POLITIET
POLITIDIREKTORATET

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

NATIONAL POLICE DIRECTORATE

Deres referanse:	Vår referanse:	Sted, Dato
15/8216	201504848-16 008	Oslo, 18.03.2016

HØRINGSINNSPILL - DIGITAL SÅRBARHET - SIKKERT SAMFUNN

Det vises til brev fra Justis- og beredskapsdepartementet av 09.12.2015 med anmodning om innspill til høring om utredningen "Digital sårbarhet – sikkert samfunn" (NOU 2015:13). Frist for høringssvar er 15.03.2016. Etter avtale med departementet har Politidirektoratet fått fristen forlenget til 18.03.2016.

Innledning, avgrensing og videre struktur:
Politidirektoratet har forelagt høringen for underliggende politidistrikter og særorgan. Høringsinnspillene følger vedlagt.

Politidirektoratet støtter utvalgets vurderinger av digitale sårbarheter i samfunnet, utfordringer i forbindelse med bekjempelse av IKT-kriminalitet og generelt behov for samarbeid med de ulike sikkerhetsaktører nasjonalt og mellom politimyndigheter på tvers av landegrenser.

For en gjennomgang av utfordringer når det gjelder IKT-kriminalitetsbekjempelse vises til innspill fra Kripos av 01.03.2016 og Oslo politidistrikt av 01.03.2016. Oslo politidistrikt omtaler en rekke eksempler fra sin saksportefølje, som gir et nyttig supplement til utvalgets rapport.

NOU 2015:13 favner bredt. Politidirektoratet har begrenset seg til å kommentere forslag til tiltak som har direkte berøringspunkter med politiet. NOU 2015:13 har ingen enhetlig opplisting av tiltaksforslag, disse er spredt rundt i utredningen. Vi har lagt følgende struktur til grunn for vårt innspill:

Vi kommenterer foreslåtte tiltak i kapittel 21 *Avdekke og håndtere digitale angrep,* punkt 21.11 og kapittel 23 *Tverrsektorielle sårbarhetsreduserende tiltak (*da begrenset til kryptografi, i tråd med vårt forbehold om fortrinnsvis å kommentere punkter som berører politiet). Deretter knyttes noen merknader til ulike deler av rapporten, som vi finner det naturlig å kommentere. Hovedvekt legges på svakheter Politidirektoratet mener foreligger ved utvalgets omtale av roller og ansvar i forbindelse med IKT-krisehåndtering, hvor vi mener politiets rolle undervurderes.

Politidirektoratet

Tlf: 23 36 41 00 | Org. nr.: 982 531 950
Post: Postboks 8051 Dep., 0031 Oslo | Faks: 23 36 42 96 | Giro: 7694.05.02388
Besøk: Fridtjof Nansens vei 14/16 | E-post: politidirektoratet@politiet.no | www.politi.no

Kapittel 21 *Avdekke og håndtere digitale angrep*

21.11.1 Etablere og øve et helhetlig rammeverk for digital hendelseshåndtering

Politidirektoratet støtter forslaget fra utvalget om at Justis- og beredskapsdepartementet etablerer et helhetlig rammeverk for å avklare og tydeliggjøre innsatsen og rolleutøvelsen mellom relevante aktører innen hendelseshåndtering og straffeforfølgning. Se nærmere kommentar om dette under punktet Del IV Tverrsektorielle forhold, kapittel 20 Styring og kriseledelse.

21.11.2 Forbedre den nasjonale operative evnen gjennom samlokalisering

Politidirektoratet støtter forslaget fra utvalgets mindretall om en samlokalisering i tråd med forutsetningen om at politiet har en helt sentral rolle i samfunnssikkerhetssporet. Politidirektoratet mener politiet må være vert for en slik samlokalisering.

Direktoratet støtter mindretallets betraktninger om å etablere en form for felles arena i nybygg hos Kripos for å bidra til mer helhetlig analyse og etterforskning av digitale trusler og hendelser.

Dette forslaget har likhetstrekk med en god samarbeidsmodell i USA, "Pittsburgh-modellen", som anbefales i Politidirektoratets datakrimstrategi[1] utviklet i 2015. Modellen er et samarbeidsforum mellom politiet som vertskap, privat og offentlig sektor og akademia. Samarbeidet legger stor vekt på felles innsats innen forebygging og 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 informasjonsdelingen. Det kan bli nødvendig å vurdere endringer i dagens regler om informasjonsutveksling, opplysningsrett og taushetsplikt.

Politidirektoratet mener mindretallet peker på et tiltak som kan samle ressurser fra privat og offentlig sektor for å få bedre informasjonsdeling, hendelseshåndtering, teknisk analyse og å oppnå stordriftsfordeler. Det vil kunne gi mer nærhet til de fleste digitale hendelser som griper inn i politiets kjerneoppgaver forebygging, etterforskning, påtale og iretteføring. Dette tiltaket bør ikke erstatte, men supplere det eksisterende samarbeidet mellom NSM NorCERT, E-tjenesten og virksomheter som har eget nettverk for hendelser rettet mot rikets sikkerhet. Denne modellen har et sentralisert preg og må ses i sammenheng med en tett kobling til nærpoliti i distriktene og virksomheter.

I likhet med mindretallet mener Politidirektoratet at det burde være mulig å se nærmere på et konsept hvor en etablerer et «Cyber Crime Center» i politiet i nybygg og i det samme bygget tilby arealer utenfor politiets egne virksomhetsarealer som kan samle den nasjonale operative kapasiteten med EOS-miljøet/etterretningssporet. Her må det også legges til rette for at samlokaliseringen omfatter liaisoner fra sektorvise responsmiljøer og sertifiserte leverandører. Det bør i tillegg dimensjoneres en bygningsmasse for at sentrale offentlige og private virksomheter med kritiske samfunnsfunksjoner kan inngå i dette fagmiljøet, enten regelmessig eller ved alvorlige hendelser. Et slikt konsept er fremtidsrettet, ambisiøst og krever betydelig midler, men bør kunne bygges over tid.

[1] Politidirektoratets forslag til Datakrimstrategi: Datakrimstrategien (alle strategier og tiltak) https://www.regjeringen.no/no/dokumenter/datakrimstrategien/id2411804/

Flertallets forslag om at en samlokalisering skal baseres på NSM NorCert som vert for forsvaret, politi og sivile aktører gir etter Politidirektoratets vurdering et for stort spenningsfelt mellom på den ene siden rikets sikkerhet og militær etterretning, og på den annen side åpenhet og informasjonsdeling sett fra et sivilt privat/offentlig ståsted der individ, samfunn og politi skal samarbeide om forebygging og straffeforfølgning.

Flertallets forslag tar utgangspunkt i det miljøet som i dag er etablert ved NSM NorCert der PST og E-tjenesten deltar. Utvalget ber departementet følge opp særlig ovenfor de sivile aktørene i samarbeidet. Politidirektoratet er av den oppfatning at den eksisterende samarbeidsmodellen og videreutvikling av samme modell, ikke klarer å fange opp alle aktører som må være med å bidra, og følgelig ikke gir politiet tilstrekkelig tilgang på informasjon fra sektorene om trusselbildet og hendelseinformasjon for å kunne forebygge og eventuelt iverksette etterforskning. Dagens modell synes ikke å gi politiet en tilstrekkelig tydelig posisjon når det gjelder deltakelse og tilgang på digitale hendelser som er en forutsetning for politiets arbeid i det digitale rom. I dagens ordning har politiet begrenset tilgang på informasjon fra kilder som dekker både enkeltpersoners IKT-kriminalitet, organisert kriminalitet og rikets sikkerhet. Dette er ikke tilfredsstillende.

Dersom et nasjonalt Cyber Crime Center legges til NorCERT vil dette kunne bidra til et skille mellom politiets rolle i cyber og annen kriminalitetsbekjempelse. Dette er uheldig ut fra hensynet til politioperativ innsats for å bekjempe kriminalitet i cyber.

Politidirektoratet understreker at politiets ivaretakelse av digitale hendelser ut fra samfunnssikkerhetsformål der en etablerer bedre samhandling og lokalisering med relevante private/offentlige sikkerhetsaktører sammen med et nasjonalt datakrimsenter, ikke skal utelukke en økt deling av informasjon ut fra et mer begrenset formål knyttet til rikets sikkerhet.

Også Kripos og Oslo politidistrikt støtter mindretallets forslag, det vises til deres innspill.

Se for øvrig kommentar under punkt 21.11.5.

21.11.3 Øke deteksjonsevnen og sammenstille et felles situasjonsbilde

Utvalget mener NSM NorCERT må etablere en teknisk informasjonsdelingsplattform for ugradert informasjon mot virksomheter for å kunne dele informasjon raskt og sikkert. Dette vil kunne være en viktig tjeneste for et tettere privat–offentlig samarbeid.

Politidirektoratet støtter forslaget og mener dette er helt vesentlig også for samarbeidet med politiet. Det er nødvendig at VDI-systemet utvikles videre og at politiet får delta, slik at systemet kan benyttes og tilrettelegges for et felles situasjonsbilde som automatisk deles også med politiet.

21.11.4 Styrke kapasitet og kompetanse knyttet til håndtering av digitale angrep

Politidirektoratet ser positivt på et sivilt-militært samarbeid ved spesielle datahendelser og slutter opp om å utrede en nasjonal cyberreserve for digital hendelseshåndtering. Politiet, Forsvaret og NSM bør delta for å finne ut hvordan en slik cyberreserve kan bygges opp, driftes og organiseres.

21.11.5 Etablere et nasjonalt "Cyber Crime Center"

Politidirektoratet støtter utvalgets vurderinger, som også samsvarer med Justis- og

beredskapsdepartementets forslag, om å opprette et nytt nasjonalt senter i politiet for å forebygge og etterforske kompleks og grenseoverskridende IKT-kriminalitet. Se også kommentar under punkt 21.11.2.

Kripos er i sitt høringsinnspill positive til etableringen av et nasjonalt senter, jf. innspill av 01.03.2016 og tilleggsinnspill av 04.03.2016. Oslo politidistrikt støtter også en slik etablering. Det vises til begge innspill for nærmere omtale av dette.

21.11.6 Sikre sterke fagmiljøer for IKT-kriminalitet i politidistriktene
Utvalget anbefaler at det gjennomføres et stort løft innenfor etter- og videreutdanning for allerede uteksaminerte tjenestemenn og -kvinner. Utvalget mener også at Justis- og beredskapsdepartementet bør gi klare føringer til politidistriktene for å sikre nødvendig tverrfaglig kompetanse i politiet, inkludert sivilt ansatte med teknisk bakgrunn. Det pekes på at politiets arbeid på Internett bør være slik at den åpne tilstedeværelsen, herunder «politi-stasjon og patruljering på nett», skal ligge til det enkelte politidistrikt for å ivareta politiets primæroppgave med å sikre trygghet, lov og orden.

Politidirektoratet støtter utvalgets vurderinger, men presiserer at det ligger til Politidirektoratets ansvar å gi føringer til politidistriktene for å sikre nødvendig tverrfaglig kompetanse i politiet, herunder sivilt ansatte med teknisk bakgrunn. Politidirektoratet sørger for at dette kommer inn i utforming av nærpolitireformen og i det praktiske arbeidet med å bygge sterke fagmiljøer i distriktene.

Politidirektoratet bekrefter at beskrivelsen av mangelfull kapasitet i politiet er dekkende for situasjonen, og støtter utvalgets syn på at Kripos og politidistriktenes fagmiljøer må styrkes betraktelig.

Utredningen peker på at det er uklarheter knyttet til hvilke aktører som skal etterforske. Anmeldelse av digitale angrep skal skje til det lokale politidistriktet – det til tross for at lokale politidistrikter ofte verken har ressurser eller kompetanse til å etterforske IKT-kriminalitet. Her skal nærpolitireformen bidra til at distriktene skal bli i stand til å etterforske vanlig IKT-kriminalitet. Det er et mål med nærpolitireformen å heve kvalitet og effektivitet slik at ulike distrikter og enheter i politiet får en mest mulig lik håndtering av saker slik at det ikke skal ha betydning for utfallet av saken hvilken instans i politiet som etterforsker. Imidlertid vil organisatoriske endringer som følge av nærpolitireformen og sammenslåingen av politidistrikter og større fagmiljøer ikke alene gi den nødvendige kapasitet og kompetanse politiet trenger for å møte fremtidens IKT-kriminalitetsutfordringer. Det må følges opp med ressurser og prioriteringer.

Oslo politidistrikts understreker i sitt høringsinnspill (side 7) viktigheten av at politiets løsning av IKT-kriminalitet i vid forstand foregår i politidistriktene. Kripos berører også dette i sitt innspill av 01.03.2016 (side 5).

21.11.7 Sikre en IKT-infrastruktur til støtte for politiets kriminalitetsbekjempelse
Politidirektoratet støtter utvalgets vurdering av at IKT-situasjonen i politiet er kritisk. Som utvalget påpeker, knytter bekymringen seg til to hovedkomponenter, ineffektiv kriminalitetsbekjempelse og uro for at hele IKT-systemet politiet baserer arbeidet sitt på, ikke har nødvendig robusthet og sikkerhet.

Politiet har et stort og veldokumentert etterslep på IKT-området. Politiets infrastruktur og IKT-løsninger er kritiske for politiets oppgaveløsning og må sikres i henhold til dette.

Utvalget mener at Justis- og beredskapsdepartementet bør iverksette tiltak for å sikre politiet et teknologiløft, med fokus på IKT-ledelse og styring, økt bestillerkompetanse og klare prioriteringer for ressursutnyttelse i et langsiktig perspektiv.

Politiet har iverksatt tiltak i forhold til IKT-ledelse, IKT-styring og bestillerkompetanse. Det er nå behov for å gjennomføre en helt nødvendig modernisering av politiets IKT-infrastruktur som gir sikker og høy tilgjengelighet til politiets IKT-løsninger, og etablering av nye digitale løsninger for å løse samfunnsoppdraget (herunder kriminalitetsbekjempelse) på en bedre måte.

Politidirektoratet understreker behovet for styrking av IKT-infrastrukturen. Dette vil kreve betydelige midler de neste årene. Politiets IKT-infrastruktur har betydelige sårbarheter, noe som utgjør en operativ risiko for politiets virksomhet. Tilstrekkelig robust IKT-infrastruktur er dessuten en forutsetning for politiets samhandling med andre aktører, herunder utveksling av gradert informasjon. En robust IKT-infrastruktur og robuste IKT-løsninger er avgjørende for politiets faktiske kriminalitetsbekjempelse i cyberdomenet.

Politidirektoratet viser til Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet[2] tiltak 11: kartlegge politiets behov for investeringer i teknologiske løsninger for å styrke og effektivisere innsatsen mot IKT-kriminalitet. En rapport som angir resultatet fra første fase i en kartlegging og har forslag til videre oppfølging er sendt departementet.

21.11.8 Sikre balansen mellom personvern og et sikrere samfunn
Politidirektoratet støtter opp om utvalgets syn på at det må være en balanse mellom personvern og sikkerhet, og mellom hensyn til personvern og kriminalitetsbekjempelse.

Politidirektoratet er imidlertid bekymret for at personvernet på noen områder får for sterk vektlegging framfor hensynet til kriminalitetsbekjempelse. I særlig grad gjelder det tilgangen på trafikkdata, og særlig IP-adresser med sletteplikt innen 21 dager. Politidirektoratet mener personvernet har fått for stor vekt ved lagring av IP-adresse for sendere og mottakere av informasjon på internett. Når vi forutsetter at slike IP-adresser ikke gir vesentlig innholdsdata, kan dette sammenliknes med en offentlig telefonkatalog. I en rapport til Samferdselsdepartementet om datalagringsloven av 2011 utarbeidet av professor Hans Petter Graver, UiO og advokat Henning Harborg pekes det på at knytningen mellom IP-adresser og en abonnent er et av de minst inngripende tiltakene i datalagringsdirektivet.

Det vises for øvrig til omtale av personvern i høringsinnspill fra Kripos av 01.03.2016, som Politidirektoratet slutter seg til. Hensett til de spesielle utfordringene bekjempelse av IKT-kriminalitet innebærer, viser Kripos særskilt til viktigheten av at man ikke i iveren etter å "sikre personvernet og hindre et overvåkningssamfunn" får en situasjon hvor det i hovedsak er de kriminelle som gis beskyttelse.

[2] Justisdepartementets strategi for å bekjempe IKT-kriminalitet (Inkludert foreløpige strategier og tiltak i 2015/2016) https://www.regjeringen.no/contentassets/8de0db6aff3e4dd79c92519057af690f/strategi_ikt-kriminalitet.pdf

Oslo politidistrikt omtaler utfordringer knyttet til lagring av IP-adresser på side 3 og 4 i sitt innspill.

Kapittel 23 *Tverrsektorielle sårbarhetsreduserende tiltak*

23.8 *Regulering av kryptografi*

Utvalget konkluderer med at bruk av kryptografi ikke bør reguleres**.** Det pågår en internasjonal diskusjon om hvorvidt bruken av sterk kryptografi bør reguleres. Utvalget mener det ved regulering blir svært vanskelig – kanskje umulig - å ivareta legitime behov for beskyttelse og legitimt behov for avlytting. Begrensninger vil trolig kun ramme norske borgere, virksomheter og myndigheter, og ikke i vesentlig grad hindre uærlige aktørers bruk av kryptografi.

Politidirektoratet mener utvalget legger seg på en for forsiktig linje. På grunn av betydelig økning i bruk av krypteringsprogrammer, gir kommunikasjonskontroll i dag mindre lesbar informasjon til politiet enn tidligere. De moderne krypteringsprogrammene er så kompliserte at meldingen ikke lar seg dekryptere. Den eneste måten å få tilgang til innholdet på er å sikre seg informasjonen *før* den krypteres. Dette har ført til at flere land har åpnet opp for metoden "dataavlesning" ved å plassere et program i datamaskinen som sender opplysninger til politiet. Programmet installeres gjennom et datainnbrudd, og gir politiet opplysninger både om hva som meddeles og hvilke internettadresser som oppsøkes. Politidirektoratet vil i likhet med andre land som Norge samarbeider med, anbefale at dataavlesning innarbeides som en metode med minstegrenser for når metoden skal tillates, og at det følger reglene for bruk av kommunikasjonskontroll. Det vises ellers til tidligere utredninger, bl.a. Metodeutvalget i 2004, der flertallet foreslår innføring av regler for dataavlesning, og NOU 2009:15 der utvalget går inn for å tillate dataavlesning både i etterforskning og i forebyggende øyemed.

Politidirektoratet merker seg at regjeringen nå har lagt frem forslag til endringer i straffeprosesslovens regler om skjulte tvangsmidler[3], herunder at politiet skal gis adgang til bruk av metoden dataavlesning. Bakgrunnen for dette er blant annet at de eksisterende skjulte tvangsmidlene har tapt mye av sin effekt som følge av den teknologiske utviklingen.

Norge må se an den internasjonale utviklingen. I dagens situasjon er kryptert informasjon blitt en kritisk utfordring og stenger for vesentlig informasjonsinnhenting i politiets etterretnings- og etterforskningsarbeid. Nye metoder og hjemler må derfor i økende grad utvikles og tas i bruk for å sikre et effektivt politiarbeid. Det er også behov for samarbeid om å få mest mulig lik lovgivning i land vi naturlig samhandler med. Hvilke virkemidler som kan tas i bruk og hvordan dette er inngripende for personvernet, må vurderes hvis kryptografien blir gjenstand for en regulering.

Det vises til omtale av kryptering i høringsinnspill fra Kripos av 01.03.2016 (fra side 8) og Oslo politidistrikt (fra side 3). Politidirektoratet støtter synspunktene, og viser til følgende kommentar fra Kripos: *"I et kriminalitetsbekjempende perspektiv er det vanskelig å akseptere at kommunikasjon på internett skal ha et sterkere vern mot innsyn og kontroll, enn annen kommunikasjon".*

Øvrige merknader til utredningen:

Del IV Tverrsektorielle forhold, kapittel 20 Styring og kriseledelse

Politidirektoratet mener at rapportens del IV Tverrsektorielle forhold, kapittel 20 *Styring og kriseledelse* er svært viktig, og at politiet burde ha fått omtale som utøver av en viktig

[3] Prop.68 L (2015 - 2016)

samfunnsrolle i digitale kriser og kriseledelse. Også Kripos og Oslo politidistrikt adresserer dette i sine uttalelser.

Under punkt 20.1.5 *Sivilt-militært samarbeid i kriser* er det riktignok nevnt at politiet har en sentral lederrolle i krisesituasjoner og via bistandsinstruksen kan be forsvaret om assistanse. Videre omtales politiets ansvar etter politiloven § 2, § 7 og § 27 i punkt 21.3.3 om håndtering av IKT-hendelser.

Politiet er imidlertid ikke omtalt i nærmere grad, det er kun kort vist til planverket politiets beredskapssystem (PBS) i punkt 20.1.2 om sentral kriseledelse.

Politiet er heller ikke nevnt i kapittel 8.4, der sentrale koordineringsarenaer for IKT-sikkerhet omtales. Her er koordineringsgruppen (CKG) nevnt. Politidirektoratet mener det også burde vært nevnt at politiet ved Kripos gis informasjon en gang i uken hvis det er hendelser som NSM og E-tjenesten mener kan være relevant for politiet. Politiet deltar ikke i analysen av hendelser, og er ikke et fullverdig medlem av gruppen. Politidirektoratet mener politiet svekkes når det gjelder å forebygge og bekjempe IKT-kriminalitet ved ikke å få være en fullverdig deltaker i informasjonsdelingen fra NSM-NorCert om digitale hendelser. Slik informasjonsdeling kan identifisere hvem som står bak en hendelse og hva vedkommendes motiv er.

Vi mener også at informasjon om hendelser blir liggende så lenge at de ikke er egnet til bruk av politiet i forebygging og straffesaksoppfølging.

Den manglende omtalen av politiet i kapittel 8, er trolig årsaken til at politiet heller ikke er nevnt i kapittel 20. Dette er uheldig og indikerer at politiets rolle i den digitale verden er ulik politiets rolle i den fysiske verden, selv om disse er koblet tett sammen og kobles ennå tettere som følge av den raske teknologiutviklingen.

I utredningens del III Sårbarheter i kritiske samfunnsfunksjoner, 11.4 *Beredskap og hendelseshåndtering* omtales Nkom, DSB, NVE, Telenor, Cert funksjoner og beredskapen som Forsvaret bidrar med. Politiet er ikke nevnt. I punkt 11.4.1 *Øvelsesfunn* vises det til den nasjonale tverssektorielle Øvelse IKT i 2008. Her kunne det vært nevnt at politiet deltok i øvelsen i forhold til avverging og etterforskning. Øvelsen avdekket at det er behov for avklaring av ansvar og roller vedrørende viktige beslutninger knyttet til håndtering av slike hendelser.

Politidirektoratet understreker at politiet har en viktig rolle dersom det skulle inntreffe IKT-hendelser som er så omfattende at det får tverrsektorielle samfunnsmessige konsekvenser.

Hendelser i den digitale verden har ofte en annen utstrekning og form enn den man finner i den virkelige/analoge verden. Utstrekningen kan være overveldende. Formen er vanskelig å tolke før den blir kjennbar og rammer den virkelige verden. Et IKT-angrep kan sette viktige samfunnsfunksjoner ut av spill og få store konsekvenser for landets trygghet og sikkerhet. Et datainnbrudd kan medføre at identitetsinformasjon for millioner av mennesker blir stjålet, og at penge- og valutasystemet, produksjon og leveranse av matvarer og transport stopper opp. Dette berører store deler av en befolkning. Online svindel og hackingangrep er bare noen eksempler på digital kriminalitet som daglig prøves ut på internett og som i en målrettet fase kan, hvis forsøkene lykkes, utløse alvorlige hendelser i stor skala. Det begynner i den digitale verden, rammer den virkelige verden raskt og får konsekvenser for mange mennesker.

Det kan diskuteres hvor alvorlig den virkelige verden skal rammes før krisebegrepet benyttes. I dette tilfellet vil det fort kunne kalles en digital krise med følger for den virkelige verden ganske raskt dersom viktige samfunnsfunksjoner rammes. I det øyeblikket hendelsen skjer, er det ingen som aner om det er organisert kriminell aktivitet eller en provokasjon fra en annen statsmakt som sannsynlig benytter andre til å utføre handlingen, eller et terroristangrep. Andre lands erfaringer med digitale varslingssystemer tyder på at majoriteten av digitale hendelser som fanges opp, er forankret i forsøk på kriminell virksomhet og i mindre grad kan knyttes til rikets sikkerhet.

Politidirektoratet peker på at mange offentlige organer deler på ansvaret for å håndtere alvorlige IKT-hendelser. Vi mener det tidvis er dårlig utveksling av informasjon, og noe overlapp og uklare grenser opp mot politiets lovpålagte arbeidsoppgaver i henhold til politiloven. Det er derfor viktig at alvorlige digitale hendelser og mulige konsekvenser i den virkelige verden kan forstås og håndteres av politiet og at håndteringen av slike kriser blir koordinert og ledet riktig med tanke på at mange sektorielle myndigheter og aktører skal ivareta sine delansvar.

En avklaring av myndighetsaktørenes roller er en forutsetning for en effektiv og riktig håndtering av en alvorlig IKT-hendelse. Politidirektoratet ville forventet at utvalget hadde gått i dybden av denne sikkerhetsmessige utfordringen. Utredningens kapittel 8, 20 og 21 bidrar til å videreføre og forsterke uklarheten ytterligere ved at politiet knapt nevnes som en myndighetsaktør.

POD oversendte et skriftlig innspill til utvalget i mai 2015. Utvalget ble her presentert sikkerhetsutfordringen med en manglende avklaring av ansvarsforholdene mellom NSM og politiet. Det ble vist til DSBs ”Nasjonale risikobilde av 2014”, og et scenario som angikk cyberangrep mot Telenors transportnett med en nedetid på fem dager. Skadeomfanget av et slikt scenario krever en umiddelbar nasjonal krisehåndtering. Dette reiser spørsmålet om hvem som har myndigheten til eventuelt å beslutte stenging av infrastrukturen ved et slikt angrep. En slik beslutning vil kunne være avgjørende for å unngå en ytterligere forlenget opprettingstid med et betydelig større skadeomfang både samfunnsøkonomisk og for liv og helse. For en objekteier vil det være naturlig å fatte en avgjørelse som er økonomisk motivert, eksempelvis hva som vil gi minst erstatningskrav fra avtaleparter. NSMs rolle vil være begrenset til å være rådgivende og koordinerende, uten myndighet til å gripe inn. Dersom det forventes at politiet skal ta ansvaret for en helhetlig krisehåndtering, må to forutsetninger innfris: Politiet må gis tilgang til informasjonen fra NSMs NorCERT-funksjon og være til stede for å beslutte avvergende tiltak. Behovet for konfidensialitet, både klausulert informasjon og informasjon fra NSMs samarbeidspartnere, vil bli ivaretatt i det forebyggende sporet. Politiet har en rett og plikt til både å forebygge kriminalitet så vel som å avverge den. Et stedlig samarbeid med NSMs NorCERT funksjon ville skapt forståelse og enighet om hvilke hensyn som må gå foran i det enkelte tilfelle. Dette forutsetter videre en styrking av politiets evne og kapasitet innenfor IKT-kriminalitet.

Politidirektoratet advarer mot å bygge opp strukturer og organisasjoner med ansvarsområder som lever side om side med politiets samfunnsoppgave med å avverge kriminalitet, lede og håndtere kriser i tillegg til etterforskning og påtale, når samhandling er helt påkrevet for å oppnå alle aktørenes formål.

Det er viktig å ta inn over seg at både cyber og den virkelige verden utgjør et felles kriminalitetsbilde med tilhørende avhengigheter. Kriminaliteten med størst samfunnsøkonomisk skadeomfang vil kunne foregå i cyber, og politiet kan ikke holdes utenfor. De sammensatte, sektorovergripende verdikjeder finner vi i alle de kritiske samfunnsfunksjonene denne utredningen omhandler. Dette har betydning for hvordan vi bør forholde oss til både tilsiktede og utilsiktede hendelser. Konsekvensene av en digital hendelse kan ligge i en annen sektor enn hendelsen selv, og vissheten om at en angriper ikke forholder seg til sektorgrensene utfordrer vår evne til å håndtere skarpe situasjoner på en effektiv og hensiktsmessig måte.

Politidirektoratet ser frem til at utvalgets arbeid snarlig følges opp på departementsnivå med en gjennomgang av roller og ansvar for krisehåndtering. Dette må ha en nødvendig forankring slik at et alvorlig IKT-angrep med et nasjonalt skadepotensiale blir håndtert i tråd med prinsipper for nasjonal krisehåndtering, hvor politiet har ansvaret på øvrige kriminalitetsområder.

Det kan avslutningsvis nevnes at Politiets beredskapssystem (PBS) er under revisjon. Herunder vil beredskap i forhold til IKT-hendelser bli ivaretatt.

Del III Sårbarheter i kritiske samfunnsfunksjoner, kapittel 11 Elektronisk kommunikasjon, punkt 11.7.5 Etablere tiltak for å regulere utlevering av trafikkdata til politiet

Utvalget trekker frem at signaliseringsdata fra mobiltelefon i stadig større grad benyttes i etterforskning, og ønsker at denne formålsglidningen (å benytte data til noe annet enn opprinnelig formål) bør utredes, hjemmelsgrunnlaget avklares og at det bør vurderes om det er behov for egen lovregulering av slik data som et særskilt tvangsmiddel (i likhet med varetekt, beslag, ransaking, osv.)

Politidirektoratet mener det vil være uheldig å innføre særhjemler for bevishenting avhengig av type opplysninger. Det finnes i dag knapt en opplysning som opprinnelig er lagret med det formål at den skal tjene som bevis ved en mulig fremtidig etterforsking. Det er helt avgjørende for politiets mulighet for effektiv kriminalitetsbekjempelse at relevante opplysninger kan hentes inn der de er tilgjengelig, uavhengig av hvorfor opplysningene er samlet inn. Straffeprosessens system med generelle regler om utlevering av beslag, gir tilstrekkelig rammer og skranker for en behovsprøvet mulighet for innhenting, undergitt legalitetskontroll. En utvikling i retning av det Lysneutvalget foreslår, vil bryte med et gjennomarbeidet system, og vil virke sterkt begrensende på politiets muligheter for nødvendig bevisinnhenting upåvirket av hvor bevisene til en hver tid finnes. Basert på politiets erfaring med etterforsking av IKT-kriminalitet, mener Politidirektoratet at mangel på etterforskningsmetoder og tilgjengelige sporkilder representerer et stort hinder for effektiv bekjempelse og er et større hinder enn manglende straffebud.

Politidirektoratet mener det i liten grad foregår en formålsutglidning ved bruk av opplysninger om trafikkdata som politiet ber om utlevert. Vi opplever at domstolene gjør en grundig vurdering av anmodningene. Det er imidlertid slik at IKT-kriminalitet og teknologiutviklingen krever ny kunnskap. Oppdatert kompetanse må besittes eller gjøres tilgjengelig for domstolene i komplekse saker, når komplekse anmodninger fra politiet skal vurderes.

For en effektiv kriminalitetsbekjempelse er det viktig at politiet kan innhente opplysninger uavhengig av hvorfor opplysningene er samlet inn. Et ensidig negativt fokus på "formålsutglidning" blir uheldig sett i forhold til politiets arbeid med bevissikring.

De straffeprosessuelle hjemlene anses som dekkende for innhenting av bevis. Politiregisterloven tar også utgangspunkt i at nødvendig hensyn til rettssikkerhet og personvern er innebygget i straffeprosesslovens bestemmelser, og forutsetter at det straffeprosessuelle sporet ivaretar disse hensynene. Politiregisterloven henviser derfor dels til straffeprosessloven, dels inneholder den presiseringer for behandling av opplysninger i straffesaker. Politiregisterforskriften inneholder nærmere regler om behandling av opplysninger i straffesaker.

Politidirektoratet kan i likhet med Kripos ikke se at det er behov for særregulering av innhenting av teledata som eget tvangsmiddel. Kripos omtaler dette på side 7 og 8 i sin høringsuttalelse av 01.03.2016.

Del IV Tverrsektorielle forhold, kapittel 19 Kompetanse, punkt 19.8.1 Etablere en overordnet nasjonal kompetansestrategi innen IKT-samarbeid
Politidirektoratet mener at det er nødvendig med en strategisk satsing på forskning og utdanning for å sikre befolkningens og nasjonens interesser i møte med IKT-trusler.

Vi støtter tiltaket om å etablere en overordnet langsiktig nasjonal kompetansestrategi for IKT-sikkerhet som et samarbeid mellom Justis- og beredskapsdepartementet og Kunnskapsdepartementet. Når det gjelder prioriteringer i en overordnet strategi, støttes det å bygge opp og vedlikeholde tilstrekkelig forskningskapasitet, opprettholde forskningsinnsats på IKT-sikkerhet, øke kapasitet på masterutdanning innen IKT-sikkerhet og opprette øremerkede stipendiatstillinger som kan sikkerhetsklareres. Politidirektoratet vil tilrettelegge for at Politihøgskolen skal styrke sin forskningskapasitet innen digitalt politiarbeid og utnyttelse av elektroniske spor. Politiet vil de nærmeste årene ha behov for et stort antall sivilt personell som er spesialister i å utnytte teknologi i politiets kjerneoppgaver. Disse må rekrutters blant annet gjennom en økt utdanningskapasitet på masterutdanningen innen IKT-sikkerhet.

Politidirektoratet ønsker i tillegg tiltak rettet mot grunnskole og videregående opplæring i særlig grad for å forebygge kriminalitet på internett og gi ungdom en kompetanse på hva som er god atferd på nett og sosiale medier og gjøre dem i stand til å beskytte seg. Politiet vil være åpne for å samarbeide med andre aktører, bl.a. skoleverket, for å utvikle egnet materiell.

Politidirektoratet bidrar til styrking av den nasjonale kompetansen innen IKT-sikkerhet gjennom finansiering av akademiske stillinger. Det gis støtte til at en overordnet kompetansestrategi bør ha et mål om at et minimum av IKT-sikkerhet må inngå i alle IKT-bachelorgrader, og at det må etableres en økt kapasitet på masterutdanning i IKT-sikkerhet. Det utvikles også egne strategier for digital kompetanse og IKT-sikkerhet ved Politihøgskolen som kan inngå i en slik nasjonal kompetansestrategi.

Del IV Tverrsektorielle forhold, Kapittel 21 Avdekke og håndtere digitale angrep
21.3.4 Etterforske
Utvalget peker på at etterforskningspersonell dedikert til arbeid med IKT-kriminalitet primært brukes til sikring av elektroniske spor i «vanlige» straffesaker og ikke til å etterforske IKT–kriminalitet. Rapporten viser til potensialet for endring gjennom nærpolitireformen.

Politidirektoratet peker på at nærpolitireformen skal bidra til å gi økt kapasitet og gjøre politidistriktene i stand til å ha tilstedeværelse på internett og kunne utføre digitalt politiarbeid med bedre kvalitet og effektivitet. Dette skal ivareta en bred, effektiv og hensiktsmessig bruk av digital informasjon i politiarbeidet, herunder etterretning, operativt politiarbeid, forebygging, etterforskning og iretteføring. Etablering av et nasjonalt datakrimsenter ved Kripos vil også styrke politiets evne til å håndtere den mest kompliserte IKT-kriminaliteten og sette felles normer for metode- og verktøybruk.

21.7.1 Utfordringer knyttet til rammefaktorer

Utvalget peker på at dagens system for internasjonal informasjonsutveksling mellom politi på tvers av landegrenser går for tregt. Bekjempelse av IKT-kriminalitet krever ofte internasjonalt samarbeid, men Norge deltar i for liten grad i internasjonale innsatsstyrker rettet mot bekjempelse av IKT kriminalitet.

Politidirektoratet mener politiet og påtalemyndigheten står overfor en rekke, og til dels større, utfordringer på IKT-kriminalitetens område enn på andre kriminalitetsområder, som følge av at ny teknologi kan utføre slik kriminalitet uten landegrenser. Det er prosessuelle utfordringer knyttet til å få tilgang til nødvendige opplysninger fra andre land som kan benyttes som bevis i norske straffesaker, og den teknologiske utviklingen medfører at det også rent praktisk og teknisk blir stadig vanskeligere å få tilgang til opplysninger som kan tjene som bevis. Et forbedret og mer effektivt internasjonalt samarbeid vil derfor være avgjørende for i større grad å lykkes med å forebygge, avdekke og bekjempe denne typen kriminalitet.

Politidirektoratet viser til Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet tiltak 13 og 14, der det arbeides med å gi forslag om hvordan det internasjonale samarbeidet kan styrkes og hvordan samarbeidet med andre land kan forenkles og standardiseres.

21.5.3 Mangelfullt grunnlag for et helhetlig IKT-trusselbilde

Politidirektoratet viser til Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet tiltak 2: utarbeide en særskilt felles, årlig trusselvurdering for IKT-kriminalitet. Kripos vil lede arbeidet med å utarbeide en slik rapport for Justis- og beredskapsdepartementets ansvarsområde i samarbeid med de andre sikkerhetsaktørene. Dette skal gi en felles nasjonal trusselvurdering som grunnlag for en målrettet politiinnsats.

Utvalget konstaterer at det mangler statistikk fra IKT-feltet, og at det derfor er utfordrende å forstå omfang og innhold i trusselbildet. Politidirektoratet viser til Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet tiltak 3: etablere en sentral statistikkrapportering. Relevante STRASAK-koder for IKT-kriminalitet gjennomgås der, og det skal foreslås bedre måter å fange opp anmeldelser som skal inngå i IKT-kriminalitet. Samtidig følges mørketallsundersøkelsen fra Næringslivets sikkerhetsråd opp med finansiering slik at svarprosenten i undersøkelsen kan økes og at det blir lettere å se sammenheng mellom undersøkelsen og politiets database for anmeldelser.

21.6.2 Fragmentert analysekapasitet mellom offentlige og private aktører

Utvalget peker på at i større og/eller flere parallelle digitale angrep opplever flere av virksomhetenes operative miljøer at analysekapasiteten er begrenset og fragmentert. Manglende og forsinkede analyser kan føre til at håndteringen av en sak blir forsinket. I tillegg fører det gjerne til at beslutninger må tas på mangelfullt eller feil grunnlag, noe som igjen kan føre til økte eller ukjente konsekvenser av hendelsen.

Politidirektoratet deler utvalgets bekymring for at analysemiljøene er fragmenterte og begrensede. Resultatet av analyser er viktig for å kunne håndtere digitale angrep, og vi mener det er behov for å styrke analysekapasiteten og utnyttelse av analysekompetansen mellom offentlige og private aktører.

Del IV Tverrsektorielle forhold, Kapittel 23 Tverrsektorielle sårbarhetsreduserende tiltak, punkt 23.3 Styrke Justis- og beredskapsdepartementet på IKT-sikkerhetsområdet
Politidirektoratet slutter seg til utvalgets syn på at Justis- og beredskapsdepartementet bør settes bedre i stand til å gjennomføre sektorovergripende tiltak. Det kan gjøres ved å samle representanter for relevante aktører og sektorer og utvikle et effektivt felles og helhetlig ramme- og virkemiddelapparat.

Del V, Kapittel 24 Økonomiske og administrative konsekvenser
Politidirektoratet ser positivt på at utvalget støtter forslaget om å opprette et nytt nasjonalt senter for å forebygge og etterforske kompleks og grenseoverskridende IKT-kriminalitet. For å kunne iverksette dette forslaget, har Politidirektoratet fremmet oppfølging av tiltak 5 i departementets strategi for å bekjempe IKT-kriminalitet med angivelse av de rammer som senteret bør ha innen oppgaver, kapasitet og ressurstilførsel de nærmeste årene. Det bør også legges til at er det er behov for både en grunnleggende oppgradering av IKT-infrastrukturen i politiet, og et betydelig løft for å styrke politidistriktenes fagmiljøer og kapasitet innen bekjempelse av IKT-kriminalitet og håndtering av elektroniske spor.

Oppsummering av Politidirektoratets viktigste tilbakemeldinger
Det er behov for en gjennomgang av roller og ansvar i forbindelse med IKT-hendelser som er så omfattende at det får tverrsektorielle konsekvenser. Politiet har en sentral rolle i forhold til samfunnssikkerhet.

Direktoratet er av den oppfatning at den nasjonale evnen til å håndtere IKT-hendelser kan forbedres gjennom samlokalisering og etablering av et nasjonalt senter i politiet for å forebygge og etterforske kompleks og grenseoverskridende IKT-kriminalitet.

Det er nødvendig å styrke politiets kapasitet og kompetanse både ved håndtering av digitale angrep og i forhold til generell bekjempelse av IKT-kriminalitet, herunder må det sikres sterke fagmiljøer for IKT i politidistriktene.

Politidirektoratet understreker avslutningsvis behovet for å sikre politiet et teknologiløft i form av utvikling av moderne IKT-løsninger og robust infrastruktur.

Med hilsen

Vidar Refvik
assisterende politidirektør

Kristine Langkaas
seksjonssjef

Vedlegg:
- Innspill fra Kripos av 01.03.2016 og 04.03.2016
- Innspill fra Oslo politidistrikt av 01.03.2016
- Innspill fra Sør-Vest politidistrikt av 23.02.2016

Saksbehandlere:
Rune Erlend Fløisbonn
Politiinspektør
Telefon 916 60 053

Hege Lise Glent
Seniorrådgiver
Telefon 415 38 393