
64 Justis- og beredskapsdepartementet, NOU 2003: 27 Lovtiltak mot datakriminalitet.
65 Justis- og beredskapsdepartementet, NOU 2007: 2 Lovtiltak mot datakriminalitet – Delutredning II.
66 Ibid., s. 9.
67 *Ot.prp. nr. 22 (2008–2009)*, s. 17.

straffeloven 2005 at det «viderefører i hovedsak gjeldende rett», og at «enkelte av forslagene videreutvikler gjeldende bestemmelser for å fange opp flere straffverdige handlinger».[68]

En viss nykriminalisering skjedde. Nytt i departementets forslag, som nå er en del av både straffeloven 1902 og straffeloven 2005, var kriminalisering av «identitetskrenkelse» (1902 § 190a og 2005 § 202) og «uberettiget befatning med dataprogram mv.» (1902 § 145b bokstav b og 2005 § 201 bokstav b).

Departementet fant derimot ikke tilstrekkelig grunn til å følge opp Datakrimutvalgets forslag om å kriminalisere elektronisk kartlegging av datasystemer, ulovlig anbringelse av utstyr som kan påvirke databehandling, eller masseutsendelse av elektroniske meldinger.

Datakrimutvalget fikk heller ikke gehør for forslaget om egne straffebestemmelser mot dataskadeverk, uberettiget bruk av datasystemer mv., etterfølgende befatning med ulovlig tilegnet data og databasert informasjon, driftshindring og kontomisbruk. Også etter straffeloven 2005 skal altså generelle bestemmelser, om blant annet heleri (§§ 332 og 337) og ulovlig bruk (§§ 343 og 344), anvendes mot skadelige handlinger knyttet til datateknologi. I noen av de generelle bestemmelsene presiseres det imidlertid at datakriminalitet rammes, blant annet i § 351 annet ledd (dataskadeverk) og § 371 bokstav b (databedrageri).

Departementet tok utgangspunkt i Straffelovkommisjonens skisse til kapittelinndeling. Her var straffebestemmelser mot datakriminalitet og annen informasjonsvirksomhet slått sammen i samme kapittel. Denne systematikken er brukt i straffeloven 2005 kapittel 21 om vern av informasjon og informasjonsutveksling.

Departementet fulgte heller ikke opp Datakrimutvalgets øvrige generelle endringsforslag og gikk gjennomgående inn for vesentlig lavere strafferammer enn Datakrimutvalget hadde foreslått. Departementet fant heller ikke grunn til å endre jurisdiksjonsbestemmelsen i straffeloven 2005 § 7. Stortinget sluttet seg til dette.

68 Ibid., s. 12.

Oppsummering. Kriminaliseringsstrategien for datakriminalitet har altså vært kontroversiell.

Datakrimutvalget, som hadde faglig ekspertise på datakriminalitet, mente at den eksisterende kriminaliseringen ikke var godt nok tilpasset den eksisterende trusselen, og at en betydelig oppgradering og effektivisering av det strafferettslige vernet måtte til.

Justisdepartementet som fagmyndighet vektla derimot alminnelige kriminaliseringshensyn som at straff skal brukes med varsomhet, og at datakriminalitet bør behandles mest mulig på linje med annen kriminalitet. Hensynet til de profesjonelle brukerne av straffebestemmelsene (politiet, påtalemyndigheten, domstolene og advokatene) anses vanligvis best tjent med generelle bestemmelser som kan anvendes på et stort spekter av handlinger. Generelle bestemmelser gjør også revisjonsbehovet mindre.

De lovgivende myndighetene anså ikke de nasjonale utfordringene knyttet til trusselen fra datakriminalitet som spesielt store. Den sterke økningen i databruk og utviklingen av stadig mer sofistikert datautstyr som også kan brukes til kriminalitet, har endret dette. Kriminaliseringsbehovet må vurderes ut fra dagens trusler – ikke ut fra trusselbildet fra midten av 2000-tallet.

8.2.3. Budapestkonvensjonen

Budapestkonvensjonen var en viktig utløsende faktor for utredningsarbeidet på 2000-tallet.[69] Vi skal derfor gå nærmere inn på konvensjonens innhold og betydning for kriminaliseringsstrategien.

Arbeidet med Budapestkonvensjonen ble innledet i 1996, etter en erkjennelse av at samfunnet gradvis blir mer avhengig av datateknologi og dermed mer sårbart for nye former for kriminalitet. Europarådet (ved styringskomiteen for strafferettslige og straffeprosessuelle spørsmål) så derfor et «behov for en konvensjon med både strafferettslige og straffeprosessuelle bestemmelser, for å sikre at lovgivningen i medlemsstatene ble bedre tilpasset til den nye tids krav. Konvensjonen burde i tillegg legge til rette for et tett internasjonalt samarbeid».[70] Konvensjonen ble vedtatt 8. november 2001. Norge ratifiserte den 30. juni 2006.

69 Europarådets konvensjon av 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (Budapestkonvensjonen).

70 *Ot.prp. nr. 40 (2004–2005)*, s. 7.

Budapestkonvensjonen består av tre hoveddeler. Den første delen er konvensjonens forslag til straffebestemmelser (art. 2–10), som pålegger partene å kriminalisere ulike former for samfunnsskadelig bruk av informasjonsteknologi, for eksempel

- datainnbrudd (art. 2)
- dataskadeverk (art. 4)
- besittelse og spredning av tilgangsmidler/ hackerprogramvare (art. 6)

De foreslåtte straffebestemmelsene rammer bare forsettlige handlinger. I tillegg omfatter artikkel 11 og 12 bestemmelser om forsøk, medvirkning, etterfølgende bistand og foretaksansvar.

Artikkel 13 stiller krav til at lovbrudd «skal kunne straffes med effektive, forholdsmessige og forebyggende straffereaksjoner».

Straffebestemmelsene fastsetter minstekrav til gjennomføringen av konvensjonen i nasjonal rett, og statene kan opprettholde eller vedta straffebestemmelser som er mer vidtgående enn konvensjonens bestemmelser.

Målet med harmonisering av straffebud er primært å «lette bekjempelsen av datakriminalitet, både på nasjonalt og internasjonalt nivå. Videre reduseres risikoen for jurisdiksjoner med lavere standarder, såkalte 'data havens'».[71]

Den andre hoveddelen inneholder konvensjonens straffeprosessuelle bestemmelser (art. 14–21), som blant annet pålegger partene å gi regler om ulike tvangsmidler, som midlertidig sikring av lagrede data (art. 16), utlevering av elektronisk lagrede data (art. 18) og ransaking og beslag av datasystemer og lagringsmedier (art. 19). Disse bestemmelsene kommer vi tilbake til i kapittel 10.

Den tredje hoveddelen er konvensjonens bestemmelser om internasjonalt samarbeid om bekjempelse av datakriminalitet og sikring av elektroniske bevis i alle typer straffesaker (art. 23–35). Bestemmelsene er delt i to. Den første delen inneholder generelle prinsipper for internasjonalt samarbeid, og den andre delen etablerer egne mekanismer for internasjonalt samarbeid i saker som gjelder datakriminalitet og elektroniske bevis. Mekanismene gjelder blant annet sikring av lagrede data, tilgang til lagrede data og offentlig tilgjengelige data, avlytting av innholdsdata i sanntid og etablering av et 24/7-nettverk.

Konvensjonen er per i dag ratifisert av 44 stater og kan i henhold til artikkel 36 også tiltres av stater som ikke er medlemmer av Europarådet. Blant annet har USA, Canada og Japan tiltrådt konvensjonen.

Da ratifikasjonsspørsmålet ble behandlet i Norge, ble det lagt til grunn at «norsk strafferett er i det alt vesentlige i samsvar med de krav konvensjonen stiller».[72] Departementet fant at det kun var artikkel 6 som nødvendiggjorde en lovendring, og det førte til at en ny § 145b i straffeloven 1902 om ulovlig spredning av tilgangsdata ble vedtatt 8. april 2005.

I tillegg ble det lagt til grunn at norsk straffeprosess i hovedsak var i samsvar med kravene i konvensjonen.[73] Kun tre av artiklene (art. 16, 17 nr. 1 bokstav b og 19 nr. 4) nødvendiggjorde endringer i straffeprosessloven, og følgelig ble en ny § 199a om opplysningsplikt under ransaking og en ny § 215a om sikringspålegg vedtatt 8. april 2005.

Det er kun utarbeidet én tilleggsprotokoll til konvensjonen, om kriminalisering av rasistiske og fremmedfiendtlige handlinger begått ved hjelp av et datasystem. Norge har ikke signert tilleggsprotokollen, siden den anses for å være problematisk med hensyn til ytringsfriheten. Protokollen skal også ha fått begrenset betydning.

Konvensjonen har ikke vært gjenstand for endringer, og tilpasning til nye former for datakriminalitet skjer gjennom retningslinjer kalt TCY Guidance Notes, som forankres i konvensjonens bestemmelser. Land som har undertegnet konvensjonen, møtes årlig for å diskutere strategier og retningslinjer. I disse møtene besluttes det hvordan konvensjonen skal følges opp, etter forslag fra et sekretariat eller nedsatte arbeidsgrupper.

Det er flere kriminalitetsformer og problemstillinger som ikke eksplisitt nevnes i konvensjonens bestemmelser, men som omhandles i TCY Guidance Notes. Noen eksempler er identitetstyverier, tjenestenektangrep, søppelpost og botnett. Arbeidet med disse retningslinjene pågår fortløpende, og konvensjonen har vist seg å være fleksibel med hensyn til

71 *NOU 2003: 27 Lovtiltak mot datakriminalitet*, s. 13.

72 *Ot.prp. nr. 40 (2004–2005)*, s. 12.
73 Ibid., s. 22.

nye problemstillinger, blant annet på grunn av den teknologinøytrale teksten.

Utover denne regelutviklingen arbeider Europarådet for å tilse at partenes nasjonale lovgivning er i samsvar med konvensjonen, også etter ratifikasjonen.

Omfattende internasjonalt samarbeid om bekjempelse av datakriminalitet er en vesentlig del av nær sagt alle hovedstrategiene i konvensjonens videre arbeid. Konvensjonen er et sentralt instrument for folkerettslig utvikling av forpliktelsen til å kriminalisere uønskede og skadelige datahandlinger. Visjonen om at Norge skal være blant de ledende landene i den internasjonale utviklingen,[74] tilsier at vi bør legge stor vekt på å delta i Europarådets fora for å videreutvikle konvensjonen. Se også punkt 10.7.2.

Det kan innvendes at Europarådets folkerettslige regelutvikling er en langsom og lite effektiv prosess for kriminalisering, siden den er basert på konsensus mellom medlemsstatene og følgelig ikke kan gå lenger enn det de minst reforminteresserte statene ønsker.

Den er imidlertid et viktig forum for uformelt påtrykk og informasjonsutveksling, og de forpliktelsene en stat har påtatt seg, er det vanskelig å neglisjere helt uten legitim kritikk fra andre medlemsstater. Budapestkonvensjonen hindrer heller ikke et land i å gå lenger i bekjempelsen av datakriminalitet enn det konvensjonen krever. Den definerer bare minimumsforpliktelser til å kriminalisere uønskede datahandlinger.

Norge bør derfor ligge i forkant av utviklingen når det gjelder nasjonal kriminalisering. Datakriminaliteten er internasjonal. Hvis vi tar sikte på å være et eksempel for andre land og påvirke dem til en mer effektiv nasjonal bekjempelse av datakriminalitet, kan vi også redusere datakriminaliteten som aktører i andre land retter mot Norge. Det kan være en vel så effektiv metode som at norsk politi forsøker å forhindre og straffeforfølge datakriminelle i andre land. Uansett kan disse to metodene kombineres.

8.3. Svakheter ved dagens kriminalisering

8.3.1. Endringer i trusselbildet

Et hovedtrekk ved datakriminaliteten er som nevnt at den er dynamisk. Trusselbildet kan som følge av den teknologiske utviklingen endre seg raskt, og raskere enn på andre kriminalitetsområder. Dette setter lovverket under press, og det er viktig at straffelovgivningen er oppdatert i tråd med teknologiutviklingen.

I tillegg omfatter definisjonen av datakriminalitet mange og ulike kriminalitetsformer. Noen av dem, og da gjerne de tradisjonelle, som omsetning av narkotika over nettet, rammes greit av generelle straffebestemmelser. Andre former er vanskeligere å regulere og kan også kreve dataspesifikke gjerningsbeskrivelser. Et eksempel er de identiske bestemmelsene om «uberettiget befatning med tilgangsdata, dataprogram mv.» i straffeloven 1902 § 145b bokstav b og straffeloven 2005 § 201 bokstav b.

På bakgrunn av dette er det grunn til å stille spørsmål ved om gjeldende lovgivning er god nok, og om hvordan man på en hensiktsmessig måte kan sikre en løpende oppfølgning av eventuelle fremtidige behov for endringer i straffelovgivningen.

En vurdering av hvorvidt det er behov for endringer i straffelovgivningen i dag, bør gjøres på grunnlag av den nye straffeloven, siden den skal tre i kraft i løpet av 2015. Som nevnt over er likevel elementene av nykriminalisering i straffeloven 2005 i all hovedsak allerede inkorporert i gjeldende straffelov, men med en noe annerledes plassering av bestemmelsene.

I forbindelse med vedtakelsen av straffeloven 2005 kapittel 21 i 2009 foretok lovgiver en rekke veivalg. Blant annet ble ikke kapittelet forbeholdt typiske datakriminelle handlinger, og det ble fastholdt at «det som utgangspunkt ikke bør vedtas særregler for handlinger som begås ved hjelp av moderne teknologiske hjelpemidler når handlingene rammes av allerede eksisterende straffebud mot tyveri, utroskap, dokumentfalsk mv.»[75] Man kan spørre seg om det er for tidlig å revurdere alle eller noen av disse valgene, blant annet fordi lovens bestemmelser og system ennå ikke er iverksatt i sin fulle bredde. Men i datasammenheng er det allerede gått lang tid,

74 Se kapittel 6.

75 *Ot.prp. nr. 22 (2008–2009)*, s. 20.

og det bør uansett undersøkes om det er behov for oppdatering. Kriminaliseringen holder ikke følge med teknologiutviklingen.

Bildet av datakriminaliteten fra midten av 2000-tallet er et helt annet enn bildet på midten av 2010-tallet. Samfunnet har i langt større grad satset på databruk som et sentralt verktøy og gjort seg langt mer avhengig av at det fungerer uforstyrret. Behovet for å analysere og ruste opp innsatsen mot datakriminalitet er nå erkjent i flere offentlige dokumenter (se punkt 5.2). Strategigruppen vil derfor drøfte kriminaliseringsstrategien på nytt og uavhengig av de tidligere politikkvalgene på området.

8.3.2. Utilstrekkelig kriminalisering

Datakrimutvalget kom med flere forslag til kriminalisering som Justisdepartementet ikke fulgte opp, blant annet

- elektronisk kartlegging av datasystemer
- ulovlig anbringelse av utstyr mv.
- masseutsendelse av elektroniske meldinger

Datakrimutvalget ønsket også egne, særskilte straffebestemmelser mot

- dataskadeverk
- uberettiget bruk av datasystemer mv.
- etterfølgende befatning med ulovlig tilegnet data og databasert informasjon
- driftshindring og kontomisbruk

Her mente Justisdepartementet at de eksisterende straffebestemmelsene mot tilsvarende handlinger i den fysiske verden var tilstrekkelige. I noen av de generelle bestemmelsene i straffeloven 2005 presiseres det imidlertid at datakriminalitet rammes, blant annet i § 351 annet ledd (dataskadeverk) og § 371 bokstav b (databedrageri).

Datakrimutvalget foreslo også ytterligere kriminalisering av forberedelseshandlinger uten at lovgiver fant gode nok grunner til å følge opp dette.

Etter forslag fra Kripos i mai 2014, aktualisert av omsetning på nettet av spionprogramvaren Blackshades, vurderte Justis- og beredskapsdepartementet om det skulle gjøres straffbart å kjøpe og selge spionprogramvare. Arbeidet er foreløpig stilt i bero. I dag kan slik befatning med spionprogramvare trolig rammes av straffeloven 1902 § 145b bokstav b, dersom kjøp og salg skjer «med forsett om å begå en straffbar handling».

Strategigruppen har også identifisert noen områder som ikke er lovregulerte. I vår kontakt med ulike private og offentlige aktører har vi bedt om å få vite om det finnes skadelige handlinger knyttet til datateknologi som ikke er straffbare per i dag, men som bør kriminaliseres. Strategigruppen har også foretatt egne kartlegginger og vil peke på noen aktuelle problemstillinger knyttet til kriminalisering:

- Kjøp og salg av skadevare (slik som spionprogramvare) har gitt økt tilgang til verktøy som kan brukes til å utføre datakriminalitet. Per dags dato er ikke slikt salg og kjøp ulovlig, med mindre forsettet er å begå en kriminell handling.
- Elektronisk kartlegging av datasystemer og ulovlig anbringelse av utstyr som kan samle store mengder informasjon, er en økende trussel mot lovlig virksomhet og personvernet.
- Gjennom barnelokking ('grooming') på nettet forledes ofre til å vise seg frem gjennom seksuelle handlinger som dokumenteres og spres over nettet.
- Vernet mot krenkelser av privatlivets fred over Internett har svakheter som blant annet ble eksponert i Snapchat-saken, som gjaldt spredning av store mengder private bilder og andre data.

Straffeloven 2005 § 204 rammer innbrudd i datasystemer og viderefører straffeloven 1902 § 145 annet ledd hva gjelder lagrede data. Det kan stilles spørsmål ved om Høyesterett[76] har begrenset denne bestemmelsen for mye, og om dette gir grunnlag for å vurdere å endre den. I den aktuelle saken ga fornærmede PC-en sin og påloggingspassordet sitt til tiltalte for at han skulle ordne opp i virusproblemer på maskinen. Høyesterett la til grunn at tiltalte fikk anledning til å undersøke maskinen i sin helhet. Tiltalte benyttet anledningen til å kopiere privat informasjon fra PC-en over på sin egen maskin. Høyesterett fant at tiltalte i

76 *Rt. 2012*, s. 1669.

denne situasjonen ikke uberettiget hadde skaffet seg tilgang til data som lå åpne for ham etter påloggingen. Tiltalte kunne følgelig ikke straffes selv om handlingen var klart straffverdig.

Denne dommen illustrerer også at selve tilegnelsen av data og databasert informasjon ikke har noe generelt strafferettslig vern i dag. Straffeloven 2005 § 204 gjelder det å skaffe seg tilgang til data.[77] Datakrimutvalget[78] foreslo i §§ 5 og 6 i lovutkastet sitt egne bestemmelser om henholdsvis informasjonstyveri og datatyveri. Departementet fant imidlertid, under tvil, ikke grunn til å kriminalisere den uberettigede tilegnelsen i tillegg til den uberettigede tilgangen.[79] Departementet pekte på at det er en rekke bestemmelser som rammer ulike tilfeller av tilegnelse av data og informasjon, blant annet i straffeloven, om utroskap og bedriftshemmeligheter, og i personopplysningsloven.[80]

Nye straffverdige former for utnyttelse av datateknologi vil stadig oppstå. Også Datakrimutvalget fremhevet dette og sa at «utviklingen nødvendiggjør jevnlig ettersyn med lovgivningen på dette området».[81] Kriminaliseringsstrategien bør inneholde forslag til hvordan dette bør gjøres.

Konklusjon. Påpekte svakheter i kriminaliseringen av datakriminalitet dokumenterer et klart behov for en løpende oppdatering av straffelovgivningen.

8.3.3. Straffenivå

Strafferammer. Strafferammene i straffeloven 2005 ligger på 2 år for de fleste bestemmelsene som fanger opp typisk datakriminalitet, med 6 år for databedrageri og 15 år for grovt heleri og skadeverk. En mer detaljert oversikt viser følgende strafferammer:

§ 201 Uberettiget befatning med tilgangsdata, dataprogram mv.: bot eller fengsel inntil 1 år
§ 202 Identitetskrenkelse: bot eller fengsel inntil 2 år
§ 203 Uberettiget tilgang til fjernsynssignaler mv.: bot eller fengsel inntil 1 år, og inntil 3 år ved grov overtredelse
§ 204 Innbrudd i datasystem: bot eller fengsel inntil 2 år
§ 205 Krenkelse av retten til privat kommunikasjon: bot eller fengsel inntil 2 år
§ 206 Fare for driftshindring: bot eller fengsel inntil 2 år
§ 207 Krenkelse av forretningshemmelighet: bot eller fengsel inntil 2 år
§ 208 Rettsstridig tilegnelse av forretningshemmelighet: bot eller fengsel inntil 1 år
§§ 332–336 Heleri: fra bot til fengsel inntil 15 år, avhengig av forholdets grovhet
§§ 343–344 Ulovlig bruk av løsøre: bot, og fengsel inntil 2 år ved grov overtredelse
§§ 351–353 Skadeverk: fra bot til fengsel inntil 15 år, avhengig av forholdets grovhet
§§ 371–374 Bedrageri: fra bot til fengsel inntil 6 år, avhengig av forholdets grovhet

Straffeutmålingsnivået. Strategigruppen har observert at sammenlignet med annen kriminalitet er det lite rettspraksis på dette området, og den gir derfor begrenset veiledning. Straffenivået synes å være relativt lavt, og det reflekterer strafferammene beskrevet over.

Under følger noen aktuelle eksempler fra rettspraksis.

Fra Høyesterett:

Rt. 2004-94: I IT Huset-saken ble det ilagt 60 timers samfunnsstraff og 10 000 kroner i bot for datainnbrudd og sletting av abonnentdata hos et konkurrerende firma. Høyesterett kom til at skadepotensialet ikke gjorde at skadeverket kunne karakteriseres som grovt, men det ble lagt vekt på samfunnets behov for å kunne stole på datasystemers konfidensialitet og pålitelighet.

Rt. 2012-1669: I Photobucket-saken idømte lagmannsretten ett års fengsel, hvorav ni måneder betinget, for datainnbrudd mv., jf. LB-2011-102720. Både påtalemyndigheten og forsvarer innga anke over lovanvendelsen under skyldspørsmålet. Førstevoterende i Høyesterett uttalte: «Den straff lagmannsretten fastsatte, er etter mitt syn ikke for streng.» Dommen var enstemmig. Utmålingen fra lagmannsretten ble opprettholdt. Lagmannsretten betegnet forholdene som alvorlig datakriminalitet

77 *Ot.prp. nr. 22 (2008–2009)*, s. 63.
78 *NOU 2007: 2 Lovtiltak mot datakriminalitet – Delutredning II.*
79 *Ot.prp. nr. 22 (2008–2009)*, s. 66.
80 Straffeloven 1902 § 275 om utroskap (straffeloven 2005 § 390), straffeloven 1902 § 294 nr. 2 og 3 om bedriftshemmeligheter (straffeloven 2005 § 207) og personopplysningsloven § 48 jf. § 2 nr. 1.
81 *NOU 2007: 2*, s. 9.

(avsnitt 46) og påpekte at det er lite praksis vedrørende omfattende datainnbrudd. Lagmannsretten la således til grunn at «det finnes ikke rettspraksis av betydning for straffutmålingen ved en slik overtredelse av straffeloven § 145 annet ledd». Lagmannsretten fant at «det er tale om en meget alvorlig overtredelse av straffebestemmelsen i straffeloven § 145», men endret ikke tingrettens straff på fengsel i ett år, hvorav ni måneder var betinget.

Rt. 2012-1968: Det ble gitt ett år og ti måneders fengsel for medvirkning til datainnbrudd og bedrageri (nettbanksvindel). Høyesterett la vekt på at tapsfaren utgjorde ca. 800 000 kroner, og uttalte at allmennpreventive hensyn derfor tilsa et strengt alminnelig straffenivå ved slik nettbanksvindel, jf. Rt. 2009-397, selv om den faktiske vinningen var beskjeden. Det ble også lagt vekt på at det dreide seg om organisert kriminalitet, der svindlerne ofte opererer på tvers av landegrensene, at det har vært en kraftig økning i antall nettsider som sprer banktrojanere og annen skadevare, og at Internett-kriminalitet er et økende samfunnsproblem som truer tilliten til blant annet nettbankene, som dagens betalingsformidling er basert på.

Fra lagmannsrettene og tingrettene:

LB-2014-98247 og TOSLO-2015-106355: Fem personer fra blant annet Anonymous-miljøet ble i Noria-saken dømt for datainnbrudd overfor en privatperson (blant annet hacking av en Facebook-konto) samt for tjenestenektangrep mot nettsiden til Arbeiderpartiet (grovt skadeverk). De tiltalte fikk betinget straff, blant annet på grunn av sin lave alder.

LF-2011-37540: En tidligere IT-ansvarlig ble dømt til betinget fengsel og fikk en bot på 5000 kroner for datainnbrudd hos sin tidligere arbeidsgiver. Han gikk inn på arbeidsgiverens datasystemer fra sin private PC og gjorde programmer som han som ansatt hadde utarbeidet for arbeidsgiveren, utilgjengelig for brukerne. Programvaren tilhørte arbeidsgiveren.

LB-2010-18170: I Tele 2-saken ble det ilagt 30 dagers betinget fengsel og en bot på 20 000 kroner for datainnbrudd og ulovlig nedlastning av rettighetsbeskyttet materiale i form av ca. 4830 norske personnavn, inkludert adresse, personnummer og kredittsjekk.

TOSLO-2013-87847 og LOD-2013-116-35: Fire tiltalte ble i Hemmelig.com-saken dømt til inntil 57 timers samfunnsstraff for datainnbrudd, der det ble tatt sensitive personopplysninger.

TNERO-2013-89352: Tre personer på 20 og 16 år ble dømt for en rekke tjenestenektangrep (skadeverk) i DotNetFuckers-saken. De to eldste ble dømt til 90 timers samfunnsstraff, mens den yngste fikk 14 dagers betinget fengsel med prøvetid.

LB-2007-69411: En 45 år gammel mann ble i Pitbullterje-saken dømt for ulovlig kopiering og tilgjengeliggjøring av en rettighetsbeskyttet film via Pirate Bay. Han fikk betinget fengsel i 15 dager og ble dømt til inndragning og til å betale 50 000 kroner i erstatning.

LB-2005-111089: En IT-sikkerhetsarkitekt i en bank ble dømt til sju måneders fengsel, hvorav 120 dager var betinget, for grov utroskap. Like før han sluttet i jobben, hadde han ulovlig kopiert en stor mengde materiale, blant annet kildekode knyttet til bankens nettbankløsninger.

Listen er ikke uttømmende, men illustrerer noen fellestrekk.

Som for annen kriminalitet og i tråd med lovgivers ønsker ender straffutmålingen i saker med unge tiltalte ofte med betinget fengsel eller samfunnsstraff samt inndragning av datautstyret som ble brukt ved handlingene. Dette gjelder ofte saker om datainnbrudd, tjenestenektangrep (skadeverk), brudd på åndsverkloven og trusler, sjikane og personvernkrenkelser knyttet til e-post og sosiale medier.

For saker knyttet til økonomiske forhold (nettbankbedragerier) tilpasses reaksjonene annen rettspraksis fra saker med tilsvarende størrelse på det økonomiske tapet.

Foretaksstraff. TAHER-2006-24950: I SAS Braathens-dommen ble SAS Braathens AS dømt til en foretaksstraff på 400 000 kroner for brudd på markedsføringsloven, men ble frifunnet for datainnbrudd. Straffeloven § 145 annet og tredje ledd ble imidlertid endret 8. april 2005, slik at de forholdene saken gjaldt, nok ville vært omfattet av lovteksten etter endringen. Tingretten skrev følgende i begrunnelsen for den frifinnende dommen:

Retten finner ikke grunnlag til å ta stilling til om tilgangen for Braathens' ansatte til NAS' PNR-data var uberettiget etter 8. april 2005. Dette fordi påtalemyndigheten, etter rettens vurdering, ikke har bevist utover rimelig tvil at de ansatte i Braathens brukte adgangen etter nevnte tidspunkt.

Til tross for at ordbruken i flere av dommene antyder at datakriminaliteten er alvorlig og utgjør et alvorlig samfunnsproblem, kan neppe straffene betegnes som annet enn milde.

Konklusjon. Sett i forhold til den potensielle samfunnsskaden ved datakriminalitet er dagens straffenivå for mildt, også sammenlignet med annen kriminalitet og andre relevante land.

8.3.4. Påtalereglene

Etter straffeloven 1902 kan straffebudene deles inn i to hovedgrupper hva gjelder påtalereglene:

- ubetinget offentlig påtale
- påtale betinget av begjæring fra fornærmede

Utelukkende privat påtale er en tredje hovedgruppe, men dette brukes knapt i praksis.

Innenfor disse hovedgruppene finnes det igjen forskjellige kategorier. Flere straffebud foreskriver at offentlig påtale bare skal finne sted når allmenne hensyn krever det.

Påtalemyndigheten har imidlertid en betydelig skjønnsmyndighet når det gjelder hvordan en straffesak skal håndteres eller avgjøres.

For det første skal det bare etterforskes når det er rimelig grunn til å undersøke om det foreligger et straffbart forhold som er gjenstand for offentlig forfølgning, jf. straffeprosessloven § 224. Avgjørelsen vil bero på «et skjønn hvor viktige momenter vil være sannsynligheten for at det foreligger et straffbart forhold og sakens alvor sammenholdt med hvilken etterforskingsinnsats og hvilke etterforskingstiltak som vil kunne være aktuelle».[82] Hvis det for eksempel er liten eller ingen mulighet for å oppklare en sak, noe som kan være spesielt aktuelt i datakrimsaker, kan det gi grunnlag for å unnlate etterforskning. Politiet har dessuten rom til å gjøre en del undersøkelser for å kunne ta standpunkt til om det foreligger rimelig grunn til å iverksette etterforskning.

For det andre har man en rekke henleggelsesgrunner dersom det iverksettes etterforskning. Særlig praktisk er det å henlegge på grunn av bevistvil, trolig også i datakrimsaker.

For det tredje gjelder det et alminnelig opportunitetsprinsipp i straffeprosessen, jf. særlig straffeprosessloven § 69. Påtalemyndigheten har i utgangspunktet plikt til å reise tiltale hvis den finner straffeskyld bevist, men § 69 gir en nokså vid adgang til å la være å straffeforfølge hvis påtalemyndigheten finner at det er den beste løsningen. Påtalemyndigheten har ikke fullstendig frihet til selv å avgjøre om det skal reises tiltale, men som Andenæs påpeker,[83] går loven lenger i å gjennomføre opportunitetsprinsippet i Norge enn i de fleste andre land.

Påtalereglene er endret i straffeloven 2005, siden ordningen med påtalebegjæring fra fornærmede ikke videreføres, jf. straffeprosesslovens nye § 62a annet ledd. Den nye påtaleordningen ventes å tre i kraft samtidig med ny straffelov. Departementet legger til grunn at «den økte skjønnsmyndigheten som tillegges påtalemyndigheten ved denne endringen, i noen grad reduseres ved blant annet at det i den nye bestemmelsen i straffeprosessloven § 62a oppregnes hvilke momenter det skal legges vekt på i vurderingen av om allmenne hensyn foreligger».[84] Etter den nye ordningen vil hovedregelen ved straffebud med en strafferamme på to år eller mindre være at lovbrudd bare påtales der allmenne hensyn tilsier det. Dette gjelder for de fleste datalovbruddene i listen i punkt 8.3.3.

Hovedpoenget er at påtalemyndigheten på alle stadier av straffesaksbehandlingen allerede i dag har stor grad av fleksibilitet når det gjelder hvordan en sak bør avgjøres. Muligheten til å la være å straffeforfølge kan være viktig for at ofrene skal være villige til å bidra med opplysninger om datakriminalitet. Dette behandles nærmere i kapittel 10.

Konklusjon. Opportunitetsprinsippet og den alminnelige fleksibiliteten i straffesaksbehandlingen må benyttes aktivt i dialogen med fornærmede i

82 H.K. Bjerke, E. Keiserud og K.E. Sæther. 2011. *Straffeprosessloven*, s. 832.

83 J. Andenæs og T. Myrer. 2009. *Norsk straffeprosess*, bind 1, s. 330.
84 *Ot.prp. nr. 22 (2008–2009)*, s. 392.

datakriminalitetssaker. Dette gjelder særlig større bedrifter og lignende som i dag vegrer seg for å anmelde alvorlig datakriminalitet fordi de da føler at de mister kontroll over opplysningene sine og ikke vet hvordan en eventuell straffesak vil kunne slå ut for virksomheten.

8.4. Viktige kriminaliseringshensyn

8.4.1. Samfunnstrusselen og visjonen

Samfunnstrusselen fra datakriminalitet fremstår samlet sett som alvorlig, og sett under ett har utviklingen vært klart negativ. Datatrusselen har blitt mye mer skadelig og utgjør et vesentlig større samfunnsproblem i dag enn den gjorde for ti år siden. Dette bør avspeiles i det strafferettslige vernet. Straffebudene må løpende tilpasses utviklingen.

Visjonen vår sier at Norge skal være et av foregangslandene i internasjonal bekjempelse av datakriminalitet. Uønskede og skadelige datahandlinger som i dag ikke rammes tilstrekkelig av straffelovgivningen, må kriminaliseres bedre. Både strafferammene og straffeutmålingsnivået bør heves vesentlig, både for å markere at datakriminaliteten i økende grad skader samfunnet, og for å styrke allmennprevensjonen og moraldanningen.

8.4.2. Kriminaliseringsmetoder

Egne straffebestemmelser for datakriminalitet. Lovgivningspolitikken for datakriminalitet har i stor grad tatt utgangspunkt i straffebestemmelser mot handlinger i den fysiske verden. Det har vært et mål at straffebestemmelser mot datahandlinger bør være mest mulig like dem som allerede forbyr handlinger i den fysiske verden. Det antas at dette alt i alt er arbeidsbesparende både for lovgivende og rettshåndhevende myndigheter. Behovet for lovendringer blir holdt på et minimum, og rettspraksis fra den fysiske verden kan også gi veiledning ved kriminalitet i den virtuelle verden. Rettsanvenderne, altså politiet, påtalemyndigheten og domstolene, kan benytte straffebestemmelser de allerede kjenner og er vant med å praktisere. Potensielle lovbrytere vil også stå overfor en kjent straffetrussel, som gir dem et ganske presist varsel om hva de kan forvente hvis de bryter bestemmelser som rammer datakriminalitet.

Men en slik mer eller mindre automatisk utvidelse av straffebestemmelser fra den fysiske verden til den digitale verden har også negative sider. Dataverdenen er forskjellig fra den fysiske verden. Selv om det kan føre til overlappende bestemmelser, bør datahandlinger derfor kriminaliseres ut fra sin egenart, og ikke nødvendigvis mest mulig likt handlinger i den fysiske verden – i hvert fall frem til det er etablert fornuftige mønstre for digital adferd i befolkningen, næringslivet og det offentlige. I tråd med dette bør forskjellene vies større oppmerksomhet enn det som har vært vanlig til nå, fordi en standard overføring av bestemmelser fra den fysiske til den digitale verden ikke gir en like effektiv utnyttelse av straffesystemet som spesialiserte bestemmelser mot datakriminalitet.

Det er neppe realistisk å regulere all datakriminalitet i egne bestemmelser som er forskjellige fra bestemmelser mot kriminalitet i den fysiske verden. Definisjonen av datakriminalitet i kapittel 3 skiller mellom handlinger rettet mot datasystemer, for eksempel for å tilegne seg dem, skade dem eller tappe dem for informasjon, og handlinger hvor data eller datasystemer brukes som et vesentlig redskap for å utføre andre former for straffbare handlinger. Definisjonen er samlet svært omfattende. For normdanningsformål må det være tilstrekkelig å skille ut et utvalg av de viktigste datalovbruddene og plassere dem i en egen datastraffelov eller i et eget kapittel om datakriminalitet i straffeloven, slik Datakrimutvalget foreslo. I tillegg bør det, i hvert fall inntil videre, uttrykkelig presiseres i andre straffebestemmelser, både i straffeloven og i spesiallovgivningen, om de omfatter datahandlinger.

Gradering. Definisjonen av datakriminalitet er vid, og handlingsspennet som dekkes, er stort – fra internasjonal organisert datakriminalitet begått av stater eller mafialignende organisasjoner med sterke profittinteresser til såkalt gutteromskriminalitet hvor formålet først og fremst er spenning. Det er derfor behov for å gradere datakriminaliteten etter hvor grov den er.

For å sikre at kriminaliseringen tar høyde for den store variasjonsbredden i datahandlingene, foreslo Datakrimutvalget å dele sentrale straffebud mot datakriminalitet i tre hovedkategorier: lite

alvorlige overtredelser, vanlige overtredelser og grove datalovbrudd. De tre kategoriene ble gitt forskjellige strafferammer.

Dette er en lovgivningsteknikk som med fordel kan brukes. Grovheten ved handlingen tydeliggjøres, og man får frem at avstanden mellom forholdsvis uskyldige og mer alvorlige overtredelser kan være kort. Teknikken er blant annet brukt i kriminalisering av narkotika.

Mange gjeldende straffebestemmelser har en gradering med to nivåer: grove og mindre grove overtredelser. Med en slik gradering kunne eksempler på grov datakriminalitet være

- enkeltovertredelser som medfører betydelig tap eller skade for én eller flere personer, forretningsvirksomheter, organisasjoner eller offentlige virksomheter
- massekriminalitet hvor datahandlingen rammer mange ofre og samlet medfører betydelige tap eller skader, selv om konsekvensene for det enkelte offer er forholdsvis beskjedne

Et eksempel på det siste er når en rekke adressater får tilsendt en e-post som fører til at mange blir fralurt mindre beløp. Beløpene innebærer ikke noe vesentlig tap for den enkelte, men den samlede gevinsten for forøverne blir stor. Dataverktøy er særlig egnet til å begå slik kriminalitet, siden datakommunikasjon gjør det mulig å nå et stort antall adressater i mange land på en enkel måte.

Teknologinøytral utforming. Departementet gikk inn for at bestemmelser mot datakriminalitet bør utformes «tidsnøytralt», altså ikke i henhold til dagens teknologi, men at det «så langt det er mulig, bør anvendes mer generelle formuleringer som tar høyde for fremtidens teknologiske utvikling».[85] Poenget er å unngå at straffebestemmelsene blir raskt utdatert og dermed må revideres.

Datautviklingen går raskt, og det er vanskelig å spå hvordan datateknologien vil utvikle seg. I realiteten skyves da ansvaret for rettsutviklingen over på domstolene. Vi har sett at datakrimsaker er sjeldne, og at rettspraksis nesten ikke gir veiledning for straffutmåling, og heller ikke evner å fange opp raske endringer i datakriminaliteten. Kriminaliseringen vil nærmest uunngåelig komme på etterskudd i forhold til kriminalitetsutviklingen. Behovet for revisjon og nykriminalisering må vurderes fortløpende. Når straffebestemmelsene skal revideres, bør det prioriteres å ramme eksisterende trusler på en presis og pedagogisk måte.

Håndhevingshensyn bør også ha betydning ved utformingen av straffebestemmelser. Det skal ikke bare angis hva slags handlinger man ønsker å motvirke – beskrivelsen vil også virke retningsgivende på hva slags bevis som må samles inn for å dokumentere en overtredelse. Den faktiske angivelsen av den straffbare handlingen i straffebudene angir også bevistemaene. Bruker man straffebestemmelser som opprinnelig ble utformet med tanke på den fysiske verden, risikerer man at de blir mindre anvendelige i den digitale verden.

Et eksempel er straffebestemmelsen mot tyveri, som også kan tenkes å være aktuell mot datatyveri, som ID-tyveri eller tyveri av forretningshemmeligheter. Men datatyveri dreier seg ikke om å «bortta en gjenstand», men om kopiering av data. De «stjålne» dataene finnes normalt fortsatt på den angrepne datamaskinen, selv om den datakriminelle også kan ha slettet dem. Det sentrale er at eieren ikke lenger har eksklusiv kontroll over dataene, for eksempel ved at forretningshemmeligheter av stor kommersiell verdi blir kjent for en konkurrent.

Hvis straffebestemmelsene utformes spesielt med uønskede datahandlinger for øye, vil man også bedre kunne utforme handlingskrav som gir presise og anvendelige bevistemaer, og vurdere hvor komplisert det vil være for politiet og påtalemyndigheten å oppfylle dem. Er kravene til bevis tidkrevende og vanskelige å oppfylle, vil håndhevingen bli mindre effektiv og henleggelsesandelen større.

Hvis den enkelte bestemmelsen dekker mange handlingstyper – fysiske som virtuelle – og setter vide strafferammer, blir adferdsbudskapet mindre presist. Med egne bestemmelser vil de spesielle utfordringene knyttet til straff for datahandlinger bli tydeliggjort for lovgiver og forhåpentligvis bli regulert på en mer innsiktsfull måte enn når bestemmelser utviklet

85 *Ot.prp. nr. 22 (2008–2009)*, s. 21.

for den fysiske verden overføres mer mekanisk til datahandlinger.

Ved å samle viktige straffebestemmelser mot datakriminalitet i et eget kapittel i straffeloven eller eventuelt i en egen datastraffelov vil man sende et viktig signal om at datakriminalitet skal tas alvorlig, og sette søkelyset på denne typen kriminalitet. Et slikt signal vil ikke bare kunne påvirke potensielle gjerningspersoner, men også være nyttig for ofre for datakriminalitet og for politiet og andre sikkerhetsmyndigheter. Politiet har i dag ikke god nok kunnskap om de viktigste bestemmelsene mot datakriminalitet, spesielt ikke i tilfeller der det er snakk om bestemmelser utviklet for den fysiske verden, og hvor det i hovedsak er underforstått i teksten at datahandlinger også rammes. Dette kan være én av grunnene til den lave oppklaringsprosenten i datakrimsaker. Klare, eksplisitte bestemmelser mot datakriminalitet vil redusere risikoen for at straffbare datahandlinger går under radaren og ikke blir straffeforfulgt.

Kriminalstatistikken for datalovbrudd er ufullstendig. En grunn til dette er at det er vanskelig å skille ut datakriminalitet i tilfeller der straffebestemmelsen rammer handlinger i både den fysiske og den virtuelle verden. Med egne straffebestemmelser mot datakriminalitet vil i hvert fall overtredelser av disse kunne registreres på en entydig måte og gi grunnlag for en bedre statistikk.

8.4.3. Strengere straffer

Særskilte straffebestemmelser mot datakriminalitet vil også åpne for å fastsette andre strafferammer enn for lignende handlinger i den fysiske verden. Strategigruppens vurdering er at strafferammene bør heves betydelig. Med egne straffebestemmelser mot datakriminalitet kan dette gjøres forholdsvis presist. I det minste vil det være klart at strafferammen kun er ment brukt på datakriminalitet. Det vil ikke være samme rom for å argumentere for at datahandlinger er mindre skadelige enn handlinger i det fysiske rom og følgelig bør straffes mildere.

En slik reguleringsmåte vil først og fremst være effektiv for datalovbrudd med en egen straffebestemmelse. I tillegg kunne man gjøre det til en skjerpende omstendighet etter straffeloven 2005 § 77 å rette lovbruddet mot eller utføre det ved hjelp av data eller datautstyr. Da ville straffenivået kunne heves også for uønskede datahandlinger som ikke er dekket av særskilte straffebestemmelser mot datakriminalitet, men som faller inn under generelle bestemmelser som også omfatter handlinger i den fysiske verden.

Dagens lave strafferammer for datakriminalitet har betydning for tilgangen til bruk av tvangsmidler. De mest inngripende tvangsmidlene krever siktelse for straffbare handlinger med høye strafferammer. Med særskilte straffebestemmelser mot datakriminalitet kan behovet for tvangsmidler også vurderes mer presist. Se mer om dette i kapittel 10.

Strafferammen er et viktig uttrykk for grovheten ved en straffbar handling, og den vektlegges når Riksadvokaten og politiet prioriterer hvor mye kapasitet som skal brukes på å forfølge ulike typer straffbare handlinger. De lave strafferammene for datakriminalitet har åpenbart virket negativt på prioriteringene. Når datakriminaliteten utgjør et økende samfunnsproblem som krever strengere straffer, vil straffeskjerpelser også føre til økt oppmerksomhet og innsats i straffeforfølgningen.

Konklusjon. Behovet for å beskytte samfunnet mot datakriminalitet er stadig økende, og strafferammene må avspeile den risikoen datakriminaliteten utgjør.

8.4.4. Sanksjonsspekteret

De viktigste formene for straff for handlinger i den fysiske verden er frihetsberøvelse og bot. Straffeloven 2005 §§ 29 og 30 gir en oversikt over alle straffeformer som kan anvendes. Disse straffeformene kan også brukes mot datakriminalitet, selv om det virker lite trolig at straffeloven § 30h om tap av retten til å kjøre motorvogn og persontransport vil bli brukt i en datakrimsak.

Egen sanksjon mot datakriminalitet. Straffeloven 2005 § 56 om tap av retten til å utøve en aktivitet gir muligheter for en tilsvarende sanksjon rettet mot datakriminalitet. Etter forarbeidene skal «bruk av telenettet mv. […] kunne forbys, under forutsetning av at det lar seg gjøre å gi rettighetstapet en fornuftig avgrensning». Også «rettighetstap med en rekkevidde som er begrenset til bestemte former for bruk av for eksempel internett» kan idømmes.[86]

86 *Ot.prp. nr. 90 (2003–2004)*, s. 321.

Det er åpenbart mange utfordringer knyttet til utformingen og bruken av en slik sanksjon, om det overhodet er mulig å få det til på en god måte. Et søk på Lovdata viser ingen eksempler på slik bruk av rettighetstap etter den tilsvarende bestemmelsen i straffeloven 1902 § 29. Hjemmelen er trolig lite kjent i påtalemyndigheten, og det kan se ut til at forbud mot bruk av Internett ikke er anvendt til nå. Men får man bestemmelsen til å fungere, vil man trolig ha en sanksjon med god preventiv effekt. Utestengelse av dem som ikke vil følge spillereglene, vil for mange også innebære en økonomisk sanksjon og sosial stigmatisering.

Oppreisningserstatning. For ofrene er oppreisningserstatning for krenkelser av privatlivets fred ofte vel så viktig som at gjerningspersonen ilegges straff. Krav om slik erstatning kan normalt tas med og avgjøres i straffesaken. En dom fra Høyesterett peker på behovet for oppgraderinger i det erstatningsrettslige vernet mot datakriminalitet, i dette tilfellet i skadeserstatningsloven § 3–6.[87]

I denne saken krevde fem fornærmede oppreisning fordi tiltalte urettmessig hadde kopiert privat informasjon og intime bilder av de fornærmede og deres nærstående, blant annet ved at han gikk inn på e-postkontoene deres og overførte vedlegg m.m. til sin egen server. Siden tiltalte ikke hadde offentliggjort informasjonen, ble han imidlertid frifunnet for oppreisningskravene. Men Høyesterett tilføyde følgende:

> *Jeg finner grunn til å føye til at reelle hensyn etter mitt syn kan tale for at § 3–6 burde kunne få anvendelse ved denne typen krenkelser av privatlivets fred, selv om krenkelsen ikke har skjedd offentlig. Svært mange har i dag lagret omfattende privat informasjon elektronisk, og det å oppleve at uvedkommende hacker seg inn på e-postkontoer eller skaffer seg tilgang til annen elektronisk lagret privat informasjon, vil for de fleste kunne oppleves som en svært ubehagelig invadering av ens privatliv. Dette er derfor et spørsmål som det kan være grunn for lovgiver å vurdere.*

87 *Rt. 2012*, s. 1669.

En slik gjennomgang skal så langt ikke være påbegynt fra Justis- og beredskapsdepartementets side.

Et effektivt erstatningsrettslig vern er et viktig supplement til det strafferettslige vernet mot datakriminalitet. Det bør inngå som en del av kriminaliseringsstrategien å oppdatere dette.

Konklusjon. Straffesanksjoner og andre reaksjonsformer må i større grad målrettes mot datakriminalitet og sikre ofre for datakriminalitet et adekvat erstatningsrettslig vern.

8.5. Normdanning

Utbredt databruk er et relativt nytt fenomen som vi har gjort oss avhengige av på en rekke samfunnsområder. Det er knapt tenkelig, og i hvert fall ikke ønskelig, å reversere denne utviklingen. Siden det historisk sett dreier seg om en ny form for aktivitet, mangler dataverdenen i stor grad uformelle adferdsnormer som kan inngå som en del av den vanlige sosialiseringen. Både foreldre og utdanningsinstitusjoner kan ha problemer med å forstå den teknologiske utviklingen, og det svekker deres evne til å lære barn og ungdom hvordan de bør opptre i den digitale verden.

De aller fleste har sterke motforestillinger mot handlinger som vold, seksualovergrep, tyveri, bedrageri, underslag og sabotasje. Straff brukes særlig for å beskytte individer og institusjoner mot grovere krenkelser av slike viktige adferdsnormer som det er bred oppslutning om, og som er en integrert del av folks alminnelige moral. Slike straffebud inneholder i stor grad normer som er i samsvar med den alminnelige moraloppfatningen.

Men straff brukes også for å innarbeide nye adferdsnormer på felter hvor det ikke eksisterer etablerte individuelle normer, eller hvor den eksisterende adferden ønskes endret. De relativt drakoniske straffene mot bilkjøring i alkoholpåvirket tilstand som kom forholdsvis raskt etter at bilbruk ble vanlig i Norge, kan tjene som eksempel. Nå har disse straffebestemmelsene eksistert i snart hundre år, og de sosiale normene mot fyllekjøring er blitt atskillig sterkere.

Utviklingen i databruk har parallelle trekk. Som et nytt område av livet gir det aktørene stor frihet også til uønsket og skadelig adferd. De vanlige,

uformelle sosialiseringsmekanismene er foreløpig svakt utviklet. Straff som virkemiddel til å innarbeide gode adferdsnormer i den virtuelle verden fremstår derfor som viktigere enn i den fysiske verden, hvor andre sosialiseringsmekanismer står sterkere.

Denne forskjellen stiller særlige krav både til utformingen av straffelovgivningen for den digitale verden og til effektiviteten i håndhevingen av den. Beskrivelsene av de straffbare handlingene bør være tydeligere og mer pedagogiske, sanksjonene strengere for å oppnå tilstrekkelig oppmerksomhet og oppklaringsprosent og det faktiske sanksjonsnivået høyere enn for annen kriminalitet.

Gode normer for dataadferd blir trolig best innarbeidet med tydelige, pedagogiske straffebestemmelser som i klart språk sier hvilke datahandlinger som er forbudt. Dette gjelder både for potensielle overtredere, ofre, offentligheten og profesjonelle aktører. Bestemmelsene bør være enkle å forstå og bør kunne brukes som grunnlag for informasjonskampanjer og opplæringstiltak i skolen og på kurs. Se også kapittel 9 om forebygging.

Tydelige straffebestemmelser vil markere et samfunnsønske om at man skal være minst like trygg i den virtuelle verden som i den fysiske. Det bør signaliseres tydelig at manglende kunnskap, naivitet eller godtroenhet ikke gjør utnyttelse legitimt, snarere tvert om. Dataverdenen bør bli en velregulert arena for interaksjon og kommunikasjon uten særlig risiko for utnyttelse og misbruk, uansett hvem brukeren er. Det er riktignok ikke noe mål å straffe flest mulig. En troverdig straffetrussel som gjør at flest mulig respekterer forbudene, er det sentrale. Datakriminaliteten omfatter også hverdagskriminalitet, og da kan sosialiseringstiltak være viktigere enn straff. Det finnes instruktive eksempler på at politiet har oppsøkt ungdomsmiljøer og skoler og advart mot for eksempel krenkende former for adferd, som spredning av seksualiserte bilder av unge jenter på nett, med god virkning. Men effektiv avdekking og forfølgning av lovbrudd er en viktig mekanisme både for å gjøre straffetrusselen troverdig og for å gi informasjon om hvor godt straffetrusselen virker.

Konklusjon. Det er et sterkt behov for normdanning i den virtuelle verden. Økt bruk av straff og mer effektive straffeformer vil kunne være et effektivt ledd i samfunnets arbeid med normdanning.

8.6. Internasjonale hensyn

8.6.1. Kriminalisering og behovet for internasjonalt samarbeid

Storparten av den alvorlige datakriminaliteten er internasjonal. Strategigruppen har på sine studiereiser erfart at de førende landene er svært opptatt av internasjonalt samarbeid. FBI, som har den mest omfattende erfaringen, poengterte på flere møter at den alvorlige datakriminaliteten vanskelig lar seg bekjempe uten et omfattende og effektivt samarbeid på alle plan – fra håndtering av enkeltsaker til harmonisering av tvangsmidler og kriminalisering.

Visjonen vår er at Norge skal være et førende land internasjonalt når det gjelder bekjempelse av datakriminalitet. I de fleste land, inkludert USA og Storbritannia, hemmes bekjempelsen av en lite oppdatert straffelovgivning. Ved å modernisere vår egen straffelovgivning kan Norge bli en modell for andre land. Siden det er behov for et omfattende internasjonalt samarbeid for å sikre en mer effektiv forfølgning av datakriminalitet, er det grunn til å tro at gode modeller vil ha betydning for det internasjonale utviklingsarbeidet som foregår i folkerettslige fora, spesielt Europarådets oppfølgning av Budapestkonvensjonen, og for utviklingen av nasjonal lovgivning. Er Norge en spydspiss her, kan det sette fart på utviklingen også i andre land. Se også punkt 10.7.2.

Både Storbritannia og USA begrunner den sterke prioriteringen av velfungerende datasystemer med deres betydning for økonomisk vekst og bedre velferd. Velfungerende datasystemer innebærer et konkurransefortrinn. For Storbritannias del fremgår dette direkte av deres strategi for datasikkerhet og bekjempelse av datakriminalitet. Ifølge den skal Storbritannia være et av de sikreste landene i verden for å gjøre forretninger på nett.

Flere representanter for FBI har fremholdt at USA har gått glipp av enorme gevinstmuligheter ved at bedriftshemmeligheter har blitt ulovlig kopiert. Deretter har andre virksomheter i så vel USA som andre land brukt kopiene til å utvikle nye produkter og slik slippe unna utviklingskostnadene. Utilstrekkelig

datasikkerhet ga dermed virksomhetene som fikk tilgang til de ulovlige kopiene, et enormt konkurransefortrinn. I ytterste konsekvens har dette ført til konkurs for virksomhetene som ble utsatt for piratkopieringen, eller de har gitt opp å produsere for det aktuelle markedet. På lengre sikt innebærer den omfattende tappingen av bedriftshemmeligheter en alvorlig trussel mot utviklingspotensialet i USAs næringsliv.

Effektive sikkerhetsordninger er naturligvis et sentralt virkemiddel mot slik bedriftsspionasje. De kan stoppe angrep, men de forhindrer ikke at piratkopierne finner andre og bedre metoder eller angriper andre mål. De økonomiske fordelene ved vellykket kopiering av bedriftshemmeligheter er trolig så store at insentivene til å fortsette er sterke.

Slik alvorlig industrispionasje må åpenbart bekjempes internasjonalt, og store industrinasjoner som USA og Storbritannia legger stor vekt på internasjonalt samarbeid. Ved å delta her har Norge som et lite land en gyllen sjanse til å få uvurderlig hjelp til å beskytte sin egen konkurransedyktighet. Selv om anslag mot bedriftshemmeligheter i første omgang skjer mot virksomheter i andre land, fordi det er flere interessante objekter der, øker de risikoen for tilsvarende anslag mot norske virksomheter.

Strenge straffetrusler både mot piratkopiering og uforsvarlighet knyttet til manglende sikkerhetstiltak er trolig det eneste virkemiddelet som kan bremse en slik utvikling, og må kombineres med en rimelig effektiv håndheving.

Som analysen viser, er det ikke bare kriminaliseringen av handlingen som har betydning. En viktig faktor er hvor streng straffetrusselen er. Her ble det avdekket viktige forskjeller under strategigruppens studiereise til USA, der strafferammer på opptil 20 års fengsel for alvorlig datakriminalitet ikke er uvanlig. Hvis norske strafferammer er lave sammenlignet med andre land, kan det ha omtrent samme effekt som å la uønskede datahandlinger stå ustraffet. Det kan åpne for at Norge blir en frihavn for datakriminalitet. En viktig del av kriminaliseringsstrategien bør derfor være en vesentlig heving av strafferammene for datakriminalitet.

Konklusjon. Norge må sikre opphavsrettigheter og gi kunnskapen i bedrifter et sterkere vern. Videre må Norge ta initiativ til – og legge til rette for – økt internasjonalt samarbeid i kampen mot datakriminalitet. Norge må ha ambisjoner om å bli et foregangsland på dette området.

8.6.2. Jurisdiksjon

Datakriminalitet påvirkes i liten grad av landegrenser, og det kan være både vanskelig og usikkert å forankre datahandlinger geografisk. Gjerningspersonen kan oppholde seg i ett land, datautstyret som benyttes, i et annet, datautstyret som rammes, i et tredje og offeret i et fjerde. Mye av datakriminaliteten er masseovertredelser, hvor for eksempel et stort antall systemer i mange land infiseres eller mange personer i ulike land rammes. Straffesystemet er mye sterkere forankret nasjonalt, og komplikasjonene øker ofte betydelig dersom en straffeforfølgning helt eller delvis må gjennomføres utenfor norsk territorium.

Jurisdiksjonsreglene i straffeloven 2005 §§ 4–8 synes ikke å være særlig godt tilpasset datakriminalitet. Dels er kriteriene vanskelige å anvende på datakriminalitet, og dels fremstår de som altfor snevre for en effektiv straffeforfølgning. Lite hensiktsmessige jurisdiksjonsregler for datakriminalitet så vel i Norge som i andre land kan være en viktig årsak til ineffektiv straffeforfølgning og høy henleggelsesprosent.

Effektivt, uformelt og fleksibelt internasjonalt samarbeid må være en hjørnestein i datakrimstrategien. Norge må satse vesentlig mer enn i dag på internasjonalt samarbeid for å bekjempe alvorlig datakriminalitet. Et viktig skritt er å sørge for smidige jurisdiksjonsregler som gjør slikt samarbeid så enkelt som mulig.

Prinsipielt er universelle straffebestemmelser det mest effektive. Norske bestemmelser bør omfatte straffbare datahandlinger som rammer norske interesser uansett hvor virkningen inntreffer, handlingen er utført, dataverktøyet befinner seg eller gjerningspersonen oppholder seg. For å sikre smidighet bør imidlertid adgangen til påtalefrafall være fleksibel, slik at ressursene brukes på de prinsipielt viktige sakene og der det er mulig å oppnå resultater.

Norge er som andre land avhengig av et bredt og effektivt internasjonalt samarbeid for å komme

alvorlig datakriminalitet til livs. Norge bør derfor ved behov også kunne forfølge alvorlig datakriminalitet som rammer andre interesser enn norske – i likhet med ordningen som gjelder for forbrytelser mot menneskeheten. Spesielt i internasjonalt samarbeid om bekjempelse av alvorlig datakriminalitet kan det være nyttig å legge til rette for slik myndighetsutøvelse.

Det kan hevdes at straffeforfølgning av andre lands borgere i utlandet, særlig i hjemlandet deres, som oftest har små muligheter for å føre frem og derfor har liten hensikt. Strategigruppen er for så vidt enig i at ressursene bør brukes der de har best effekt. Men den alvorlige datakriminalitetens internasjonale karakter gjør det nødvendig å utvikle metodene for bekjempelse. USA har nylig siktet flere kinesiske offiserer som befinner seg i Kina, for dataangrep i USA. Siktelsen tydeliggjør at slik internasjonal kriminalitet foregår. Selv om Kina ikke vil utlevere de siktede, vil de risikere utlevering hvis de skulle reise til et annet land med utleveringsavtale. Hvis andre land i tillegg har en universell kriminalisering av de aktuelle handlingene, vil de siktede også risikere straffeforfølgning i disse landene.

Tidsmomentet er oftest langt viktigere ved bekjempelse av datakriminalitet enn ved tradisjonell kriminalitet. Norske jurisdiksjonsregler bør derfor gi politiet og påtalemyndigheten i samarbeidende stater liberal adgang til selv å etterforske datakriminalitet innenfor norsk jurisdiksjon og ha bistandsordninger for dette.

Konklusjon. Tid er en kritisk faktor for etterforskning av datakriminalitet, og Norge bør i størst mulig grad arbeide for at straffeprosessuelle skranker blir redusert og sikrer et effektivt internasjonalt samarbeid.

8.7. Oppdatering av kriminaliseringen

På grunn av datakriminalitetens dynamiske karakter må den eksisterende kriminaliseringen gjennomgås jevnlig. Selv om gjerningsbeskrivelsen fortsatt er dekkende, kan hyppigheten, grovheten og samfunnsskadeligheten ved handlingene ha endret seg, slik at både strafferammer og straffeutmålingsnivå må justeres. Dette er spesielt viktig ved grovere datakriminalitet. En straffeutmålingspraksis basert på prejudikater avsagt en del år tilbake i tid, kan fort bli for mild, og domstolene bør få de nødvendige signalene slik at denne skjerpes.

Forrige gjennomgang av straffebestemmelsene mot datakriminalitet ble sluttført i 2007. Som vi har sett, var denne basert på andre kriminaliseringsprinsipper enn dem strategigruppen anbefaler. I hovedsak hadde den sitt grunnlag i et trusselbilde som fremsto som atskillig mindre farlig enn dagens, hvor utviklingstrendene dessuten peker mot en fortsatt økende trussel. Skal Norge bli blant foregangslandene, må den eksisterende kriminaliseringen oppdateres i takt med kriminalitetsutviklingen.

Også det erstatningsrettslige vernet bør justeres i takt med datautviklingen, på samme måte som straffebestemmelsene.

8.8. Samordning og organisering

8.8.1. Kombinasjon med andre tiltak

Kriminalisering er ett av flere virkemidler for å motvirke uønskede datahandlinger og bør derfor ses i sammenheng med andre former for kontroll og reparasjon og helst samvirke med disse på en god måte. Trygge, robuste sikkerhetssystemer vil bidra til å gjøre Norge til et lite attraktivt mål for datakriminalitet. Det kan hevdes at jo bedre sikkerhetssystemene er, desto mindre behov er det for straffesystemet. Motsatt kan en effektiv straffeforfølgning virke avskrekkende og redusere behovet for sikkerhetstiltak.

Med lave strafferammer og få domfellelser har nok den avskrekkende virkningen av straffeforfølgningen så langt vært begrenset. Det er klart at gode sikkerhetssystemer kan forhindre mange forsøk på kriminalitet og gjøre det mindre fristende med nye forsøk. Men gjerningspersonen mister ikke muligheten til å prøve på nytt så lenge vedkommende finner det interessant. Straffeforfølgning vil derimot kunne ramme en overtreder med personlige sanksjoner og sette vedkommende ut av spill for en kortere eller lengre periode.

Det bør være stor grad av samsvar mellom sikkerhetsaktørenes oppfatning av hva som er uønskede og skadelige datahandlinger, og hva de prioriterer i sin virksomhet, og vilkårene for straff. Straffbarhetsvilkårene bør så langt som mulig samordnes

med inngrepsvilkårene til de øvrige sikkerhetsaktørene, såfremt dette ikke går på bekostning av viktige rettssikkerhetshensyn. Dette vil fremme en felles forståelse av hvilke datahendelser som bør motvirkes.

8.8.2. Organisering

Det bør opprettes et organ som kan støtte Justis- og beredskapsdepartementet i arbeidet med problemstillinger knyttet til datakriminalitet. En hovedoppgave for dette organet bør være å løpende vurdere behovet for endringer i straffelovgivningen og det strafferettslige vernet i tråd med denne kriminaliseringsstrategien.

Dette arbeidet kan med fordel kombineres med å

- gjennomføre analysestrategien foreslått i kapittel 7
- følge opp at politiet har nødvendige og hensiktsmessige metoder ved etterforskning av datakriminalitet, se kapittel 10
- fremme internasjonale avtaler og samarbeid, se kapittel 10

8.9. Avgrensninger

Kriminaliseringsstrategien omfatter først og fremst hva det er hensiktsmessig å belegge med straff, og hvordan selve straffebestemmelsene bør formuleres og bygges opp. Spørsmålet om hvordan straffebestemmelsene bør håndheves overfor dem som bryter dem, tas opp i kapittel 7, 9 og 10 og omfatter

- datainnsamling og analyse av konkrete datalovbrudd
- forebygging og avverging
- straffeforfølgning

Her behandles også behovet for lovreformer for å gjennomføre disse oppgavene.

8.10. Hovedstrategi for kriminalisering

Straff skal brukes aktivt i utviklingen av normer mot uønsket og skadelig dataadferd i samfunnet. Sanksjonene må ligge på et nivå som gjør datakriminalitet ulønnsomt, og som forebygger at Norge blir en frihavn for internasjonal datakriminalitet.

Norge trenger en straffelovgivning som oppdateres i takt med trusselen fra datakriminalitet, og som har anvendelige bevistemaer og avskrekkende strafferammer. Nye straffverdige datahandlinger bør kriminaliseres raskt og tydelig for å markere at de er uønskede, og for å sikre allmennprevensjonen.

Jurisdiksjonsreglene må legge til rette for effektiv straffeforfølgning uavhengig av landegrenser, og for utstrakt internasjonalt samarbeid.

Anbefalte tiltak:

NB: Nummereringen av de anbefalte tiltakene nedenfor angir ikke prioriteringer.

8.1 *Kriminalisere datahandlinger ut fra deres egenart, uavhengig av hvordan handlinger utenfor den digitale verden er kriminalisert.* Nytten av å samle flere egne straffebestemmelser for grovere datakriminalitet i et eget kapittel i straffeloven bør vurderes. Også for andre straffebestemmelser, både i straffeloven og i spesiallovgivningen, bør behovet for å presisere om de omfatter datahandlinger, vurderes. Se punkt 8.4.2.

8.2 *Opprette et organ som løpende følger utviklingen, og som tar initiativ til nødvendig oppdatering av straffelovgivningen mot datakriminalitet.* Se punkt 8.4.2, 8.7 og 8.8.2.

8.3 *Heve strafferammene for datakriminalitet.* For internasjonal datakriminalitet bør straffenivået i andre sammenlignbare land inngå i vurderingen. Det bør vurderes å dele opp sentrale straffebud mot datakriminalitet etter grovhet, med forskjellige strafferammer. Se punkt 8.3.3, 8.4.1, 8.4.3 og 8.7.

8.4 *Utrede muligheten for mer effektive reaksjonsformer spesielt rettet mot datakriminelle.* Det bør utredes om de som dømmes for datakriminalitet, også kan ilegges restriksjoner i adgangen til å disponere datautstyr og bruke dataverktøy. Det bør spesielt vurderes om straffeloven 2005 § 56 om tap av retten til å utøve en aktivitet kan gjøres praktisk anvendelig for databruk. Se punkt 8.4.4.

8.5 *Gjennomgå jurisdiksjonsreglene for datakriminalitet og gjøre dem mer universelle.* Norske bestem-

melser bør omfatte straffbare datahandlinger som rammer norske interesser uansett hvor virkningen inntreffer, handlingen er utført, dataverktøyet befinner seg eller gjerningspersonen oppholder seg. Alvorlig internasjonal datakriminalitet bør ved behov kunne straffes i Norge også dersom den ikke rammer norske interesser. Se punkt 8.6.2.

8.6 *Påvirke andre land til en mer effektiv bekjempelse av datakriminalitet og innføring av universelle straffebestemmelser.* Norge bør delta aktivt i Europarådets fora for å videreutvikle Budapestkonvensjonen. Også andre konvensjoner av betydning for å bekjempe datakriminalitet bør følges aktivt opp. Se punkt 8.2.3.

8.7 *Supplere det strafferettslige vernet mot datakriminalitet med et effektivt erstatningsrettslig vern som oppdateres i takt med endringene i trusselbildet.* Se punkt 8.4.4.

9. STRATEGI FOR FOREBYGGING OG AVVERGING

9.1. Ansvaret for å forebygge

Kriminalitetsforebyggende arbeid er en av de viktigste oppgavene for politiet og sikkerhetsaktørene i det globale nettsamfunn. Kriminalitet skal forhindres både ved å gripe inn i årsakene til kriminaliteten og ved å hindre lovbrudd. For å få en effektiv forebygging er det viktig å følge samfunnsutviklingen og teknologiutviklingen. Trusselvurderinger (kap. 3) og analyser av datakriminalitet (kap. 7) vil gi nødvendig grunnlagsinformasjon for å utøve det forebyggende arbeidet.

Å forebygge er lønnsomt fordi det generelt koster mindre enn å håndtere og reparere skade. Antall ofre per gjerningsperson er i tillegg svært høyt for mange datakriminalitetsformer, noe som gjør forebygging spesielt viktig.

Effekten av forebyggende strategier og tiltak mot datakriminalitet kan imidlertid være vanskelig å måle på kort sikt. For å kunne vurdere resultatene av forebyggende strategier er man avhengig av:

- god deteksjonsevne – det må være mulig å oppdage datakriminaliteten
- vilje til rapportering – insentivene må legges til rette
- evne og ressurser til å sammenstille det som rapporteres inn – god statistikk må utarbeides

Politiet og sikkerhetsaktørene tilrettelegger for målbar forebyggende virksomhet. I det følgende beskrives de viktigste elementene som inngår i forebyggingen av datakriminalitet. Videre diskuteres problemstillinger ved krisehåndtering tilknyttet forebygging, avverging og etterforskning av alvorlige uønskede hendelser.

I tillegg til å etterforske har politiet et vidtrekkende ansvar for å forebygge, avdekke og stanse datakriminalitet, se politiloven § 2 nr. 2 og 3. Politiloven sier også at politiet kan bruke maktmidler for å avverge eller stanse lovbrudd (§ 6 (4) og 7 (1) nr. 3).

Politiet har også et generelt ansvar for å «beskytte person, eiendom og fellesgoder og verne om all lovlig virksomhet, opprettholde den offentlige orden og sikkerhet og enten alene eller sammen med andre myndigheter verne mot alt som truer den alminnelige tryggheten i samfunnet», se politiloven § 2 nr. 1. Dette ansvaret prioriteres ofte fremfor forebygging av kriminalitet. Politiet har en klar plikt til å beskytte mot trusler og skadelige hendelser, uansett om de er straffbare eller ikke.

Mange uønskede datahandlinger avverges av andre sikkerhetsaktører enn politiet. Disse gjenoppretter også sikker tilstand og reparerer eventuelle skader. Mandatet deres er ofte videre enn politiets i den forstand at det kan omfatte uønskede handlinger som ikke er straffbare. Andre sanksjoner enn straff kan også være aktuelle. En rekke tilsyns- og kontrollorganer, normalt spesialorganer, har til oppgave å beskytte mot trusler og farer. Deres oppgaver er avgrensede og spesifiserte.

Spesialorganene har ansvar for forebygging og avverging, men politiet skal støtte og hjelpe dem i medhold av politiloven § 2 nr. 6.[88] Politiet kan også – som en midlertidig løsning – gripe inn etter politiloven § 7 (4) i akutte situasjoner hvor «vedkommende organ ikke er tilgjengelig». Det samme prinsippet finnes i politiloven § 27 om redningsinnsats ved ulykkes- og katastrofesituasjoner.

Etterforskning av straffbare handlinger i det digitale samfunn er politiets primæransvar – også

88 R. Auglend, H. J. Mæland og K. Røsandhaug. 2004. *Politirett*, s. 222–225.

i tilfeller hvor selve krisehåndteringen er lagt til et spesialorgan som NSM. Men det hender at spesialorganet i praksis «initierer straffeforfølgning i form av rapporter eller anmeldelser, og ikke sjelden fungerer også organets fagpersonale som sakkyndige under politiets arbeid med saken».[89]

9.2. Noen dilemmaer

Det kan oppstå konflikter mellom alminnelig forebygging og etterforskning. Integrerte sikkerhetsfunksjoner som kryptering og makulering av digitale data vil vanskeliggjøre etterforskernes tilgang til digitale bevis i etterkant, men beskytter samtidig allmennheten mot kriminalitet. Avsløringer av enkelte sikkerhetsaktørers masseovervåkningsprogrammer har redusert tilliten til dem og mulighet for å samle inn og analysere informasjon. Det vil på samme måte kunne oppstå interessekonflikter mellom straffeforfølgningshensyn som krever sikring av bevis, og sikkerhetshensyn som krever rask gjenoppretting av kritiske samfunnsfunksjoner.

Utfordringer her vil være å tilrettelegge for tilfredsstillende ivaretakelse av begge hensyn samt å klargjøre beslutningsansvaret.

De komplekse tekniske og juridiske problemstillingene som oppstår i kampen mot nettkriminalitet, kan noen ganger virke vanskelig å løse med tradisjonelle metoder. Forebygging av datakriminalitet fordrer et vidt spekter av metoder. Hovedintensjonen til myndighetene er å beskytte individ og samfunn, men sterkt inngripende metoder kan benyttes til sensur, kontroll og overvåking. Det spesielle ved det digitale samfunn er at metodene ikke bare benyttes av politi og sikkerhetsaktører, men også av private virksomheter i forretningsmessig styring og påvirkning av kundene.

Grensen mellom det å beskytte individ og samfunn og det å sensurere, kontrollere og overvåke er blitt mindre tydelig, og områdene går over i hverandre. Flere opplever at ny teknologi er i ferd med å overvåke og kontrollere det meste. Skjørheten i denne grensen må selvsagt avveies når demokratiske land skal vurdere nye metoder som nettsidefiltrering og blokkering av tilgang til nettsider. Dette er inngrep som diskuteres for bruk ved sensur og stansing av tilgangen til overgrepsmateriale av barn, eller ytringer som støtter terror og rasehat.

9.3. Informasjon og kunnskap for å beskytte individ og samfunn

Bevisstgjøring for å beskytte seg. Det er vanskelig å forebygge og forhindre datakriminalitet uten at brukere og virksomheter beskytter seg selv. Alle som bruker digital teknologi, har et ansvar for egen sikkerhet på nettet og for å utøve sikkerhet i praksis.

Datakriminalitet kan forebygges ved kunnskap. Offentlige aktører og næringslivet har et spesielt ansvar for å hjelpe brukerne til å forstå hvilke mottiltak som kan iverksettes, og til å gjenkjenne faresignalene.

Den gjeldende nasjonale strategien for informasjonssikkerhet påpeker at «alle aktører på eget initiativ skal bidra til å forebygge og begrense tap eller skade som følge av datakriminalitet, ID-tyveri og misbruk av identitet». Detaljkunnskapen om objektet som skal sikres i den digitale verden, er avgjørende. Det gjeldende prinsippet er derfor at ansvaret for forebygging primært ligger hos objekteieren så lenge det handler om å beskytte datasystemer og informasjon. Det kan likevel være behov for minimumskrav og strengere regulering der markedet ikke klarer å regulere dette selv. Grunnleggende kunnskap i befolkningen er også et område hvor det offentlige, også politiet, bør bidra.

Det er viktig å bevisstgjøre brukerne gjennom informasjon, slik at de kan beskytte seg selv. Det må gis råd til individer, virksomheter og samfunn om trygg nettbruk, og det bør utvikles mekanismer for å vurdere effekten av disse tiltakene gjennom

- informasjon, opplæring og bevisstgjøring om trygg opptreden i det digitale samfunn samt forståelse for sikkerhetsrisikoer; dette vil også være med på å bedre evnen til å oppdage datakriminalitet
- vilje til rapportering og en samordnet oppfølging av meldinger om datakriminalitet på tvers av nasjonale aktører og privat/offentlig virksomhet; insentivene må legges til rette for dette

Partnerskap mellom myndigheter og private aktører. Finansinstitusjoner, kunnskapsbaserte virksomheter

89 Ibid. s. 223.

og e-handelstjenester står for enorme mengder transaksjoner og kundeforhold. Norske myndigheter må arbeide tett med disse sektorene og utvikle partnerskap for å spre råd til kunder om å beskytte seg mot datakriminalitet. Det må være et mål at alle virksomheter iverksetter en god digital praksis som fremmer sikker adferd og avdekker trusler på nettet.

Strategigruppen mener det er viktig å etablere et samarbeid mellom offentlig og privat sektor for opplæring av innbyggerne i Norge, slik at de kan ta del i et ansvarlig digitalt statsborgerskap. Dette vil bidra til en god felleskapskultur.

Behov for enklere rapportering. Forslagene i analysestrategien om enklere rapportering og mottak av tips og anmeldelser er også av stor betydning for forebygging og stansing av datakriminalitet. Det vises til analysene i punkt 7.3.1 og tiltakene knyttet til analysestrategien.

Publikumskontakt og informasjon til publikum. En del av politiets arbeid har alltid bestått i å informere publikum om ulike tiltak som kan forebygge kriminalitet, informasjon knyttet til akuttsituasjoner og informasjon om regelverk og praktisering av dette. En del av denne typen informasjon finnes på politiets nettside politi.no. Det er imidlertid behov for informasjon og dialog mellom politi og publikum som er mer rettet mot trusler og kriminelle hendelser i det globale nettsamfunnet. Man kan se for seg bedre informasjon og enklere måter å kontakte politiet på ved antatt straffbare forhold, som tilgang til vakttjeneste på nett, hurtigtilkalling fra ulike sosiale nettverk m.m.

Årlig sikkerhetsmåned. USA har siden 2003 arrangert National Cyber Security Awareness Month (NCSAM) i oktober. EU initierte i 2012 oktober som informasjonssikkerhetsmåned og har besluttet at den skal gjennomføres årlig fra 2014. Norge deltar i ordningen, og Norsk senter for informasjonssikring (NorSIS) er arrangør. Målgruppen er alle brukere av Internett i Norge, inkludert offentlige og private virksomheter. Den brede målgruppen er særlig viktig siden skillet mellom datautstyr brukt i jobbsammenheng og privat, er i ferd med å viskes ut.

Kampanjen i 2014 var forankret hos Justis- og beredskapsdepartementet. Konferanser ble holdt over hele landet, internt opplæringstilbud ble gitt til ansatte i norske virksomheter, og det ble arrangert nasjonal PR- og medieaktivitet. En viktig målgruppe var barn og ungdom som trenger informasjon om hva som er lovstridig. Slik én-til-mange-formidling er langt mer effektiv enn én-til-én-kommunikasjon. Kampanjen ble arrangert som en dugnad i tett samarbeid med private og offentlige virksomheter. Erfaringene fra arrangementet viser at politiet bør delta aktivt og at finansiering bør sikres og forankres bedre hos aktørene. NorSIS og lignende tiltak bør spille en sentral rolle i hendelsene som politiet ikke kan følge opp.

Behov for å beskytte barn. Tidlig opplæring rettet mot unges bruk av Internett, særlig dagens mobiltelefoner og nettbrett med kamera og geografisk lokalisering, er et viktig tiltak for å beskytte barn. Tilpassede rapporteringsfunksjoner i mobile applikasjoner og på websider kan gjøre det lettere for barn å rapportere uønsket aktivitet.

Konklusjon. Informasjon og kunnskap må gis til brukere og virksomheter slik at de kan beskytte seg selv, sin virksomhet og samfunnet mot datakriminalitet. Det bør være en nasjonal oppgave å bevisstgjøre om truslene, trendene og sårbarhetene som finnes. Politiet bør delta i nasjonale sikkerhetskampanjer med særlig vekt på hva som er kriminelt på nett. Allerede fra grunnskolen må det tas i bruk programmer for å lære opp barn i utfordringer tilknyttet digitalt liv og personvern.

9.4. Forebygging rettet mot sårbarheter

Forebygging rettet mot sårbarheter[90] omfatter å avverge, begrense eller forsinke skadelige handlinger uten å oppsøke aktøren bak den uønskede handlingen. Å forebygge og begrense tap faller inn under kategorien 'defensiv forebygging'. Eksempler på kjente mekanismer er tetting av sårbarhetshull i programkode, tilgangskontroll med sikker identifisering og kryptering av kommunikasjon samt organisatoriske rutiner for å vurdere, merke og håndtere informasjon. Tanken bak denne forebyggingskategorien er å bygge murer rundt våre verdier. Målet er at færre prøver å

90 'Sårbarhet' som nevnt i punkt 2.3.

ramme disse verdiene, samt at det blir lettere å oppdage dem som forsøker.

Sikkerhetsbransjens kapasitet til defensiv forebygging er stor, men mye av arbeidet bærer preg av å «plastre sår». Teknologi brukes på måter man ikke opprinnelig forutså, og i tillegg stilles det krav om at ny teknologi kan inngå i eksisterende løsninger og gi samme eller økt tilgjengelighet.

Vi har lover med forskrifter og sikkerhetsstandarder som regulerer den defensive forebyggingen. Lovreguleringen har både sektorovergripende og sektorspesifikke krav. Eksempler på sektorovergripende lover er personopplysningsloven, sikkerhetsloven, beskyttelsesinstruksen og eForvaltningsforskriften. Eksempler på sektorspesifikke regelverk er energiloven, ekomloven og IKT-forskriften for finanssektoren. En velkjent sikkerhetsstandard er ISO 27000-serien.

De tekniske sidene av denne formen for forebygging omfatter stort sett å sikre konfidensialitet tilknyttet informasjon og tjenester i tillegg til integritet og tilgjengelighet. 'Konfidensialitet' handler om at uvedkommende ikke skal få tilgang. 'Integritet' dreier seg om at informasjonen er riktig og uendret, mens det med 'tilgjengelighet' menes at informasjonen eller tjenesten er tilgjengelig når det er behov for den. De menneskelige sidene innebærer ofte overstyrende tilgang på datasystemer og representerer kanskje en større sårbarhet enn de tekniske. Opplæring og organisatoriske systemer kan brukes for å unngå feil begått i uvitenhet, uhell og ondsinnede handlinger utført av innsidere.

9.4.1. Forebygging fra Nasjonal kommunikasjonsmyndighet (NKOM)

Det er Nasjonal kommunikasjonsmyndighet (NKOM), tidligere Post- og teletilsynet (PT), som regulerer eiere og tilbydere av nasjonal datainfrastruktur.

Internett. En Internett-leverandør eller -tilbyder er ofte en virksomhet. For å koble seg opp mot en Internett-leverandør er det vanlig å benytte trådløs kommunikasjon via mobiltelefon eller nettbrett, telefonlinjen (ekstern tilkobling) eller bredbåndstilkobling (kabel). Mange Internett-leverandører tilbyr tilleggstjenester som e-postkontoer, weblesere og lagringsplass der du kan legge ut ditt eget webområde. Det har etter hvert kommet mange typer virksomheter som tilbyr Internett til kundene sine – særlig borettslag, hoteller, butikkjeder, transportsektoren og etterhvert mange andre sektorer.

Definisjonen av 'Internett-tilbyder' og hvordan denne typen virksomhet følges opp av Nasjonal kommunikasjonsmyndighet, er uklart. Av en eller annen grunn er det blitt flere Internett-leverandører i Norge enn i en del andre europeiske land tilsammen. Det er uheldig at det har vært stilt få krav til leverandører om sikkerheten på Internett. Disse aktørene er viktige for mye av det forebyggende arbeidet mot datakriminalitet. Behovet for å følge opp sikkerheten og sørge for rapportering er klart tilstede. Det eksisterer en fast ordning for godkjenning av teletilbydere, mens dette mangler for Internett-leverandører generelt.

Et viktig spørsmål tilknyttet tilbyderne er om de bare skal kunne detektere datatrafikken, eller om de også skal kunne blokkere datatrafikk. Manipulering av senderadresse ('spoofing'), kjente former for tjenestenektangrep og masseutsendelse av e-post for kriminell utnyttelse, bør helt klart blokkeres. Seriøse Internett-leverandører har allerede systemer på plass for å kunne detektere og blokkere slikt. Dette kan gå ut over andre kunder, slik at leverandørene ikke overholder sine tjenestevilkår.

Kripos samarbeider med noen tilbydere som aktivt blokkerer tilgang til websider kjent for å distribuere innhold relatert til seksuelt misbruk av mindreårige. Dette samarbeidet fungerer godt, men er basert på frivillighet blant leverandørene. Tilsvarende kan gjøres for andre typer datakriminalitet, men spørsmålet er om det bør være en frivillig ordning, eller om det skal kunne lovreguleres som et pålegg. I tillegg er det usikkert om det er en akseptert og hensiktsmessig metode å bruke. Politiet må selv vurdere dette og eventuelt fremme forslag om videre tiltak.

En konsesjon kan blant annet omfatte:

- krav om oppbevaring av logger for tildeling av IP-adresser til kunder, og eventuelt krav om overlevering til et sentralt lager (se punkt 7.5.3); for nettkafeer og tilsvarende kan loggføringskrav eventuelt kompenseres ved kameraovervåkning,

registrering/SMS-aktivering og andre tilsvarende metoder for å ansvarliggjøre sluttbrukerne
- et minimum av sårbarhetskartlegging av kunder, med mindre avtalevilkår eksplisitt forbyr slikt (se kap. 9.4.2)
- elementær forebyggende filtrering, som utsending av søppelpost, tjenestenektangrep og manipulering av senderadresse

Mobilnettverkene. Det har lenge vært kjent at telesystemene kan overvåkes av uvedkommende. Andregenerasjonssystemet GSM, som vi faller tilbake på om nyere 3G-/4G-systemer ikke er tilgjengelige, er særlig sårbart. Antatt falske basestasjoner i Oslo okkuperte nyhetsbildet på slutten av 2014. Mediene og myndighetene spurte hvem som har ansvar for slike falske basestasjoner, for å avverge og eventuelt straffeforfølge slik virksomhet.

Nasjonal kommunikasjonsmyndighet (NKOM) har et ansvar for å hindre misbruk av tildelte frekvensbånd, noe falske basestasjoner gjør. Tjenesteleverandørene bør også ha et ansvar for å avdekke uautorisert utstyr for teknologien det gjelder, på lik linje med at de må vokte tilgangen til sitt eget utstyr i kjernenettverkene. Hvis falske basestasjoner registreres, må politiet sørge for straffeforfølgningen. Her pågår det et eget utredningsarbeid.

Konklusjon. Nasjonal kommunikasjonsmyndighet bør ha et strengere oppfølgingsregime for Internett-tilbydere som tilbyr tjenester (trådløst og via kabel) for å bidra til en tryggere infrastruktur og bedre rapportering om uønskede hendelser. Det bør vurderes å innføre konsesjonskrav for e-kom- og Internett-leverandører.

9.4.2. Bedre sårbarhetskartlegging

Svært få virksomheter og myndighetsorganer har så god kompetanse innen informasjonssikkerhet at de er i stand til – med egne ressurser eller gjennom innleid kompetanse – å kartlegge sine digitale sårbarheter. NSM har nylig lansert to tjenester[91] for å redusere sårbarheter i datasystemer knyttet til NSM NorCERT-samarbeidet. Det ene er en felles DNS ('Domain Name System'), et system for å koble domenenavn sammen med IP-adresser på Internett. Poenget er strengere retningslinjer for å blokkere og unngå helt åpne DNS-servere som normalt brukes på Internett. Dette kan da være med på å blokkere visse typer målrettede angrep samt vannhullsangrep. Tilsvarende løsninger har vært tilgjengelige fra private selskaper i flere år.

Den andre tjenesten er et initiativ for avlesning av kommunikasjonsporter inspirert av hvordan Shodan ble benyttet i Null_CTRL-serien til Dagbladet.[92] Reportasjene blottla store, åpne sårbarheter i konsumprodukter og usikre datanettverk. NSMs tjeneste kalles foreløpig 'Allvis NOR'.[93] Den utfører Internett-søk som Google og Bing, men leter på helt andre tjenester enn websider.

Formålet er å utføre en enkel kartlegging og søke etter kjente sårbarheter. Basert på resultatene av den kontinuerlige skanningen kan NSM varsle eieren av utstyret. Tjenesten er åpen for alle virksomheter i Norge og er av juridiske grunner samtykkebasert. Listen med deltagende virksomheter er stadig økende og inneholder allerede virksomheter i 'små og mellomstore bedrifter'-segmentet. NSM benytter etablerte kanaler og fagmiljøer for å følge opp avdekkede sårbarheter.

Kartlegging av enheter på Internett gjøres kontinuerlig av aktører med varierende motiver. Noen søk er spesifikt rettet mot nyoppdagede sårbarheter, mens andre, som Shodans, er langt mer generelle. Balansen mellom risiko for skade ved forsøk på å detektere sårbarheter og skade grunnet uvitenhet er vanskelig, men går trolig i favør av avlesning dersom den utføres av ansvarlige autoriserte aktører og kun er rettet mot norske IP-adresser.

Et pålegg om sårbarhetskartlegging i form av konsesjonskrav, som omtalt i punkt 9.4.1, vil da i hovedsak ha som formål å oppdage og varsle om forbrukerutstyr med manglende elementær tilgangskontroll direkte tilkoblet Internett, i tillegg til kjente sårbarheter.

Konklusjon. Kartlegging av sårbarheter ved datautstyr er et viktig preventivt tiltak. En stor utfordring er at vanlige forbrukere ikke kan forventes å ha kompetanse til å utføre slikt selv. For å oppnå bedre

91 https://www.nsm.stat.no/aktuelt/scanner-og-dns/

92 http://www.dagbladet.no/nullctrl/
93 http://www.dagbladet.no/2014/11/20/nyheter/innenriks/nullctrl/nsm/datasikkerhet/36336640/

forståelse for samfunnets sårbarheter samt å varsle dem det gjelder før de blir utsatt for noe kriminelt, vil det være hensiktsmessig om en grunnleggende kartlegging utføres for dem. NSM har bygget opp ressurser og kompetanse på området, så det kan være store synergieffekter ved å se en slik funksjon i sammenheng. NorSIS vil også kunne spille en rolle. For å dekke flest mulig med en slik løsning bør også Internett-leverandører tas med i betraktningen, da i form av konsesjonskrav.

9.4.3. Hindre uttak av kriminell økonomisk gevinst

Mye av datakriminaliteten er økonomisk motivert og kan forebygges ved å gjøre det vanskeligere å oppnå økonomisk gevinst. De fleste transaksjoner i Norge utføres digitalt. Dette gjør økonomien vår mer gjennomsiktig ved at det blir vesentlig lettere å drive tilsyn og ansvarliggjøre personer som står bak uønskede transaksjoner.

Tradisjonell betalingsteknologi. Chip-teknologi som erstatning for magnetstripen på betalingskort har redusert omfanget av kortkopiering. Geografisk sonebegrensning, begrensninger ved maksimumsbeløp og bankenes utstrakte bruk av algoritmer for å oppdage unormal aktivitet er alle viktige faktorer i begrensningen av uønskede pengeoverføringer.

Tofaktorautentisering, slik som bruk av kodebrikke (noe du har) i kombinasjon med passord (noe du vet), har gjort innlogging i nettbank tryggere, og vi ser en gradvis overgang der autentiseringen flyttes nærmere den enkelte transaksjon. Kundens datamaskin kan imidlertid være kompromittert, for eksempel av en banktrojaner. Det hjelper lite at kunden identifiserer seg på en svært sikker måte når en programkode på innsiden av maskinen er i stand til å manipulere alt kunden ser på skjermen.

Kontaktløs betaling. Kontaktløse betalingskort (slik som Zwipe MasterCard) og forskjellige typer betaling med mobiltelefon (slik som Apple Pay og Google Wallet*)* er på vei inn. I utgangspunktet er dette en positiv trend med mange flere sikkerhetsmekanismer, som fingeravtrykk og mulighet for tilbakekallelse i transaksjonsprotokollene. En ulempe ved mobiltelefoner er at de i bunn og grunn er datamaskiner som kriminelle kan bryte seg inn i. En annen ulempe er den muligheten kriminelle har til å kunne betale uten å måtte oppgi en PIN-kode.

Implementering og utvikling av disse sikkerhetstiltakene reguleres av markedet i balansen mellom behovet for effektiv betaling (tilgjengelighet) og viljen til å risikere økonomisk tap.

Elektroniske uregulerte (ofte anonyme) betalingssystemer overtar rollen som kontanter har hatt. Disse nye betalingssystemene har eksistert en stund, men mye tyder på at mer svart økonomi på Internett vil foregå gjennom slike anonyme betalingssystemer. Det utfordrer politi og myndigheter. Fremveksten av disse systemene støtter opp under kriminell aktivitet, slik som å kjøpe ulovlige tjenester og å skjule formue for å slippe offentlige skatter. Valutaen bitcoin har blant annet blitt brukt av kriminelle til å presse individer og bedrifter for penger ved hjelp av løsepengeviruset CryptoLocker. Det er likevel viktig å se slik ny teknologi i et positivt lys. Desentraliserte valutasystemer gjør det mulig å overføre penger enda raskere enn gjennom dagens sentraliserte banker, noe som er særlig interessant på tvers av landegrenser. I tillegg er det marginale kostnader knyttet til overførselen, fordi partene tar på seg en større risiko ved selv å sikre de virtuelle verdiene.

Mulige tiltak kan være lovregulering av slike betalingsløsninger både for individer og virksomheter. Land som Kina og Russland har innført diverse forbud mot bruk av bitcoin, mens vestlige land til nå har godtatt slik bruk forutsatt regulering av markedene som veksler mellom disse nye digitale valutaene og etablerte statsstøttede fiat-penger. Effektiv teknologi har historisk sett banet seg vei tross motstand, og det vil trolig være mer hensiktsmessig å få den frem i lyset enn å kriminalisere den.

Konklusjon. Myndighetene bør utrede en politikk med retningslinjer for bruk av uregulerte digitale penge- og betalingssystemer, for å hindre at de utnyttes til kriminell virksomhet.

9.4.4. Forbrukerrelaterte krav til sikrere IKT-systemer

Mange av de tekniske sikkerhetsutfordringene vi har i dag, og som kan resultere i datakriminalitet, kunne

vært forhindret ved smartere designløsninger og standardinnstillinger. Det er kjent at usikre innstillinger, ofte satt for å forenkle brukeropplevelsen, som regel ikke endres av brukeren av produktet. I motsetning til de fleste andre bransjer der produsenter blir stilt ansvarlig for alvorlige feil ved produktene, ser vi lite av dette innen programvareutvikling. Spørsmålet er om vi kan snu denne trenden ved å stille strengere krav til produsenter og tjenesteleverandører. Vi lærer opp ansatte til ikke å åpne mistenkelige vedlegg, mens det egentlige problemet er at et enkelt e-postvedlegg kan kompromittere et helt datasystem.

Lovkrav er en mulighet, men fordi bransjen er internasjonal, vil det trolig være irrelevant med særnorske krav. Trolig vil et samlet press fra forbrukerne, for eksempel gjennom felles europeiske krav, fungere bedre. EU har allerede stilt flere store selskap til ansvar, blant annet ved Microsofts integrasjon av nettleser i operativsystemet og Googles innsamling av data fra trådløse basestasjoner. Vi kan pålegge offentlige innkjøpsstrategier og tilrettelegge markedets insentiver for utvikling av sikre og robuste maskinvare- og programvareprodukter, ny sikkerhetsinnovasjon og sikre administrative tjenester. Det samme gjelder tilbydere av webtjenester, aviser og offentlige tjenesteleverandører som må forhindre at ondsinnet kode distribueres via deres webportaler. En viktig aktør her er Forbrukerrådet.

Bestillerkompetanse hos ledere og innkjøpsansvarlige er vesentlig for å kunne stille de rette kravene og ta sikkerhetsbevisste valg i innkjøpsprosesser, i utviklingsprosjekter og ved utsetting av datatjenester. Under strategigruppens besøk hos Forbrukerrådet ble det påpekt at bestillerkompetansen er for lav i Norge.

Konklusjon. Forbrukerrådet bør øke sin innsats for å fremme forbrukerrelaterte krav som bedre kan ivareta både personvern og den enkeltes informasjonssikkerhet. Staten bør øke sin bestillerkompetanse på ledernivå, slik at informasjonssikkerhet blir en naturlig del av alle anskaffelser.

9.4.5. Behov for sikker identifisering

Digital svindel skyldes dels at vi ikke har god nok identifisering, men også i høy grad naivitet og godtroenhet. I mange tilfeller ville sikker identifisering kunne forhindret svindel, fordi svindleren ikke lenger kunne lyve om sin identitet. Kunnskap om hvordan svindlere opererer, ville trolig kunne motvirke noe naivitet.

Utvikling av gode løsninger for elektronisk ID er utfordrende grunnet mange, til dels motstridende, krav. En offentlig nasjonal elektronisk ID burde være lett å bruke, selv for eldre og personer uten god teknisk innsikt, og bør ikke kreve tilgang på spesielt utstyr som smarttelefoner. Det er mange behov utover verifikasjon av identitet, for eksempel signering av dokumenter, og det er behov på forskjellige sikkerhetsnivåer. Difi har i dag løsningen MinID[94], hovedsakelig basert på et passord samt engangskode per SMS. I tillegg kan Commfides- og Buypass-basert identitet også brukes på offentlige nettjenester.

Mange nettsteder og tjenester tillater i dag innlogging gjennom eksisterende brukerkontoer hos populære sosiale nettsteder som Google, Facebook og Twitter. Denne teknologien heter OAuth ('Open Authorization') og illustrerer kreativiteten og viljen til å samarbeide for å oppnå smarte løsninger i det digitale samfunn.

Politiet, og sikkerhetsmyndigheter generelt, har behov for å identifisere seg digitalt for publikum, og publikum må i visse tilfeller identifisere seg digitalt for politiet. Dette gjelder for eksempel ved en digital anmeldelse eller ved bekjempelse av skremselspropaganda der kriminelle utgir seg for å være politi ved bruk av logo, se 7.2.1 om anmeldelse.

Andre løsninger er knyttet til administrasjon av ID, deriblant elektronisk ID. Følgende tiltak fra identitetstyveriprosjektet[95] bør nevnes i denne sammenheng:

- Et register for oppslag over identifikasjonsdokumenter som er meldt tapt eller stjålet. Tanken er at dette registret skal være tilgjengelig for aktører som kontrollerer identitet. Oppslag i et oppdatert register vil kunne begrense misbruk av stjålne identiteter.
- Et sted borgeren skal kunne henvende seg for å legge inn frivillig sperre mot kredittvurdering. Enkeltaktører har slike løsninger i dag, men sperringen bør være felles for alle.
- Hjelpelinje med sperretjeneste for ID-, bank- og kredittkort. Dagens løsning der eier er ansvarlig

94 Difi - Velg elektronisk ID selv! http://www.difi.no/artikkel/2011/03/velg-elektronisk-id-selv.
95 NorSIS – Identitetstyveri – Strategi og tiltaksplan https://idtyveri.info/files/Strategi-tiltaksplan-ID-tyveriprosjektet.pdf.

for å varsle alle partene individuelt, er lite effektiv, og det har allerede dukket opp kommersielle aktører på markedet som tar betalt for slike tjenester.

Det er fortsatt et problem at verdidokumenter som pass og bankkort blir sendt i posten. En del av dem forsvinner på veien ut til kundene, og disse kan misbrukes.

Konklusjon. Gode løsninger for elektronisk ID er et viktig tiltak for å forebygge mange former for svindel. Det er behov for regulering av utstedelse, verifikasjon og oppheving av (digital) identitet, slik at alle håndterer og sender identitetsinformasjon på en sikker og forsvarlig måte.

9.5. Forebygging rettet mot trusselaktørene

Forebygging rettet mot trusselaktørene skal forhindre planlegging og iverksetting av straffbare handlinger. *Politiets patruljering og tilstedeværelse på nett* (se tiltak 7.2 og punkt 7.2.2) faller inn under denne type forebygging siden den retter seg mot potensielle kriminelle aktører og datasystemer som aktivt utøver trusler.

Virkemidlene man lovlig kan ta i bruk for å respondere overfor en trusselaktør, er forskjellige for private aktører og offentlige myndigheter – spesielt politiet. Det er kjent at også private aktører tilbyr tjenester som innebærer gjengjeld i mangel på oppfølging fra myndighetene. Det er da snakk om motangrep rettet mot dem man tror står bak angrep på egen virksomhet, for eksempel i form av nye datainnbrudd og digital sabotasje. Dette er svært uheldig for et nettverk der attribusjon, det å identifisere hvem som faktisk står bak, er svært krevende, om ikke umulig, og kan gjøre utenrikspolitisk skade.

Deteksjon er et virkemiddel. Tiltak som øker faren for å bli oppdaget, straffeforfølgning og straff er vesentlige virkemidler for å redusere datakriminalitet. Det er imidlertid mye politiet kan gjøre for å forebygge, avverge og redusere skade. Det kan være så enkelt som å gå offentlig ut og informere om hvilke datahandlinger som er ulovlige. Politiet kan bli mye bedre til å oppfylle sin rolle innen slik forebygging.

Datakriminalitet omfatter en rekke uønskede handlinger, og trusselaktørene varierer mye når det gjelder grad av organisering og tilgang på ressurser. Skadeomfanget kan derfor være alt fra irritasjon hos et enkeltindivid til alvorlige nasjonale kriser som i verste fall kan innebære død og store materielle skader. Det er viktig å se det forebyggende arbeidet i lys av de konkrete datakriminalitetsformene og velge fremgangsmåte etter den aktuelle datakriminalitetens karakter.

Det er også avdekket store svakheter i forbrukerutstyr, bedriftsservere og styringssystemer tilkoblet norske IP-adresser i Dagbladets Null_CTRL-serie. I skyggen av identifikasjonsproblemene i det digitale samfunn har det over lang tid dukket opp store utfordringer knyttet til identitetstyveri og misbruk av stjålet identitet.

Å forhindre potensielle kriminelle fra å planlegge og utføre uønskede handlinger foregår på flere nivåer. Mange vil avstå fra slike handlinger fordi de anser dem som umoralske eller uetiske. Her vil blant annet oppdragelse, utdanning og livssituasjon spille inn. Noen vil avstå fordi handlingene er ulovlige og dermed kan føre til straff. For dem som ikke lar seg avskrekke av dette, må man sørge for at potensielle gjerningspersoner vurderer ulempene ved den kriminelle handlingen som større enn nytten. Høy risiko for å bli oppdaget og straffeforfulgt vil derfor også virke forebyggende.

Dette kapitlet fokuserer på *deteksjons- og varslingsevne,* både for private og offentlige aktører. Det trengs avvergende og skadereduserende metoder samt et opplegg for bevissikring dersom handlingen kommer til utførelse.

Deteksjonskapasiteten er fordelt på private og statlige aktører, men har hovedtyngden hos de private. Et velfungerende privat-offentlig samarbeid innen innsamling, sammenstilling og spredning av relevant kunnskap er en nøkkelfaktor for effektiv bekjempelse av datakriminalitet. Samarbeidet bør tilrettelegges av myndighetene og organiseres slik at alle parter får noe igjen. Tradisjonell polititenkning med politidistrikter eller landegrenser, språk- eller kulturbarrierer er i realiteten mindre interessant ved uønskede hendelser og kriminalitet på Internett. Politiet må alltid forholde seg til at personer og bevis kan befinne seg på flere

fysiske lokasjoner med ulike politiutøvende myndigheter og jurisdiksjoner. Samarbeidet må ha både en nasjonal og en internasjonal dimensjon. Det gir ekstra organisatoriske utfordringer.

9.5.1. Politiets rolle i offensiv forebygging på nett

Økningen av alvorlig datakriminalitet, økonomisk og industriell spionasje, organisert kriminalitet og terroraktivitet har gitt flere land grunnlag for å utvikle evne, kompetanse og ressurser til å utføre offensivt forebyggende politiarbeid på Internett. Det forebyggende arbeidet krever tilgang på spesialtrent politimannskap, dataanalytikere og eksperter på datatekniske undersøkelser på nett. Ulovlig virksomhet på nettsteder, botnett og skadevare kan være spesielle mål for målrettet offensivt politiarbeid på Internett, siden det utgjør en betydelig trussel mot sluttbrukere, privat og offentlig virksomhet og i økende grad kritisk, nasjonal infrastruktur og myndigheter.

Gevinsten kan være stor ved å hindre større utbredelse og skade gjennom mottiltak som kan bringe kriminelle nettverk ut av funksjon. Politiet har behov for å utvikle større evne til forebyggende arbeid blant annet som følge av de økonomiske og teknologiske faktorene som de kriminelle utnytter. De kriminelle motiveres av stadig mer økonomisk gevinst og tar raskt i bruk nye teknologiske muligheter.

Økt tilstedeværelse av politiet på Internett, både åpent og skjult som beskrevet i punkt 7.2.2 om analyse, vil ha en sterk forebyggende effekt. Jo høyere reell eller opplevd risiko, desto færre forbrytelser vil bli begått. At den opplevde oppdagelsesrisikoen trolig vil være langt høyere enn den reelle, er et faktum – men mediet kan benyttes til å skape et inntrykk av at faren for oppdagelse ved å begå digital kriminalitet generelt, og rettet mot barn spesielt, er høy.

Konklusjon. Politiet bør også være til stede på Internett, både med synlig og skjult patruljering, for å forebygge, avverge og etterforske kriminelle hendelser. Det handler om å gi Internett-brukerne inntrykk av at det er en faktisk oppdagelsesrisiko ved å begå kriminalitet på nettet. Opplevd oppdagelsesrisiko er en av de viktigste metodene politiet har til å forebygge kriminalitet. For mange vil oppdagelsesrisikoen være avgjørende for hvorvidt forbrytelsen blir begått eller ikke.

9.5.2. Politiets forhold til virksomheter og interessegrupper

Politiet er avhengig av at individer, offentlig og privat virksomhet og interesseorganisasjoner bidrar til å forebygge og stoppe datakriminalitet. Blant private virksomheter er det atskillig motvilje mot å dele sensitiv informasjon om datakriminalitet som rammer dem selv, med politiet, fordi informasjonsdeling kan være risikofylt og uten klare fordeler for dem. Informasjon kan bedre konkurrenters markedsposisjon, kundebaser eller gi dem andre viktige opplysninger. Forebyggende tiltak kan også bli neglisjert, blant annet av kostnadsmessige hensyn. Private selskaper vil heller ikke risikere å måtte oppgi informasjon i kostbare og tidkrevende rettssaker.

Disse faktorene gjør det nødvendig å etablere et troverdig samarbeidsforhold mellom politi og privat sektor. Politiet må respektere konfidensialiteten og verdien av opplysninger og hemmeligheter som privat sektor kan gi dem, uten automatisk å starte en straffesak. Det er avgjørende med rask informasjonsdeling. Dessuten må alle parter i et samarbeid ha tillit til at informasjonen som deles, beskyttes mot utlevering og videre bruk i politiet og hos andre partnere. Det må være mulig å danne troverdige relasjoner og dele data som senere kan gi grunnlag for etterforskning og straffesaksoppfølging.

Erfaringen tilsier at en virksomhet som blir utsatt for datakriminalitet, ofte prioriterer gjenoppretting av kompromitterte systemer fremfor å bruke tid og ressurser på etterforskning. Gjenoppretting vil kunne forringe digitale bevis, og man kan allerede ved deteksjonstidspunktet oppleve at nødvendige spor er tapt. 'Forensic readiness' kan forklares som å maksimere evnen til å sikre pålitelig bevis samtidig som man minimerer kostnaden ved hendelseshåndtering.[96] Det handler om å gå fra reaktiv til proaktiv håndtering. Hensikten er å redusere virksomheters kostnader samt øke handlingsrommet knyttet til myndigheters etterforskning i virksomhetens datasystemer.

Viktige momenter er:

96 R. Rowlingson. 2004. *A Ten Step Process for Forensic Readiness. International Journal of Digital Evidence*, vol. 2 (3).

- *Identifikasjon av relevante trusler* og hvilke data som vil være viktige i en etterforskning, samt utførelse av nødvendig loggføring.
- *Rutiner for sikring og oppbevaring av bevismateriale.* Her gjelder samme krav som for politiet: beskyttelse av integritet og sporing. Eksempler er uttak av logger, filer og nettverkstrafikk.
- *Opplæring og trening av nøkkelpersonell.* Det er også viktig at samarbeidet mellom virksomhetens personell og politi (og andre sikkerhetsaktører) er på plass før en hendelse inntreffer.

Når politiet involveres, vil det raskt fokusere på etterforskning for å finne ut hva og hvem som står bak hendelsen. Politiet vil om nødvendig bruke tvangsmidler for å sikre bevis ved ransaking og beslag. En utfordring for virksomheter og for politiet er at bevis ofte er lagret sammen med systemer som er avgjørende for virksomhetens drift. Bevis kan også være lagret sammen med kunders systemer og dermed medføre skade på tredjeparter. En best mulig bevissikring avhenger av et godt samarbeid mellom virksomheten og politiet. Innhentede data kan inneholde bedriftshemmeligheter, børssensitive opplysninger, advokatkorrespondanse, informasjon som tilhører partnere, og informasjon dekket av personopplysningsloven.

Retningslinjer for sikring av bevis og anmeldelsesrutiner kan være med på å styrke tilliten til politiet samt å øke antallet anmeldelser av datakriminalitet. For å sikre at næringslivet føler seg forpliktet av slike retningslinjer og samvittighetsfullt følger dem opp, bør næringslivet delta aktivt i utarbeidelsen av retningslinjene i samarbeid med politiet.

Viktige temaer er:

- varsling og anmeldelsesprosess, hvordan og til hvem
- krav og prosess rundt sikring av bevismateriale
- politiets håndtering av sensitive opplysninger
- tilbakelevering og destruksjon av innsamlede data etter endt rettsprosess

Noen av de viktigste interessegruppene som politiet må samarbeide med i bekjempelsen av kriminalitet, er:

- Internett-brukere og andre brukergrupper
- ledelse og styring av digitale samfunn som sosiale medier
- leverandører av nettinfrastruktur og tjenester
- enheter som organiserer nettsikkerhet i bedrifter
- private sikkerhetsorganisasjoner
- statlige ikke-polisiære organisasjoner som NSM, Forsvaret, Tollvesenet, Skatteetaten og Finanstilsynet

Det er viktig for politiet å etablere nye typer relasjoner med relevante aktører, relasjoner som krever endringer hos politiet og andre aktører for å bedre effektiviteten og legitimiteten. Her kan en del faktorer ha betydning: utflating av organisatoriske strukturer med mindre hierarki, bedre juridiske definisjoner og forståelse på tvers av myndighetsområder, mer ansvarlighet for innbyggerne, felles verdier, dialog og samspill mellom departementale og tverrsektorielle sikkerhetsaktører.

Konklusjon. Det er behov for å etablere et partnerskapsorientert samarbeid mellom politiet, virksomheter og de viktigste interessegruppene i bekjempelsen av datakriminalitet. Myndighetene bør sørge for at det utarbeides retningslinjer for samspillet mellom virksomheter og politiet ved forebyggende arbeid og anmeldelse av datakriminalitet for sikring av digitale bevis. Se også 7.4.2 om offentlig/privat samarbeid.

9.5.3. Minimumskrav til datalagring

Krav til datalagring vil virke preventivt og motvirke potensiell kriminalitet ved å øke deteksjonsfaren. Se punkt 7.2.4.

9.6. Sektorovergripende forebygging

Strategigruppen har vurdert om politiets helhetlige ansvar for forebygging av datakrimtrusler bør endres i lys av de utfordringene som en effektiv bekjempelse av datakriminalitet innebærer, men har ikke funnet tilstrekkelige grunner for dette.

Politiet og sårbarhetsfokusert forebygging. Strategigruppen har vurdert hvorvidt politiet i lys av datakriminalitetens egenart bør gis et utvidet ansvar for å utøve sårbarhetsfokusert forebygging utenfor de

områdene som dekkes av NSM, men mener at ansvarsprinsippet står seg også i denne sammenhengen. Det vil alltid være virksomhetene selv som kjenner egne systemer best, og som dermed vil være best i stand til å sikre dem. Arbeidsgruppen peker imidlertid på viktigheten av at virksomhetene rapporterer sikkerhetstruende hendelser som antas å stamme fra kriminelle handlinger, til politiet (se forslag til tiltak for å bedre anmeldelseshyppigheten blant annet i kapittel 10).

NSM som koordinerende instans. Strategigruppen har vurdert NSMs helhetlige rolle som nasjonal sektorovergripende og koordinerende instans på det sårbarhetsreduserende feltet og ser det som vesentlig at denne rollen videreføres, og at forholdet til sektorene styrkes. Den informasjonen politiet eller PST kan få om datakriminalitet gjennom deltakelse i den nasjonale CERT-funksjonen i NSM, danner et vesentlig grunnlag for risikobildet knyttet til datakriminalitet og påfølgende målrettet politiinnsats. Tilstedeværelse i NSM NorCERT er også viktig fordi NSM er en bistandsressurs ved etterforskning av datakriminalitet.

Forholdet mellom politiet og PST. I det forebyggende arbeidet er det nødvendig at PST og det øvrige politiet har et tett samarbeid. Det trengs gode mekanismer for å avgjøre hvilket spor datakrimsaker skal håndteres i (straffesakssporet eller for eksempel forebygging og avverging), og hvordan overføring av saker gjøres etter hvert som disse utvikler seg. Mekanismene for erfaringsoverføring bør utvikles slik at den samlede kompetansen til å beskrive, forebygge og bekjempe datakriminalitet i politiet blir best mulig. Gitt alvoret i kriminalitetsformene PST er satt til å motvirke, bør PST selv sørge for å utvikle evnen og funksjonene som skal til for å bekjempe særlig alvorlig og sofistikert datakriminalitet. Det kan konkluderes med at det er behov for tettere samarbeid, men det foreslås ingen formell endring i arbeidsdelingen mellom politiet og PST.

Politiet må bidra med trusselinformasjon. Strategigruppen mener at trusselinformasjon om datakriminalitet som politiet besitter – når og hvis den kan frigis – så raskt som mulig må gå fra politiet og PST over til det sårbarhetsreduserende arbeidet, slik at barrierer, deteksjonstiltak og reaksjonstiltak så godt som mulig kan tilpasses den aktuelle trusselen man antas å stå overfor. Informasjonen er også viktig for videreutvikling av regelverk, rådgivning overfor virksomheter og iverksetting av beredskapstiltak. Særlig viktige mottakere er NSM som sektorovergripende myndighet, sektormyndigheter, NorSIS og tjenester som Nettvett.

Realisering av behovene for informasjonsutveksling beskrevet ovenfor vil neppe kreve organisatoriske endringer mellom politiet/PST og øvrige sikkerhetsaktører. En optimal informasjonsflyt vil imidlertid kunne kreve en tydeliggjøring, effektivisering og styrking av samarbeidet mellom alle aktørene. Det anbefales derfor at styrende dokumenter og praksis gjennomgås med det for øye.

Forsvaret bør samarbeide tett med offentlige og private aktører. Forsvaret forvalter viktige digitale nettverk og systemer og er derfor en viktig samarbeidspartner som besitter både spesifikk kunnskap og funksjoner som er relevante i det forebyggende arbeidet. Om nødvendig bør kunnskapen og funksjonene være tilgjengelige for sivile myndigheter på forespørsel. På grunnlag av en formell forespørsel fra politiet om støtte, som godkjennes i henhold til regelverket, kan tiltak iverksettes under politiets myndighet. Forsvarets bistand til håndtering av alvorlige datahendelser, skal være koordinert med NSM jf. cyberretningslinjene for forsvarssektoren. Videre er det grunn til å vurdere om ressurser i Forsvarets organisasjon bør bringes inn i interdepartementale avtaler som spesifikke garantier, tilgjengelige som en del av et økt sivilt-militært samarbeid. Forsvarets kunnskap og ressurser i fredstid bør kunne bidra til bedret nasjonal sikkerhet ved håndtering av alvorlige digitale hendelser i spesielle tilfeller.

9.7. Gjenoppretting

Gjenoppretting handler om hva vi kan gjøre for å rette opp skade og returnere til normal tilstand. Det kan handle om teknisk gjenoppretting av kompromitterte systemer, kodeendringer for å tette oppdagede sårbarheter og omdirigering av trafikk på reservelinjer.

Det handler også om å ta vare på ofre for datakriminalitet ved å bistå i skadereduksjon, for eksempel med gjenoppretting av identitet og opprydding i personopplysningslekkasjer.
Gjenoppretting etter datakriminalitet bør utføres på en helhetlig måte. Forsikring er et eksempel på tiltak som ofte vil være samfunnsmessig økonomisk, og som vil være med på å tvinge frem sikkerhetstiltak, men det er ikke all skade som kan repareres økonomisk. Det bør derfor vurderes om ofrene for enkelte typer kriminalitet bør motta noe støtte eller tilrettelegging fra det offentlige.

Ansvar for gjenoppretting ligger hos eier, og forsikringsordninger er samfunnets måte å spre kostnader på. Markedet har svart med egne forsikringsordninger knyttet til identitetstyveri, og et naturlig spørsmål er hvor gode disse er. Det positive ved forsikringsordninger er at de bidrar til å etablere sikkerhetstiltak mot trusselen forsikringen gjelder. Erstatningskrav fra ofre mot skadevolder ved datakriminalitet er også relevant og står omtalt i punkt 8.4.4. Støtte til ofre for datakriminalitet bør vurderes nærmere, men det er særlig ett behov som bør nevnes spesifikt: Slettmeg-tjenesten levert av NorSIS er i realiteten det eneste tilgjengelige tiltaket politiet kan henvise til i saker som henlegges på grunn av kapasitet, eller usikkerhet om forholdets straffbarhet, og hvor de fornærmede kan få hjelp. Tjenesten er også den eneste som spesifikt ivaretar interessene til ofrene for datakriminalitet. Det dukker stadig opp nye typer krenkelser på nettet. Utviklingen går raskt, og det er viktig å styrke hjelpelinjen for å møte problemene. Nettroll-problematikken øker, et område hvor tjenesten også kan bistå.

Det er en fordel at Slettmeg.no ikke drives av et myndighetsorgan. Mange henvendelser fra tjenesten ligger utenfor eller i det som kan kalles en lovbruddsgråsone. Her vil en henvendelse fra et offentlig organ kunne oppfattes som et pålegg. Henvendelser fra Slettmeg.no oppfattes mer som en oppfordring, noe som i mange tilfeller gir et større handlingsrom. Tjenesten kan derfor hjelpe flere. Mange saker er av en slik art at offeret ikke opplever det som hensiktsmessig å gå til politiet. Uønsket distribusjon på Internett av personlige og sensitive bilder er et eksempel på et lovbrudd der ofre ofte vil ha hjelp av Slettmeg.no i stedet for å gå til politiet.

Konklusjon. Myndighetene bør vurdere om forsikringsordninger knyttet til identitetstyveri er gode nok, om de dekker det de påstår, og om det offentlige bør tilby utvalgte støttetiltak. NorSIS' arbeid med å følge opp ofre for datakriminalitet må styrkes og driften av Slettmeg.no sikres.

9.8. Kriseforståelse og krisehåndtering i det digitale samfunn

9.8.1. Noen hovedtrekk ved digitale kriser

Strategigruppens mandat gjelder datakriminalitet, ikke primært krisehåndtering. Likevel er det behov for en viss rolleavklaring når det gjelder krisehåndtering tilknyttet datakriminalitet.

Når blir hendelser kriser? Hendelser defineres som kriser når de får en viss størrelse, kompleksitet og alvorlighetsgrad som gjør det aktuelt å iverksette de spesielle regelverkene for håndtering av kriser. Et dataangrep kan etter omstendighetene sette viktige samfunnsfunksjoner ut av spill og få store konsekvenser for landets trygghet og sikkerhet. Et datainnbrudd kan medføre at identitetsinformasjon til millioner av mennesker blir stjålet, og at penge- og valutasystemet, produksjon og leveranse av matvarer og transport stopper opp og berører store deler av befolkningen. Nettsvindel og hackerangrep er bare noen eksempler på digital kriminalitet som daglig prøves ut på Internett og som kan – hvis forsøkene lykkes – utløse alvorlige hendelser i stor skala. Om slike alvorlige datahendelser resulterer i at krisehåndteringsmekanismer iverksettes, eller kun blir gjenstand for daglig hendelseshåndtering, beror på en konkret vurdering gjort av myndighetene som er ansvarlige for å håndtere utfordringene i det daglige, herunder på sektor- og nasjonalt nivå.

Datakriser behøver imidlertid ikke være rene digitale kriser. Selv om de har sitt utgangspunkt i den digitale verden, kan de raskt ramme også den fysiske verden og få alvorlige konsekvenser for mange mennesker. Digitale angrep kan dessuten skje i kombinasjon med andre former for sabotasje. Slås det elektroniske styringssystemet på et damanlegg ut som

følge av et dataangrep, med en stor flom som resultat, må også skader på folk og eiendom avverges så langt som mulig. Ved slike kombinerte alvorlige hendelser og kriser kan de ikke-digitale konsekvensene bli vel så alvorlige som de digitale aspektene ved angrepet. Hendelser som rammer både den digitale og den fysiske verden, antas å øke, fordi samfunnet i stadig større grad benytter elektronisk kommunikasjon for styring, samhandling og utveksling av informasjon.

Det kan være uklart hvem som står bak en krise. Er det en kriminell aktivitet utført av enkeltpersoner, en organisert kriminell aktivitet, en provokasjon fra en annen statsmakt som eventuelt benytter andre til utføre handlingen, eller et terrorangrep? Erfaringene fra NSM og CERT tyder på at de fleste alvorlige hendelsene er forankret i kriminell virksomhet. Sannsynligvis gjelder det samme for kriser. Europol mener at en av de største truslene mot EU fremover vil være organisert kriminell virksomhet utført som 'Crime as-a-Service' (se punkt 3.3.3) på Internett. Denne kriminalitetsformen kan rettes mot viktige samfunnsfunksjoner.

Det er viktig at slike komplekse krisestuasjoner diagnostiseres riktig og at håndteringen blir godt koordinert og ledet – særlig når flere myndigheter og aktører skal ivareta delansvar.

En detaljert analyse av spørsmålene om koordinerings- og ledelsesansvar faller utenfor mandatet for denne rapporten. Strategigruppen nøyer seg derfor med noen generelle synspunkter og peker på enkelte viktige spørsmål som bør utredes videre.

9.8.2. Juridiske rammer

Nasjonal sikkerhetsmyndighet. NSM er ansvarlig for «å håndtere koordineringen av alvorlige IKT-angrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsinstitusjoner» og for «å organisere og drifte et nasjonalt varslingssystem for digital infrastruktur» (se instruks for sjefen for Nasjonal sikkerhetsmyndighet pkt. 12 og 13).

NSM skal dessuten utføre forhåndsplanlagte oppgaver ved alvorlige IKT-angrep som et ledd i den nasjonale krisehåndteringen, i henhold til det nasjonale beredskapssystemet. NSM har døgnkontinuerlig operativitet og rapporterer til Justis- og beredskapsdepartementet og Forsvarsdepartementet. Dersom et annet lederdepartement er utnevnt, skal NSM rapportere til dette i tillegg til Justis- og beredskapsdepartementet og Forsvarsdepartementet.

Politiet. Som redegjort for i punkt 7.1 har politiet både et ansvar for å etterforske datakriminalitet, en plikt til å forebygge og avverge datakriminalitet samt et alminnelig ansvar for å verne samfunnet mot hendelser som «truer den alminnelige tryggheten i samfunnet» og som ikke er begrenset til kriminalitet Politiet kan bruke maktmidler for å få gjennomført nødvendige tiltak.

På andre offentlige myndigheters ansvarsområder kan politiet, med hjemmel i politiloven § 7 4. ledd, gripe inn når en situasjon medfører alvorlige ordensforstyrrelser, eller fare for dette, dersom det må antas at vedkommende myndighet ikke kan håndtere hendelsen tilfredsstillende selv. Den ansvarlige myndigheten skal snarest mulig underrettes om inngrepet. Utenfor normal arbeidstid er det ofte bare politiet som har tilgjengelig beredskap.

Når menneskers liv eller helse trues, er det politiets ansvar å iverksette og organisere redningsinnsatsen hvis ikke en annen myndighet er pålagt ansvar. Dette følger av politiloven § 27 som regulerer politiets oppgaver i ulykkes- og katastrofesituasjoner. For koordinering og ledelse av dette arbeidet i politiet har Politidirektoratet utarbeidet Politiets beredskapssystem (PBS) 1–3.

Politiloven § 27 tredje ledd dekker ulykkes- og katastrofesituasjoner som ikke omfattes av den organiserte redningstjenesten, altså tilfeller der menneskers liv og helse ikke er truet. Kriser knyttet til for eksempel bortfall av e-komtjenester kan være en slik situasjon.

9.8.3. Ansvarsspørsmålet ved sektorovergripende kriser

Politiets vide fullmakter og ansvar etter politiloven overlapper med fullmaktene til NSM. Foreligger det et alvorlig «IKT-angrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsinstitusjoner» som krever krisehåndtering, legger strategigruppen til grunn at det da fortsatt må være NSM som har koordineringsansvaret. NSM må gjøre vurderingen

av angrepet, og politiets ansvar blir av subsidiær karakter.

Digitale kriser som følge av angrep på samfunnskritisk infrastruktur vil som oftest innebære alvorlig datakriminalitet. Håndtering av selve krisen faller da i stor grad sammen med forebygging av konsekvensene av de straffbare handlingene. Hvis NSM sørger for nødvendige tiltak for å stoppe angrepet og gjenopprette en sikker tilstand, kan PST og politiet konsentrere seg om å etterforske aktuelle straffbare handlinger. NSM vil i tråd med praksis kunne bistå med nødvendig bevissikring, analyse og rådgiving.

Det er NSMs ansvar å vurdere om datahendelser innebærer «alvorlige IKT-angrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsinstitusjoner». I så fall vil NSM i henhold til NBS som nevnt selv iverksette eller gi anbefalinger om iverksettelse av visse forhåndsbestemte eller situasjonsavhengige tiltak, og ellers koordinere håndteringen. Men selv om NSM ikke finner grunnlag for å iverksette krisehåndtering, må politiet fortsatt vurdere om det skal gripe inn i medhold av sine fullmakter.

Er det mistanke om straffbare handlinger, kan også forebyggende og avvergende tiltak etter politiloven § 2 nr. 2 og 3 være aktuelle i tillegg til etterforskning. Ved kombinerte kriser der de ikke-digitale konsekvensene er de alvorligste, vil det da være fornuftig at PST/politiet står for koordineringen.

Hvis alvoret tilsier det, kan det også være aktuelt å sette stab etter beredskapsinstruksen. Da telefonnettet sviktet i Ålesund i 2014, og befolkningen ikke kunne kommunisere med verken politi, helsepersonell eller andre, etablerte lokalt politi stab og utplasserte politipatruljer som kunne benytte politiets samband.

Behovet for samhandling med og bistand til andre myndigheter og/eller private virksomheter synes åpenbart i krisesituasjoner. Det er derfor nødvendig å øve slik samhandling med utgangspunkt i eksisterende planverk, og utvikle dette videre. I situasjoner hvor datahendelser har alvorlige, krisepregede fysiske virkninger, kan det være nødvendig å etablere det samme ledelsesapparatet og samarbeide med andre offentlige etater, både lokalt og sentralt, som ved vanlige redningsaksjoner. Også her må politiet sørge for forsvarlig etterforskning av straffbare datahandlinger, som ved annen kriminalitet.

PBS I inneholder ingen beskrivelse av scenarioer knyttet til kriser i det digitale samfunn – uavhengig av om det er oppstått fysisk skade som følge av dem, eller motsatt ved at de har oppstått som en følge av fysiske hendelser. Verken NSM eller Nkom er beskrevet som mulige koordinerings- eller bistandsaktører med oppgaver i en ulykkes- eller krisesituasjon der datateknologi utgjør et sentralt element. Særlig i starten kan en krisesituasjon være uklar, og det kan oppstå spørsmål om hvilke sikkerhetsaktører som har ansvaret for å håndtere situasjonen, og hvor alvorlig den er. Ved uklarheter bør de aktuelle sikkerhetsaktørene raskt avklare ansvaret seg imellom, slik at hendelses- og krisehåndteringen kommer i gang med fornøden kraft og uten unødig opphold, og ta hensyn til at det kan være nødvendig med etterforskning av mulige straffbare forhold. Det må unngås at sikkerhetsaktørene sitter på gjerdet og venter på at en annen myndighet tar initiativ.

CKG er et koordineringsforum for NSM, E-tjenesten og PST i arbeidet med å koordinere de mest alvorlige datahendelsene. Gruppens aktivitet er forankret i retningslinjer fastsatt av sjefene for de tre tjenestene. Politiet, ved Kripos, kan i likhet med Cyberforsvaret ved behov stå for koordineringen i CKG. Kripos har dessuten i dagens ordning en avtale om tilstedeværelse i den nasjonale CERT-funksjonen for å få tilgang til frigitt informasjon om sikkerhetstruende hendelser i virksomheter og sektorer rapportert opp til nasjonalt nivå, eller til informasjon som NSM har blitt kjent med på annen måte – for eksempel gjennom internasjonalt samarbeid. Imidlertid deltar ikke Kripos ved oppdagelse av eller analyse av enkelthendelser ved NSM NorCERT i en normalsituasjon, da dette vil være problematisk sett opp mot NSMs bistandsrolle mot virksomheter og det faktum at eierskapet til slik hendelsesinformasjon ligger hos virksomheten. Tiltak som NSM NorCERT ønsker iverksatt umiddelbart i en krisesituasjon, og som krever maktmidler som NSM selv ikke råder over, kan være vanskelig å gjennomføre uten at politiet har en beredskapsfunksjon ved NSM NorCERT. Slik deltakelse kan også føre til at etterforskningen kommer raskere i gang, men kan som nevnt by på rettssikkerhetsmessige utfordringer når informasjonen ikke kan spres videre til andre, se også punkt 7.4. Et slikt behov for beredskapsmessig

tilstedeværelse må ses opp mot at PST alt nå er tilstede og vil kunne benytte sine maktmidler.

Datakriminalitetsaspektet i nasjonale krisehåndteringsøvelser. Under Sivil nasjonal øvelse 2008 opplevde man interessekonflikter knyttet til det å blokkere Internett-kommunikasjon samt utfordringer knyttet til balansen mellom forebyggings- og etterforskningshensyn. Under øvelsen Cyber Dawn i 2013 inngikk momenter der datakriminelle hendelser førte til parallelle hendelser både i den digitale og den fysiske verden. Evalueringen og erfaringen derfra peker på viktigheten av at politiet ikke forbigås i krisehåndteringen. Det er behov for å trekke datakriminalitetsaspektet ved digitale kriser inn i nasjonale krisehåndteringsøvelser, slik at sikkerhetsaktørene får tydeliggjort roller og ansvar i særlig komplekse og tverrsektorielle kriser.

9.8.4. Utredningstemaer og øvelser

Det er viktig at beredskapsplaner og prosedyrer følges opp for å inkludere politiet og PST i informasjonsflyt og beslutninger på en best mulig måte. Beredskapssystemene bør øves jevnlig på med tanke på forbedringer. Det er i denne sammenheng også behov for å vurdere om man har egnede lokaliteter for digital formidling, digitale presentasjoner og kommunikasjon for samhandling.
Temaer som bør utredes nærmere:

- Begrepet 'nasjonal krise' i datasammenheng bør presiseres. Begrepet bør også omfatte kombinerte kriser hvor skadevirkningene truer både den digitale og den fysiske verden. Det er behov for gode prosedyrer for ansvarsoverføring og ansvarsdeling ved håndtering av slike kriser.
- Behovet for oppdatering av Nasjonalt beredskapssystem og politiets beredskapssystem for å samordne nødvendig digital beredskap i politiet med beredskapen i Nasjonal kommunikasjonsmyndighet (NKOM) og Nasjonal sikkerhetsmyndighet (NSM).

9.9. Hovedstrategi for forebygging og avverging

Kriminalitetsforebyggende arbeid og avverging er de viktigste virkemidlene for å sikre at datakriminaliteten holdes lav. Sikkerhetsaktørene må arbeide for å øke evnen til selvbeskyttelse mot datakriminalitet i befolkningen og virksomhetene. Politiet må dele kunnskap om pågående og forventede kriminelle aktiviteter og metoder for å avverge dem, med andre sikkerhetsaktører, potensielle ofre og publikum.

Politiet må samarbeide med databransjen om å stille strenge krav via regulering og tilsyn for å oppnå høyere innebygget sikkerhet i utvikling og leveranse av datatjenester, produkter og programvare. Minimumskrav og konsesjonskrav bør benyttes aktivt.

Politiet må styrke sin forebyggende virksomhet med tilstedeværelse og patruljering på Internett, og stadig utvikle metodene for å forebygge og avverge datakriminalitet. Politiets ansvar for krisehåndtering i det digitale rom må være like klart, og bygge på de samme prinsippene som for den fysiske verden.

Anbefalte tiltak:
NB: Nummereringen av de anbefalte tiltakene nedenfor angir ikke prioriteringer.

Tiltak 9.1 *Gjennomføre et nasjonalt løft for å spre kunnskap om datakriminalitet til borgere og virksomheter for å bedre evnen til selvbeskyttelse.* Det skal særlig legges vekt på sikker deltakelse i det digitale samfunn for barn, ungdom og eldre. Se punkt 9.3.

Tiltak 9.2 *Skjerpe reguleringen av Internett-tilbydere.* Innføring av konsesjonskrav som omfatter sårbarhetskartlegging og deteksjon av trafikk knyttet til kriminell aktivitet. Se punkt 9.4.1 og 9.4.2.

Tiltak 9.3 *Utrede tiltak for å redusere muligheten for kriminell utnyttelse av uregulerte digitale penge- og betalingssystemer*. Se punkt 9.4.3.

Tiltak 9.4 *Gjennomgå reguleringen av utstedelse, verifikasjon og oppheving av (digital) identitet*. Se punkt 9.4.5.

Tiltak 9.5 *Stimulere forbruker-, bransje- og næringslivsorganisasjoner og aktuelle myndigheter til å fremme krav til produsenter og selgere om bedre vern mot datakriminalitet ved kjøp av datautstyr og datasystemer.* Se punkt 9.4.4.

Tiltak 9.6 *Tydeliggjøre roller og videreutvikle prosedyrer for håndtering av kriser som omfatter både den digitale og den fysiske verden*. Se punkt 9.8.1

Tiltak 9.7 *Trekke datakriminalitetsaspekter ved digitale kriser systematisk inn i nasjonale krisehåndteringsøvelser og oppdatere politiets beredskapssystem basert på erfaringene*. Se punkt 9.8.3.

Tiltak 9.8 *Utvikle samarbeid mellom politi og virksomheter på lokalt nivå for å skape tillit og større vilje til anmeldelse.* Se punkt 9.5.2.

Følgende tiltak i andre kapitler vil også ha klare forebyggende og avvergende virkninger:

7.12 *Et sentralt mottak for tips*
7.2 *Åpen og skjult tilstedeværelse av politiet på nett*
7.8 *Samarbeidsarena*
7.11 *Internasjonalt samarbeid*, jf. 10.4 *Lagring av informasjon om kobling mellom IP-adresse og juridisk eier.*

10. STRATEGI FOR STRAFFEFORFØLGNING

10.1. Nåsituasjonen

Visjonen krever et *effektivt* vern mot datakriminalitet for å sikre trygg bruk av datasystemer for alle. En velfungerende straffeforfølgning er et vesentlig virkemiddel for å nå dette målet. Mens sikkerhetstiltak særlig kan avverge skadelige datahandlinger og bidra til en sikker tilstand, er straff et sentralt redskap for å hindre gjerningspersoner i å gjøre nye forsøk og for å innarbeide minimumskrav til akseptabel adferd for databruk i befolkningen, se drøftelsen under punkt 8.5.[97] Dagens system for straffeforfølgning er langt fra i stand til å oppfylle visjonen, og det er behov for en langt bedre bekjempelse av datakriminalitet. Særlig politiets evne til å avdekke og etterforske denne typen kriminalitet må forbedres.

Analysen i kapittel 3 viser at datakriminalitet har noen særtrekk som skiller den fra annen kriminalitet:

- Den er sterkt teknologidrevet.
- Datamengden og sakskompleksiteten er gjennomgående svært høy.
- Tidsfaktoren er mer kritisk fordi de digitale sporene ofte har kortere levetid enn andre spor og anonymiseres, endres eller slettes oftere.
- Digitale spor kan være distribuert på en stor mengde e-kom- og tjenestetilbydere og private aktører som i liten grad ønsker eller kan gjøre kritiske, digitale bevis tilgjengelig for politiet – eller vet at de besitter slike.
- Datakriminaliteten er internasjonal. Det kan enkelt gjennomføres lovbrudd i Norge fra andre steder på jordkloden.
- Datakriminaliteten er dynamisk. Dagens trussel- og risikobilde viser at datakriminaliteten er sterkt økende både i omfang og kompleksitet. Økningen vil høyst sannsynlig fortsette. Bildet vil også endre seg ved at gjerningspersoner tar i bruk nye metoder. Parallelt vil eksisterende metoder miste effekt og benyttes mindre på grunn av beskyttelses- og bekjempelsestiltak.
- Datakriminaliteten dekker spesielle og nye kunnskapsområder der tverrfaglig tilnærming er viktig.
- Det kreves mer spesialistkompetanse i politiarbeid på nett og i bruk av digitale spor og bedre tilgang på teknologikompetanse i datatekniske undersøkelser og analyse.

Datakriminalitet utført av andre stater vil kunne være basert på svært avansert teknologi og ha potensielt betydelige skadevirkninger. Det kan dreie seg om operasjoner de benekter, og som er nær sagt umulige å rettsforfølge.

Disse spesielle momentene synes i dag å kjennetegne datakriminalitet, men det er mye som tyder på at dette også vil prege annen kriminalitet i fremtiden og på sikt gjelde digitale spor innen de fleste typer kriminalitet.

10.2. Svakheter ved politiets rolle i dag

Straffesakskjeden består av flere ledd. Politiet og påtalemyndigheten har ansvaret for straffeforfølgningen, som består i å avdekke, etterforske, påtale og iretteføre straffbare handlinger for domstolene for å avgjøre spørsmål om skyld og straff. Kriminalomsorgen gjennomfører i siste instans idømt straff. Politiets og PSTs evne til å oppdage og etterforske

97 Samvirket med forebygging ligger – som påpekt av blant annet Riksadvokaten – i at straffeforfølgningen har «som sitt viktigste mål å virke forebyggende (...). Gjennom allmennpreventive virkninger skal straffeforfølgningen bidra til at potensielle lovbrytere avstår fra kriminalitet». (Riksadvokatens høringsuttalelse av 9. oktober 2013 i anledning Politianalysen).

datakriminalitet er avgjørende for at straffesakskjeden skal fungere effektivt. Strategigruppen legger derfor hovedvekten på å analysere og vurdere denne delen av straffeforfølgningen, men vil også se kort på utfordringene ved iretteføring av datakrimsaker for domstolen.

10.2.1. Eksterne faktorer som påvirker etterforskningseffektiviteten

I dag får politiet informasjon om datakriminalitet primært gjennom anmeldelser fra ofrene, og informasjon på et overordnet eller aggregert nivå om mulige datalovbrudd fra CERT-ene, i hovedsak NSM NorCERT. Det er store avvik mellom straffbare handlinger som ofre eller andre får kunnskap om, og handlinger anmeldt til politiet, noe mørketallsundersøkelsene dokumenterer (se punkt 7.2.1 og 7.3.1). Av Mørketallsundersøkelsen 2014 fremgår det at årsakene til at virksomhetene ikke anmelder hendelser, er at de «ikke tror det er mulig å finne gjerningsmannen», «saken er ubetydelig», «saken er håndtert internt i virksomheten» og «manglende tiltro til politiets kompetanse».

Samarbeidet med næringslivet er ikke godt nok, noe som også illustreres av Mørketallsundersøkelsen. I den utstrekning Kripos har samarbeidet med private virksomheter i saker under etterforskning, har erfaringene imidlertid vært gode. Dette gjelder blant annet samarbeidet med DNB i etterforskningen av flere bølger av nettbankbedragerier.

Datakriminalitetens internasjonale karakter fører til lang saksbehandlingstid. Gjerningspersoner og utstyr (servere mv.) befinner seg ofte i utlandet og gjerne i flere forskjellige land. Strategigruppens inntrykk, basert på tilbakemeldingene fra politiet og påtalemyndigheten, er at det internasjonale sakssamarbeidet ofte er ineffektivt. Det er normalt tidkrevende og vanskelig å få sikret elektroniske spor i utlandet og å få disse utlevert til Norge. Erfaringen er videre at spor og gjerningspersoner ofte befinner seg i land som er krevende å samarbeide med, som Russland og Ukraina. Dette medfører at straffeforfølgningen i beste fall forsinkes og noen ganger hindres fullstendig.

Etterforskningsenheter, inkludert Kripos, opplyser at *tilgjengelige etterforskningsmetoder* – også skjulte metoder – i stor grad oppfyller behovene for en hensiktsmessig etterforskning av datakriminalitet i dag, men flere peker på behovet for en lovhjemmel for å gjennomføre dataavlesning, se punkt 10.4.2. Mange metoder er krevende å bruke. Gitt datakriminalitetens dynamiske karakter har metodene stadig kortere levetid.

10.2.2. Interne faktorer som påvirker etterforskningseffektiviteten

Det er bare et fåtall anmeldte datakriminalitetssaker som faktisk er gjenstand for etterforskning, og enda færre saker oppklares og ender med positiv påtaleavgjørelse i form av forelegg eller tiltalebeslutning og dom. Dette gjelder ikke bare hverdagskriminaliteten, men også alvorlige former for datakriminalitet. Nøyaktige tall for anmeldt datakriminalitet finnes ikke, idet det i dag ikke eksisterer noen god statistikk på området, se punkt 7.3.1.

Dette medfører at politiets egen saksutvelgelse sjelden er strategisk forankret. Selv Kripos' egne saker iverksettes sjelden basert på kunnskap og strategiske valg. Dette er en utfordring.

Saksbehandlingstiden i større datakriminalitetssaker er ofte lang. Dette skyldes manglende kapasitet til å analysere svært store og komplekse datamengder, at stadig mer av kommunikasjonen blir kryptert, og at behovet for internasjonal bistand kompliserer dette ytterligere. Politiet erkjenner også at spesielt tvangsmiddelpregede etterforskningsmetoder per i dag ikke utnyttes godt nok.

Politiet har *liten tilstedeværelse på Internett*, og etterretningsinnsatsen på området er begrenset, se punkt 7.2.2. Med unntak av visse aktiviteter i Kripos og PST er politiets kjennskap til kriminalitet eller kriminelle miljøer på Internett svært tilfeldig og i stor grad basert på anmeldelser og delt informasjon fra for eksempel Europol og Interpol.

Den samlede kapasiteten til å etterforske datakriminalitet og elektroniske spor i andre typer kriminalsaker er for lav både i politidistriktene og hos Kripos, og gjelder samtlige stadier av etterforskningsarbeidet; etterretning, sikring og undersøkelse av elektroniske spor, analyse og taktisk etterforskning for øvrig. En vesentlig del av den lokale kapasiteten går i dag til innhenting og analyse av elektroniske

spor i vanlige straffesaker, ikke til etterforskning av datakriminalitet. Det finnes ikke brukbar statistikk som viser hvor stor kapasitet som brukes til datakriminalitet, men det klare inntrykket er at datakrimsaker taper i konkurransen om etterforskningsressursene.

Slik situasjonen er i dag, må Kripos prioritere å bruke spesialistressurser fra Internett-etterforskning og datatekniske undersøkelser til annen type organisert kriminalitet som avgir e-spor. Slik organisert kriminalitet har en høy strafferamme og får ofte høyere prioritet enn datakriminalitet. Det er derfor et stort behov for å avgi mer ressurser til datakrimområdet.

Kripos og politidistrikter som strategigruppen har vært i kontakt med, rapporterer at kompetansen i mange politidistrikter har økt de siste årene innen ordinær sikring og undersøkelse av elektroniske spor. Noen av distriktene har også egne enheter for dette arbeidet.

Mye gjenstår imidlertid når det gjelder distriktenes evne til taktisk etterforskning av datakrimsaker, og det er behov for å øke både den spesialiserte og den generelle etterforskningskompetansen i politidistriktene. De færreste politidistriktene har i dag tilstrekkelig kompetanse til å etterforske datainnbrudd eller andre datahendelser av en viss størrelse. Politidistriktenes dataetterforskere arbeider med sikring og analyse av databeslag og digitale spor i alle typer saker. Behovet for dataetterforskere har i lang tid vært større enn tilgjengelig kapasitet. Til tider opplever dataetterforskere en kø av ubehandlede oppdrag som skaper en flaskehals i mange etterforskningssaker.

I tillegg blir kapasiteten altså ikke benyttet til etterforskning av datakriminalitet, men til sikring av spor innen annen type kriminalitet. Selv om dataetterforskeren ikke nødvendigvis er en del av saksetterforskningen, og i utgangspunktet ikke har detaljkunnskap om saken, får vedkommende ansvaret for gjennomgang av databeslag og digitale spor. Hvert politidistrikt har en egen infrastruktur og egne dataløsninger for oppbevaring av speilkopier og bevissikrede data. Ingen har nasjonalt ansvar på fagområdet, og det finnes ingen standarder for sikring og analyse av digitale spor. Politidistriktene benytter ulike løsninger, fra kommersiell dataetterforskningsprogramvare til programmer som gratis kan lastes ned fra Internett.

Politidistriktene kan få bistand fra Kripos, men terskelen for bistand er ofte svært høy. I dag finnes det også politidistrikter helt uten dataetterforskere. Når politiet behandler forholdsvis få saker, medfører det at få medarbeidere får opplæring i og erfaring med saksfeltet. Dette gjelder både politi- og påtalefaglig behandling av sakene. Etter å ha vært i kontakt med blant annet Kripos, utvalgte politidistrikter, øvrige sikkerhetsaktører og næringslivsaktører, legger strategigruppen til grunn at politiet og påtalemyndigheten per i dag har *for lav kapasitet og kompetanse* til å etterforske de fleste former for datakriminalitet. Den totale kapasiteten må økes betraktelig. For å kunne klare dette innen rimelig tid må det utdannes flere egne datakrimetterforskere og rekrutteres personer med høy datateknisk kompetanse. Se kapittel 11.

Konklusjon. Det trengs en betydelig økning av den samlede etterforskningskapasiteten for datakriminalitet. Økningen må også ses i sammenheng med det generelle behovet for å styrke datatekniske undersøkelser av digitale spor, både lokalt og sentralt. Kapasitetsøkningen må også komme datakriminaliteten til gode.

10.2.3. PST

Innen PSTs ansvarsområde er trusselaktørene ofte stater, det vil si statlige etterretningstjenester med til dels enorm kapasitet til å gjennomføre skjulte operasjoner de selv benekter eksistensen av. Det er i praksis vanskelig å straffeforfølge disse. Teknologiutviklingen er også så rask at Norge trolig blir utsatt for jevnlige dataangrep som ikke blir registrert. Andre sentrale aktører er transnasjonale terrorgrupper som legger ut propaganda og oppfordringer til vold. Dette blir også gjort av nordmenn i utlandet.

Konklusjon. På bakgrunn av teknologiutviklingen og konsekvensene dette har for trusselbildet, er det behov for en betydelig styrking av PSTs evne til å etterforske og forebygge trusler i det digitale rom. Dette inkluderer også utvikling av nye og endring av eksisterende lovhjemler som PST allerede har fremmet forslag om.

10.3. Påtalemyndigheten og domstolene

Påtalemyndighetens arbeid med datakrimsaker preges også av at kun et fåtall av dem er gjenstand for straffeforfølgning. Påtalemyndighetens første nivå – politiadvokatene – har ansvaret for å lede etterforskningen også i denne type saker. De fleste datakriminalitetssakene faller også inn under politiets påtalekompetanse, jf. straffeprosessloven § 67. Det innebærer at enda færre behandles av de to andre påtalenivåene, statsadvokatene og Riksadvokatembetet.

Strategigruppens erfaring så langt er at det kun er politiadvokatene tilknyttet Kripos' Seksjon for datakriminalitet som har spesialkompetanse innen etterforskning og iretteføring av datakrimsaker for domstolen. På statsadvokatnivå er det ingen med slik kompetanse.

Strategigruppens inntrykk er at både politi- og statsadvokater har for lite kjennskap til spesialbestemmelsene om datakriminalitet, selv om flere av disse er blitt vedtatt relativt nylig gjennom forskuttering av bestemmelser i straffeloven 2005, se kapittel 8.2. Erfarne politi- og statsadvokater vil gjennomgående ha betydelig erfaring med tolkning av ulike elektroniske spor og presentasjon av disse for domstolen, men den generelle datakunnskapen er ikke god nok. Kompetansen er også for lav innen bruk av utradisjonelle etterforskningsmetoder. Norsk politi har god kompetanse og erfaring innen internasjonalt samarbeid i straffesaker generelt – men ikke i datakrimsaker.

Domstolenes behandling av datakrimsaker preges også av at dommere og meddommere ofte har begrenset kunnskap om datateknologiske spørsmål. I saker der tilegnelse av digitale bevis kan være utfordrende, kan aktor be om at retten settes med fagkyndige meddommere i medhold av straffeprosessloven § 277 jf. domstolloven § 94. Svært få saker av denne typen omfatter straffebud med så høy strafferamme at ankeforhandlingene skal behandles med lagrette.

Politidirektoratet og Domstolsadministrasjonen har besluttet at det skal gjennomføres to pilotprosjekter – henholdsvis *Digitale aktorater* og *Digitale rettsmøter* – fra oktober 2014, hvor utvalgte politidistrikter og domstoler skal praktisere og videreutvikle den papirløse løsningen i både små og store straffesaker. Erfaringene fra pilotprosjektene vil danne grunnlag for utviklingen av de endelige digitale saksbehandlingssystemene hos politiet og domstolene. Implementeringen vil stille krav til opplæring av politietterforskere, påtalejurister, forsvarere og dommere. Politiet og domstolene må få tilgang til datateknisk utstyr og programvare som muliggjør en digital straffesakskjede.

Konklusjon. Påtalemyndighetens og domstolenes kompetanse i datakrimsaker må forbedres gjennom spesifikke kompetansekrav i politidistriktene. Det kan i en periode være nødvendig å kanalisere datakrimsakene til særlig utvalgte politiadvokater, statsadvokater og domstoler.

10.4. Viktige hensyn ved straffeforfølgning av datakriminalitet

10.4.1. Etterforskningsmessige utfordringer

Oppdagelse. Det er helt avgjørende å styrke ofrenes tillit til politiets og påtalemyndighetens evne til å håndtere datakriminalitet. Dette tilsier særskilte tiltak for å øke deres, politiets og øvrige sikkerhetsaktørers muligheter for å oppdage datakriminalitet.

Kilder og innsamling. Digitale spor skapes ved bruk av datateknologi. Dette er informasjon som med stor grad av sikkerhet kan knyttes til en bruker, en person, en elektronisk enhet, et sted eller en hendelse.

Elektroniske spor stammer fra tre hovedkilder:

- Data under overføring.
- Data lagret på et beslaglagt lagringsmedium:
  - Slike lagringsmedier kan være i ofrenes og de mistenktes besittelse under beslag.
  - Beslaglagte enheter kan ha tilgang til datalager i «skytjenester», og disse dataene kan nås ved å bruke tilgangsdata hentet fra beslag.
- Data lagret hos tredjeparter. De samme dataene kan skaffes gjennom tilrettelegging hos tilbyder av skytjenester og andre tjenesteleverandører dersom lovverket gir mulighet for det.

Alle undersøkelser av digitale spor bør utføres på «speilkopier», det vil si kopier av dataene. Frem til

digitale data blir sikret, vil de være flyktige og kunne endres kontinuerlig. Det er viktig å sikre de digitale sporene mot manipulasjon etter bevissikringen for å unngå å trekke feil konklusjoner basert på uønsket fjerning, tillegg eller modifikasjon av opprinnelige spor.

Samtidig tillater speilkopiering at flere kan undersøke sporene parallelt; både politiet, sakkyndige og andre. Det er viktig å forstå at digital sporsikring ikke krever beslag av digitale enheter og løse lagringsmedier, men ofte bare sikring av spor til etterforskningen. Det kan i dag ta lang tid fra digitale enheter blir samlet inn, til bevissikringen finner sted. Det er også store tekniske utfordringer knyttet til utkopiering av data.

Digitale spor vil kunne forekomme i flere kilder samtidig, med ulik varighet og tilgjengelighet og ulikt format. Det er beskyttelsesinnretninger i form av tilgangskontroll og kryptering samt jurisdiksjon, kompetanse, sikringsutstyr og kapasitet som avgjør om politiet kan sikre, undersøke og utnytte de digitale sporene.

Bearbeiding og analyse. Etter bevissikringen utfører politiet tidslinjeanalyse, innholdsanalyse, kommunikasjonsanalyse, datasøk, posisjonsanalyse, analyse av brukeraktivitet m.m.

Kildene til digitale spor endres med teknologiutviklingen og -bruken. Politiets metoder for bevissikring og analyse må kontinuerlig ivaretas og utvikles. Det trengs en standardisering av utprøvde og aksepterte metoder, metodeutvikling og utprøving av nye metoder, samt kompetansemiljøer som kan ivareta disse oppgavene.

Data som bevis. Etterforskningen av datakriminalitet innebærer at det må innhentes digitale bevis – ofte i stort omfang – med data som er vanskelig å tolke, fordi de er lite søkbare og dermed fører til en tidkrevende, manuell gjennomgang.

I saker der informasjonsteknologien er selve målet for handlingen, vil det ofte være avgjørende å få kunnskap om sanntidshendelsen og kunne observere hva som skjer. Det som ligger igjen av spor i etterkant, gir mindre informasjon om hendelsen, da denne informasjonen ofte er manipulert, slettet eller anonymisert. Det kreves en raskere og mer presis reaksjon for å hindre fortsatt kriminalitet og sikre spor fra hendelser for videre tiltak fra politiet og sikkerhetsmyndighetene. Tidsfaktoren – særlig tilgang på nødvendig kompetanse – er mer kritisk enn i mange andre typer saker.

Det kan være teknisk krevende å sikre, forklare, forstå og anvende digitale spor som bevis i en straffesak. Det kreves ofte teknologisk kompetanse i flere ledd av straffesakskjeden. Det gjelder stort sett alle typer datakriminalitet og blir etter hvert også aktuelt for annen type kriminalitet som etterlater elektroniske spor. Politiet må sørge for at digitale bevis innhentes og presenteres på en mest mulig uangripelig måte. Man må også ha personell med god teknologisk og politifaglig kompetanse til å utføre arbeidet og til å bistå påtalemyndigheten når saken skal behandles i retten.

10.4.2. Aktuelle tvangsmidler

I likhet med etterforskning av annen kriminalitet må etterforskning av datakriminalitet kunne benytte alle tilgjengelige metoder, og disse må utvikles for å holde tritt med de kriminelles bruk av moderne teknologi. Relevante bevis befinner seg oftest i lukkede datasystemer. For å få tilgang her er det ofte behov for tvangsmidler som krever lovhjemmel. Alternative, ikke digitale bevis, eksisterer oftest ikke, eller kan ikke innhentes.

Datakriminaliteten endrer stadig form og gir nye muligheter for å tilegne seg og utveksle informasjon knyttet til kriminell virksomhet. Kriminelle benytter stadig oftere teknologiske løsninger som begrenser nytten av politiets tradisjonelle metoder, slik tilfellet er med kryptering av kommunikasjon og dermed begrenset nytteverdi av kommunikasjonskontroll. Strategigruppen mener det er behov for en stadig utvikling og utnyttelse av nye metoder ved å justere eller tydeliggjøre eksisterende regelverk.

Metodene som er tilgjengelige i dag, må brukes mer aktivt. Den rene datakriminaliteten vil imidlertid normalt ha for lave strafferammer til at skjulte metoder kan anvendes. I det følgende gjennomgår strategigruppen aktuelle tvangsmidler for etterforskning av datakriminalitet og vurderer om adgangen til å bruke dem er tilstrekkelig ut fra dagens trusselbilde.

Kommunikasjonskontroll (KK). Kommunikasjonskontroll innebærer avlytting av signalene som kommuniseres mellom enhetene man ønsker å overvåke. Telefonavlytting er et klassisk eksempel.

Tradisjonelle tjenester som telefoni (PSTN, ISDN, mobil) og tekstmeldinger (SMS, MMS) leveres av teleleverandøren, som også administrerer kryptografiløsningene som sikrer innholdet. Leverandøren kan derfor på anmodning gi myndighetene tilgang til innholdet som blir sendt til og fra en abonnent. Det samme er tilfelle for datatrafikk som lenge har vært uten noen form for kryptering. Ofte vil trådløse tilgangspunkter være beskyttet med kryptering i siste transportetappe ut til sluttbrukeren, men det hindrer ikke tilgang til kommunikasjonskontroll inne i kjernenettverket. To ting har endret seg vesentlig de senere årene: økt konfidensialitetssikring av kommunikasjon (kryptering) og bruk av kommunikasjonstjenester som ikke er levert av nettverksleverandøren. Dette i kombinasjon gjør det vanskelig for myndighetene å nyttiggjøre seg kommunikasjonskontroll som metode.

Bruk av sikre nettsider (HTTPS via TLS) basert på sertifikater (PKI) begrenser muligheten til å forstå innholdet for tredjeparter, inkludert Internett-leverandører. Den nye versjonen av IP-protokollen (IPv6) vil i større grad tilrettelegge for ende-til-ende kryptering av datatrafikk for andre tjenester enn websurfing, og vil redusere nytteverdien av ren kommunikasjonskontroll ytterligere.

Selv om innholdet er uleselig, vil det være metadata ved kommunikasjonen som av tekniske grunner ikke alltid kan skjules, slik som posisjoneringsdata, nettverksidentifikasjon, tidspunkter og volum på trafikkdata.

Mobilregulerte soner. Den trådløse kommunikasjonen i mobilnettverkene våre har gjennomgått en gradvis utvikling der økt sikkerhet og hastighet på datatrafikk har vært dominerende, samtidig som gamle standarder brukes som reserveløsninger for å kunne støtte eldre utstyr. 'Mobilregulerte soner' er et begrep som benyttes om myndighetenes metoder for å kontrollere og avlytte slike mobilnettverk fremfor å be tjenesteleverandør om støtte. Man ønsker med dette å oppnå følgende:

- Å få en oversikt over hvem som er i området, for eksempel i en drapssak hvor man må kartlegge mulige gjerningspersoner eller potensielle vitner.
- Å midlertidig hindre bruk av nettverkene. Ved en bombetrussel ønsker man for eksempel å redusere mulighetene for fjerndetonasjon ved å bruke en form for signalblokkering for å oppnå dette.
- Å avlytte kommunikasjonen i en etterforskning. Det er flere metoder tilgjengelig, og de går normalt ut på å tvinge den kommuniserende ned på eldre teknologiske standarder med kjente sårbarheter. Et eksempel er GSM-nettverkets manglende autentisering av basestasjonen, som igjen gjør at samtaler kan tvinges over på falske basestasjoner før de sendes videre.

Stille SMS. Begrepet 'stille SMS'[98] innebærer sending av en mindre kjent SMS-type, som når den er sendt til en telefon, ikke gir noen indikasjon på mottak, samtidig som mobiltelefonens radiodel svarer tilbake med bekreftelse på mottatt melding og identiteten til de nærmeste basestasjonene. Alle mobiltelefoner i mobilnettverket kommuniserer og holder oversikt over de nærmeste basestasjonene. Teleoperatøren kan estimere lokasjon basert på triangulering ut fra kjennskap til de tre sterkeste (nærmeste) basestasjonene. Under normal bruk vil ikke denne informasjonen være oppdatert til enhver tid. Stille SMS sørger for at mobiltelefonen oppdaterer sin status hos basestasjonene, slik at en mer nøyaktig posisjon kan fastslås. Nøyaktigheten vil avhenge av hvor tett basestasjonene er plassert i området telefonen befinner seg. Stille SMS har vært en god metode for politiet, men etter en vurdering fra myndighetene og teletilbyderne er den imidlertid blitt satt ut av funksjon.

Dataavlesing. Dataavlesing (DA) er en aktuell metode for politiet ettersom innholdsinformasjonen i kommunikasjonen mellom datamaskiner i økende grad blir kryptert. Bruk av alternative tjenesteleverandører som Facebook Chat, Skype og lignende har svekket politiets evne til å oppnå tilsvarende samarbeid fordi tjenesteleverandøren holder til i utlandet, ikke ønsker å samarbeide eller fordi teknologien er tilrettelagt på en slik måte at leverandøren ikke har mulighet til å

98 http://www.up.ac.za/media/shared/Legacy/sitefiles/file/44/1026/2163/8121/innovate7/onforensicsasilentsmsattack.pdf.

Kommunikasjonskontroll er metoder rettet mot kommunikasjon mellom kommunikasjonsenheter. Dataavlesing innebærer å koble seg inn på kommunikasjonsenhetene.

åpne en «bakdør»[99]. Økt bruk av kryptering hindrer tilgang til innholdet i transitt mellom enhetene, men på visse deler av kommunikasjonen må den gå over fra å være menneskelesbar til å bli kryptert og motsatt. Tilgang til den interne kommunikasjonen i en enhet vil kunne avdekke det opprinnelige budskapet.

I disse situasjonene oppstår det et ønske om å plassere en overvåkningsfunksjon på innsiden av brukerutstyret, for eksempel ved å pålegge produsentene å bygge inn en bakdør, det vil si en fysisk modifikasjon av utstyret, eller ved at man bryter seg inn over nettverket.

Siden disse metodene også benyttes av kriminelle, jobber sikkerhetsbransjen for å bøte på sårbarhetene. Departementet utreder for tiden spørsmålet om hvorvidt politiet skal gis adgang til å bruke dataavlesing som metode.

Ofte er både gjerningspersonenes identitet og lokasjon ukjent. Manglende hjemmel for dataavlesning og kravet til strafferamme ved bruk av kommunikasjonskontroll kan i dag begrense politiets muligheter til å avdekke produsenter og distributører av overgrepsmateriale av barn ved bruk av Internett. Et annet eksempel er identifisering av bakmenn knyttet til botnett.

Strafferammekravet. Kriminalitetsutviklingen skaper behov for en løpende vurdering av hvorvidt det bør åpnes for økt adgang til skjult metodebruk ved flere former for datakriminalitet. Det gjelder særlig datainnbrudd, dataskadeverk og tjenestenektangrep.

En mulighet er å senke strafferammekravet for datalovbrudd generelt eller å angi spesifikt at aktuell metode kan benyttes til bestemte straffebud. Av personvernhensyn er mest mulig spesifiserte hjemler å foretrekke. Strategigruppen er som nevnt av den oppfatning at strafferammene for datakriminalitet i dag er for lave, se kapittel 8. Som departementet har gitt uttrykk for i andre sammenhenger, kan behovet for metodebruk vanskelig begrunne høyere strafferammer alene. Men en økning av strafferammene ut fra kriminaliseringshensyn, som foreslått i kapittel 8, kan innebære at man også utvider adgangen til å bruke tvangsmidler.

For å etterforske organisert datakriminalitet, jf. straffeloven § 60a, vil enkelte skjulte etterforskningsmetoder likevel kunne benyttes. Kripos har for eksempel foretatt kommunikasjonskontroll i nettbankbedragerisaker, noe som var av vesentlig betydning for oppklaringen.

PST har særlig behov for å gjennomføre kommunikasjonskontroll i tilfeller der trusselaktørene benytter kryptert kommunikasjon. Dette er bakgrunnen for forslaget om å kunne benytte dataavlesing. PST har også behov for å bruke mobilregulerte soner, både i etterforskning og forebygging. PST mener at dette bør reguleres etter samme regler som KK, det vil si med en rettslig kjennelse og etterfølgende kontroll av EOS.

Konklusjon. Politiets arbeid med utvikling av arbeids- og etterforskningsmetoder på Internett, som tydeliggjøring av rettslige rammer, må prioriteres. Flere arenaer som benyttes til distribusjon av overgrepsmateriale av barn, bruker deling av slikt materiale som inngangsbillett for tilgang til et område. En metode kan være at politiet som ledd i skjult tilstedeværelse gis anledning til å benytte ulovlig materiale som et virkemiddel til undercover[100]

99 En ubeskyttet og ukjent vei inn i et datasystem. Den kan være plassert inn av hackere eller av programvareprodusenten.

100 'Undercover' (UC) innebærer at politiet opptrer uten å synliggjøre seg som politi.

infiltrasjon og provokasjon på Internett. Her er det imidlertid behov for en rettslig avklaring.

Politiets metodetilgang og muligheter for å benytte metadata, dataavlesning, mobilregulerte soner og såkalt stille SMS-kommunikasjon må utredes nærmere. Dette gjelder særlig svært alvorlig organisert kriminalitet eller alvorlige samfunnshendelser. For PST er dette relevant for forebygging og etterforskning av terror og angrep mot nasjonal, kritisk infrastruktur. PSTs oppgaver tilsier også at de må få anledning til å benytte inngripende etterforskningsmetoder også i det forebyggende arbeidet.

Det dynamiske kriminalitetsbildet innebærer at det jevnlig bør vurderes hvilke metoder som skal anvendes. Oppgaven kan legges til det organet som har det praktiske ansvaret for den løpende oppdateringen av straffelovgivningen mot datakriminalitet. Organet bør også ha ansvar for at metodebruken vurderes ut fra personvernhensyn og nytteverdi, se tiltak 7.11 om utredning av personvernkonsekvenser.

10.4.3. Internett-kriminalitet

Etterforskning og etterretning på Internett krever spesialkompetanse, teknologisk utstyr og spesielt utviklede dataverktøy og metoder. Politiet må skaffe seg erfaring, nødvendige metoder og verktøy for å kunne utføre politiarbeidet på nettet profesjonelt og effektivt. Noe av det karakteristiske ved Internett-kriminaliteten er at den ofte ikke kan knytte gjerningsperson eller offer til et politidistrikt. Videre er bevisene lagret i flere politidistrikter og hos utenlandske tjenestetilbydere.

Av etterforskningshensyn bør politiet ha både en åpen og en skjult tilstedeværelse på Internett, som foreslått under punkt 7.2.2. I etterforskningssammenheng er både kommunikasjonskontroll og dataavlesing eksempler på digitale, skjulte metoder. Politiet må være i stand til å sikre informasjon fra Internett fra e-postmeldinger, chat, sosiale medier, surfehistorikk med mer i alle typer straffesaker og til å gjennomføre sporinger, det vil si identifisere kriminelle som skjuler seg bak IP-adresser, e-postsendinger, chatting, brukernavn, nettsider, bilder, publiseringer eller ytringer på Internett som politiet eller nasjonale og internasjonale samarbeidspartnere retter sin etterforskning mot.

Politiet må ha kapasitet til å analysere, bearbeide og presentere sikret/innhentet informasjon fra Internett på en god måte.

Ansvaret for utviklingen av etterforskningsmetoder bør forankres hos datakrimsenteret, som foreslått i punkt 10.5.2, og de bør gjøres tilgjengelig og anvendes etter behov. Dette betyr at datakrimsenteret også må ha kapasitet til bistand og opplæring i bruk av metodene.

Konklusjon. Politiet bør utvikle kapasitet for synlig og skjult tilstedeværelse på Internett. I tilknytning til den synlige tilstedeværelsen må det legges til rette for at publikum kan gi tips til politiet, se punkt 7.2.1. Evnen til å sikre digitale spor må også styrkes i den forbindelse.

10.4.4. Elektroniske spor som bevis i datakrimsaker og annen kriminalitet

Strategigruppens mandat er begrenset til datakriminalitet. Vår drøftelse av digitale bevis har derfor primært denne kriminalitetsformen for øye. Men den teknologiske utviklingen har medført at det kan være elementer av databruk – som nettbasert kommunikasjon – og dermed forekomster av elektroniske spor i de fleste typer straffbare handlinger. Kriminalitet som involverer data eller databruk i en eller annen form, har blitt dagligdags kriminalitet; snart er all kriminalitet datakriminalitet.

Digitale spor finnes derfor stort sett i alle typer alvorlige straffesaker. Sikring og analyse av elektroniske spor har blitt en viktig kriminalteknisk metode for all kriminalitet. Det kan derfor være hensiktsmessig med en felles utvikling av en rekke teknologiske og politifaglige metoder med mønsterpraksis, uavhengig av kriminalitetsform.

Både sentralt og lokalt må man derfor ha personell med nødvendig teknisk kompetanse og utstyr til å foreta sikring og analyse av elektroniske spor. Kripos har høy kompetanse på området, men har behov for å bygge ytterligere teknologisk kompetanse på behandling av elektroniske spor i forbindelse med Internett-etterforskning.

Det er likevel noen elementer som gjør straffeforfølgning av datakriminalitet krevende, og som gir bevishåndteringen i denne kriminalitetstypen et

særpreg. Ny teknologi og nye arenaer benyttes raskt til ulovlige formål og skaper utfordringer for informasjonsinnhenting og bevissikring (dataangrep, strømming av ulovlig innhold etc.). Dette krever oppdatert datateknisk og politifaglig kunnskap og kontinuerlig metodeutvikling.

Datalagringstid for IP-adresser. Det er store utfordringer knyttet til lagringstid for IP-adresselogger. Spørsmålet om lagringstid er behandlet i punkt 7.5.3. Innen etterforskning er lagringstiden en vesentlig faktor fordi datakriminalitet ofte oppdages lenge etter at handlingen ble begått. Med dagens lagringstid på maksimalt 21 døgn vil selv de viktigste sporene ofte være slettet. Avdekking av riktig IP-adresse kan være en lang prosess som krever flere etterfølgende undersøkelser. Vi kan nevne at Seksjon for seksuallovbrudd ved Kripos årlig mottar ca. 100 saker der gjerningspersonen(e) ikke kan identifiseres fordi IP-adressen er for gammel til at man kan sende Internett-leverandøren en anmodning om abonnementsdata.

Konsekvensene for personvernet øker jo lengre lagringstiden er. Et sentralt datalager med begrenset tilgang, hvor dataene innleveres etter at ordinær tillatt lagringstid er utløpt, vil kunne bøte på dette. Her vil dataene kunne oppbevares til 2-årsfristen for etterforskningsbruk utløper, for så å slettes. Kun politiet bør ha adgang til dataene. Lageret bør, i likhet med for eksempel Riksarkivet, være uavhengig og nøytralt hva gjelder andre interesser – som eierne av dataene, objektene i dataene, ofrene, politiet eller offentligheten. Adgangen til å innlevere og få tilgang til ulike typer data bør være nøye regulert med henblikk på formål, analyseformer, tilbakelevering og sletting. Se også punkt 7.6 om rettssikkerhet og personvern.

Konklusjon. Også av etterforskningshensyn er det behov for en betydelig forlengelse av lagringstiden for kobling mellom IP-adresser og eier. En lagringstid på inntil 2 år bør innføres. Eventuelt kan dataene leveres til et sentralt og nøytralt datalager etter utløpet av ordinær lagringstid, med tilgang kun for politiet som ledd i etterforskningen av straffesaker. Ytterligere begrensninger – i form av strafferammekrav – kan også vurderes.

10.5. Organisering og samarbeid

10.5.1. Sentral eller lokal modell?

Et viktig spørsmål er om datakriminalitet skal forfølges sentralt, lokalt eller i en kombinasjon. Organiseringen av politiet er i støpeskjeen. Politidistriktenes rolle er i fokus. Politianalysen innebærer et forslag om en ny organisering med en reduksjon av antall politidistrikter fra dagens 27 til 12. Håndteringen av datakriminalitet er knapt omtalt i analysen.

Forslagene er omstridte, og strategigruppen vil ikke gi seg ut på å spå utfallet eller utarbeide tilpassede modeller til de foreslåtte alternativene. Men graden av desentralisering er et relevant spørsmål i en effektiv bekjempelse av datakriminalitet. Strategigruppen vil derfor peke på noen hensyn som den mener er viktige:

- Dagens modell med 27 politidistrikter med desentraliserte fagmiljøer fungerer dårlig for datakriminalitet. Den skjulte datakriminaliteten er stor, og anmeldelsesprosenten, oppklaringsprosenten og sanksjonsprosenten lav. Det er bare Oslo politidistrikt som har et kompetansenivå som vil kunne svare på noen av utfordringene i dag.
- Datakriminaliteten er internasjonal og grenseløs. Den opererer i stor grad på tvers av geografiske grenser, og gjerningspersonene befinner seg sjelden i geografisk nærhet til offeret. Datautstyret som er brukt, er ofte lokalisert på et tredje sted, og viktige bevis på et fjerde. En desentralisert modell forutsetter derfor svært ofte et samarbeid over både distriktsgrenser og landegrenser. Behovet for koordinering er stort sammenlignet med en sentralisert modell.
- Mer enn for andre typer kriminalitet har datakriminaliteten preg av massekriminalitet. Samme handling rammer ofte ofre med forskjellig geografisk lokalisering, hvor en oversikt over det samlede kriminalitetsbildet og en samordning er vesentlig for en effektiv etterforskning.
- Norge er et lite land i internasjonal målestokk. Ingen andre ledende nasjoner har en tilnærmelsesvis så sterk desentralisering som Norge. FBIs datakrimdistrikter i USA har gjennomgående en

størrelse som langt overstiger hele befolkningen i Norge.
- Det blir stadig viktigere for politiet å samarbeide med øvrige sikkerhetsaktører og næringslivet, og det er ikke minst et stort behov for et effektivt internasjonalt samarbeid. Mye av dette må tilrettelegges og følges opp sentralt.

Argumentene for fortsatt å legge det geografiske prinsippet til grunn og å gi lokalt nivå ansvaret for førstehåndshåndteringen av datakriminalitet er at dette er et gjennomgående prinsipp for hele politiorganiseringen i Norge. Også dagens ordning innebærer muligheter for å søke bistand sentralt i vanskelige saker og ved behov la sentralt nivå overta saken. Denne ordningen har fungert bra i enkeltsaker, men det er også eksempler på det motsatte, hvor kapasiteten er for liten på sentralt nivå, og lokalt nivå mangler både kapasitet og kompetanse til å håndtere saken selv. Det er også grunn til å anta at lokalt nivå ikke er i stand til å vurdere bistandsbehovet tilfredsstillende.

Etter strategigruppens syn er en av hovedgrunnene til at dagens straffeforfølgning av datakriminalitet fremstår med vesentlige svakheter, at for mye har vært overlatt til lokalt nivå. De beste resultatene – spesielt når det gjelder den alvorlige datakriminaliteten – er oppnådd der straffeforfølgningen har vært ledet sentralt.

Selv om Riksadvokaten i prioriteringsrundskriv har sagt at alvorlig datakriminalitet skal prioriteres, er prioriteringen i praksis uklar og varierer betydelig mellom distriktene. NCA[101] i Storbritannia har utarbeidet følgende prioriteringer:

1. Offeret skal oppleve håndteringen av datakriminalitet som god.
2. Alle statsborgere og andre som bruker landets infrastruktur til datakriminalitet, skal straffeforfølges når de oppdages.
3. Internasjonalt samarbeid og etterforskning av store saker sammen med andre nasjoner vektlegges.
4. Næringskjeden brytes opp ved å prioritere markedsplassene der kriminelle kjøper og selger kriminelle tjenester.

Det er viktig at organisasjonsmodellen er fleksibel og kan endres i takt med trusselbildet.

Strategigruppens analyser viser at det er behov for en betydelig utvikling av bekjempelsen av datakriminalitet. De kommende fem til ti årene bør organiseringen tilpasses dette behovet. Skal Norge være blant foregangslandene, må hovedprioriteringen være å sikre at de ledende etterforskningsmiljøene utvikler og vedlikeholder en internasjonal toppkompetanse som gjør dem i stand til å håndtere alle former for alvorlig datakriminalitet minst like bra som andre land. Dette er avgjørende for at Norge kommer med i den internasjonale utviklingsprosessen og får ta del i etterforskningsmessige nyvinninger i andre land. Denne toppkompetansen må brukes til å utvikle den beste organisasjonsmodellen for landet som helhet – noe som innebærer en passende funksjonsdeling mellom sentralt og lokalt nivå.

Konklusjon. Bekjempelse av datakriminalitet stiller andre krav til innsats og organisering enn den øvrige kriminaliteten. Det er behov for mer presise og ensartede prioriteringer for etterforskning: Det sentrale nivået bør få større ansvar for metodeutvikling og koordinering enn for annen kriminalitet, se forslaget om et nasjonalt datakrimsenter i neste punkt. Det nasjonale datakrimsenteret må også utvikle og vedlikeholde en høy kompetanse slik at man kan håndtere alle former for alvorlig datakriminalitet.

10.5.2. Nasjonalt datakrimsenter

Høy kompetanse og en kontinuerlig utvikling av politiets metoder og metodebruk er en forutsetning for at politiet skal kunne svare på utfordringene som datakriminalitet representerer i dag og i fremtiden. Dette antas best ivaretatt med en sentral enhet med nasjonalt ansvar for vedlikehold og utvikling av metodene. Når det gjelder straffeforfølgning, bør enheten både etterforske egne saker og bistå andre enheter sentralt og lokalt, primært gjennom fag- og metodeansvar, se en nærmere redegjørelse under.

101 National Crime Agency (NCA) i Storbritannia med National Cyber Crime Unit (NCCU) står i spissen for bekjempelsen av den mest alvorlige datakriminaliteten. http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit.

Det må legges til rette for at senteret skal gi bistand til politidistriktene i konkrete saker. Slik bistand bør omfatte både teknologisk og politi- og påtalefaglig kompetanse.

Det nasjonale senteret skal håndtere den mest alvorlige og komplekse datakriminaliteten, saker som innebærer et stort behov for internasjonalt samarbeid, og saker som reiser nye problemstillinger. Senteret bør også ha evne og kapasitet til å etterforske og avslutte saker innen rimelig tid.

Senteret bør ha en sentral rolle i forvaltningen av fagansvar, kunne si noe om hvordan digitale spor bør håndteres i årene fremover, og være det ledende nasjonale fagmiljøet for sikring og analyse av digitale spor. Senteret bør også yte bistand til datatekniske undersøkelser og digitale spor på lokalt nivå i tillegg til metodeutvikling.

Lokalt nivå må rustes opp til å kunne håndtere øvrig datakriminalitet, samt mer ordinær sikring og undersøkelse av databeslag og elektroniske spor. Siden datakriminaliteten er dynamisk, bør samarbeidsmodellen stadig utvikles og med passende mellomrom revurderes.

Oppgaver for et nasjonalt datakrimsenter:

- være et *spisset kompetansemiljø* med *fagansvar* for bekjempelse av datakriminalitet ved å fastsette *mønsterpraksis, fellesløsninger* og drive *teknologisk metodeutvikling*
- *være en aktiv deltaker i kunnskapsutviklingen* i samarbeid med PHS og forsknings- og utdanningssektoren
- være *faglig ansvarlig* for håndteringen av digitale spor, samt sørge for at verktøyene for håndtering av slike spor er oppdaterte i henhold til den teknologiske utviklingen, og løpende vurdere om etterforskningsmetodene er tilstrekkelige, hensiktsmessige og holder tritt med de kriminelles bruk av moderne teknologi
- *etterforske* den mest alvorlige og komplekse datakriminaliteten; saker som innebærer internasjonalt samarbeid og nye teknologiske eller juridiske utfordringer
- *bistå* andre enheter sentralt og lokalt
- fungere som et *24/7-mottakssenter* for etterforskningsforespørsler til og fra andre land (utlevering og forespørsler)
- ha ansvar for en *felles tips- og innrapporteringsportal* for datakriminalitet (også med et forebyggende formål)

Konklusjon. Det bør opprettes et nasjonalt datakrimsenter som skal etterforske egne saker og bistå andre enheter sentralt og lokalt, primært gjennom fag- og metodeansvar. Det bør også vurderes om senteret skal gi lokalt nivå bistand i konkrete saker, også på kort varsel ('riksjour'). Bistanden kan være både politi- og påtalefaglig.

Det nasjonale senteret skal håndtere den mest alvorlige og komplekse datakriminaliteten, saker som innebærer et stort behov for internasjonalt samarbeid, og saker som reiser nye problemstillinger. Senteret bør også ha evne til å etterforske og avslutte saker innen rimelig tid. En opprettelse kan ses i sammenheng med Kripos' pågående arbeid med å utvikle etterforskningsmetoder til bruk på Internett.

10.5.3. Politiets datalager

Sentralt datalager og tjenestearkitektur. Verktøyene for håndtering av digitale spor må oppdateres i henhold til den teknologiske utviklingen og bruken av ny teknologi i samfunnet. Et sentralt datalager og en felles tjenestearkitektur[102] vil sikre fortløpende oppdateringer og metodeutvikling innen nye digitale sportyper og analysefunksjoner. Metodene kan implementeres fortløpende og umiddelbart bli tilgjengelige for lokalt nivå og særorganer samtidig.

Dette vil også gjøre det mulig å automatisere og standardisere innledende, manuelle og repetitive dataoppgaver på sikrede bevis, som i dag utføres manuelt av dataetterforskere i distriktene. Eksempler på dette kan være å fjerne duplikatdata, pakke ut komprimerte data, gjenopprette slettede data, sammenstille aktivitetshistorikk, passord, e-post og annen kommunikasjon, utføre skadevare-isolering og ikke minst gjøre alt raskt søkbart.

Resultatene av denne klargjøringen kan deretter tilrettelegges for analyse uavhengig av lokasjon. Etterforskere får muligheten til å jobbe sammen på samme

102 Tjenestearkitektur innebærer at noen andre enn dem som bruker tjenesten, leverer eller drifter den.

data og sammen på samlingen av bevissikrede data i sakene, uavhengig av organisasjon og geografi. Et sentralt datalager og tjenestearkitektur vil gi mulighet for å forene de ulike verktøyene og grensesnittene for behandling av digitale spor. Dette bidrar også til å samkjøre og effektivisere driften.

Overgrepsmateriale av barn. Det bør utredes en felles nasjonal løsning for håndtering og gjennomgang av overgrepsmateriale av barn i politidistriktene ved bruk av Internett. I dag behandles også denne typen beslag uavhengig av hverandre og på tvers av politidistriktene, med lite felles struktur for analyse av innhold og ofte mangelfulle lokale rutiner for beslagshåndtering. En sentral bilde- og videodatabase vil forhindre dobbeltarbeid, bedre forutsetningene for å analysere informasjon på tvers av saker, og dermed øke muligheten for identifisering av ofre og gjerningspersoner.

Det bør være et profesjonelt IKT-driftsmiljø som har ansvaret for infrastruktur, datalager, informasjonssikkerhet, tilgangskontroll, back-up mv.

Det finnes i dag programvare og systemer som kan forenkle håndteringen av overgrepsmateriale, øke kvaliteten på etterforskningen og hindre at den samme jobben gjøres flere ganger. I dag tilbyr Kripos et såkalt omvendt bistandskonsept ved at politidistriktene kan komme til Kripos for å gjennomgå sitt beslag med effektive verktøy og i et miljø som er tilpasset et slikt arbeid.

Vi ser at konseptet ikke fungerer tilfredsstillende, og at det er et stort behov for å finne en løsning hvor distriktene og et fremtidig nasjonalt datakrimsenter kobles sammen slik at gjennomgang av bilder og film kan foregå lokalt etter en felles standard og med like verktøy.

10.5.4. Samarbeid

Internt politisamarbeid. Politiets evne til å se anmeldelser av datakriminalitet i sammenheng og til å kanalisere anmeldelser knyttet til samme fenomen eller aktør til rette etterforskningsenhet, må bedres. Dette gjelder internt på lokalt nivå og på tvers av aktuelle geografiske inndelinger. Det gjelder også mellom lokalt og sentralt nivå og mellom særorganene.

Dette fordrer bedre kommunikasjonsflyt enn i dag, og en større evne og vilje til å iverksette sentralisert etterforskning der dette vil gi bedre resultater.

Andre sikkerhetsaktører. Et godt og tett samarbeid mellom politiet og øvrige sikkerhetsaktører er viktig for en velfungerende straffeforfølgning og muligheten for å oppklare de alvorligste tilfellene av datakriminalitet.

Sikkerhetsaktørene bør være enige i hvordan bevis skal sikres, for at de mest hensiktsmessig kan overtas og håndteres videre av politiet. Dette gjelder spesielt frysing av data, sikring av logger og eventuelle skadevareprogrammer. Det nasjonale datakrimsenteret (eventuelt Riksadvokaten i samarbeid med POD) bør utarbeide en mønsterpraksis, med tanke på NSM NorCERT og øvrige CERT-ers bevissikring i perioden før politiet eventuelt mottar beskjed om en hendelse.

Virksomheter. Justis- og beredskapsdepartementet har ved flere anledninger pekt på at det er verdifullt for politiet å samarbeide med næringslivet for å kunne avdekke og etterforske lovbrudd på en effektiv måte.[103] Dette er enda viktigere innen datakriminalitet enn i den fysiske verden. Erfaringer fra Kripos – og særlig fra utlandet, blant annet Storbritannia og USA – viser at de mest avanserte og komplekse formene for datakriminalitet sjelden vil kunne avdekkes av politiet, og at en vellykket etterforskning av disse sakene også vil være avhengig av private og offentlige aktørers bistand. Samarbeid kan være aktuelt både med enkeltvirksomheter og deres organisasjoner, som NSR.

Andre organisasjoner. Det finnes også flere organisasjoner som ivaretar interessene til enkeltpersoner som det kan være verdt å samarbeide med om bekjempelse av datakriminalitet, se kapittel 7 og 9. Et nasjonalt datakrimsenter bør ivareta slike oppgaver sentralt, mens lokalt nivå bør vurdere muligheten for et samarbeid med aktuelle informasjonskilder lokalt.

Samarbeidsforum. Et tiltak som vil være av stor betydning for politiet og påtalemyndighetens straffeforfølgningsevne, er et åpent samarbeidsforum

103 Jf. *Prop. 1 S (2013–2014)*, s. 103.

koordinert med eksisterende fora. Her vil flere parter – politiet, sikkerhetsaktører, private virksomheter, akademia – kunne jobbe spesifikt med utfordringer som ikke faller inn under NSM NorCERT sitt hovedområde (dataangrep og datainnbrudd/spionasje), slik som bekjempelse av botnett og vinningskriminalitet. En modell for dette er drøftet under punkt 7.4.1 og 7.4.2. Samarbeidsfora kan også opprettes lokalt.

Frykten for å anmelde. En vesentlig innvending fra virksomhetenes side mot å anmelde datakriminalitet til politiet, er frykt for at straffeforfølgning vil eksponere virksomheten på en uheldig måte og skade inntjeningen. Å fremskaffe bevis, stille til avhør og vitne i en eventuell straffesak kan være ressurskrevende og virke negativt inn på viljen til å anmelde og bidra i straffeforforfølgningen.

FBI i California garanterte derfor virksomheter som var villig til å bidra med informasjon om datakriminalitet de hadde vært utsatt for, at det ikke ville bli igangsatt straffeforfølgning uten at virksomheten var enig. Denne garantien hadde hatt en positiv effekt. Strategigruppen fikk et klart inntrykk av at FBI visste vesentlig mer om forekomsten av datakriminalitet enn det norsk politi gjorde. Strategigruppen oppfatter en slik garanti som et mulig virkemiddel for å få en bedre oversikt over datakriminaliteten både i forebyggings- og etterforskningsøyemed og har vurdert muligheten for en tilsvarende ordning i Norge.

En ordning hvor saker kan henlegges dersom en virksomhet ønsker dette som en garanti for å bidra med informasjon og bevis, vil være et effektivt tiltak både med tanke på forebygging og etterforskning. Strategigruppen oppfatter en slik garanti som et viktig virkemiddel for å få bedre oversikt over datakriminaliteten. Særlig ved et nasjonalt datakrimsenter, som bør ha tett kontakt med næringslivet, bør forutsetningene være gode for å oppnå tilstrekkelig forståelse for virksomhetenes behov.

Det er også motforestillinger mot en slik ordning: For det første er påtalereglene, som nevnt, endret i straffeloven 2005, idet ordningen med påtalebegjæring fra fornærmede ikke videreføres. En slags garantiordning vil derfor bli et markant avvik både fra de nye påtalereglene og fra hvordan annen kriminalitet håndteres påtalemessig.

For det andre kan ofre for annen kriminalitet også ha berettigede og velbegrunnede ønsker om at påtale ikke skjer. Ofre for seksualovergrep kan være et eksempel.

For det tredje er 'datakriminalitet' et vidtfavnende og upresist begrep. En garantiordning vil omfatte mange saker, med mindre ordningen avgrenses til definerte sakstyper, som datakriminalitet av 'første kategori'.

For det fjerde vil det i enkelte situasjoner være en betydelig samfunnsmessig interesse i å påtale oppklarte saker, spesielt ved grov datakriminalitet. Dette er særlig aktuelt der siktede er varetektsfengslet under etterforskningen. Henleggelse av en oppklart sak vil da utløse rett til erstatning for siktede, noe som vil fremstå underlig i en oppklart sak.

For det femte kan det være flere ofre i en datakrimsak med motstridende interesser.

Endelig vil en fornuftig praktisering av opportunitetsprinsippet trolig imøtekomme virksomhetenes ønsker i de aller fleste tilfeller, noe som for øvrig må kunne kommuniseres bedre til virksomhetene.

Ny § 62a i straffeprosessloven lyder (med vår utheving):

> *Den offentlige påtalemyndighet skal påtale straffbare handlinger når ikke annet er bestemt ved lov.*
> *For overtredelse av straffebud med en strafferamme på 2 år eller lavere kan påtale unnlates hvis ikke allmenne hensyn tilsier påtale.* ***Ved vurderingen av om allmenne hensyn foreligger, legges det blant annet vekt på*** *overtredelsens grovhet, hensynet til den alminnelig lovlydighet og* ***om den fornærmede, en annen som har lidt skade ved overtredelsen****, eller vedkommende berørte* ***myndighet ønsker påtale****.*

Nesten alle straffebestemmelsene som uttrykkelig gjelder datakriminalitet i straffeloven 2005, har i dag en strafferamme på 2 år eller mindre, se punkt 8.3.3 om straffenivå. Også i saker med strafferammer høyere enn 2 år har påtalemyndigheten, som tidligere nevnt, en betydelig mulighet til å utvise skjønn. Hensynet til offerets ønsker vil nok tillegges særlig vekt i komplekse datakrimsaker der politiet og påtalemyndigheten er mer eller mindre avhengig av offerets bistand under etterforskningen.

Selv med et godt samarbeid med virksomhetene vil alvorlige datakrimsaker være tid- og ressurskrevende for politiet, og praktiseringen av opportunitetsprinsippet smøres nok også av at det ikke er tilstrekkelige ressurser i strafferettspleien.

Et alternativ til å innføre en egen påtaleregel/henleggelsesgrunn for datakrimsaker vil være å styrke virksomhetenes tillit til politi og påtalemyndighet gjennom de øvrige tiltakene beskrevet i punkt 10.5.4, og ikke minst øke politiets og påtalemyndighetens forståelse for virksomhetenes ønsker og behov.

Et annet alternativ – en slags mellomløsning – kan være å innføre en saksbehandlingsregel, enten i straffeprosessloven eller som en retningslinje fra Riksadvokaten, der påtalemyndigheten pålegges å drøfte påtalespørsmålet med offeret før avgjørelse fattes.

Konklusjon. Når hendelsene kan være aktuelle for straffeforfølgning, må kontakten mellom fornærmede, NSM NorCERT, politiet og PST etableres raskt, og de foreslåtte retningslinjene for anmeldelser og bevissikring hos virksomhetene bør benyttes. Se punkt 9.5.2 om politiets forhold til virksomheter og interessegrupper.

Politiets samarbeid med eksterne aktører bygger i stor grad på tillit, og dette fordrer gode arenaer for samhandling, som faste, felles møter, erfaringsdeling og samarbeidsavtaler der dette er naturlig.

Fornærmedes oppfatning av hvorvidt man skal igangsette etterforskning eller ei, bør tillegges større vekt enn i dag, og det bør derfor avklares om påtalereglene bør justeres for å legge forholdene bedre til rette for at virksomheter som er ofre for datakriminalitet, skal bidra med informasjon og bevis.

10.6. Kompetanse

10.6.1. Digital tjenestemodell

Datakriminalitet knyttet til distribusjon av ulovlige innholdsdata på Internett kan illustrere behovet for spesielle typer metoder ved blant annet:

- fildelingsnettverk for kartlegging av omfang, ettersom enkelte fildelingsnettverk krever bruk av skjulte metoder som undercover (UC) på nett
- deling av ulovlig innholdsmateriale via ulike varianter av skylagringstjenester eller lukkede nettverk, fora, websider
- web-hosting av ulovlig materiale hvor betaling/tilgang foregår gjennom lovlige sider, såkalte 'gateway sites'
- betaling for ulovlig innholdsmateriale via ulike betalingstjenester som anonymiserer sender og/eller mottaker
- bruk av anonymiseringstjenester (TOR)
- bruk av kryptering både i kommunikasjonsutveksling og lagring av informasjon
- begrensning av den ekstreme tilgjengeligheten av ulovlige bilder og videoer på nett. Spørsmålet blir hvordan man teknisk kan hindre en fortsatt krenkelse av fornærmede / hvordan forebygge misbruk av bilder / videoer til bruk i seksuell utpressing

Etterforskning av enkelte nettverk er for øvrig så teknisk og ressursmessig krevende at det fordrer samarbeid på tvers av landegrenser hvor enkeltland bidrar med spesiell kompetanse og mye ressurser.

Særtrekkene ved mange av disse sakene er at gjerningspersonene tar i bruk metoder for å skjule egen identitet og ulovlig virksomhet ved å sørge for at data og logger som legges igjen, er svært vanskelige for politiet å analysere og tolke. Det vil i mange saker kreve mer spesialistkompetanse for å kunne avdekke og stanse kriminaliteten, samt identifisere aktørene som står bak, enn hva som er tilfelle for tradisjonell kriminalitet.

Bekjempelse av datakriminalitet forutsetter at politiet har tilstrekkelig kompetanse, utstyr og personell til å sikre, undersøke og utnytte digitale spor i etterforskningen. God håndtering av digitale spor er en viktig forutsetning for å ivareta siktedes rettssikkerhet. En vellykket etterforskning av datakrimsaker av et visst omfang og en viss kompleksitet fordrer et tett og løpende samarbeid mellom teknolog og dataetterforsker og etterforsker og politiadvokat.

Etterforskeren har detaljkunnskap om etterforskningsarbeidet i en sak, og vedkommende bør derfor selv gjennomgå databeslag og digitale spor. Det gir også bedre forutsetninger for raskere

etterforskningsresultater enn i dag. Raskere utnyttelse av digitale spor kan effektivisere etterforskningen. Etterforskeren bør videre gis anledning til å undersøke databeslag og til å følge de digitale sporene fra sitt eget kontor.

Dataetterforskeren er spesialist på sikring, analyse og utnyttelse av digitale spor på lokalt nivå. Ved et nasjonalt datakrimsenter vil teknologene ved avdelingen for elektroniske spor fylle den samme rollen. Dataetterforskerens rolle bør rendyrkes og frigjøres fra andre oppgaver med unntak av rollen som støttefunksjon i lokal etterforskning. Dataetterforskeren skal være god på datatekniske undersøkelser. Det er kun i datakrimsaker at dataetterforskeren bør ha en sentral etterforskningsrolle, i andre sakstyper vil vedkommende kun være en lokal rådgiver. Dataetterforskere på lokalt nivå vil være en naturlig del av en fagkontaktordning knyttet opp mot det sentrale kompetansemiljøet ved et nasjonalt datakrimsenter. Dataetterforskeren bør ikke ha ansvar for lokal infrastruktur, som sorterer under IKT-drift.

I dag benyttes dataetterforskerne i for stor grad til å gjennomgå databeslag. I et felles grensesnitt vil resultatene raskt bli klargjort og tilrettelagt for at etterforskeren selv kan utføre gjennomgangen og analysen fra et selvvalgt (kontor)sted. Etterforskere får muligheten til å jobbe på samme data og sammen på samlingen av bevissikrede data i sakene, uavhengig av organisasjon og geografi. Et sentralt datalager og tjenestearkitektur vil gi mulighet for å forene de ulike verktøyene og grensesnittene for behandling av digitale spor. Dette bidrar også til å samkjøre og effektivisere driften.

Konklusjon. Det bør utvikles en digital tjenestemodell, en standardisert og enhetlig behandling av databeslag, samt raskere tilgang på sikring og analyse og generell utnyttelse av de digitale sporene under etterforskningen. Formålet er å sikre en mest mulig ensartet og uangripelig behandling av elektroniske spor i politiet. I denne sammenheng bør det også utvikles sertifiseringsordninger med kompetansekrav for dataetterforskere og andre som skal arbeide med sikring av elektroniske spor.

10.6.2. Påtalemyndigheten må styrke evnen til å straffeforfølge datakriminalitet

Datakriminalitet kan ikke straffeforfølges effektivt uten høy kompetanse i alle ledd i straffesakskjeden. Det bør vurderes hvilke krav som bør stilles til påtalemyndigheten og domstolene.

Når det gjelder den *påtalemessige behandlingen* av datakrimsaker, er det generelt behov for å heve den grunnleggende teknologiske forståelsen, og forståelsen av hvordan sosiale medier og andre Internett-baserte tjenester fungerer. Som tidligere nevnt må det under etterforskningen være et tett samarbeid mellom politiadvokaten og etterforskeren/dataetterforskeren. Se punkt 10.6.1.

Politiadvokater tilknyttet et nasjonalt datakrimsenter må ha spesialkompetanse på området, og behovet for en statsadvokat med spesialisert kompetanse ved det statsadvokatembetet som senteret vil høre inn under, bør vurderes.

Politi- og statsadvokatenes kjennskap til straffebestemmelsene for datakriminalitet må forbedres, og kompetansen innen bruk av utradisjonelle etterforskningsmetoder og internasjonalt straffesakssamarbeid bør økes.

Også når det gjelder *den rettslige* behandlingen av datakrimsaker, har dommere og meddommere ofte begrenset kunnskap om datateknologiske spørsmål. I saker der tilegnelse av digitale bevis kan være utfordrende, kan det anmodes om at retten settes med fagkyndige meddommere. Det er også forholdsvis vanlig å oppnevne sakkyndige.

10.7. Internasjonalt etterforskningssamarbeid

Samarbeid med andre land er helt sentralt i kampen mot datakriminalitet. Det er et stort behov for å forenkle og standardisere samarbeidet med utenlandske myndigheter og tjenestetilbydere. Gjennom økt samarbeid både nasjonalt og internasjonalt kan man styrke den generelle sikkerheten og robustheten mot datakriminalitet i flere land. Gjennom et slikt samarbeid kan man oppdage og håndtere trusler og risiko på en god måte og bidra til at Norge og samarbeidende land fremstår som lite attraktive mål for datakriminalitet. Norge bør derfor være blant de

ledende landene innen forfølgelse av alvorlig internasjonal datakriminalitet.

10.7.1. Tilgang til informasjon

Internasjonale avtaler om samarbeid er svært viktig for etterforskningen av datakriminalitet. Handlinger utføres i ett land, mens virkninger inntrer i et annet, og ikke sjelden må bevisene sikres i et tredje. Det betyr at geografisk avstand ikke er noe hinder for utenlandske kriminelle som ønsker å målrette sin virksomhet mot norske ofre på nettet.

Politiet møter stadig større utfordringer i straffeforfølgningen av datakriminelle i andre land som utøver sin kriminelle virksomhet i Norge. Datakriminalitet er en internasjonal utfordring som krever koordinert internasjonalt samarbeid og utveksling av informasjon. Erfaring viser at forskjeller i nasjonal lovgivning, ulike nasjonale systemer og manglende evne til å håndheve lovene over landegrenser hindrer effektiv straffesaksbehandling.

Behov for tilgang til informasjon som er lagret i utlandet, synes å øke i omfang, særlig bruk av såkalte skytjenester hvor norske brukere lagrer informasjonen eksternt, og etterforskernes tilgang forutsetter enten samtykke eller bistand fra andre lands myndigheter. Utfordringene gjelder både datakriminalitet og elektroniske spor.

Suverenitetsprinsippet innebærer blant annet at det kun er en stats egne myndigheter som kan utøve myndighet på landets territorium, noe som i straffesaker medfører at man er tvunget til å be om bistand for sikring av databevis som er lagret i utlandet. Rent praktisk betyr dette at det må sendes en rettsanmodning til det landet man ønsker bistand fra, men dette er en tidkrevende prosess hvor tidsbruken er utenfor norsk kontroll.

Datakriminelle kan kompromittere en maskin i land A, og fra den kompromittere en maskin i land B og så videre i en lang kjede. Bevisene må i slike tilfeller nøstes opp i omvendt rekkefølge. Slik bevissikring er vanskelig nok selv med direkte tilgang til alle maskiner. En ventetid på dager eller måneder umuliggjør en slik etterforskning.

Utformingen av og innholdet i rettsanmodninger er ikke tydelig regulert i folkeretten, men fremkommer gjennom forskjellige konvensjoner og nasjonale regelverk som har regler om blant annet hvilke opplysninger rettsanmodninger skal inneholde, og hvem som i de enkelte land har kompetanse til å fremsette og besvare dem, mv.

Norge har heller ikke noen lov om rettsanmodninger eller internasjonal rettslig bistand. De relevante bestemmelsene er spredt i ulike lover og i særlig forskrift om internasjonal bistand i straffesaker.[104] Bistand og anmodninger om rettshjelp fra andre land vedrørende datakriminalitet er omfattet av de samme generelle konvensjonene som annen kriminalitet hva gjelder former for bistand, prosedyrer for oversendelse mv.

I tillegg til de mer generelle konvensjonene har Norge også ratifisert konvensjoner knyttet til bestemte kriminalitetsformer i regi av FN, samt europeiske konvensjoner som blant annet Budapestkonvensjonen. Disse konvensjonene er i begrenset grad tilpasset mulighetene datateknologien i løpet av få år har gitt for utveksling og oversendelse av etterforskningsinformasjon.

ITU er et FN-organ for informasjons- og kommunikasjonsteknologi som er fundert på prinsippet om internasjonalt samarbeid mellom regjeringer og privat sektor. ITU, myndigheter og privat sektor arbeider for konsensus på et bredt spekter av strategisaker som berører data- og telekombransjen. ITU søker å etablere internasjonale avtaler som fremmer utveksling av data og teletjenester over landegrensene. Det er utgitt en rekke publikasjoner som peker på utfordringene med datakriminalitet, datasikkerhet og manglende felles lovgivning.

Selv om et land ikke har ratifisert de aktuelle konvensjonene, er man ikke forhindret fra å be om bistand, men landet er ikke i samme grad forpliktet til å bistå, og oversendelse av rettsanmodninger er en langt mer omstendelig og tidkrevende prosess. I tillegg må Norge ofte avgi såkalte gjensidighetserklæringer om at Norge i en tilsvarende sak vil yte samme bistand. I mange tilfeller må diplomatiske kanaler også involveres. Dette er et svært tidkrevende arbeid som ofte innebærer unødig tidsbruk.

Kripos har gjennom nettsiden KO:DE samlet alt sentralt regelverk og lagt ved eksempler på hvordan man kan utforme rettsanmodninger mv. En

104 Forskrift av 14. desember 2012 nr. 1227.

internasjonal revidering vil være et omfattende og tidkrevende arbeid, men av stor betydning.

10.7.2. Effektivisering av dagens ordninger

Digitale spor og datakriminalitet kjenner ingen geografiske grenser, og dermed er godt internasjonalt samarbeid i mange saker avgjørende for en vellykket straffeforfølgning.

Bevis. Bevissikring og -innhenting må styrkes gjennom bilaterale avtaler om informasjonsutveksling med andre land og utvalgte private aktører. Erfaringsmessig er det noen land og private aktører det er særlig viktig å oppnå et tettere og mer formalisert samarbeid med. USA mottar svært mange av rettsanmodningene fra norsk politi, dette fordi mange større sosiale medier og databedrifter har sentrale deler av sin virksomhet der.

Kripos har gjennom Seksjon for elektroniske spor allerede et godt samarbeid med land som har god kompetanse innen datatekniske undersøkelser, som Nederland, Tyskland, Storbritannia, Canada og USA. Erfaringen er at jo bedre fagkompetanse man har, jo mer attraktiv blir man som samarbeidspartner.

Rettsanmodninger. Dagens ordninger med postforsendelse eller fysisk frakt av rettsanmodninger fremstår som svært utdaterte og lite hensiktsmessige i lys av dagens krav til effektiv etterforskning og rettshåndhevelse. Dette forsterkes av at man kan sitte og «samtale» med etterforskeren som skal bistå, og som kanskje har opplysningene tilgjengelig, men som ikke kan sette i gang med arbeidet før hele prosessen er gjennomført – gjerne etter noen måneder. Imens kan gjerningspersonene ha rammet nye ofre, eller den siktede kan ha tilbrakt unødvendig tid i varetekt inntil bevisene er sikret og bevisforspillelsesfaren er over.

Nasjonalt er det liten tvil om at det er et betydelig effektiviseringspotensial i å standardisere og forenkle dette arbeidet ved å etablere en mer enhetlig praksis for utforming og oversendelse av rettsanmodninger. Det er også behov for forbedringer i opplæringen i internasjonal bevisinnhenting hos påtalemyndigheten og politiet.

Det bør derfor foretas en gjennomgang av nasjonalt regelverk og rutiner for rettsanmodninger og legges til rette for bruk av digitale løsninger for behandling og oversendelse.

For datakriminalitet gjelder dette særlig rettsanmodninger til USA. Det er behov for å utrede et bilateralt samarbeid nærmere og søke å få et mer formalisert samarbeid og helst en bilateral avtale med USA, en såkalt MLAT (Mutual Legal Assistance Treaty).

Uansett bør Norge for egen del – som et foregangsland – legge til rette for en gjensidig, enkel og rask prosess for bevissikring i Norge. Dette kan stimulere til tilsvarende ordninger i andre land, som norsk etterforskning kan dra nytte av.

Deltakelse og permanent tilstedeværelse i internasjonale fora anses som svært viktig, og Norges deltakelse i Europol fremstår som stadig viktigere for norsk politi. Norge bør ha permanent representasjon ved Europols datakrimsenter (EC3). Det samme bør vurderes for Interpols datakrimsenter i Singapore. Norge må også søke å være en pådriver i Europarådets arbeid for å utvikle og håndheve Budapestkonvensjonen.

Konklusjon. Det er et økende behov for tilgang til digital informasjon lagret i utlandet, både for alminnelig datakriminalitet og elektroniske spor innen andre former for kriminalitet. For å forenkle det internasjonale samarbeidet bør Norge delta aktivt og bidra til arbeidet i alle sentrale internasjonale fora som kan påvirke prosessene og arbeide for bilaterale avtaler med strategisk viktige land, særlig USA.

10.8. Hovedstrategi for straffeforfølgning

Datakriminelles risiko for å bli oppdaget, straffeforfulgt og domfelt skal være høy. Norge bør være en pådriver i den internasjonale bekjempelsen av alvorlig datakriminalitet.

Rettsvesenets evne til å forfølge denne typen kriminalitet må styrkes vesentlig og henleggelsesfrekvensen reduseres tilsvarende slik at tilliten fra publikum og ofre blir større.

Politiet trenger et vesentlig løft for å ha kapasitet, kompetanse og evne til å fange opp og etterforske datakriminalitet. Kapasiteten og metodene må kontinuerlig tilpasses nye former for lovbrudd og endret teknologibruk i samfunnet. Politi, påtalemyndighet og

domstoler må også ha nødvendig kunnskap og erfaring for å vurdere, iretteføre og pådømme datakrimsaker.

Samarbeidet med andre sikkerhetsaktører må bedres. Spesielt må hindringer for et smidig og effektivt internasjonalt etterforskningssamarbeid fjernes.

Anbefalte tiltak:

NB: Nummereringen av de anbefalte tiltakene nedenfor angir ikke prioriteringer.

10.1 *Etablere et nasjonalt datakrimsenter som en pådriver for en felles bekjempelse av datakriminalitet.* Se punkt 10.5.2 for oppgaver som kan tillegges senteret.

10.2 *Øke kapasiteten til å etterforske datakriminalitet og digitale spor, både lokalt og sentralt.* Se punkt 10.2.2.

10.3 *Styrke PSTs evne til å etterforske digitale trusler.* Dette inkluderer også utvikling og endring av relevante lovhjemler som PST allerede har fremmet forslag om. Se punkt 10.2.3.

10.4 *Betydelig utvide lagring av informasjon om kobling mellom IP-adresser og juridisk eier.* Inntil 2 år anbefales av etterforskningshensyn. Eventuelt kan slik informasjon leveres til et sentralt og nøytralt datalager etter utløpet av ordinær lagringstid med tilgang kun for politiet som ledd i etterforskningen av straffesaker. Se punkt 10.4.4.

10.5 *Sørge for en fleksibel arbeidsdeling mellom sentralt og lokalt nivå i datakrimsaker med vekt på funksjon og kompetanse*. Også i en mer fleksibel modell må eierskap og ansvar være avklart. Organisasjonsmodellen bør kunne endres i takt med trusselbildet. Se punkt 10.5.1.

10.6 *Sørge for at ledende etterforskningsmiljøer – også det foreslåtte datakrimsenteret – utvikler og vedlikeholder en høy kompetanse som gjør dem i stand til å håndtere alle former for alvorlig datakriminalitet.* Se punkt 10.5.1.

10.7 *Utarbeide klarere, mer presise og ensartede prioriteringer for etterforskning av datakriminalitet.* Det bør utvikles en digital tjenestemodell med en standardisert og enhetlig behandling av databeslag, raskere tilgang på sikring og analyse og generell utnyttelse av de digitale sporene under etterforskningen. Oppgaven kan legges til det foreslåtte datakrimsenteret. Se punkt 10.5.1.

10.8 *Utarbeide anbefalinger og mønsterpraksis ('beste praksis') for hvordan sikkerhetsaktører og virksomheter bør sikre og håndtere bevis i datakrimsaker med sikte på overlevering til politiet for etterforskning.* Oppgaven kan legges til det foreslåtte datakrimsenteret. Se punkt 10.5.4. Kan ses i sammenheng med tiltak 9.8.

10.9 *Opprette et sentralt datalager for politiet med en sentral bilde- og videodatabase for håndtering av bilder av overgrep mot barn*. Se punkt 10.5.3.

10.10 *Sørge for at andre sikkerhetsaktører deler informasjon om datasikkerhetshendelser med politiet så raskt som mulig der det er mistanke om datakriminalitet, med de begrensningene som følger av regelverket og avtaler med informasjonseiere.* Se punkt 10.5.4. Se også tiltak 7.6.

10.11 *Bruke eksisterende adganger til å avslutte saker uten påtale eller dom mer bevisst i samråd med ofrene for å redusere motviljen mot å anmelde datakriminalitet hos virksomheter og publikum*. Se punkt 10.5.4.

10.12 *Bedre påtalemyndighetens kompetanse i datakrimsaker gjennom kanalisering av saker til utvalgte politiadvokater og statsadvokater*. Se punkt 10.6.2 (og tiltak 11.6 om videreutdanning).

10.13 *Etablere permanent tilstedeværelse i internasjonale samarbeidsorganer*. Europols datakrimsenter (EC3) og Interpols datakrimsenter i Singapore er naturlige arenaer å delta på. Norge må være en pådriver i Europarådets arbeid med utvikling og håndheving av Budapestkonvensjonen også når det gjelder etterforskningsmetoder. Se punkt 10.7.2 (se også tiltak 7.3 og 8.6).

10.14 *Foreta en gjennomgang av rutiner og prosedyrer for digital utforming og oppfølging av*

rettsanmodninger. Dette bør kombineres med digitale oversendelsesmetoder som sikrer rask og effektiv oversendelse så vel nasjonalt som til samarbeidende nasjoner og myndigheter. Se punkt 10.7.1 og 10.7.2.

10.15 *Inngå en bilateral avtale med USA, en såkalt MLAT (Mutual Legal Assistance Treaty) knyttet til datakriminalitet og sikring av elektroniske spor*. Tilsvarende avtaler med andre land må kontinuerlig vurderes. Se punkt 10.7.2.

10.16 *Legge til rette for at andre lands etterforskningsorganer enkelt og raskt kan innhente bevis i Norge i datakrimsaker*. Dette forutsetter normalt gjensidighet. Nødvendige regelendringer må gjennomføres for å tilrettelegge for dette. Se punkt 10.7.2.

Følgende tiltak i andre kapitler vil også ha klare virkninger for straffeforfølgningen:

7.12 *Opprette et sentralt tipsmottak i politiet*.
7.2 *Mer åpen og skjult tilstedeværelse av politiet på nett*.
Disse er begge relevante virkemidler for å avdekke datakriminalitet.
7.8 Et *åpent samarbeidsforum* vil også være verdifullt for utviklingen av etterforskningsmetoder.

11. STRATEGI FOR KOMPETANSEHEVING

11.1. Dagens situasjon for forskning om datakriminalitet

11.1.1. Norske forskningsinstitusjoner av betydning for bekjempelse av datakriminalitet

Blant norske kunnskapsmiljøer har vi både forskningsinstitutter, utdanningsinstitusjoner og diverse forskningsprogrammer. Strategigruppen har søkt å kartlegge forskningsinstitusjoner med relevans for datakriminalitet.

Universitetet i Oslo (UiO). Institutt for informatikk (IFI) har startet en større satsing på informasjonssikkerhet. Instituttet fokuserer på tre relevante temaer: autentisering, applikasjonsarkitektur og formell sikkerhetsmodellering. Forskningsrådet tildelte i 2014 midler til et nytt senter for forskningsdrevet innovasjon (SFI). Institutt for informatikk ved Universitetet i Oslo er vertskap for det nye senteret, Centre for Scalable Data Access (SIRIUS). Dette er et senter som skal utvikle ny teknologi for å identifisere og behandle relevant informasjon fra den store og økende mengden digitale data. Forskningen vil bygge på og utnytte teknologiske nyvinninger innenfor blant annet tungregning og skyteknologi.

Institutt for kriminologi og rettssosiologi er et forskningsmiljø som tar for seg kriminalpolitiske forskningstemaer og har et nært samarbeid med Politihøgskolen. Instituttet forsker på temaer som flyktningpolitikk, kriminalitet og avvik, overvåking og personvern, rettsstaten, rettssystemet og straff. Temaene er i mindre grad knyttet til det digitale samfunn og utfordringene som datakriminalitet utgjør.

Senter for rettsinformatikk er en del av Institutt for privatrett. Rettsinformatikk er et fagområde som ser på juridiske problemstillinger som oppstår i forbindelse med bruk av datateknologi. Forskningen deres berører temaer som personvern, informasjonssikkerhet, elektronisk handel samt medierett, og er preget av tverrfaglighet og nær tilknytning til forskningen ved fagmiljøet innen forvaltningsinformatikk.

Simulasenteret ble, som en del av utbyggingen på Fornebu, opprettet i 2001. Senteret er finansiert gjennom en statlig grunnbevilgning og er organisert som et aksjeselskap eid av Kunnskapsdepartementet. Simulasenteret utfører grunnleggende langsiktig og anvendt forskning på utvalgte områder innen informasjonsteknologi som er av spesiell interesse for samfunnet, samt utdanning og innovasjon knyttet til forskningen.

Simulasenteret fikk i 2007 bevilgning til et senter for fremragende forskning finansiert av Norges forskningsråd. I 2011 fikk de bevilgning til et senter for forskningsdrevet innovasjon (SFI). Simulasenteret har siden 2006 drevet senteret Robuste nett med bevilgning fra Samferdselsdepartementet. Forskningen fokuserer på motstandsdyktighet og sikkerhet i infrastruktur for digital kommunikasjon. Det jobbes blant annet med å kartlegge tilstanden til norske e-komnettverk. Det er plassert ut sensorer for å kontrollere nettverksstabilitet på noen kjernerutere, og det er tilsammen 200 målepunkter mot mobile tilknytningspunkter. De skal også videreutvikle den nasjonale kompetansen på kryptografi i samarbeid med universitetet i Bergen og Selmersenteret.

Universitetet i Bergen (UiB). Institutt for informatikk (IFI) har lang fartstid innen forskning på kryptografi, kodeteori og datasikkerhet og er i toppsjiktet

internasjonalt. Selmersenteret er etablert med tilknytning til Institutt for informatikk. Målet er å synliggjøre forskningsområdet for bevilgende myndigheter og bidra til oppdragsorientert forskning på området. Ved Selmersenteret drives det for tiden forskning innen sikker og robust kommunikasjon, inkludert kryptologi (design og analyse av kryptoprimitiver og kryptografiske protokoller), informasjons- og kodeteori samt design og analyse av anti-fragile systemer.

Juridisk fakultet har et stort miljø for strafferett og straffeprosess. Det pågår en satsing innen politirettssikkerhet. Ett av temaene er hvordan politiet kan bruke persondata og informasjonsflyt mellom politi og andre organer. De har ingen egen satsing mot datakriminalitet, men det er stor interesse for temaet. Av særlig interesse er jurisdiksjon på Internett og utlevering av data fra tjenesteleverandører i andre land.

Norges teknisk-naturvitenskapelige universitet (NTNU) har fokus på mobil databehandling og trådløs sikkerhet. Universitetet har hatt et doktorgradsstudium finansiert av Norges forskningsråd innen digital etterforskning, og hvert år skriver mange av studentene masteroppgaver innen informasjonssikkerhet.

Universitetet i Tromsø (UiT) utfører noe forskning innen rask tilgang til og bearbeiding av store datamengder (stordata) via skytjenesteteknologi.

Høgskolen i Gjøvik (HiG) forsker på informasjonssikkerhet. Forskningen er organisert under NISlab, som finansieres av blant annet EU FP7 og NIST[105]. NISlab har to laboratorier særlig rettet mot dataetterforskning (TestimonLab) og biometri (BiometricsLab). Særlig forskningsmiljøet innen digital etterforskning ('digital forensics') ved HiG er unik i skandinavisk sammenheng. Høgskolen leder COINS[106], et samarbeid med flere av de store norske utdanningsinstitusjonene. Prosjektet er et forsøk på å samle norske og internasjonale doktorgradsstudenter i Norge innen datatekniske- og informasjonssikkerhetsrelaterte fagområder. Det er per nå 46 aktive studenter, og 21 av dem tilhører HiG. I tillegg til forskningsarbeidene gir samarbeidet en talentpool for langsiktig rekruttering til forskerstillinger som må tas vare på. Særlig gjelder dette utlendingene, som utgjør majoriteten av doktorgradsstudentene, og som ofte forlater Norge etter endt utdanning. Høgskolen er også vertskap for CCIS (se under). Det ble i januar 2015 vedtatt at HiG (med flere) skal fusjonere med NTNU i 2016.

Center for Cyber and Information Security (CCIS) ble offisielt åpnet i august 2014. Det er et partnerskap for forskning og utdanning innen informasjonssikkerhet. Foruten HiGs eget fagmiljø NISlab deltar også Politihøgskolen, Telenor, Statkraft, Statnett, Eidsiva, PwC, NSM, Politidirektoratet, PST, Økokrim, Kripos, Nasjonalt ID-senter, Cyberforsvaret og FFI med egne professorater.

SINTEF IKT har tre grupper som fokuserer på informasjonssikkerhet:[107] forebygging, risikoanalyse og sikkerhetstesting. Noen utvalgte områder er programvaresikkerhet, nettverkssikkerhetsarkitektur, mobile nettverk og skytjenester, hendelseshåndtering og innebygd personvern. Prosjektene deres er hovedsakelig EU-finansierte.

Forsvarets forskningsinstitutt (FFI) driver særlig med forskning som er relevant for Forsvarets behov, men har også noen prosjekter på oppdrag fra politiet, særlig Kripos, samt noen oppdrag direkte fra politidistriktene. Innen informasjonssikkerhet dekker de mange relevante forskningsområder: kryptografi, trusselforståelse og digital maktutøvelse, risikoanalyser, behandlingssystemer for flere sikkerhetsgraderingsnivåer, trådløs kommunikasjon og trådløs kommandoplass, informasjonslekkasje innen skytjenester, omvendt utvikling ('reverse engineering'), anonymisering og skyggenettverk på Internett.

VERDIKT[108] var Forskningsrådets store satsingsprogram innen IKT frem til 2014. Det ble opprettet fire ulike verdinettverk. Det mest relevante for denne rapporten var FRISC[109], som fokuserer på sikkerhet og kommunikasjon. Satsingen ble ledet av NTNU og

105 EUs sjuende forskningsprogram for 2007–2013 (EU FP7), National Institute of Standards and Technology (NIST).
106 COINS - Research school of COmputer and INformation Security: https://ccis.no/nb/fagomrader/lab/.
107 For informasjon om SINTEFs informasjonssikkerhetsmiljø, se http://infosec.sintef.no.
108 http://www.forskningsradet.no/verdikt.
109 Forum for Research and Innovation in Security and Communications https://www.frisc.no/.

var et samarbeid med flere av de store høyskolene og universitetene i landet.

Politihøgskolen (PHS) har en egen forskningsgruppe med rundt 20 ansatte. Relevante forskningsområder er taktisk bruk av digitale spor, digitalt politiarbeid på Internett og sosiale medier. For tiden er forskningsinnsatsen på området svært begrenset, men det er planer om å øke den. Behovet for teknisk forskning er tenkt ivaretatt gjennom deltakelse i CCIS-samarbeidet.

Kripos har en egen utviklingsvirksomhet og samarbeider med forskningsmiljøer om datatekniske analyser. Dette gjelder særlig for minnemodulavlesning og utviklingsaktivitet for å støtte opp under sikring og analyse av nye typer digitale spor.

11.1.2. Norges forskningsråd og rammefaktorer for forskningsinnsatsen

Norges forskningsråd (NFR) er et nasjonalt og strategisk forskningsfinansierende organ med et budsjett på over 7,5 milliarder.[110] Forskningsrådet utga i 2012 en rapport om tilstanden innen forskning på informasjons- og kommunikasjonsteknologi.[111] Den konkluderte med at underinvesteringer er et alvorlig problem, og foreslo en nasjonal strategi for å øke forskningsinnsatsen.

Nasjonal strategi for IKT-forskning og -utvikling (2013–2022) peker ut informasjonssikkerhet som ett av tre kjerneområder det skal satses på i perioden. Det er et viktig mål å øke deltakelsen i EUs rammeprogram for forskning. Strategien påpeker at størstedelen av bevilgningene til IKT-forskning nå går til finansiering av studieplasser, og at forskningsgruppene på området er for små og fragmenterte. Regjeringen vil at kvalitet skal være det viktigste kriteriet for finansiering av IKT-forskning og -utdanning. Teknologirettede forskningsmiljøer har gitt uttrykk for at forskningsstrategien er mer samfunnsvitenskapelig enn teknologirettet, og at oppfølgingen så langt har vært begrenset.

Lite midler blir kanalisert til informasjonssikkerhet, for disse miljøene er små og dermed ikke i stand til å konkurrere med de store aktørene. Forskningsrådet ønsker ikke å detaljstyre ved prioritering, men ber om at det identifiseres områder med behov for forskning og utvikling. Forskningsrådet oppfordrer forskningsinstitusjonene til å søke EU-midler via Horizon 2020, slik at de selv kan prioritere sine behov.[112] Basert på Nasjonal strategi for IKT-forskning og -utvikling (2013–2022) planlegges det en ny satsing gjennom programmet IKT2025 fra 2015.

Kripos har i en kommentar[113] fremhevet noen viktige temaer i Horizon 2020. Det pekes blant annet på datatekniske undersøkelser, digitale spor på nett og nye metoder for bekjempelse av alvorlig organisert kriminalitet, intelligent analyse av stordata ('big data'), biometriske metoder, krypteringsteknologi, anonymisering, kommunikasjonsteknologi / trådløse nett og interoperabilitet. Det foreløpige bildet viser at Norge har aktuelle faglige virksomheter og internasjonale samarbeidspartnere som kan være relevante, men veien frem mot å sende inn søknader til dette programmet synes lang.

EU-kommisjonens Network and Information Security Platform har gjennom en arbeidsgruppe identifisert de mest relevante teknologiene og forskningsområdene for etablering av en strategisk forskningsinnsats i EU. Det omfatter følgende hovedområder:

- Grunnleggende teknologier: Basisteknologier og trusler knyttet til nettverk og informasjonssikkerhet. Hver teknologi og trussel er angitt for å definere «det siste og beste» på området, dagens verktøy og hjelpemidler samt utviklings- og forskningsutfordringer.
- Tingenes Internett ('Internet of Things'): Nettskyen skal studeres svært bredt og grundig og kan omfatte flere ulike grunnleggende teknologier og typer trusler. Disse nye teknologiene forventes å utgjøre en høy risiko for datainnbrudd og infiltrasjon i nær fremtid.
- Anvendelser: Selv om de fleste samfunnssektorene tilknyttet energi, mat, transport, bank og forsvar eksisterte før Internett, har interaksjon med den digitale verden skapt nye og interessante

110 http://www.forskningsradet.no/no/Nokkeltal/1138785797239.
111 Forskningsrådet. 2012. Research in Information and Communication Technology in Norway – an Evaluation.
112 http://www.forskningsradet.no/no/Nyheter/_Sok_EU_for_du_soker_Forskningsradet/1253998390084/p1174467583739.
113 «Kommentar til EUs nye program for forskning og innovasjon – Horizon 2020». Brev til Norges Forskningsråd fra Kripos av 27.09.2013.

tverrfaglige utfordringer med muligheter for nye varianter av datakriminalitet.

Forskningsrådet har egne støtteordninger for å hjelpe til i søknadsprosessen, blant annet stimuleringsordning for forskningsinstitutter (STIM-EU) og prosjektetableringsstøtte (PES).

11.2. Viktige forskningshensyn

11.2.1. Forskningens relevans for bekjempelse av datakriminalitet

Gjennomgangen av de mest aktuelle forskningsmiljøene viser at dagens forskningsinnsats innen juridisk og samfunnsvitenskapelig forskning ikke vektlegger kriminalitetsbekjempelse i den digitale verden.

De teknologiske fagmiljøene ved UiO, UiB, Simula, SINTEF og Norsk Regnesentral har bygget opp en del kompetanse gjennom enkeltforskere. Fagdisipliner som datatekniske undersøkelser, jus i det digitale rom og digitale undersøkelser på nett m.m. er ikke etablerte akademiske disipliner. Et unntak finnes ved Høgskolen i Gjøvik, snart en del av NTNU, der man har satset spesifikt på informasjonssikkerhet. Dette blir også bemerket i Forskningsrådets evaluering av IKT-forskningen i Norge i 2012.[114]

Det ser ikke ut til å eksistere større fagmiljøer som ivaretar flere av områdene som er beskrevet av sikkerhetsaktørene. De som finnes, er små og underkritiske med lite ressurser. De har liten mulighet for å bidra i større forskningsaktiviteter innen informasjonssikkerhet og bekjempelse av datakriminalitet.

Fagmiljøene strever også med å få forskningsmidler i Norge og EU. Norges forskningsråd kanaliserer lite midler til forskning på informasjonssikkerhet og bekjempelse av datakriminalitet. Internasjonale og større nasjonale tildelinger krever ofte anerkjente forskernavn fra større fagmiljøer, helst med internasjonale samarbeidspartnere og partnerskap med andre private eller offentlig aktører.

11.2.2. Viktige forskningsområder for samfunnet

På strategigruppens møte med kompetansemiljøene i 2014 ble det diskutert en del forskningsområder som var viktige for sikkerhetsaktørene, og som tilkjennega forskningsbehov som er viktige uavhengig av om de får gjennomslag i internasjonale søknader for eksempel til EUs 7. og 8. rammeprogram for forskning. Strategigruppen vurderer følgende forskningstemaer som særlig interessante:

Analyse og situasjonsforståelse

- forskning innen aggregering av etterretning og spor for å danne situasjonsforståelse; målet kan være å bedre utnytte informasjon politiet besitter og se den i sammenheng, samt å kartlegge kapasitet og nytteverdi av stordataanalyse (se også tiltak 7.9 og punkt 7.4.1)

Forebygging

- forskning på sosiale medier og adferd på Internett
- måling av informasjonssikkerhetstilstanden i virksomheter og hos privatpersoner (inkludert mørketall)
- effektiv håndtering av informasjonssikkerhetshendelser
- sikkerhet og personvern i programvareutvikling og skytjenester
- krise- og terrorhåndtering, deriblant sikkerhet i kritiske infrastrukturer

Etterforskning

- vurderinger rundt påliteligheten til digitale bevis og verifikasjon av funksjonaliteten til verktøy benyttet i dataetterforskning
- forståelse av anti-etterforskningsmetoder: krypteringsteknologi, anonymiseringsteknologi og digital valuta. Inkluderer også anonyme og desentraliserte valutasystemer
- biometrisk forskning på metoder innen identitet/ID-systemer
- digitale spor i Tingenes Internett og populære mobile applikasjoner ('apper')
- sikker oppbevaring og datatekniske undersøkelser av store mengder digitalt bevismateriale; som algoritmer og verktøy for å støtte etterforskeren i arbeidsprosessen[115]

114 Forskningsrådet. 2012. *Research in Information and Communication Technology in Norway – an Evaluation*.

115 Fagområde også kjent som 'computational forensics'.

- metoder og verktøy for kommunikasjonskontroll og dataavlesing

Temaene vil endres som følge av den raske teknologiutviklingen, og de må oppfattes som et utvalg satsingsområder.

11.2.3. Behov knyttet til en større forskningsinnsats

Større nasjonal innsats. Kompetansemiljøene mente at det var behov for en betydelig og mer langsiktig satsing og bygging av større fagmiljøer som kan ta for seg temaer som er viktige for sikkerhetsaktørene. Det trengs insentiver som kan gi informasjonssikkerhet, datakriminalitet og digital adferd vesentlig større forskningsmessig oppmerksomhet enn i dag.

Justis-, sikkerhets- og beredskapssektoren bør i større grad gjøres i stand til å løfte blikket, sette langsiktige mål, forebygge hendelser og være godt forberedt til å ta i bruk nye metoder og teknikker etter hvert som de utvikles.

Det er behov for å etablere en større nasjonal satsing som knytter FoU-miljøer som er viktige for sikkerhetssektoren, sammen i et partnerskap. Nasjonale forskningsmidler bør kanaliseres til området og støttes finansielt av Justis- og beredskapsdepartementet. Oversikten over forskningstemaer gjengitt i punkt 11.2.2 kan være et utgangspunkt.

Den raske teknologiske utviklingen gir trusselaktørene stadig nye metoder for å begå kriminalitet. Kontinuerlig forskning er nødvendig om ikke sikkerhetsaktørene skal bli akterutseilt. Behovene og etterslepene hos norsk politi er store, men også andre sikkerhetsaktører har behov for bedre oppdatering av både grunnlagsforståelse og spesialkunnskap på sine ansvarsområder.

I dag legger politiet vekt på umiddelbare utfordringer og reaktiv oppfølging i den digitale verden. Tverrfaglig kunnskap med komponenter fra teknologi, samfunnsvitenskap og juridiske fag er av økende betydning. I særlig grad er det behov for anvendt forskning på områder som er viktige for politietaten, påtalemyndigheten og domstolene. Det er viktig for sikkerhetsaktørene at forskningen har nytteverdi.

Et eksempel på en slik satsing er Senter for cyber- og informasjonssikkerhet (CCIS) som nevnt ovenfor, en større satsing fra Forsvaret, NSM, politiet, Høgskolen i Gjøvik og ca. 25 partnere fra offentlig og privat virksomhet. Partnerne har bundet seg til å bidra med å finansiere professorater over en tiårsperiode, hvorav politiet bidrar med finansiering av tre av dem. Det skal bygges faggrupper som tar for seg de faglige utfordringene politiet står overfor i det digitale samfunn. Politiets IT-tjeneste, Kripos, Økokrim, Oslo politidistrikt og Politihøgskolen vil være sentrale i faggruppene. Faggruppene vil samle høyt spesialiserte etterforskere og forskere og utføre datatekniske analyser av digitale og digitaliserte fysiske bevis, audiovisuelle medier, datakriminalitet og Internett-undersøkelser. Visjonen er at faggruppene skal representere et bredt spekter av fag innen datatekniske undersøkelser, beregningsvitenskap, samfunnsvitenskap og rettsvitenskap. Forskningen og utdanningen skal være basert på praktisk involvering av eksperter og hospitanter som bidrar med en rekke tilknyttede partnere fra politi og offentlige etater.

Politihøgskolen bør også styrke sin egen politifaglige forskning på det digitale samfunn for å bekjempe datakriminalitet.

Internasjonalt samarbeid. Det nordiske politidirektørmøtet i 2014 hadde datakriminalitet som tema.[116] Her ble det fremmet et forslag om at alle de nordiske politienhetene sammen med sine fremste akademiske institusjoner bør etablere et partnerskap forankret i modellen som er etablert med CCIS. En slik modell kan utvides til et nordisk samarbeid som kan gi et større nordisk bidrag i Europol/EC3 og bedre søknader til EUs rammeprogram for forskning. Politisjefene i Norden var enige om at dette var et godt forslag som de skulle se nærmere på.

Nye akademiske disipliner som i større grad tar for seg datasikkerhet, og som er teknologisk og tverrfaglig basert, har sprunget frem i andre land. Norske akademiske fagmiljøer bør være internasjonalt orientert og følge opp denne utviklingen.

Politiet bør samarbeide bredere med politiet i andre land for å dele kunnskap om metoder og verktøy. De norske kunnskapsmiljøene bør delta oftere på internasjonale møter for forskning og utvikling som er relevante for politiet. De bør også etablere et bedre

116 Politidirektørmøte som ble holdt i Oslo i november 2014.

samarbeid med forskningssentre i andre land og delta i internasjonale forskningskonsortier.

Politiet bør bidra med personell med teknologisk eller forskningsfaglig kompetanse i Europol/EC3, Interpol og andre internasjonale forskningsrelaterte satsinger for bekjempelse av datakriminalitet. Formålet er å fange opp viktig informasjon og kunnskap og vedlikeholde et forskningsnettverk.

Konklusjon. Det er behov for en større nasjonal satsing innen forskning og utvikling basert på tverrfaglighet og partnerskap. Det er viktig at forskningen får praktisk nytteverdi for politiet og andre sikkerhetsaktører, og politiet bør bli flinkere til å fremme egne forskningsbehov. Det er videre nødvendig å styrke det nordiske og internasjonale samarbeidet. Norske forskningsmiljøer bør sammen med politiet delta i forskningsaktiviteter og utviklingsarbeid som settes i gang av samarbeidspartnerne.

11.2.4. FoU-strategi for justissektoren

Justis- og beredskapsdepartementet bør bli en større bidragsyter og premissleverandør for anvendt og langsiktig forskning i sin sektor. Den departementsinitierte forskningen bør bidra til kunnskapsutvikling om datakriminalitet og ha nytteverdi for bekjempelsen.

Justis- og beredskapsdepartementet har også en koordinerende nasjonal sikkerhetsrolle og bør ta ansvaret for å styrke forskning og kunnskapsutvikling innen digital sikkerhet og bekjempelse av datakriminalitet. I mangel av større forskningsmiljøer på de relevante områdene bør vi knytte fagmiljøene sammen gjennom større tverrfaglige forskningsprosjekter. Samarbeidet bør være basert på partnerskap mellom offentlige og private etater, virksomheter, universiteter og forskningsmiljøer. Ett av målene bør være å sette oss i stand til å levere forskning på et høyt internasjonalt nivå og dermed bedre evnen til å hente forskningsfinansiering fra internasjonale kilder.

Justis- og beredskapsdepartementet bør utvikle en FoU-strategi, først frem til 2020, som en del av den nasjonale sikkerhets- og beredskapspolitikken, ikke bare som en forskningspolitikk. Forskningsstrategien må være langsiktig, med rom for endringer og tilpasninger i takt med utviklingen av den digitale kriminaliteten. Et viktig mål bør være å bygge opp en generell forskningskapasitet som både kan håndtere nye langsiktige forskningsutfordringer og løpende analysere aktuelle problemstillinger. Særskilte forskningsbehov kan dekkes gjennom avgrensede oppdrag til forskningsinstitusjonene. Øremerkede forskerstillinger kan brukes for å ivareta langsiktige, permanente forskningsbehov.

FoU-strategien bør også stimulere til samarbeid mellom offentlig og privat sektor og forskningssektoren. Det trengs kontakt og kunnskapsutveksling med sektorer som har lignende utfordringer, inkludert Forsvaret, andre sikkerhetsmiljøer, finanssektoren, kritisk infrastruktur og kommersielle aktører.

Konklusjon. Det bør utarbeides en FoU-strategi for justissektoren for å stimulere forskning på datakriminalitet som en del av den nasjonale sikkerhets- og beredskapspolitikken, ikke bare som en forskningspolitikk. Strategien må være langsiktig og tilpasses utviklingen av datakriminaliteten. Den bør fokusere på generell forskningskapasitet som både kan håndtere langsiktige forskningsutfordringer og løpende analysere kortsiktige problemstillinger. Strategien bør frem mot 2020 søke å bygge et større nasjonalt forskningsmiljø som kan ivareta politiets kunnskapsbehov og etablere Norge som en attraktiv samarbeidspartner for kunnskapsutvikling i internasjonale nettverk for politisamarbeid.

11.3. Dagens utdanningssituasjon

11.3.1. Norske utdanningsinstitusjoner

Strategigruppen har også søkt å kartlegge hva Norge har av utdanningstilbud med relevans for datakriminalitet. De fleste forskningsinstitusjonene på området er også utdanningsinstitusjoner.

Politihøgskolen (PHS) vil være sentral både i grunnutdanning og i videreutdanning av politiansatte som skal utføre politiarbeid i det digitale samfunn. Digitalt politiarbeid har kommet inn som en obligatorisk del av grunnutdanningen fra og med høsten 2014. Etter- og videreutdanningen[117] er for tiden begrenset, men det er planer om utvidelser av tilbudet.

117 http://www.phs.no/studietilbud/etter--og-videreutdanning/utdanninger/etter-forskning-og-kriminalteknikk/.

Innen etterforskning og kriminalteknikk har PHS etterutdanning innen digital etterforskning med programvarepakkene EnCase og X-Ways samt utnyttelse av digitale spor. Innen videreutdanning har de NCFI-kurs (Nordic Computer Forensic Investigator) som består av to moduler på tilsammen 30 studiepoeng med opplæring i teknisk sikring og tilrettelegging av digitale bevis. Disse studiene er i utgangspunktet åpne for alle, både politiutdannede, sivile og jurister.

Høgskolen i Gjøvik (HiG) har studieprogrammer innen informasjonssikkerhet på bachelor-, master- og doktorgradsnivå, og har tett tilknytning til forskingsmiljøet NISlab. Masteren i informasjonssikkerhet består av tre valgfrie linjer: teknologi, management og dataetterforskning. Linjen for dataetterforskning er særlig relevant for datakriminalitetsbekjempelse. Den fokuserer blant annet på 'computational forensics' (stordata og maskinlæring). I tillegg til vektleggelsen av politiets digitale etterforskning undervises det også i temaer knyttet til undersøkelser av uønskede hendelser i privat virksomhet. Ambisjonen er tett samarbeid med politi og private aktører. Linjen for teknologi er blant annet rettet mot biometri og kryptografi.

Noroff er en av landets største private utdanningsinstitusjoner. Utdanningstilbudet består av fagskole, høyskole, nettstudier og videregående skole. Noroff har nylig etablert et treårig bachelorstudium i digital etterforskning. Det omhandler datasikkerhet og etterforskning av digital kriminalitet og gir studentene relevant kunnskap om sikring og undersøkelser av digitale systemer. Utdanningen dekker kjerneteori kombinert med et solid praktisk fundament for å oppnå kompetansenivået som kreves i sikkerhetsroller i bransjen. Utdanningen skal gi en grundig metodisk innføring i å sikre, analysere og etterforske digital kriminalitet samt å håndtere sikkerhetsbrudd for raskt å gjenvinne kontrollen over en situasjon. Høyskolen tilbyr 50 studieplasser for en nettbasert bachelor i digital etterforskning.

Universitetet i Oslo (UiO) har utdanningstilbud innen informatikk, jus og samfunnsvitenskap, men fokuset på datakriminalitet er begrenset. På teknisk side har universitetet, ved Det matematisk-naturvitenskapelige fakultetet, startet en større satsing på informasjonssikkerhet. Vektlagte områder er autentisering, applikasjonsarkitektur og formell sikkerhetsmodellering samt nettrobusthet og sikkerhet innen telekommunikasjon og skytjenester. Juridisk fakultet tilbyr ingen kurs rettet spesifikt mot informasjonssikkerhet, men har et tilbud i rettsinformatikk som omfatter datateknologisk lovverk der håndheving, tvist i digitale saker og personvern er viktige tema.

UiO tilbyr en 1,5-årig mastergradsutdanning i informasjons- og kommunikasjonsteknologisk jus. Hovedmålet med dette studieprogrammet i 'Master of Laws' er å forklare de sentrale rettslige problemstillingene som oppstår som følge av utviklingen av datateknologien. Generelt dreier det seg om hvordan IKT påvirker anvendelsen av gjeldende rett, hvordan gjeldende rett påvirker bruk av IKT, og på hvilken måte IKT fungerer som en reguleringsmekanisme i seg selv. Studiet tar for seg personvern, anonymitet, eierskap til personlig informasjon, restriksjoner knyttet til bruk av opphavsrettslig beskyttede produkter og regulering av Internett.

Universitetet i Bergen (UiB) har også teknisk og juridisk fokus. På teknisk side underviser Institutt for informatikk (IFI) på masternivå innen sikkerhet, pålitelighet og kryptografi. Det planlegges en bachelorgrad fra høsten 2015. Juridisk fakultet har et stort miljø for strafferett, og det pågår en større satsing innen politirettssikkerhet. Den fokuserer på hvordan politiet kan bruke persondata og informasjonsflyt mellom politi og andre organer. Det er ingen egen satsing mot datakriminalitet, men det er stor interesse for temaet. Særlig jurisdiksjon på Internett og utlevering av data fra tjenesteleverandører i andre land er viktig.

Norges teknisk-naturvitenskapelige universitet (NTNU) har kun teknisk fokus og utdanner sivilingeniører på mastergradsnivå med spesialisering innen telematikk, datateknologi og sikkerhet i mobil databehandling. Informasjonssikkerhet inngår som et obligatorisk fag, og det tilbys også valgfag innen digital etterforskning og trådløs sikkerhet som inneholder mobilnettetterforskning og etisk hacking med mye laboratorievirksomhet.

11.4. Viktige utdanningshensyn

11.4.1. Utdanningens relevans for bekjempelse av datakriminalitet

På høyskoler og universiteter har emner som det digitale samfunn, digital sikkerhet, datatekniske undersøkelser og digital kriminalitet liten plass i teknologiske, samfunnsvitenskapelige og juridiske utdanninger. Disse temaene bør gis større oppmerksomhet.

Politihøgskolen har kun helt nylig fått inn digitalt politiarbeid i grunnutdanningen, og annen relevant utdanning er under oppbygging.

Det er stor mangel på personell med digital og grunnleggende datateknisk kompetanse, både generelt i samfunnet, i politiet og blant de andre sikkerhetsaktørene. Det fører til hard konkurranse om kandidatene.

11.4.2. Behovet for kompetanse innen datakriminalitet

Forskning, utvikling og utdanning bør ses i sammenheng. I et teknologidrevet samfunn i hurtig endring er det særdeles viktig at studieprogrammene i justis-, beredskaps- og sikkerhetssektoren er oppdaterte med den siste kompetansen, erfaringen og kunnskapen. Det er viktig at undervisningen bygger på aktuelle forskningsresultater, og at den formidler en vitenskapelig tenkemåte.

Det er stor bredde på kunnskapsområdene med relevans for datakriminalitet. Her vil de akademiske institusjonene ha et vesentlig ansvar for å tilby utdanning innen temaer som er viktige for datasikkerhet og bekjempelse av datakriminalitet. Dette gjelder særlig nye temaer som ikke er tilstrekkelig dekket av politiets eget utdanningstilbud.

Behovet for kompetanse gjelder alle sikkerhetsaktørene, men for bekjempelse av datakriminalitet er det særlig politiet (og PST) vi her kommer til å behandle.

Politiet må kunne samarbeide med andre aktører og eksperter på nye kunnskapsområder for å utvide det teknologiske og vitenskapelige grunnlaget. Dette er nødvendig for å kunne undersøke, forstå og tilpasse seg nye og komplekse datasikkerhetsrisikoer.

Basiskompetanse i politiet. Operativt personell i politiet har behov for generell opplæring i digitalt politiarbeid. Polititjenestepersoner må være i stand til å gjenkjenne og håndtere digitale bevisformer slik som USB-pinner, mobiltelefoner og alle de nye tingene som etter hvert blir digitalisert.[118] Alle etterforskere trenger kompetanse for å etterforske forbrytelser som involverer teknologi. De som mottar henvendelser fra publikum, trenger forståelse for god registreringspraksis, oppfølging og annen henvisning.[119] Det er også viktig at ledere får økt kompetanse innen digital kriminalitetsbekjempelse for å kunne prioritere ressursene. Høy kvalitet blant operativt personell fordrer en basiskompetanse basert på følgende prinsipper:

- *Bevisintegritet:* Så langt som mulig unngå at håndtering av digitale bevis endrer på data som senere skal benyttes i retten.
- *Sporbarhet i beviskjeden:* Når personer i politiet gis tilgang til data som ligger på et nettverk, på en datamaskin eller på lagringsmedier, må vedkommende kunne gjøre rede for relevansen og konsekvensene av sikringen som utføres.
- *Etterprøvbarhet.* Dokumentasjon av analyseprosessen fra databeslag til digitale bevis presentert i retten, slik at en uavhengig tredjepart kan etterprøve resultatene.

Spesialkompetanse. Det er behov for personell med nødvendig digital spesialkompetanse på flere områder innen oppdagelse, sikring og forvaltning av digitale bevis. Det trengs tilgang på «dataetterforskere», spesialetterforskere med høy teknologisk kompetanse, i team støttet av ingeniører og programvareutviklere. Behovene omfatter oppgaver som:

- datatekniske undersøkelser (tilrettelegging av digitale bevis)
- taktisk etterforskning av særlig kompleks datakriminalitet
- digital etterretning og politiarbeid på Internett

Påtalemyndigheten. Det er nødvendig å sikre at også politijurister og statsadvokater i påtalemyndigheten får en grunnleggende innføring i elektroniske spor med vekt på kvalitet i etterforskningen, teknikker,

118 Tingenes Internett, se punkt 3.3.2.
119 Noen henvendelser kan det for eksempel være naturlig å henvise til Slett-meg-tjenesten. Se også tiltak for felles digital innrapporteringsfunksjon for datakriminalitet i punkt 7.2.1.

metoder, rettssikkerhet og personvern. Et slikt tilbud vil styrke kompetansen i hele straffesakskjeden ved at politiadvokater og statsadvokater vil kunne bidra mer aktivt i etterforskningsarbeidet gjennom økt innsikt innen fagfeltet og større oppmerksomhet rundt potensialet til elektroniske spor i en straffeforfølgning. Studiene knyttet til Nordic Computer Forensic Investigators ved Politihøgskolen er åpne for jurister, men det er bare introduksjonsmodulen som er direkte relevant for dem. De øvrige modulene har en teknisk orientering.

11.4.3. Dekking av utdanningsbehovet

Utdanningsbehovene kan dels møtes med flere og mer relevante studietilbud i politiet og ved de sivile utdanningsinstitusjonene. Behovet for personell kan dekkes på to måter: etterutdanning av politi eller ansettelse av sivil kompetanse med relevant teknisk kunnskap. Begge modellene vil være nødvendige, og tverrfaglig samarbeid i sammensatte team må vektlegges. Digital kompetanse bør være en vesentlig del av undervisningen ved Politihøgskolen. Det bør være en organisert utdanning med et årlig oppdaterings- og etterutdanningstilbud. Utdanningen i politiet må, så langt den makter, ta sikte på å gi nødvendig kompetanse som ikke dekkes av de sivile utdanningsinstitusjonene. Det er behov for videreutdanningstilbud på standardisert verktøy samt forebyggings- og etterforskningsmetoder. Mye kan innarbeides i eksisterende studieprogrammer. PHS har som nevnt i punkt 11.3.1 et NCFI-kurs med opplæring i teknisk sikring og tilrettelegging av digitale bevis. Etterutdanningen kan også skje gjennom praktisk arbeid og ekstern kursing. Det er behov for å justere utdanningstilbudet etter kompetansebehovet.

Kunnskap utover politiets egenutdanning. Politiet har et stort behov for kunnskap som ikke gis i den vanlige utdanningen på Politihøgskolen, men som gis i bachelor-, master- og doktorgradsstudier ved høyskoler og universiteter. Forsvaret har i lang tid rekruttert spesialisert sivilt personell direkte fra høyskoler og universiteter. I tillegg utdanner Forsvaret også telematikkingeniører ved Forsvarets ingeniørhøgskole (FIH) for eget behov. Begrunnelsen er behovet for lederutdanning, kunnskap om egne datasystemer og forståelse for det særegne ved arbeidsplassen.

Politihøgskolen og Høgskolen i Gjøvik har inngått avtaler om et omfattende samarbeid for å styrke utdanning og forskning innen datasikkerhet. Samarbeidspartnerne er spesielt opptatt av å styrke utdanning og forskning innen etterforskning av datakriminalitet og digitale spor, gjenkjenning av digitale spor og mønstre, rettssikkerhet og personvernsaspektet knyttet til datakriminalitet. Dette skal oppnås ved at de to høyskolene samarbeider for å øke omfanget og kvaliteten på undervisning, kompetanseutvikling og forskning innen datasikkerhet.

Som en del av dette arbeidet etablerer høyskolene en felles erfaringsbasert mastergrad i informasjonssikkerhet. Studieretningene 'Digital Forensics' og 'Cybercrime Investigation' vil gi studentene kunnskaper, ferdigheter og generell kompetanse som setter dem i stand til å bruke etablerte metoder og verktøy til å håndheve lovene og beskytte personvernet. Utdanningen knytter politiets digitale etterforskning sammen med datasikkerhet for å legge til rette for samarbeid mellom involverte partnere som politiet, Forsvaret og dem som drifter samfunnskritisk infrastruktur. Studieretningene vil bli tilrettelagt for deltid og utstrakt bruk av fleksible undervisnings- og eksamensmetoder, slik at studiet enkelt kan gjennomføres som nettstudier. Utdanningens målgruppe er personell som arbeider i politiet nasjonalt og i de nordiske landene.

På kort sikt må politiet tette et stort kunnskapsgap, og det vil neppe være realistisk å fylle dette gjennom etterutdanning. De mest teknisk krevende etterforskningssakene, særlig de som angår angrep mot datasystemer, vil ikke kunne analyseres tilfredsstillende av personell uten høyere utdanning innen datatekniske fag. Politiet vil derfor ha behov for personell med utdanning fra høyskole og universitet. For å gi dem den nødvendige politifaglige forståelsen og fordypningen i teknologiske spesialtemaer knyttet til datakriminalitet, bør det opprettes videreopplæringsprogrammer for personell med sivil bakgrunn (særlig ingeniører). Denne politifaglige etterutdanningen kan gis ved Politihøgskolen og bør gi grunnlag for begrenset politimyndighet.

På lengre sikt vil alle nyutdannede fra Politihøgskolen ha grunnleggende opplæring i digitalt politiarbeid. Flere vil da ha hatt mulighet til å ta nødvendig etterutdanning for å kunne utføre standardisert etterforskning. Dette vil likevel ikke gi like stor dybde og bredde som 3–5 års bachelor- og masterutdanning innenfor teknologiske fag. Det bør derfor tilrettelegges for ansettelser av sivilt utdannede med spesialkompetanse.

Konklusjon. Alle i politiet bør sikres en digital grunnkompetanse. Dette gjelder særlig operativt personell som kommer i kontakt med digitale bevis i beslag, og som mottar henvendelser om datakriminalitet fra publikum. De som skal etterforske datakriminalitet, må ha tilstrekkelig kompetanse. Politistudenter og ansatte med politiutdanning bør gis mulighet for påbygning til master- og doktorgrad på spesielle kunnskapsområder med relevans for digital kriminalitet. Jurister i straffesakskjeden må tilbys utdanning i digital kompetanse og digitale bevis i straffesaker. For personer med sivil utdanning bør det fastsettes egne krav til politifaglig og juridisk kompetanse, med tilhørende utdanningstilbud som kan gi grunnlag for politimyndighet.

11.4.4. Kompetansekrav

Det er i dag ingen nasjonale kompetansekrav for å kunne utføre politiarbeid på Internett eller sikre, analysere og utføre datatekniske undersøkelser ved bekjempelse av datakriminalitet. Dette gjelder også håndtering av elektroniske spor ved alle typer kriminalitet. Digital kompetanse blir fort foreldet om den ikke videreutvikles og oppdateres. Nye måter å bruke og misbruke teknologi på, nye verktøy og nye metoder taler for å innføre minimumskrav for faglig oppdatering. Arbeidsgruppen kan som eksempel vise til studiereisen til USA, der FBI opplyste om at de krever minimum ett kurs årlig.

Det som ligger nærmest opp til nasjonale kompetansekrav, er å ha gjennomført relevante kurs, blant annet i datatekniske undersøkelser, som del av grunnopplæringen eller videre- og etterutdanningen ved PHS.

I forbindelse med aktiviteten «polititjeneste på Internett» har Kripos utarbeidet retningslinjene som skal synliggjøre vilkårene for bruk av metoden, og hvordan de prosessuelle vilkårene oppfylles, i tillegg til å gi en overordnet beskrivelse av prosedyren som skal følges ved bevisinnhenting. Retningslinjene angir beslutningsnivå og beslutningsansvar ved utstedelse av etterforskningsordre, samt krav til notoritet ved bruk av infiltrasjon og provokasjonslignende virksomhet på Internett. Retningslinjene gir også overordnede føringer for arbeidsmetode, opplæring, utstyr og tjenester/verktøy som er relevante for utførelse av polititjeneste på Internett. Kripos anser polititjenesten på Internett som instruksen beskriver, som en UC-tjeneste, og mener at de generelle prinsippene og retningslinjene for UC gjelder så langt de passer.

Kompetansekrav internasjonalt er et viktig tema som diskuteres i flere land, blant annet i USA og EU. Kompetansekrav er blitt en del av kvalitetssikringen ved akkreditering av metoder og personell som må være godkjent i henhold til internasjonale standarder. Begrunnelsen er å trygge individets rettssikkerhet og utveksle bevismateriale over landegrenser.

Norge har fri bevisførsel, og krav til digital bevishåndtering kan ikke sette begrensninger på denne. Høyesterett[120] har akseptert at innhentede bevis via kommunikasjonskontroll fra Litauen ble tillatt fremlagt, selv om materialet var avgrenset slik at bare samtaler av betydning for etterforskningen ble tatt med. En slik sletting av bevis kan ikke gjøres etter norsk straffeprosess og vil normalt ikke tillates i Norge. Høyesterett tillot likevel bevisene ført, og la da vekt på at man i motsatt fall ville innføre for store begrensninger for bruk av utenlandsk materiale i norske straffesaker. Høyesterett satt som vilkår at bevissikringen ikke måtte være gjennomført i strid med grunnleggende norske verdioppfatninger, da dette i realiteten ville være en skranke mot menneskerettsbrudd.

Kvaliteten på politiarbeid på Internett, datatekniske undersøkelser, elektroniske bevis og metoder vil være avgjørende ved bekjempelse av datakriminalitet. De internasjonale kravene utvikles både i European Network of Forensic Science (ENFSI), nasjonale og internasjonale akkrediteringsorganer og politiorganer. Kompetansekravene vil omfatte temaområder og rutiner som skal følges for å oppfylle ønsket kvalitet.

120 Rt. 2005 1524.

Som eksempel kan det vises til Forensic Technical Expert Competency Matrix utarbeidet av en prosjektgruppe underlagt ENFSI. Den angir faglige temaer som en spesialist må ha tilstrekkelig kompetanse på for å ha troverdighet i retten og få adgang til å arbeide med datatekniske undersøkelser og elektroniske bevis. De skiller mellom dybde- og breddekunnskap på høyt teoretisk og praktisk nivå, og ren praktisk arbeidskompetanse.

Konklusjon. Det bør etableres nasjonale kompetansekrav for digitalt politiarbeid for å sikre god kvalitet og ivaretakelse av rettssikkerheten. Norge bør følge de internasjonale kravene for akkreditering av metoder og personell. På den måten kan Norge dele bevismateriale med andre land også i fremtiden.

11.5. Organisatoriske vurderinger

Politihøgskolens rolle. Politihøgskolen bør fortsatt være den sentrale utdanningsinstitusjonen for politiet, også etter etablering av et nasjonalt datakrimsenter. PHS må være i stand til å utføre egen forskning og forskning i samarbeid med universitetene på problemstillinger tilknyttet digitalt politiarbeid. Forskningen må styrkes for å kunne være kilde til faglig utvikling og utvikling av studietilbudene. Den nyeste kunnskapen må bli tilført politiutdanningen og politietaten for øvrig. Den tekniske forskningen er i dag styrket ved samarbeidet med CCIS/HiG-miljøet. Politihøgskolen bør øke egen forskningsinnsats på både det taktiske og det forebyggende området innen digitalt politiarbeid. Utdanningsansvaret består i å gi politistudentene tilstrekkelig digital kompetanse i grunnutdanningen og at de gis mulighet for etterutdanning og påbygningsmuligheter til master- og doktorgrad i samarbeid med andre høyskoler og universiteter.

Et nasjonalt datakrimsenter vil ha oppgaver knyttet til utvikling av metoder og fastsettelse av mønsterpraksis, for eksempel ved utarbeidelse av kompetansekrav. Senteret vil ha en viktig rolle gjennom å fremme behov for relevant forskning og utdanning ved Politihøgskolen og andre forskningsinstitusjoner.

Omsette forskning til praktiske verktøy og metoder. Strategigruppen fikk under studieturen til USA presentert Software Engineering Institute (SEI) ved Carnegie Mellon University. SEI er et bindeledd mellom myndighetene og kommersielle aktører/akademia. Målet er ikke å utvikle fullstendige løsninger på alle relevante områder, men å fylle inn de områdene som mangler. Universitetene generelt er veldig opptatt av grunnforskning og tenker i mindre grad på den praktiske nytteverdien av det de utvikler og forsker på. Akademia vil søke nye områder det ikke er mye forskning på, da ingen får anerkjennelse for å «pusse» på eksisterende løsninger. SEI tar derfor rollen med å se sammenhenger på tvers av grunnforskningen samt å utvikle prototyper videre. Målet er så å få kommersielle aktører til å overta ideene for å slippe å vedlikeholde prosjekter som markedet selv er i stand til å støtte kommersielt.

Netherlands Forensics Institute (NFI) samler mange disipliner innen teknisk etterforskning og har over 550 ansatte. De jobber med alt fra biologi, kjernekraft, bil-/kjørecomputer, stemmegjenkjenning til digital etterforskning. Som Kripos har NFI en egen lab for såkalt «chip-off» der integrerte lagringsmoduler kobles fra enheter og leses av direkte. De har også utviklingsprosjekter knyttet til raske søk i store datamengder (stordata), som er viktig under analyse av store databeslag.

Eksempler som SEI og NFI peker på, er behovet for å omsette forskningen i verktøy som kan øke politiets og andre sikkerhetsaktørers effektivitet. Initiativ som CCIS og datakrimsenteret bør ses i sammenheng i FoU-strategien som foreslås i punkt 11.2.4. Blant oppgavene som er tiltenkt et nasjonalt datakrimsenter, finner vi utviklings- og implementeringsprosjekter.

Felles utdanning og kompetanseutvikling. Det vil være synergier ved samordning av utdanning og forskning på tvers av politiet/PST og andre sikkerhetsaktører som E-tjenesten og NSM. Når det gjelder datatekniske undersøkelser, vil for eksempel E-tjenesten ha utbytte av å delta i et kompetansefelleskap med politiet og PST. Det samme gjelder for miljøer som analyserer skadevare.

Konklusjon. Politihøgskolen må styrke utdanningen og forskningen innen digitalt politiarbeid. Egen forskning sammen med CCIS-samarbeidet bør kunne bidra i utviklings- og implementeringsprosjekter ved det nasjonale datakrimsenteret som foreslås opprettet.

11.6. Hovedstrategi for kompetanseheving

Sikkerhetsaktørene må samlet ha tilstrekkelige teknologiske, juridiske, politifaglige og samfunnsvitenskapelige kunnskaper til å kunne bekjempe datakriminaliteten effektivt. For å oppnå dette trengs det en vesentlig oppgradering av forskning, utdanning og systematisk opplæring på arbeidsplassen samt en løpende videreutvikling av kunnskapsbasen.

Forskningen bør blant annet omfatte temaer som kriminalanalyse, forebygging, etterforskning, digitale kriser og personvern. Den bør også undersøke de store mørketallene for datakriminalitet.

Norge må delta aktivt i den internasjonale kunnskapsutviklingen og erfaringsutvekslingen. Ny kunnskap og nye erfaringer fra de beste kompetansemiljøene i landet og internasjonalt må spres raskt til alle som deltar i bekjempelsen av datakriminalitet. Politiet må løpende vurdere sine forskningsbehov og formidle dem til forskningsinstitusjonene.

Utdanningen må gi nødvendig basiskompetanse til alle som deltar i bekjempelse av datakriminalitet. Den må også gi tilstrekkelig spesialkompetanse til å håndtere den mest komplekse datakriminaliteten. Sikkerhetsaktørene bør legge til rette for felles utdanning og kompetanseutveksling.

Politiet må også i større grad benytte seg av sivil utdanningskapasitet og rekruttere sivil kompetanse. Det skal være enhetlige og tydelige kompetansekrav for oppgaveutføring i bekjempelsen av datakriminalitet.

Anbefalte tiltak:

NB: Nummereringen av de anbefalte tiltakene nedenfor angir ikke prioriteringer.

11.1 *Opprette en langsiktig FoU-strategi med formål å stimulere forskning på datakriminalitet som en del av nasjonal justis- og beredskapspolitikk*. Se punkt 11.2.4.

11.2 *Legge til rette for at forskningen ved CCIS og PHS bidrar i utviklings- og implementeringsprosjekter ved det nasjonale datakrimsenteret som foreslås opprettet*. Se punkt 11.5.

11.3 *Utarbeide nasjonale kompetansekrav for digitalt politiarbeid som følger internasjonale krav for akkreditering av metoder og personell.* Kravene må oppdateres i takt med endringene i trusselbildet. Relevante utdanningsprogrammer kan så gjennomgås for å sikre at de samlet ivaretar kompetansekravene. Se punkt 11.4.4.

11.4 *Øke etterforskningskapasiteten for datakriminalitet og digitale spor ved etterutdanning av politiet og ved rekruttering av sivile med relevant digital kompetanse*. Se punkt 11.4.3.

11.5 *Fastsette egne krav til politifaglig og juridisk kompetanse for sivile teknologer, med tilhørende etterutdanningstilbud og karrieremuligheter*. Se punkt 11.4.3.

11.6 *Tilby påtalejurister og dommere videreutdanning innen digital kompetanse for økt forståelse av digitale kriminalitetsformer og digitale bevis i straffesaker*. Se punkt 11.4.2.

11.7 *Tilrettelegge for påbygning til bachelor-, master- og doktorgrad for politiansatte på kunnskapsområder med relevans for datakriminalitet*. Se punkt 11.4.3.

11.8 *Sørge for at Politihøgskolen spiller en sentral rolle i å styrke den politifaglige utdanningen i datakriminalitet og viderefører den nyeste kunnskapen til studenter og til politietaten ellers*. Se punkt 11.5.

7.3 og 10.13, som begge gjelder «deltakelse i internasjonale samarbeidsorganer», er viktige med tanke på tilgang til et internasjonalt forskningsmiljø og felles forskningsprosjekter. Felles internasjonal dataetterforskning vil også bidra til utvikling og utveksling av avanserte datatekniske metoder og verktøy.

12. HOVEDKONKLUSJONER

Til slutt skal vi oppsummere hovedspørsmålene i mandatet og hvordan de er besvart i utredningen.

12.1. Trusselvurderingen

Mandatet etterspør hvilken trussel og risiko datakriminalitet utgjør i vårt land.

Strategigruppens svar er at faren er betydelig og truer vesentlige verdier på nær sagt alle samfunnsområder. Alvorlighetsgraden varierer fra gutteromskriminalitet til handlinger som kan innebære store tap og skader på person, integritet, eiendom, frihet, næringsvirksomhet, samfunnsstruktur og forsvarsevne.

Mye av datakriminaliteten er organisert. Statlige organer i andre land, virksomheter og kriminelle nettverk inngår blant trusselaktørene.

Massekriminalitet er et vesentlig trekk. Enkelthandlinger kan ramme et stort antall ofre i mange land. Selv om tapene for de enkelte ofrene ikke er dramatiske, kan de samlet generere store summer for de kriminelle.

Trusselen er internasjonal. Den geografiske forankringen er svak sammenlignet med andre kriminalitetsformer. Ofrene kan befinne seg i ett land, datautstyret i et annet og de kriminelle nettverkene i et tredje land.

Teknologiinnslaget er høyt, og metodene er ofte teknologisk avanserte. Men det utvikles og markedsføres også programvare for å utføre datakriminalitet som ikke krever høy kompetanse hos brukeren.

Trusselen er dynamisk. Datautviklingen går fort, og det samme gjelder for datakriminaliteten. Det dukker stadig opp nye måter å begå denne formen for kriminalitet på.

Sårbarheten er høy, spesielt blant mindre virksomheter, som blant annet av økonomiske grunner ofte ikke prioriterer sikkerhetstiltak, og i deler av befolkningen hvor datakompetansen er lav, som hos barn og unge, eldre og lavt utdannede.

Trusselen er økende. Datateknologi brukes i stadig større grad, og samfunnet blir stadig mer avhengig av den. Det øker også sårbarheten, selv om sikkerhetsarbeidet skulle holde tritt med utviklingen av kriminelle metoder.

For å få dømt datakriminelle trenger man normalt digitale bevis. Tradisjonelle etterforskningsmetoder er utilstrekkelige. Forebygging og avverging krever også digital kompetanse og digitale verktøy.

Datakriminalitet er en kriminalitetsform som krever høy kompetanse, og bekjempelsen fordrer en effektiv nasjonal og internasjonal organisering.

12.2. Sikkerhetsaktørenes funksjon

Mandatet etterspør hvilke etater som har ansvaret for bekjempelse av datakriminalitet, hvordan disse oppfyller sitt ansvar, og hvordan de samarbeider. Strategigruppen skal vurdere om ansvaret, rollene og samarbeidet på feltet fungerer hensiktsmessig i dag, og foreslå endringer ved behov.

Den viktigste aktøren er politiet. Spesielt gjelder dette straffeforfølgning av datakriminalitet gjennom etterforskning og iretteføring.

Politiorganisasjonen er kompleks, men dagens organisering fremstår som lite egnet for etterforskning av datakriminalitet. Den registrerte kriminaliteten er svært lav i forhold til den skjulte kriminaliteten som fremgår av Mørketallsundersøkelsen. Den registrerte kriminaliteten ser også ut til å variere betydelig på lokalt nivå, men pålitelig statistikk er mangelvare.

Kapasiteten og kompetansen til å detektere og håndtere datakriminalitet på lokalt nivå er gjennomgående begrenset, med enkelte unntak. Datakriminalitet blir ofte nedprioritert lokalt når ressursene skal fordeles, blant annet på grunn av lave strafferammer. Mye av datakompetansen som faktisk finnes, går dessuten til å håndtere digitale spor innen tradisjonell kriminalitet. Det varierer derfor mye hvordan datakriminaliteten prioriteres på lokalt nivå.

På sentralt nivå er kompetansen høy, og det gjøres mye godt arbeid, men også her er kapasiteten altfor liten, blant annet fordi datakriminaliteten også nedprioriteres sentralt til fordel for annen kriminalitet og håndtering av elektroniske bevis i andre typer saker. Sentralt nivå skal også bistå lokalt nivå når de mangler kompetanse. Også denne ordningen har svakheter, dels fordi kapasiteten er for liten på sentralt nivå, og dels fordi sentralt nivå prioriterer de kompliserte sakene. Det er grunn til å anta at mange saker blir henlagt fordi sentralt nivå ikke har kapasitet og lokalt nivå mangler tilstrekkelig kompetanse. Bildet er i hovedsak det samme for påtalefunksjonen og domstolsbehandlingen. Det er få saker, og kompetansen er begrenset.

Ikke bare er datakriminaliteten i stor grad internasjonal. Den geografiske forankringen er ofte uklar og vanskelig å spore. Prinsippet om lokalt ansvar basert på geografi er krevende å praktisere. Mange saker henlegges fordi politiet anser det som urealistisk å få stilt gjerningspersonen til ansvar fordi vedkommende oppholder seg i et annet land eller bevisene befinner seg der. Behovet for et bedre internasjonalt samarbeid er stort.

Straffelovgivningen mot datakriminalitet er en sentral rammebetingelse for politiets prioriteringer og innsats. Utilstrekkelig kriminalisering, lave strafferammer og et lavt straffeutmålingsnivå forklarer også hvorfor datakriminaliteten nedprioriteres.

En rekke aktører utenfor politiet bidrar også i kriminalitetsbekjempelsen. Selv om kriminalitetsbekjempelse ikke er noen uttalt oppgave for disse aktørene, bidrar de ofte i arbeidet fordi hendelser de håndterer, svært ofte innebærer brudd på bestemmelser mot datakriminalitet.

Deres håndtering av hendelser innebærer derfor nyttig detektering og analyse av datakriminalitet og har også en verdifull kriminalitetsforebyggende, avvergende og gjenopprettende effekt. Mye av informasjonen som for eksempel NSM og CERT-ene samler inn, er også verdifull til forebygging, avverging og straffeforfølgning, og for etterforskning, dersom den tas vare på.

Ansvarsfordelingen og samarbeidet mellom sikkerhetsaktørene virker i hovedsak fornuftig. Strategigruppen har ikke notert vesentlige svakheter i den formelle ansvars- og oppgavefordelingen og foreslår ingen konkrete endringer av denne.

Samarbeidet og informasjonsdelingen kan imidlertid bli bedre. Et hinder for informasjonsdeling er at viktige deler av informasjonen som eksempelvis NSM og PST mottar, er klausulert av kilden, slik at den ikke kan brukes i straffesaker hvor den vil bli kjent av aktører og offentlighet.

Strategigruppen ønsker også å fremheve to tilfeller der det er ønskelig med en bedre rolleavklaring:

- I startfasen av en hendelse kan det være uklart hva slags hendelse som egentlig foreligger. Da er det en viss risiko for at de ulike aktørene kan bli sittende for lenge på gjerdet i påvente av initiativ fra andre.
- Ved noen former for kriser kan det synes som om NSM og politiet har overlappende ansvar for krisehåndteringen. Dette gjelder særlig forebygging, avverging og gjenoppretting. Spesielt gjelder dette såkalte kombinerte kriser, som har virkninger for både den digitale og den fysiske verden.

Øvelser og erfaringslæring vil være sentralt for å bringe klarhet til disse spørsmålene

12.3. Nøkkeloppgaver i datakrimstrategien

Mandatet ber strategigruppen vurdere en nasjonal strategi for å forebygge og bekjempe datakriminalitet med utgangspunkt i trussel- og risikobildet.

Gruppen har utarbeidet en overordnet strategi med fem hovedpunkter:

Strategien for deteksjon og analyse foreslår en vesentlig styrking av kapasiteten på dette området.

Internasjonalt samarbeid er sentralt. Det statistiske grunnlaget må bedres vesentlig. Mulighetene for bedre informasjonsdeling mellom sikkerhetsaktørene må utredes og samarbeidet styrkes. Nøkkeltiltak er å

- øke politiets tilstedeværelse på Internett
- øke deltakelsen i relevante nasjonale og internasjonale fora for informasjonsdeling
- utarbeide en årlig nasjonal trusselvurdering
- legge til rette for utvidet lagring av eierskapet til IP-adresser, noe som også er viktig i etterforskning av datakriminalitet
- opprette et sentralt mottak i politiet for tips om og anmeldelser av datakriminalitet
- styrke kapasiteten for analyse av innhentet informasjon

Strategien for kriminalisering skal sikre en oppdatert og adekvat straffelovgivning mot datakriminalitet som virker normdannende og forebygger at Norge blir en frihavn for denne typen kriminalitet. Nøkkeltiltak er å

- opprette et organ som løpende følger kriminalitetsutviklingen og tar initiativ til oppdatering av straffebestemmelsene
- vurdere strengere straffer
- gjennomgå reglene for den geografiske rekkevidden til bestemmelsene mot datakriminalitet og utvide denne vesentlig for å ramme den internasjonale datakriminaliteten bedre
- delta aktivt i arbeidet med å utvikle internasjonale regler mot datakriminalitet

Strategien for forebygging og avverging slår fast at forebyggingstiltak er mest effektive mot datakriminalitet. Evnen til selvbeskyttelse må økes vesentlig både i befolkningen og hos virksomhetene. Spredning av informasjon om trusselen er viktig. Databransjen må påvirkes til å stille høyere krav til innebygget sikkerhet i datasystemer. Nøkkeltiltak er å

- gjennomføre et nasjonalt løft for å spre kunnskap om datakriminalitet og datasikkerhet, særlig til barn, ungdom og eldre
- skjerpe reguleringen av Internett-tilbydere
- stimulere forbruker-, bransje- og næringslivsorganisasjoner til å kreve et bedre sikkerhetsnivå på dataproduktene til produsenter og leverandører
- gjennomgå roller og ansvar ved håndtering av kriser som rammer både den digitale og den fysiske verden, og gjennomføre øvelser

Strategien for straffeforfølgning: Risikoen for å bli oppdaget og straffeforfulgt for datakriminalitet bør være høy. Norge skal være en pådriver i den internasjonale bekjempelsen av datakriminalitet. Nøkkeltiltak er å

- etablere et nasjonalt datakrimsenter som tillegges viktige oppgaver innen kompetanseutvikling og etterforskning av krevende former for datakriminalitet
- utrede skjulte etterforskningsmetoder
- sørge for en fleksibel arbeidsdeling mellom sentralt og lokalt nivå, med vekt på rask kompetanse- og kapasitetsøkning
- koble inn politiet raskere ved sikkerhetshendelser som håndteres av andre sikkerhetsaktører, for å sikre en kompetent vurdering av etterforskningsspørsmålet før bevis går tapt
- etablere permanent tilstedeværelse i viktige internasjonale samarbeidsorganer for bekjempelse av datakriminalitet
- effektivisere behandlingen av rettsanmodninger

Strategien for kompetanseheving skal heve kvaliteten på arbeidet med datakriminalitet betydelig. Det er behov for mer forskningsaktivitet, og utdanningstilbudet innen bekjempelse av datakriminalitet må bedres, både i form av flere studieplasser og et mer variert og kompetansegivende studietilbud. Nøkkeltiltak er å

- opprette en langsiktig FoU-strategi for viktige temaer innen bekjempelse av datakriminalitet
- innføre nasjonale kompetansekrav for digitalt politiarbeid i overensstemmelse med internasjonale krav
- rekruttere teknologer med høy datakompetanse og tilby dem nødvendig etterutdanning i politifag
- legge til rette for påbygning til master- og doktorgrad for politistudenter og politiansatte på kunnskapsområder av betydning for datakriminalitet

To av tiltakene bør fremheves avslutningsvis:

Det ene er forslaget om å opprette et nasjonalt datakrimsenter. Senteret vil få sentrale

oppgaver knyttet til alle deler av strategien, ikke bare etterforskning, men også analyse, forebygging, kompetansebygging og internasjonalt arbeid. Det er tenkt som et kraftsenter med en viktig rolle i gjennomføringen av datakrimstrategien.

Det andre er forslagene om at politiet bør bidra til et bedre samarbeid mellom det private og det offentlige om bekjempelsen av datakriminalitet, både når det gjelder anmeldelser, forebygging, avverging og straffeforfølgning. Dette er et sentralt grep for å effektivisere politiarbeidet og for å øke evnen til selvbeskyttelse.

VEDLEGG 1:

STRATEGIGRUPPEN, STYRINGSGRUPPEN OG ARBEIDSPROSESSEN

Strategigruppen har vært sammensatt av representanter fra følgende organisasjoner:

- Politidirektoratet (POD), seniorrådgiver Rune Erlend Fløisbonn
- Politiets sikkerhetstjeneste (PST), seniorrådgiver Atle Tangen, erstattet av fagdirektør Jon Fitje Hoffmann (ikke i perioden juni 2014 til 19. januar 2015)
- Kripos, avdelingsdirektør Eiliv Ofigsbø
- Nasjonal sikkerhetsmyndighet (NSM), underdirektør Anders Bjønnes
- Påtalemyndigheten, statsadvokat Carl Fredrik Fari
- Etterretningstjenesten (E-tjenesten), underdirektør Morten Groven (ikke i perioden november 2014 til 5. januar 2015)
- Norsk senter for informasjonssikring (NorSIS), seniorrådgiver Vidar Sandland
- Næringslivets Sikkerhetsråd (NSR), seniorrådgiver Arne Røed Simonsen

Gruppen har vært ledet av professor dr.juris. Jon T. Johnsen fra Institutt for offentlig rett ved Universitetet i Oslo.

Sekretærer har vært:

- politiadvokat Knut Jostein Sætnan, Kripos
- rådgiver Simon Kiil, NSM
- rådgiver André Nordbø, POD

En styringsgruppe med representanter fra de samme organisasjonene har bestått av:

- avdelingsdirektør Knut Smedsrud, POD (leder), med ass. avdelingsdirektør Atle Roll-Matthiessen som stedfortreder
- riksadvokat Tor-Aksel Busch (erstattet underveis av ass. riksadvokat Knut Erik Sæther)
- direktør Kjetil Nilsen, NSM
- direktør Tore Orderløkken (erstattet underveis av direktør Roger Johnsen, NorSIS)
- ass. avdelingsdirektør Atle Roll-Matthiesen, POD
- sjef for Kripos Ketil Haukaas
- direktør Kristine Beitland (erstattet underveis av direktør Jack Fischer Eriksen, NSR)
- ass. sjef Tom Rykken, E-tjenesten
- avdelingsdirektør Jan Glent (erstattet underveis av avdelingsdirektør Beate Gangås, PST)

Arbeidsprosessen. Arbeidet med utredningen kom i gang i slutten av januar 2014, og strategigruppen hadde sitt første møte 6. februar 2014. Gruppens leder vurderte fra starten av den opprinnelige tidsfristen, 1. juni 2014, som altfor kort til å utarbeide en strategi av høy nok kvalitet. Sluttfristen ble etter hvert satt til 1. mai 2015.

Strategigruppen har gjennomført:

- 17 arbeidsgruppemøter
- 2 todagers internseminarer
- møte med forsknings- og undervisningsmiljøer med 22 deltakere i Oslo 25. oktober 2014 – inkludert 9 medlemmer fra strategigruppen
- workshop med 34 deltakere på Gardermoen 8. og 9. september 2014 – inkludert 11 medlemmer fra strategigruppen
- studiebesøk i Norge

  - møte med Post- og teletilsynet (18. september 2014)
  - møte med Agder politidistrikt (18. september 2014)
  - møte med NSM NorCERT (24. september 2014)
  - møte med Telenor Norge AS (30. oktober 2014)
  - møte med Oslo politidistrikt (15. desember 2014)
  - møte med Forbrukerrådet (15. desember 2014)
  - møte med Datatilsynet (8. januar 2015)
  - representasjon ved NSMs og NSRs sikkerhetskonferanser
  - møte med Plan- og beredskapsseksjonen i POD og Politiets IKT-tjenester (PIT) (27. januar 2015)
  - møte med Follo politidistrikt (27. januar 2015)
- studiebesøk i utlandet
  - Nederland 7. og 8. oktober 2014 med besøk til Europols European Cybercrime Centre (EC3) og det nederlandske justisdepartementet
  - Storbritannia 18. og 19. november 2014 med besøk til National Crime Unit (NCA)
  - USA 8.–12. desember 2014 med besøk til:
    - Washington: FBI, Department of Homeland Security (DHS), med Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) og United States Computer Emergency Readiness Team (US-CERT), og Department of Justice (DoJ)
    - Pittsburgh: National Cyber-Forensics & Training Alliance (NCFTA) med deltakelse fra Carnegie Mellon University Software Engineering Institute (CMU-SEI) og Cyber Initiative and Resource Fusion Unit (CIRFU)
    - San Francisco: UC Hastings College of the Law, FBIs avdeling i San Francisco og Electronic Frontier Foundation (EFF)
- to seminarer med styringsgruppen (halvdagers 14. januar 2015 og halvannendagers 5.–6. februar 2015)

Strategigruppen har utarbeidet to arbeidsrapporter med foreløpige synspunkter på deler av mandatet til internt bruk for Justis- og beredskapsdepartementet:

- Arbeidsrapport 1: Trusler og trusselhåndtering – 23. mai 2014 – 50 sider
- Arbeidsrapport 2: Noen forslag til tiltak og endringer – 4. september 2014 – 21 sider

Det er ikke vist til disse rapportene i dette dokumentet, men en del av stoffet er benyttet.

Strategigruppen har i løpet av arbeidet fått god og uvurderlig hjelp med både merkantil støtte, arbeidsrapporter, språkvask, layout og trykk. En stor takk rettes derfor til Berit Beate Skarsvåg, Silje Kirkegaard, Lars Vissmark og Språkseksjonen ved Kripos.

VEDLEGG 2:

ORDLISTE OG FORKORTELSER

Autentisering – En prosess der identitet verifiseres. Også en verifisert identitet kan være i uoverensstemmelse med den faktiske identiteten, for eksempel når en identitet misbrukes etter et identitetstyveri.

Bakdør – Tilgangsmetoder til IKT-systemer som avviker fra de som normalt brukes («frontdørene»), som brukernavn, passord og åpne kommunikasjonsporter. Bakdører omgår de normale forsvarsmekanismene og kan innplasseres av produsent og av brukerne av systemet ved inntrenging i et system.

Bitcoin – En digital kryptobasert betalingsvaluta basert på åpen kildekode. Den er utenfor bankers og nasjonale tilsynsmyndigheters kontroll og er basert på prinsippet «peer-to-peer». Den har dermed en distribuert database over alle transaksjoner.

Buypass – Et system for sikker elekronisk ID, elektronisk signatur og betaling fra firmaet Buypass AS. Det benyttes blant annet til offentlige tjenester. Buypass ID fås på smartkort og som app for mobile enheter. Systemet benyttes for høyt sikkerhetsnivå.

CERT – Computer Emergency Response Team. En gruppe som har ansvar for å håndtere datasikkerhetshendelser.

CKG – Cyberkoordineringsgruppen. En delingsarena der E-tjenesten og PST får innsyn i pågående saker hos NSM/NorCERT.

Comfides – Et system for sikker elektronisk identitet og personlig ID på nett, blant annet til offentlige tjenester. Systemet benyttes for høyt sikkerhetsnivå.

CryptoLocker – Et eksempel på skadevare for å tvinge løsepenger fra offeret. Det nye ved denne skadevaren er at den krypterer innholdet på det tilkoblede lagringsmediet og ber om penger for å frigi krypteringsnøkkelen.

Datakriminalitet – Straffbare handlinger rettet mot datasystemer og datanettverk eller begått ved hjelp av data eller datasystemer. For kriminalitetsformer som benytter data eller datasystemer som redskap, må databruken være et vesentlig element i utøvelsen av handlingen for at den skal falle inn under begrepet datakriminalitet.

Datatekniske undersøkelser – Datatekniske operasjoner som er nødvendige for å innhente, sikre, gjenfinne og tilrettelegge for gjennomgang og analyse av elektroniske spor og relevante data i undersøkelser.

Den digitale verden – Se det digitale samfunn.

Den fysiske verden – Brukes som et motstykke til 'den virtuelle verden', som ikke kan eksistere uten den fysiske verden. Et torg i et bysentrum er et eksempel på en fysisk markedsplass.

Den virtuelle verden – Se det digitale samfunn.

Det digitale samfunn – Det digitale samfunn omfatter Internett, alle dets brukere, bruksområder og anvendelser og alt annet som benytter denne teknologiske infrastrukturen. Eksempler på anvendelser er nettbaserte markedsplasser, diskusjonsarenaer og andre møteplasser. Tilsvarer de engelske begrepene 'cyber domain' og 'cyber space'.

Difi – Direktoratet for forvaltning og IKT, underlagt Kommunal- og moderniseringsdepartementet (KMD).

Digital kriminalitet – Se datakriminalitet.

Digital tjenestearkitektur – Kommer av 'tjenesteorientert arkitektur', på engelsk 'service-oriented architecture' (SOA): Digitale tjenester kjennetegnes ved veldefinert funksjonalitet, ofte brukt av flere programvaresystemer, samlinger av tjenester, flere brukere og tjenestetilbydere som benytter standardiserte tjenestegrensesnitt. Slike komplekse prosesser deles inn i mindre, løst koblede enkeltkomponenter. Man bryter ned lange produksjonslinjer, slik som steg i et dataangrep, i «gjenbrukbare» enkeltkomponenter som kan kjøpes og selges, eller byttes mellom spesialiserte aktører.

Digital tjenestemodell – Resultatet av en digital tjenestearkitektur.

Digitale bevis – Se elektroniske bevis.

Digitale spor – Se elektroniske spor.

ENFSI – European Network of Forensic Science. Dette er et samarbeidsforum for nasjonale kriminaltekniske virksomheter oppnevnt av myndighetene i flere vest-europeiske land. ENFSI har en egen gruppe for datatekniske undersøkelser. Gruppen diskuterer og gjennomgår metoder, standardisering og mønsterpraksis (beste praksis) på området.

Elektroniske bevis – Elektroniske spor som har relevans i iretteføringen av et kriminelt forhold.

Elektroniske spor – Elektroniske data som skapes ved bruk av elektroniske tjenester, utstyr og datateknologi. Slike spor er informasjon som med stor grad av sikkerhet kan knyttes til en bruker, person, elektronisk enhet, et sted eller en hendelse, og er av betydning for å forebygge, avdekke og bekjempe nær sagt alle former for kriminalitet.

EOS – Står for etterretnings-, overvåknings- og sikkerhetstjeneste. EOS-utvalget er Stortingets kontrollutvalg for disse tjenestene.

E-tjenesten – Etterretningstjenesten. En del av Forsvaret.

Fiat-penger – Dette er penger som er utstedt av myndighetene, men som ikke har noen fast konverteringsrate til noe annet land, og er uten egenverdi. Penger er her midler i vid forstand for å gjennomføre transaksjoner. Sedler og tall på konto har minimal verdi i seg selv. Motstykket er varer, tjenester og metaller som gull. Digitale, desentraliserte valutaer som bitcoin har ingen verdi, men har i motsetning til penger fra sentralbankene ingen myndighet som garanterer for dens «bytteverdi».

FIRST – Forum for Incident Response and Security Teams.

Hacking – Undersøke, utprøve og utnytte sårbarheter og svakheter i datasystemer og datanettverk. Begrepet kan benyttes positivt om en dyktig programmerer som utnytter uvanlige løsninger, eller får til noe vanskelig ved å være kreativ. I denne rapporten brukes `hacking' stort sett i betydningen å utnytte sårbarheter for å bryte sikkerhetsmekanismer for et bestemt formål, som å stjele eller ødelegge informasjon.

ICANN – Internet Corporation for Assigned Names and Numbers, en ikke-kommersiell organisasjon.

IC3 – Internet Crime Complaint Center i USA.

Identifisering – En handling hvor et objekt (for eksempel en person) oppgir sin identitet. Merk at denne identiteten kan være falsk.

IKT – En forkortelse for informasjons- og kommunikasjonsteknologi, som er teknologi for innsamling, lagring, behandling, overføring og presentasjon av informasjon.

IKT-kriminalitet – Se datakriminalitet.

Integritet – Å sikre at informasjon og informasjonssystemer er korrekte, gyldige og fullstendige.

Internett – Den globale infrastrukturen med datakommunikasjon basert på TCP/IP (standardiserte kommunikasjonsprotokoller på Internett) der ulike teknologiske komponenter kommuniserer med hverandre. Dagens Internett er primært basert på at data kuttes opp i små «innholdspakker» merket med avsender og mottaker. Datapakker fra mange brukere sendes samlet til rutere som sørger for å videresende pakkene helt til de når målet sitt (eller blir borte). Se også IP-adresse.

IP-adresse – IP er en forkortelse for Internet Protocol, som er standarden som brukes for å overføre informasjon fra a til b over Internett. I dag brukes hovedsakelig versjon 4 (32 bits adresseområde), men bruken av versjon 6 (128 bits adresseområde) øker, blant annet på grunn av et større adresseområde og bedre mobilitets- og datasikkerhetsfunksjoner. Alle enheter som kommuniserer direkte over Internett, får tildelt en unik adresse, og denne kan kobles til den juridiske eieren av adressen gjennom Internett-leverandøren.

Iretteføring – Påtalemyndighetens arbeid med å fremme og føre straffesaker for domstolene.

ITU – International Telecommunication Union i regi av FN.

JD – Justis- og beredskapsdepartementet.

Kompromittert – Datamaskiner eller nettverk er kompromittert når noen har kommet seg forbi sikkerhetsmekanismene deres, eller når det ikke kan garanteres at de er i en sikker tilstand.

Konfidensialitet – Å sikre at informasjon og informasjonssystemer bare er tilgjengelige for dem som skal ha tilgang.

Mønsterpraksis – Også kalt 'beste praksis'. Det er den til nå beste kjente måten å utføre en oppgave på.

Mørketallsundersøkelsen – En undersøkelse som Næringslivets Sikkerhetsråd (NSR) utfører gjennom et Informasjonssikkerhetsutvalg der offentlige og private sikkerhetsaktører deltar. Undersøkelsen utføres annethvert år for å kartlegge sikkerhetstilstanden i privat og offentlig sektor.

NCA – National Crime Agency i Storbritannia.

NKOM – Nasjonal kommunikasjonsmyndighet, tidligere Post- og teletilsynet (PT).

NorCERT – Norges nasjonale CERT. NorCERT er underlagt NSM og håndterer alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon. I tillegg drifter de et nasjonalt sensornettverk på Internett (se VDI).

NorSIS – Norsk senter for informasjonssikring. NorSIS arbeider for at alle skal kunne bruke Internett og IKT trygt på jobb og privat.

NSM – Nasjonal sikkerhetsmyndighet er Norges ekspertorgan for informasjons- og objektsikkerhet og er det nasjonale fagmiljøet for IKT-sikkerhet. Direktoratet er den nasjonale varslings- og koordineringsinstansen for alvorlige dataangrep og andre IKT-sikkerhetshendelser.

NSR – Næringslivets Sikkerhetsråd er en organisasjon som har som formål å bekjempe kriminalitet i og mot næringslivet.

OAuth – Åpen standard for autentisering.

POD – Politidirektoratet.

Politiet – En samlebetegnelse på politidistriktene og særorganene underlagt POD. Begrepet omfatter i denne rapporten også PST. PST er imidlertid organisert direkte under Justis- og beredskapsdepartementet og vil derfor også omtales spesifikt.

PBS – Politiets beredskapssystem.

PHS – Politihøgskolen.

PST – Politiets sikkerhetstjeneste. Se politiet for utdypning.

Redundans – En redundant forklaring er gjentakende eller overflødig, og den tilfører ikke noe nytt. På systemnivå vil redundans kunne være reserveløsninger som trer inn ved bortfall av en primærfunksjon, men som ellers ikke benyttes. I normalsituasjoner merkes det ikke om reservene mangler, og de blir derfor ofte nedprioritert.

Robusthet – En egenskap ved et system som innebærer å tåle påkjenninger. Redundans er en form for robusthet, det vil si å være solid.

Sikkerhetsaktør – En aktør som har til oppgave å motvirke og bekjempe datatrusler. Brukes om aktørene som er nevnt i kapittel 4.

Skadevare – Også kalt 'ondsinnet programvare' ('malware' på engelsk). Slik skadelig programvare har ofte uønsket funksjonalitet sett fra offerets side, men må ikke forveksles med programvare med programmeringsfeil, som er vanlig i all kodeutvikling. Skadevare kategoriseres ut fra en blanding av spredningsform (virus, orm, bakdør, trojansk hest), intensjon (reklamevare, løsepengevirus, spionprogramvare, logisk bombe) og oppdagelsesresistens (rootkit).

Slettmeg.no – En råd- og veiledningstjeneste for personer som føler seg krenket på nett. Tjenesten har ikke mandat til å foreta sletting eller kreve sletting, men den hjelper krenkede personer med å komme i kontakt med dem som har lagt ut opplysningene. Tjenesten ligger under NorSIS.

Stille SMS – En teknisk metode i mobiltelefonnettet. Det kan sendes en skjult melding i form av en spesiell SMS-type til en mobilenhet uten at brukeren merker det. Det innebærer at mobiltelefonen kan svare tilbake til avsender og blant annet oppgi lokasjonsinformasjon, og hvilken basestasjon mobiltelefonen var koblet opp mot.

Strukturerte data – Data som har en form som gjør det lett for brukere og datamaskiner å «forstå» dem, det vil si at bearbeiding av innholdet lett kan automatiseres. Ofte er strukturerte data organisert i databaser, eller de leveres i et fast standardisert format, som lokasjon fra en GPS-mottaker.

Sårbarhet – Beskriver et datasystems motstandsdyktighet mot datatrusler, driftsstans eller uønsket bruk. Sårbarhet betegner da i hvilken grad det som skal beskyttes mot en spesifikk trussel, antas å ville bli påvirket slik at den potensielle risikoen går over i en konkret skade. Sårbarhet avhenger ikke bare av truslenes karakter, men også av hvor gode mottiltak sikkerhetsaktørene har etablert.

Tilgjengelighet – Å sikre at informasjon og informasjonssystemer er tilgjengelige innenfor angitte tilgjengelighetskrav.

Tjenestearkitektur – Se digital tjenestearkitektur.

TOR – The Onion Router. Et system for å anonymisere brukere og tjenester på Internett. Systemet benytter kryptering og omdirigering av datatrafikk rundt omkring i verden før informasjonen sendes til det opprinnelige målet.

Trussel – Mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet. En entitet kan være et fysisk objekt, en programvare, et individ, en organisasjon, en stat, en gruppering, en virksomhet eller en annen enhet.

Trusselaktør – En person, organisasjon eller stat som står bak datatrusler. Noen typer trusselaktører er beskrevet i punkt 3.5.1.

Undercover (UC) – Når politiet opptrer uten å synliggjøre seg som politi. I denne sammenheng er dette et politifaglig begrep som inkluderer mange metoder.

Ustrukturerte data – «Rådata» som bilder, lydklipp og menneskelig språk. I en e-post er for eksempel avsendertidspunkt, avsender og mottakeradresse strukturert informasjon, mens tittel og innholdsdata som ikke kan tolkes av en bruker eller datamaskin, anses som ustrukturerte.

VDI – En forkortelse for Varslingssystem for digital infrastruktur organisert ved NSM NorCERT. Dette er et nasjonalt nettverk med sensorer som skal oppdage uønsket dataaktivitet mot kritisk digital infrastruktur i Norge.

VEDLEGG 3:

RELEVANTE DOKUMENTER

Benyttede kilder

Andenæs, J. og T. Myhrer. 2009. *Norsk straffeprosess*. Bind I. Universitetsforlaget. Oslo

Auglend, R., H.J. Mæland og K. Røsandhaug. 2004. *Politirett*. 2. utgave. Gyldendal akademisk. Oslo

Bjerke, H.K., E. Keiserud og K.E. Sæther. 2011. *Straffeprosessloven*. Universitetsforlaget. Oslo

Cabinet Office, Storbritannia. 2011. *The UK Cyber Security Strategy*

Dagbladet. Null CTRL-serien. *Dagbladet.no*. (Nettlenke: http://www.dagbladet.no/nullctrl)

Department for Business Innovation and Skills, Storbritannia. 2009. *Digital Britain – Final Report*

Egedius, T. og N. Selbo Torset. Kripos-aksjon mot spredning av stjålne Snapchat-bilder av unge. *Aftenposten.no*. (Nettlenke pr. 18.10.14: http://www.aftenposten.no/article7749726.ece)

Etterretningstjenesten. 2014. *FOKUS 2014* (ugradert trusselvurdering). Oslo

EU. 2013. Press release IP/13/14. *Directive on Network and Information Security*

Europaparlamentet ved E. McClarkin. 2012–2013. *Thematic Paper on Organised Crime – Cybercrime – New Investigation Strategies and New Technologies*. Special Committee on Organised Crime, Corruption and Money Laundering (CRIM)

Europarådet. 2001. *Convention on Cybercrime* (Budapest-konvensjonen)

Europarådet ved A. Seger. 2011. *Discussion paper – Cybercrime Strategies*. Global Project on Cybercrime

European Court of Justice. Digital Rights. Judgment 8 April 2014 C-293/12 and C-594/12

Europol EC3. 2014. *The Internet Organised Crime Threat Assessment (iOCTA)*

Executive Office of the President, USA. 2011. *International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World*

Forskningsrådet. 2012. *Research in Information and Communication Technology in Norway – An evaluation*. Oslo

Forskrift 14. desember 2012 nr. 1227 om internasjonalt samarbeid i straffesaker

Forskrift 14. mai 2013 nr. 484 om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften)

Home Office, Storbritannia. 2010. *Cyber Crime Strategy*

Høiby, S. Farene ved nettdating. *Telenor Online*. (Nettlenke pr. 26.10.14: http://www.online.no/trender/farene-ved-nettdating.jsp)

Instruks 22. juni 2012 om Forsvarets bistand til politiet (bistandsinstruksen)

Kibar, O. Sirklet inn fra utlandet. *DN.no*. (Nettlenke publisert 13.02.15 og oppdatert 20.03.15: http://www.dn.no/magasinet/2015/02/13/2219/Teknologi/sirklet-inn-fra-utlandet)

Kripos. Høringssvar til Samferdselsdepartementet om datalagringsdirektivet av 12.04.10

Kronprinsregentens resolusjon av 4. juli 2003. *Delegering av funksjoner innen myndigheten etter lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83*

Lov 22. mai 1902 nr. 10. Almindelig borgerlig Straffelov (straffeloven)

Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)

Lov 4. august 1995 nr. 53 om politiet (politiloven)

Lov 20. mars 1998 nr. 11 om Etterretningstjenesten (etterretningstjenesteloven)

Lov 21. mai 1999 nr. 30 om styrking av menneskerettighetenes stilling i norsk rett (menneskerettsloven)

Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)

Lov 20. mai 2005 nr. 28 om straff (straffeloven)

McAfee og Center for Strategic and International Studies. 2013. *The Economic Impact of Cybercrime and Cyber Espionage*

Meld. St. 7 (2010–2011) *Kampen mot organisert kriminalitet – en felles innsats*. Justis- og politidepartementet

Meld. St. 29 (2011–2012) *Samfunnssikkerhet*. Justis- og beredskapsdepartementet

Meld. St. 21 (2012–2013) *Terrorberedskap – Oppfølging av NOU 2012: 14 – Rapport fra 22. juli-kommisjonen*. Justis- og beredskapsdepartementet

Microsoft. *Digital Trends 2014*. http://www.microsoftadvertising.ca/digitaltrends

Ministry of Security and Justice, Nederland. 2013. *National Cyber Security Strategy 2*

Nasjonal sikkerhetsmyndighet. 2014. *Sikkerhetstilstanden 2014* (ugradert rapport)

NorSIS. 2009. *Strategi og tiltaksplan for identitetstyveriprosjektet*

NorSIS. 2013. *slettmeg.no – Årsrapport 2013*

NOU 2000: 24 *Et sårbart samfunn – Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet* (Willoch-utvalget). Justis- og politidepartementet

NOU 2002: 04 *Ny straffelov – Straffelovkommisjonens delutredning VII*. Justis- og politidepartementet

NOU 2003: 27 *Lovtiltak mot datakriminalitet – Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi*. Justis- og politidepartementet

NOU 2006: 6 *Når sikkerheten er viktigst – Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. Justis- og politidepartementet
NOU 2007: 2 *Lovtiltak mot datakriminalitet – Delutredning II*. Justis- og politidepartementet
NOU 2009: 1 *Individ og integritet – Personvern i det digitale samfunnet*. Fornyings- og administrasjonsdepartementet
NOU 2009: 15 *Skjult informasjon – åpen kontroll – Metodekontrollutvalgets evaluering av lovgivningen om politiets bruk av skjulte tvangsmidler og behandling av informasjon i straffesaker*. Justis- og politidepartementet
NOU 2012: 14 *Rapport fra 22. juli-kommisjonen*. Statsministerens kontor
Næringslivets Sikkerhetsråd. 2014. *Mørketallsundersøkelsen – Informasjonssikkerhet, personvern og datakriminalitet*. Oslo
Ot.prp. nr. 22 (2008–2009) *Om lov om endringer i straffeloven 20. mai 2005 nr. 28 (siste delproposisjon – sluttføring av spesiell del og tilpasning av annen lovgivning)*. Justis- og politidepartementet
Ot.prp. nr. 40 (2004–2005) *Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)*. Justis- og politidepartementet
Ot.prp. nr. 90 (2003–2004) *Om lov om straff (straffeloven)*. Justis- og politidepartementet
Politidirektoratet. 2011. *Politiets beredskapssystem del I (PBS 1)*. Oslo
Politidirektoratet. 2012. *Politiet i det digitale samfunnet*. Oslo
Politidirektoratet. 2014. *Etterretningsdoktrine for politiet v.1.0*. Oslo
Politiets sikkerhetstjeneste. *Åpen trusselvurdering 2014*. Oslo
Prop. 1 S (2013–2014) *Proposisjon til Stortinget (forslag til stortingsvedtak) – For budsjettåret 2014 – Statsbudsjettet*. Finansdepartementet
Regjeringen. 2012. *Nasjonal strategi for informasjonssikkerhet*
Regjeringen. 2012. *Nasjonal strategi for informasjonssikkerhet – Handlingsplan*
Regjeringen. 2013. *Strategi 2013–2022 – Nasjonal strategi – IKT-forsking og -utvikling*
Riksadvokaten. Rundskriv nr. 1 2014
Rowlingson, R. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence*, Winter 2004, Vol 2, Issue 3
Secretariat of the Security and Defence Committee, Finland. Government Resolution 24.1.2013. *Finland's Cyber Security Strategy*
Standard Norge. *Norsk Standard NS 5830:2012 Samfunnssikkerhet – Beskyttelse mot utilsiktede handlinger – Terminologi*
Statistisk sentralbyrå. *Norsk mediebarometer 2012*

Annen relevant bakgrunnslitteratur og informasjon

Department of Defense, USA. 2011. Department of Defence Strategy for operating in cyberspace
EastWest Institute og World Federation of Scientists, forfattere: J.R. Westby, H. Wegener og W.A. Barletta. 2010. *Rights and Responsibilities in Cyberspace – Balancing the Need for Security and Liberty*
ENISA. 2011. *A flair for sharing – encouraging information exchange between CERTs*. Initial edition 1.0
ENISA. 2012. *The Fight against Cybercrime – Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime*
EU-kommisjonen. Press release 2004. *European Cybercrime Centre – one year on*
Europarådet og EU. 2011. *Specialised cybercrime units – Good practice study*. Joint Project on Regional Cooperation against Cybercrime
Europarådet ved H.W.K. Kaspersen. 2009. *Cybercrime and Internet jurisdiction*. Project on Cybercrime
Europarådet ved J.J Schwerha IV. 2010. *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from «Cloud Computing Providers»*. Project on Cybercrime
Europarådet ved J. Spoenle. 2010. *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* Project on Cybercrime
Europol EC3. 2014. CryptoWall. *Cyber Bits*
Europol EC3. 2014. Elderwood. *Cyber Bits*
Europol EC3. 2014. Pandemiya. *Cyber Bits*
Executive Office of the President, USA. 2014. *Big Data: Seizing Opportunities, Preserving Values*
Fahsing, I.A. og P. Gottschalk. 2008. *Kriminelle organisasjoner – Hvordan forstå organisert kriminalitet*. Fagbokforlaget. Bergen
FFI. 2013. *Cyberdomenet, cybermakt og norske interesser*. FFI-rapport 2013/02712
Forskningsrådet. 2008. *IKT-sikkerhet – Det kontinuerlige kappløpet*. Oslo
Forskningsrådet. 2013. *Veien videre for IKT-satsing i Forskningsrådet*. Oslo
Justis- og beredskapsdepartementet. 2013. *Handlingsplan for forebygging av kriminalitet (2013–2016)*

Justis- og beredskapsdepartementet. 2014. *Handlingsplan mot radikalisering og voldelig ekstremisme*
Justis- og politidepartementet ved G. Faremo. 2007. *Forebygging av internettrelaterte overgrep mot barn*
Kavanagh, C. og M. Carrieri. *Cyber Dialogue 2012 briefs: The Who's Who of Policing in Cyberspace*. 18.–19. mars 2012. Toronto, Canada
Kripos. 2011. *Den organiserte kriminaliteten i Norge – Trender og utfordringer i 2011–2012*. Oslo
Norsk Regnesentral ved J. Danielsson, A. Groven, T. Kristoffersen, H.J. Rivertz og Å. Skomedal. 2005. *Elektroniske spor – Rapport*. Rapportnr. 1008
NOU 2013: 9 *Ett politi – rustet til å møte fremtidens utfordringer – Politianalysen*. Justis- og beredskapsdepartementet
Politidirektoratet. 2008. *Politiet mot 2020 – Bemanning og kompetansebehov i politiet*. Oslo
Politidirektoratet. 2010. *Tendenser i kriminaliteten – Utfordringer i Norge i 2010–2012*. Oslo
Smart, S.J., Unites States Air Force, USA. Joint Targeting in Cyberspace. *Air & Space Power Journal*, Winter 2011
St.meld. nr. 41 (2004–2005) *Politiets rolle og oppgaver*. Justis- og politidepartementet
St.prp. nr. 63. (2003–2004) *Tilleggsbevilgninger og omprioriteringer i statsbudsjettet medregnet folketrygden 2004*. Finansdepartementet
United States Air Force, USA. 2010. *Cyberspace Operations*. Doctrine Document 3–12
White House, USA. 2009. *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*
White House, USA. 2012. *Digital government: Building a 21st Century Platform to Better Serve the American People*

Politidirektoratet
Mai 2015
Design: Kripos
Trykk: Kripos
Foto: Shutterstock.com
POD publikasjon 2015/02
ISBN 978-82-8256-058-0