Strategi

Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet

JUSTIS- OG BEREDSKAPSDEPARTEMENTET

Innhold

Innledning

Dette strategidokumentet er Justis- og beredskapsdepartementets første strategi for å bekjempe IKT-kriminalitet.

Samfunnet er blitt digitalt. IKT (informasjons- og kommunikasjonsteknologi) har gitt den enkelte og samfunnet store muligheter og gevinster. Men den økende avhengigheten av IKT har også gjort samfunnet mer sårbart, fordi de digitale tjenestene er blitt kritiske for at samfunnet skal fungere normalt. Det digitale rom er globalt, og den digitale trusselen er økende og uforutsigbar. Arbeidet med IKT-sikkerhet og kampen mot IKT-kriminalitet blir derfor stadig viktigere.

Samfunnets økende bruk og avhengighet av IKT øker skadepotensialet ved IKT-kriminalitet, samtidig som det stiller både samfunnet og politiet overfor nye utfordringer. Justis- og beredskapsdepartementet har det nasjonale ansvaret for forebyggende IKT-sikkerhet på sivil side jf. kgl. res 22. mars 2014 og samordningsansvaret for samfunnssikkerhet og beredskap jf. Kgl. res 11. november 2011. I tillegg har departementet det overordnete ansvaret for å forebygge og bekjempe kriminalitet, herunder IKT-kriminalitet. Dette helhetlige ansvaret gjør departementet i stand til å se IKT-sikkerhet, IKT-kriminalitet, kritisk infrastruktur og samfunnssikkerhet i sammenheng, og bidrar til at det blir gjennomført viktige tiltak på området. I den nasjonale strategien for informasjonssikkerhet fra 2012 er den ene av de syv prioriteringene å «sikre samfunnets evne til å forebygge, avdekke og etterforske datakriminalitet». Departementets strategi for å bekjempe IKT-kriminalitet er en konkretisering av hvordan denne prioriteringen skal følges opp.

Med IKT-sikkerhet forstås sikring av informasjons- og kommunikasjonstek-nologi i forhold til konfidensialitet, integritet og tilgjengelighet. Denne sikringen innebærer tiltak på både menneskelig, teknisk og organisatorisk nivå.

Med IKT-kriminalitet forstås kriminalitet som retter seg mot datasystemer og/eller datanettverk eller kriminalitet der sentrale elementer av handlingsforløpet begås ved hjelp av datautstyr og/eller datanettverk.

Strategien omhandler også elektroniske spor og politiarbeid på Internett. Med elektroniske spor forstås informasjon i elektronisk form som kan knyttes til en bruker, person, elektronisk enhet, sted eller hendelse. Med politiarbeid på Internett forstås etterforskning, forebyggende arbeid og etterretning basert på informasjon fra Internett. Med IKT-hendelser forstås hendelser i det digitale rom hvor det kan oppstå negative samfunnsmessige konsekvenser. I motsetning til IKT-kriminalitet, trenger ikke hendelsene å være utløst av en kriminell handling eller unnlatelse. Likevel kan politiets oppmerksomhet være påkrevd på samme måte som under andre hendelser, eksempelvis større samfunnsmessige ulykker. God forebygging er sammen med høy oppdagelsesrisiko og god evne til å etterforske og forfølge straff-bare handlinger, viktige virkemidler for å redusere IKT-kriminaliteten enten den retter seg mot enkeltpersoner, offentlige myndigheter, virksomheter eller viktige

samfunnsinstitusjoner og -funksjoner. For å sikre god fore-bygging må Norge ha evne og ressurser til målrettet innsats, og et tett og tillitsfullt samarbeid mellom offentlige og private aktører. Dette perspektivet reflekteres også i den nasjonale strategien for informasjonssikkerhet fra 2012. Forebygging er behandlet i andre særskilte dokumenter slik som Handlingsplan for forebygging av kriminalitet (2013-2016) og Handlingsplan mot radikalisering og voldelig ekstremisme (juni 2014). I dette strategi-dokumentet foreslås en rekke tiltak som skal bidra til å forebygge at IKT-kriminalitet skjer.

Strategien skal jevnlig oppdateres i takt med endringer i utfordringsbildet. Det vil bli etablert en bredt sammensatt referansegruppe som fortløpende skal gi forslag og innspill til Justis- og beredskapsdepartementets revidering av strategien.

1. Visjon og mål

Visjonen for det digitale rom, som for andre områder, er at Norge skal være trygt og sikkert. Norge må være rustet til å håndtere fremtidige kriser. Myndigheter og andre samfunnsaktører, og samspillet mellom dem, skal skape trygghet, forebygge, avverge, oppklare og straffeforfølge IKT-kriminalitet. De som utøver IKT-kriminalitet skal ikke kunne forberede eller gjennomføre kriminelle handlinger uten betydelig risiko for å bli oppdaget og straffeforfulgt.

Norges innsats mot IKT-kriminalitet skal være blant Europas fremste. Stikkordene for dette arbeidet er: Trygghetsskapende, kunnskapsorientert og innovativ, kvalitet, samarbeid og partnerskap med andre aktører, fokusert og strategisk. Borgeren, virksomheter og samfunnsfunksjonene skal være i sentrum. Når en borger, virksomhet eller viktig samfunnsfunksjon blir utsatt for IKT-kriminalitet, skal politiet ha særlig oppmerksomhet på den som er rammet, forhindre skade, etterforske og iverksette straffeforfølgning for å ivareta deres rettssikkerhet og trygghet.

Målet er å styrke samfunnssikkerheten og beredskapen. Arbeidet med å forebygge og bekjempe kriminalitet skal styrkes.

2. Trusselbildet

Det moderne samfunnet er i stor grad avhengig av IKT for å fungere. Det eksisterer en systematisk forsinkelse mellom teknologiutvikling, metodeutvikling og organisasjonsutvikling. Det betyr at utfordringene som samfunnet står ovenfor, ikke minst trussel-, kriminalitets- og sårbarhets-bildet, utvikler seg raskere enn myndighetene hittil har klart å respondere. Teknologibruken i samfunnet øker kraftig, og også kriminaliteten blir i økende grad digitalisert. Dette understreker viktigheten av en økt innsats for å bekjempe IKT-kriminalitet.

Handlinger og kommunikasjon i det digitale domenet i dag er en del av svært mange forskjellige kriminalsaker – ikke bare saker der IKT utgjør kjernen i den kriminelle handlingen. IKT er blitt et standard verktøy i samfunnet som helhet, og dermed er det også blitt et vanlig element i mange ulike former for kriminalitet. Hacking, datainnbrudd, svindel med fiktive e-poster, skjult digital kommunikasjon, tyveri av elektronisk informasjon, triksing med elektroniske regnskaper – dette kan være del av mange saker. Politiet har derfor økende behov for å integrere utsjekk av ulike digitale medier i etterforskning av kriminalsaker generelt. Med andre ord: ren IKT-kriminalitet er bare en side av saken, like viktig er det å undersøke IKT-spor som del av etterforskning generelt.

IKT-kriminalitet rettet mot norske interesser kan utføres av aktører som enten befinner seg i eller utenfor landets grenser. En særlig utfordring knytter seg til at denne type kriminalitet ofte utføres av personer og/eller ved hjelp av maskiner som befinner seg på steder som ikke er undergitt norsk jurisdiksjon. Slik sett er IKT-kriminaliteten i mye større grad «grenseløs» enn mye annen kriminalitet, og geografisk avstand til andre land er ikke noe hinder for utenlandske kriminelle. Dette innebærer at antallet potensielle gjerningsmenn er vesentlig større enn for annen kriminalitet, samtidig som bekjempelsen av begått IKT-kriminalitet er vanskeligere og/eller mer tidkrevende enn om gjerningsmannen og utstyret/serverne hadde befunnet seg under norsk jurisdiksjon. Dette innebærer at et tettere internasjonalt samarbeid er viktig.

Utviklingen medfører også nye sårbarheter og økt skadepotensial ved kriminelle anslag. IKT utnyttes også i økende grad av kriminelle som verktøy i deres gjennomføring av mer tradisjonell kriminalitet, som:

- Økonomisk kriminalitet
- ID-tyveri
- ID-misbruk
- Ulovlig innvandring
- Narkotikakriminalitet
- Seksuelt misbruk av barn
- Organisert kriminalitet av ulikt karakter
- Terrorplanlegging
- Hatkriminalitet, radikalisering og voldelig ekstremisme

Truslene rettet mot IKT-systemer/datanettverk øker sterkt i omfang. Norske virksomheter utsettes i stadig større grad for alvorlig IKT-hendelser, herunder nettverksbasert etterretning, tyveri av informasjon eller overvåkning av selskaper. NSM håndterte 50 alvorlige digitale infiltrasjonsforsøk i 2013. Ifølge Nasjonal sikkerhetsmyndighet ble det i 2013 gjennomført ca. 26 000 hackerangrep mot norske bedrifter.

En rekke forsøk på digitale spionasjeforsøk mot mål i Norge er avslørt de siste årene. Det ventes at digitale angrep vil kunne komme fra flere aktører, både statlige og private, bli mer avanserte, representere større skadepotensial og være vanskeligere å avdekke.

IKT utgjør i økende grad en vesentlig komponent i spionasje, sabotasje og terror. Grensene mellom kriminalitet, terrorisme og trusler er ikke like tydelig som før idet aktørene opererer på mange ulike felt – noe som IKT gjør enklere.

Det antas å være store mørketall for det faktiske omfanget av IKT-kriminalitet. Mange alvorlige angrep blir aldri oppdaget og mange saker meldes av ulike årsaker heller ikke.

Ifølge ansvarsprinsippet skal det organ som har ansvar for en funksjon eller oppgave til daglig, også ha ansvaret for tiltak i tilfelle ulykke, krise og krig. Hvis organet ikke gjennomfører slike tiltak, vil NSM og politiet ta ansvar innen sine fagområder. Det store skadepotensiale tilsier at myndigheter stanser et dataangrep så raskt som mulig. Etterforskningshensyn og muligheten til å avsløre hvem som står bak et angrep kan derimot tilsi at angrepet ikke stanses umiddelbart. Dette er et alvorlig dilemma. Hvordan disse hensynene skal vektes, må vurderes konkret i hvert enkelt tilfelle.

Organiserte, kriminelle grupper angriper IKT-systemer som ledd i profitt-motivert kriminalitet. I Norge forsøker slike grupper kontinuerlig å inn-hente personinformasjon som senere skal brukes til kriminelle handlinger. Identitetstyveri og planting av skadelig programvare er noen av metodene som benyttes. Tall fra Norsk senter for informasjonssikkerhet (NorSIS) fra 2013 viste en fordobling av ID-tyveri sammenlignet med 2012. Norske banker opplever at kriminelle infiserer kundenes datamaskiner med skadelig programvare for å gjennomføre urettmessige transaksjoner.

Internett benyttes også til å spre overgrepsbilder og er en arena for å oppnå kontakt med barn og ungdom med sikte på overgrep. Radikalisering, rasisme, ytringer med hatefullt eller voldelige innhold og andre krenkelser får en økt spredning gjennom bruk av internett.

3. Sentrale aktører

En rekke offentlige etater har et ansvar eller en rolle når det gjelder å møte utfordringene knyttet til IKT-kriminalitet. Nedenfor omtales noen av de mest sentrale.

Internasjonalt samarbeider både politiet og de andre aktørene med tilsvarende organ i andre land, og særlig innenfor Europol, Eurojust og Interpol og landenes nasjonale responsmiljøer omtalt som CERT-er (Computer Emergency Response Team, som i Norge er en funksjon i Nasjonal sikkerhetsmyndighet).

Politiet

Politidirektoratet leder og samordner politiet. Politiet har et generelt ansvar for blant annet å:

- Beskytte og verne lovlig virksomhet mot alt som truer den alminnelige tryggheten i samfunnet.
- Opprettholde den offentlige orden og sikkerhet.
- Forebygge kriminalitet og krenkelser av den offentlige orden og sikkerhet.
- Avdekke og stanse kriminell virksomhet.
- Etterforske og straffeforfølge lovbrudd.

Politiet har derfor et klart ansvar i forhold til innsats mot IKT-kriminalitet. Dette ansvaret ivaretar politiet primært i det enkelte politidistrikt.

KRIPOS er politiets nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet. I forhold til IKT-kriminalitet utfører Kripos blant annet datakrimetterforsking, metodeutvikling innen datatekniske undersøkelser og bidrar internasjonalt med utvikling av arbeidsmetodikk, hardware og software til kriminalitetsbekjempelse. Kripos er nasjonalt kontaktpunkt for Interpol og Europol og deres kompetansesentre for bekjempelse av IKT-kriminalitet.

ØKOKRIM er nasjonalt kompetansesenter for bekjempelse av økonomisk kriminalitet og miljøkriminalitet.

Politihøgskolen (PHS) har til oppgave å gi grunnutdanning for tjeneste i politi- og lensmannsetaten og etter- og videreutdanning til de tilsatte i etaten. Politihøgskolen driver forsknings- og utviklingsarbeid og faglig formidling innenfor fagområdene sine.

Politiets sikkerhetstjenestes (PST) primære ansvar er å forebygge og etterforske straffbare handlinger mot rikets sikkerhet, herunder også å bidra til å avverge, forestå og undersøke alvorlige IKT-hendelser. Tjenesten er også en viktig bidragsyter til trusselvurderinger og sikkerhetsrådgivning. PST samarbeider med Nasjonal sikkerhetsmyndighet og Etterretningstjenesten i den permanente faglige

koordineringsgruppen «Cyberkoordineringsgruppen», som har løpende koordinering av alvorlige hendelser som håndteres. Gruppen skal blant annet styrke det operative og øvrige samarbeidet mellom de tre EOS-tjenestene (Nasjonal sikkerhetsmyndighet, Etterretningstjenesten og PST), som alle har et nasjonalt sektoroverskridende oppdrag på cyberområdet innenfor sine respektive ansvarsområder. Koordineringsgruppen legger også forholdene til rette for et styrket samarbeid mellom EOS-tjenestene og sentrale sektormyndigheter.

Den høyere påtalemyndighet

Den høyere påtalemyndighet omfatter alle statsadvokatregionene, Det nasjonale statsadvokatembetet, Økokrim og Riksadvokatembetet. På området for IKT-kriminalitet, som på andre kriminalitetsområder, har Den høyere påtalemyndighet et overordnet og faglig ansvar for straffesaksbehandlingen i politiet og påtalemyndigheten.

Nasjonal sikkerhetsmyndighet (NSM)

NSM skal på vegne av Forsvarsministeren og Justis- og beredskapsministeren utøve sitt overordnete og sektorovergripende ansvar for forebyggende sikkerhetstjeneste iht. sikkerhetsloven. I tillegg skal NSM som det nasjonale fagmiljøet for IKT-sikkerhet i Norge, understøtte og bidra til utøvelsen av Forsvarsdepartementets (FD) og Justis- og beredskapsdepartementets (JD) ansvar på IKT-sikkerhetsområdet. Direktoratet er administrativt underlagt FD, og rapporterer med faglig ansvarslinje til JD for oppgaveløsning i sivil sektor og til FD for militær sektor. NorCERT-funksjonen som ligger i NSM koordinerer håndteringen av alvorlige IKT-angrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner. NSM leder arbeidet i Cyberkoordineringsgruppen (CKG) hvor alvorlige hendelser koordineres med PST og Etterretningstjenesten. I tilknytning til NorCERT-funksjonen driver NSM det nasjonale varslingssystemet for digital infrastruktur (VDI) som er et sensornettverk for varsling og verifikasjon av alvorlige IKT-hendelser.

Interpol

Interpol (International Criminal Police Organization) er en internasjonal organisasjon som arbeider med internasjonalt kriminalpolitisamarbeid. Organisasjonen har 188 medlemsstater. 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, distribusjon av materiale som viser seksuelle overgrep mot barn, økonomisk kriminalitet, høyteknologisk kriminalitet og korrupsjon.

Europol

Europol er EUs organisasjon for politisamarbeid. Europol har som formål å sikre økt effektivitet og samarbeid mellom myndighetene i medlemsstatene som har ansvar for å forebygge og bekjempe alvorlig internasjonal organisert kriminalitet og terrorisme. Europols oppgaver er å yte et vesentlig bidrag til EUs innsats mot organisert kriminalitet og terrorisme, særlig mot kriminelle organisasjoner.

Europols senter EC3

EC3 ble opprettet i januar 2013. Senteret er en integrert del av Europol. Norges samarbeidsavtale med Europol omfatter derfor også EC3. Senteret har tre hovedprioriteter innen IKT-kriminalitet:

- IKT-kriminalitet begått av organiserte kriminelle grupper og spesielt kriminalitet som genererer stort kriminelt utbytte,
- IKT-kriminalitet som påfører ofrene alvorlig skade, så som seksuell utnyttelse av barn og
- IKT-kriminalitet som angriper eller påvirker kritisk infrastruktur eller informasjonssystemer.

Senteret er EUs informasjonsnode for IKT-kriminalitet, og bidra til medlemsstatenes kapasitetsbygging, yte støtte til medlemsstatenes etterforskning av IKT-kriminalitet og være en felles stemme for etterforskere innen IKT-kriminalitet i EU.

Eurojust

Eurojusts oppgave er å bidra til et effektivt samarbeid mellom medlems-statene i forbindelse med saker om alvorlig, organisert og grenseoverskrid-ende kriminalitet, samt å få lovovertredere for retten hurtig og effektivt. Innenfor sitt ansvarsområde har Eurojust vært involvert i en rekke saker knyttet til IKT-kriminalitet, blant annet i saker som gjelder spredning av overgrepsbilder på nett.

Cyberforsvaret

Cyberforsvaret er en militær organisasjon som drifter, sikrer og forsvarer Forsvarets datasystemer, nettverk, og høyteknologiske plattformer mot angrep i og fra cyberdomenet. Forsvaret har IKT-kapasiteter som kan bistå politiet i henhold til gjeldende bestemmelser.

Næringslivets Sikkerhetsråd (NSR)

NSR er næringslivets sentrale organisasjon med formål å bekjempe kriminalitet i og mot næringslivet. Dette gjøres gjennom et formalisert og aktivt nettverk mot politi og offentlige sikkerhetsmyndigheter, og mot næringslivet.

Norsk senter for informasjonssikring (NorSIS)

NorSIS er et uavhengig organ som arbeider blant annet for å bevisstgjøre små- og mellomstore virksomheter, kommuner og den enkelte borger om informasjonssikkerhet. NorSIS driver «Slett meg»-tjenesten og nettsiden www.idtyveri.info.

4. Hovedutfordringer og hvordan disse kan møtes

Uavhengig av om det dreier seg om angrep rettet mot IKT-systemer og/eller datanettverk, eller om IKT brukes som redskap for å gjennomføre annen kriminalitet, står politiet overfor mange av de samme utfordringene. Disse behandles tematisk nedenfor. Tiltakene oppsummeres i kapittel 5.

4.1 Felles kunnskaps- og analysegrunnlag

Utfordringer

- En effektiv og målrettet innsats mot IKT-kriminalitet krever et godt kunnskaps- og analysegrunnlag, som tegner et realistisk situasjonsbilde, peker på utviklingstrekk og gir veiledning mht. hvordan innsatsen skal målrettes for å kunne forebygge, avverge, avdekke, etterforske og straffeforfølge slike lovbrudd.

- Det finnes i dag ikke noen god statusoversikt over kriminalitetsutvikling og nasjonale hendelser på IKT-feltet som faller innenfor politiets ansvarsområde. Enkeltpersoner og virksomheter rapporterer og anmelder i varierende grad hendelser slik at det antas å være store mørketall. 4 % av norske bedrifter og 5 % av de store bedriftene sier at de har opplevd datainnbrudd. Det fremgår av Mørketallsundersøkelsen fra 2014 at over 50 % av norske bedrifter har opplevd datainnbrudd.

Strategi for å utvikle et felles kunnskaps- og analysegrunnlag

- Det skal utarbeides en særskilt, felles, årlig trusselvurdering for IKT-kriminalitetsfeltet innen Justis- og beredskapsdepartementets ansvars-område som skal danne grunnlag for en målrettet politiinnsats. Trussel-vurderingen må dra veksler på det arbeid som gjøres med lignende trusselvurderinger i for eksempel Europol.

- Det må etableres et godt kunnskapsgrunnlag som trusselvurderingen kan baseres på. Gode årlige statistikker over vesentlig IKT-kriminalitet, er en helt nødvendig forutsetning. Statistikkverktøyet må utvikles slik at det kan gi et presist og kvalitativt godt bilde av IKT-kriminaliteten for aktuelle formål. Dette oppnås ved at det utvikles hensiktsmessige statistikk-koder for IKT-kriminaliteten, samt utarbeides gode veiled-ninger og tydelige rutiner for registrering. I og med at IKT-kriminaliteten ofte ikke blir anmeldt, skal det kartlegges om også andre rapporterings-måter kan gi politi og andre myndigheter en bedre oversikt over den faktiske IKT-kriminaliteten.

- Mørketallundersøkelsen, som skjer i regi av Næringslivets sikkerhetsråd (NSR), er enestående i sitt slag i Norge. Ingen andre aktører i Norge henter i dag inn statistikk på IKT-kriminalitet så bredt. Den er derfor en viktig kilde til data om

opplevd IKT-kriminalitet i norske virksomheter og til å fange opp nye trender i kriminalitetsutviklingen. Undersøkelsen har ikke hatt fast finansiering, men vært avhengig av frivillige økonomiske bidrag fra sponsorer fra gang til gang. Undersøkelsen gjennomføres regelmessig og utgis hvert annet år. Undersøkelsen er viktig, og skal sikres en stabil finansiering.

4.2 Kompetanse

Utfordringer

- Utviklingen av IKT skjer raskt, hvilket skaper særlige utfordringer med forebygging, avverging, avdekking, etterforsking og straffe-forfølging av IKT-kriminalitet. Det er behov for bedre og mer spesialisert kompetanse, ferdigheter og høyere kvalitet i politiarbeidet. Politiet må ha nødvendig kompetanse til å bekjempe IKT-kriminalitet, behandle elektroniske spor og arbeide på Internett. Politiet trenger bl.a. å øke den generelle etter-forskningskompetansen i forhold til IKT-kriminalitet.

- Studieprogrammene i grunnutdanningen og etter- og videreutdanningen skal i nødvendig grad vektlegge IKT-kriminalitetsbekjempelse, behandling av elektroniske spor og arbeid på Internett.

- IKT-kriminalitet representerer en utfordring i forhold til iretteføring av saker. Det er derfor også behov for en kompetansemessig styrking av påtalemyndigheten.

- Den teknologiske utviklingen og konsekvensene av den krever en intensivert innsats for å utvikle nasjonale kunnskapsorganisasjoner, som raskt kan tilpasse seg til det skiftende landskapet som den raske samfunns- og teknologiutviklingen skaper. Det krever en sterk nasjonal forskningskapasitet, relevante og FoU-baserte utdanninger og effektive kompetanseutviklingstiltak.

Strategi for utvikling av kompetanse på IKT-kriminalitet

- Norge trenger et nasjonalt senter for bekjempelse av IKT-kriminalitet («Cyber Crime Centre») som kan forebygge og etterforske den alvorlige og komplekse IKT-kriminaliteten, arbeide på Internett, behandle elektroniske spor, håndtere de mest omfattende og kompliserte sakene på området, samt drive fag- og metodeutvikling. Betydningen av et slikt høykompetent fagmiljø vil øke i tiden fremover, og det vil ha stor betydning for politiets innsats på området.

- Et nasjonalt senter for bekjempelse av IKT-kriminalitet skal ha fagansvar på området overfor politidistriktene, med ansvar for overordnet kvalitets-sikring. Da sikres en enhetlig bevissikring og straffesaksbehandling. Senteret skal ha en sentral rolle innen bekjempelse av IKT-kriminalitet og et spesielt ansvar for kunnskapsutvikling og utvikling av nye metoder i samarbeid med andre kunnskapsmiljøer. Et nasjonalt senter vil kunne tilpasses et økt samarbeid med våre

nordiske partnere, Europol og Interpol samt styrke samspillet med nasjonale aktører, slik som Nasjonal sikkerhetsmyndighet.

- Politiet må kunne utnytte de elektroniske sporene som er nødvendige i straffesaksbehandlingen. Politiet må også være tilstede på Internett for å forebygge, avverge, avdekke og etterforske saker og også foreta en systematisk «patruljering» på Internett.

- Fagmiljøene i politidistriktene må utvikles slik at de kan håndtere sine oppgaver når det gjelder bekjempelse av IKT-kriminalitet. Oslo politidistrikt kan være pilot for en slik satsing.

- Politihøgskolen (PHS) må legge større vekt på digitalt politiarbeid og bekjempelse av IKT-kriminalitet. I grunnutdanningen er det behov både for en bred skolering som sikrer den generelle evnen til å håndtere digitale utfordringer, uavhengig av hvilken vei utviklingen konkret tar, og spesialkompetanse på de skiftende utfordringene som den løpende bekjempelse av IKT-kriminalitet skaper. PHS må også vektlegge IKT-kriminalitet i videre- og etterutdanningen. Tjenestemenn som ikke har hatt elektronisk bevissikring i utdannelsen bør få styrket sin kompetanse.

- Det er viktig å ha utdanningsinstitusjoner, i tillegg til PHS, som kan tilby utdannelse innen emner som er viktig for bekjempelse av IKT-kriminalitet. Dette krever lange og forutsigbare avtaler med fagmiljøer. Her vil en kombinasjon av politifaglighet og IKT-fagutdanning være en forutsetning for å lykkes. PHS har inngått både samarbeidsavtaler og intensjonsavtaler med Høgskolen på Gjøvik om å styrke utdanningene og forskningen innen områdene IKT-kriminalitetsbekjempelse og IKT-sikkerhet.

- Politi- og statsadvokater har erfaring med håndtering av elektroniske spor. En generell heving av teknologiforståelsen også i påtalemyndig-heten vil være viktig for å bedre forståelsen av og evnen til å formidle digitale bevis. En tilsvarende kompetanseheving for dommere må vurderes.

- Effektiv bekjempelse av IKT-kriminalitet forutsetter relevant forskning. Den raske teknologiske utviklingen gir trussel-aktørene tilgang på stadig nye metoder for å begå kriminalitet. Forskning er nødvendig om ikke sikkerhetsaktørene skal bli akterutseilt. Det må utformes en dynamisk forskningsstrategi med et 5-10 års perspektiv med rom for endringer og tilpasninger i takt med endringer i trusselbildet.

4.3 Kapasitet

Utfordringer

- Den raske teknologiutviklingen, ulike sårbarheter og variasjonen i kriminaliteten tilsier at det er nødvendig å styrke politiets evne til å bekjempe trusler i det digitale rom, både på kort og lengre sikt. IKT-kriminaliteten øker mye både i volum og kompleksitet, hvilket stiller politiet overfor store utfordringer. I dag blir bare et fåtall av anmeldte saker om IKT-kriminalitet etterforsket og straffeforfulgt. Behandlingen av straffesaker om datakriminalitet tar lang tid. Erfaringene fra Det nasjonale statsadvokatembetet (NAST), viser at det er for liten kapasitet til å etterforske IKT-kriminalitet. Grunnen kan være at behovene for etterretning på internett har økt, økt kompleksitet i IKT-kriminalitets-relaterte saker, behov for spesialkompetanse og at behovene for internasjonale nettverk er blitt viktigere.

Strategi for å møte kapasitetsmessig utfordringer

- Det skal etableres et nasjonalt senter for bekjempelse av IKT-kriminalitet, som beskrevet ovenfor under pkt. 4.2. Et slikt senter vil ikke bare styrke politiets kompetanse, men også representere et kapasitetsmessig løft.

- Det skal etableres et pilotprosjekt i Oslo politidistrikt for hvordan politiet kan utvikle sine oppgaver når det gjelder etterforskning og forebygging av IKT-kriminalitet som ikke faller inn under ansvaret til et nasjonalt senter.

- Regjeringen vil øke antall politiutdannede fra i dag 1,7 pr 1 000 innbyggere til 2 pr 1 000 innbyggere. En andel av den generelle styrkingen av bemanningen i norsk politi må brukes til å øke kapasiteten på området IKT-kriminalitet.

4.4 Tilgjengelig teknologi

Utfordringer

- En effektiv innsats mot IKT-kriminalitet er betinget av at politiet har nødvendig teknisk utstyr og programvare. Det eksisterer et gap mellom hva politiet disponerer og hva det er behov for. Den raske, teknologiske utviklingen krever at utstyr og programvare må fornyes oftere enn hva som er tilfellet for mye annet utstyr politiet bruker.

Strategi for å møte teknologiske utfordringer

- Det skal foretas en kartlegging av politiets behov for investeringer i teknologiske løsninger for å styrke og effektivisere innsatsen mot IKT-kriminalitet.

- Det skal etableres et nasjonalt senter for bekjempelse av IKT-kriminalitet som vil være et tungt fagmiljø, som vil bidra til å utvikle nye metoder for å bekjempe IKT-kriminalitet.

- Det teknologiske utstyret og programvarene skal utnyttes på en best mulig måte, slik at det kan drives en kontinuerlig metodeutvikling.

4.5 Nasjonalt og internasjonalt samarbeid

Utfordringer

- IKT-kriminalitet angår en rekke av politiets ansvarsområder. Dels dreier det seg om egenbeskyttelse og sikring mot anslag, og dels dreier det seg om å etterforske og klarlegge ansvarsforhold og hendelsesforløp når et anslag har skjedd. Samhandling mellom mange aktører representerer alltid utfordringer, samtidig som ingen av aktørene alene har de samlede ressurser og kapasiteter til å møte utfordringene.

- IKT-kriminalitet er global i sin natur og internasjonalt samarbeid er avgjørende dersom man skal ha mulighet til å lykkes med effektiv bekjempelse. Det er en debatt om internasjonal IKT-politikk, både innenfor og utenfor etablerte internasjonale organisasjoner. Det internasjonale arbeidet har betydning for politiets evne og muligheter til å bekjempe IKT-kriminalitet. Dette gjelder graden av statlig kontroll over Internett, problemstillinger relatert til personvern, bilaterale og multilaterale avtaler for utveksling av informasjon og internasjonale regler for balansen mellom frihet og sikkerhet i det digitale rom.

- Europarådets konvensjon mot IKT-kriminalitet (Budapest-konvensjonen) er et viktig grunnlag for det internasjonale samarbeidet mot IKT-kriminalitet. Annet internasjonalt samarbeid mot terror og organisert kriminalitet er også relevant. Disse må utvikles i takt med utfordringene på feltet.

- Utenriksdepartementet støtter relevant kapasitetsbygging for å bekjempe IKT-kriminalitet med opphav i utviklingsland (bl.a. lovverk, politiopp-læring, etterforskningskapasitet).

- Politiet møter store utfordringer med å straffeforfølge i andre land IKT-kriminelle som utøver sin kriminelle virksomhet mot Norge, dels fordi IKT-kriminalitet utøves med utstyr/maskinvare som fysisk er plassert på steder som ikke er undergitt norsk jurisdiksjon, eller hvor mulighetene for politisamarbeid og/eller rettslig samarbeid er små eller ikke tilstedeværende, og dels fordi gjerningspersonene fysisk ikke trenger befinne seg i Norge. I mange tilfeller angår sakene mange land, og Norge vil være en del av et større bilde.

- Dagens systemer for samarbeid med andre land er etablert med utgangspunkt i at kriminalitetsbildet så vesentlig annerledes ut, og hvor bistand og bevissikring ikke var tidskritisk på samme måte som tilfellet er innen IKT-kriminalitet. Suverenitetsprinsippet innebærer blant annet at det kun er et lands myndigheter som kan utøve myndighet på eget territorium, noe som i straffesaker medfører at man er nødt til å be om bistand til bevissikring av IKT-bevis som er «lagret» i

utlandet. Rent praktisk betyr dette at det må sendes en rettsanmodning til det landet man ønsker bistand fra. Dette er en omstendelig og tidkrevende prosess, i en situasjon hvor IKT-kriminalitet skjer raskt og med et potensielt stort nedslagsfelt. Flere av de konvensjonene som Norge er tilsluttet, er i til dels liten grad tilpasset de muligheter IKT i løpet av få år har gitt når det gjelder utveksling og oversendelse av informasjon. Disse må derfor videreutvikles.

Strategi for å styrke nasjonalt og internasjonalt samarbeid

- Bekjempelse av IKT-kriminalitet krever samarbeid og kompetansedeling mellom fagmiljøer. Fagfeltet er komplekst, og Norge er et lite land. Politiet må derfor videreutvikle sine faglige kontakter med aktører som NSM med NORCERT for løpende konsultasjoner og kunnskapsdeling.

- Privat sektor er i et samfunnsmessig perspektiv en viktig aktør gjennom de ressurser og den kompetanse den disponerer. Et nærmere samarbeid mellom politiet og privat sektor er både ønsket og nødvendig i innsatsen mot IKT-kriminalitet. Som et ledd i denne tilnærmingen vil Justis- og beredskapsdepartementet regelmessig invitere Næringslivets sikkerhetsråd til møter og dialog med sikte på felles innsats for å bekjempe IKT-kriminalitet.

- For å møte fremtidens utfordringer må det internasjonale samarbeid styrkes. Det er behov for å arbeide internasjonalt. Kripos deltar i dag i enkelte faste samarbeidsfora, samt i ulike grupper innen Europol og Interpol. Dette samarbeidet er etablert med basis i internasjonale avtaler og kan etableres ved behov i forbindelse med aktuelle saker og opp-dukkende behov. Samarbeidet med Europols Cyber Crime Center (EC3) i Haag i Nederland er viktig for Norge. Norge har siden 2001 hatt en samarbeidsavtale med Europol, og samarbeidet med EC3 må utvikles så langt det er mulig innen denne avtalen.

- På grunn av IKT-kriminalitetens karakter er samarbeid med andre land svært sentralt. Det er et stort behov for forenkling og standardisering av samarbeidet med utenlandske myndigheter og tjenestetilbydere. Gjennom økt samarbeid kan man også styrke den generelle sikkerheten og motstandskraften mot IKT-kriminalitet i flere land, og gjennom dette kan man oppdage og håndterer trusler og risikoer på en god måte. Det er viktig å ta internasjonale initiativ på området.

4.6 Et godt og oppdatert lov- og regelverk

Utfordring

- Den raske utviklingen innen IKT-området setter lovverket under press. Det er derfor viktig å ha et lov- og regelverk som er oppdatert særlig sett i forhold til

teknologiutviklingen. Dette gjelder også for det internasjo-nale rammeverket. Straffelovgivningen er et sentralt virkemiddel for å motvirke kriminalitet. Ny straffelov trer i kraft i løpet av 2015. IKT-krimi-nalitet vil da rammes bl.a. av lovens kapittel 21 om vern av informasjon og informasjonsutveksling.

Strategi for å sikre et godt og oppdatert lov- og regelverk

- Det vil foretas en løpende vurdering av behovet for endringer i straffelovgivningen når ny straffelov trer i kraft i løpet av 2015.

5. Tiltak

Tiltak 1 – Foreta en løpende revidering av strategien mot IKT-kriminalitet

Det skal etableres en bredt sammensatt referansegruppe som fortløpende skal gi forslag og innspill om revidering av den overordnede nasjonale strategien for bekjempelse av IKT-kriminalitet. Gruppen skal omfatte både juridisk, politifaglig og IKT-kompetanse.

Ansvarlig: Justis- og beredskapsdepartementet
Frist: 1.8.2015

Tiltak 2 – Utarbeide en særskilt, felles, årlig trusselvurdering for IKT-kriminalitet

Det skal utarbeides en særskilt, felles, årlige trusselvurdering for IKT-kriminalitetsfeltet innen Justis- og beredskapsdepartementets ansvarsområde som skal danne grunnlag for en målrettet politiinnsats.

Ansvarlig: Politidirektoratet
Frist: 1.4.2016

Tiltak 3 – Etablere en sentralisert statistikkrapportering

Det skal etableres en sentralisert statistikkrapportering med hensiktsmessige statistikk-koder for IKT-kriminalitet. I tillegg skal det inkluderes selvrapportering fra fornærmede.

Ansvarlig: Politidirektoratet
Frist: 1.9.2015

Tiltak 4 – Sikre mørketallundersøkelsen

Mørketallsundersøkelsen skal sikres en stabil finansiering.

Ansvarlig: Politidirektoratet
Frist: 1.9.2015

Tiltak 5 – Etablere et nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet

Det skal fremmes et konkret forslag om hvordan det i politiet kan etableres et nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet, herunder hvilke oppgaver som skal legges til et slikt senter, organisatorisk forankring og ressursbehov.

Ansvarlig: Politidirektoratet
Frist: 1.9.2015

Tiltak 6 – Utarbeide en strategi for digital og politifaglig kompetanseheving

Det skal utarbeides en strategi for digital kompetanseheving i politiutdanningen som omfatter grunnutdanningen og etter- og videreutdanningen og som tar utgangspunkt i det arbeid som er gjort ved PHS. Politiet skal ha nødvendig kompetanse til å bekjempe IKT-kriminalitet, behandle elektroniske spor og arbeide på Internett.

Den teknologiske utviklingen på IKT-kriminalitetsområdet gjør det i større grad aktuelt å ansette personer med teknologisk spisskompetanse. Det skal derfor også legges til rette for å gi disse tilstrekkelig politifaglig tilleggsutdanning.

Ansvarlig: Politidirektoratet
Frist: 1.10.2015

Tiltak 7 – Utarbeide en plan for å styrke den digitale kompetansen hos påtalemyndigheten

Det skal utarbeides en plan for hvordan påtalemyndigheten kan bedre forståelsen av og evnen til å formidle digitale bevis.

Ansvarlig: Riksadvokaten i samarbeid med Justis- og beredskapsdepartementet
Frist: 1.10.2015

Tiltak 8 – Etablere et pilotprosjekt i Oslo politidistrikt

Det skal etableres et pilotprosjekt i Oslo politidistrikt for hvordan politiet kan utvikle sine oppgaver i et bredt spekter når det gjelder etterforskning og forebygging av IKT-kriminalitet som ikke faller inn under et nasjonalt senter.

Ansvarlig: Politidirektoratet
Frist: 1.9.2015

Tiltak 9 – Utarbeide en forskningsstrategi for å forebygge og bekjempe IKT-kriminalitet

Det skal utarbeides en dynamisk forskningsstrategi for å forebygge og bekjempe IKT-kriminalitet med et 5 – 10 års perspektiv med rom for endringer og tilpasninger i takt med utviklingen av trusselbildet.

Ansvarlig: Politidirektoratet
Frist: 1.12.2015

Tiltak 10 – Utarbeide en plan for styrking av etterforskningskapasiteten

Det skal utarbeides en plan for hvordan politiets kapasitet til å håndtere flere, større og mer kompliserte saker innen IKT-kriminalitet kan styrkes, herunder hvordan noe av stillingsveksten i politiet kan disponeres for dette formålet.

Ansvarlig: Politidirektoratet
Frist: 1.12.2015

Tiltak 11 – Kartlegge teknologiske løsninger

Det skal foretas en kartlegging av politiets behov for investeringer i teknologiske løsninger for å styrke og effektivisere innsatsen mot IKT-kriminalitet.

Ansvarlig: Politidirektoratet
Frist: 1.10.2015

Tiltak 12 – Styrke nasjonalt samarbeid

Justis- og beredskapsdepartementet skal regelmessig invitere Næringslivets sikkerhetsorganisasjon til møter og dialog med sikte på felles innsats for å bekjempe IKT-kriminalitet

Ansvarlig: Justis- og beredskapsdepartementet
Frist: 1.10.2015

Tiltak 13 – Styrke internasjonalt samarbeid

Det internasjonale samarbeidet for å bekjempe IKT-kriminalitet skal styrkes. Dette gjelder bl.a. deltakelse i og oppfølging av Europarådets arbeid mot IKT-kriminalitet (Budapest-konvensjonen) og det internasjonale politi-samarbeidet i EUs Cyber Crime Center (EC3). Det skal bl.a. vurderes om vårt nåværende avtaleverk i Europol er tilstrekkelig.

Ansvarlig: Justis- og beredskapsdepartementet og Politidirektoratet
Frist: 1.12.2015

Tiltak 14 – Forenkle og standardisere samarbeidet med andre land

For å effektivisere innsatsen mot IKT-kriminalitet skal det foretas en gjennomgang med sikte på å kartlegge mulighetene for å forenkle og standardisere samarbeidet med andre land.

Ansvarlig: Justis- og beredskapsdepartementet
Frist: 1.4.2016

Tiltak 15 – Vurdere behovet for å foreta endringer i straffelovgivningen

Det skal foretas en løpende vurdering av behovet for endringer av straffelovgivningen for at den skal bli et bedre virkemiddel for å bekjempe IKT-kriminalitet.

Ansvarlig: Justis- og beredskapsdepartementet
Frist: 1.7.2016