HEDMARK OG OPPLAND
STATSADVOKATEMBETER

TILSYN INNLANDET POLITIDISTRIKT

- Undersøkelse av politiets innsats mot IKT- kriminalitet

– Oppfølging av Riksrevisjonens rapport, Dokument 3:5 (2020-2021)

Innholdsfortegnelse

1 Innledning

I Riksrevisjonens Dokument 3:5 (2020–2021) *Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT* påpekes flere svakheter i politiets evne til å avdekke og oppklare IKT-kriminalitet.

Etter riksadvokatens mål og prioriteringsrundskriv for 2021 skal politiets innsats mot alvorlige dataangrep, datainnbrudd og annen IKT-kriminalitet intensiveres. Denne kriminaliteten er sterkt økende i omfang og kompleksitet, men relativt få lovbrudd straffeforfølges. For å kunne avdekke flere alvorlige straffbare forhold, er det nødvendig å legge til rette for mer samarbeid mellom politidistriktene, Kripos, Økokrim og næringslivet[1].

Riksadvokaten har i styringsdialogen med Hedmark og Oppland statsadvokatembeter våren 2021 bedt om at Riksrevisjonens rapport blir fulgt opp. I riksadvokatens brev som gir føringer for fagledelsen i 2022, bes videre statsadvokatene om å sette seg inn i arbeidet til politidistriktenes enheter for digitalt politiarbeid (DPA)[2].

Formålet med dette tilsynet er å skaffe seg oversikt Innlandet politidistrikts innsats mot IKT-kriminalitet, med særlig fokus på om politidistriktet har tilstrekkelig kapasitet og kompetanse til at etterforskning og iretteføring av IKT-kriminalitet utføres med den kvalitet som forventes. Tilsynet skal legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet.

Begrepet "IKT-kriminalitet" brukes på forskjellige måter i styrende dokumenter og utredninger, og skaper utfordringer for kriminalitetsbekjempelsen. Riksadvokaten har reist spørsmål om begrepsdefinisjonene er egnet for å gjøre riktige analyser av kriminalitetsbekjempelsen på området. Spørsmålet er minst like aktuelt for fagledelsen.

Kriminalitet hvor de straffbare handlinger retter seg mot datasystemer, eller hvor informasjonsteknologi inngår som *midlet til å utføre straffbare handlinger*, utfordrer ikke bare kapasiteten i politiet og påtalemyndigheten. Det utfordrer også kompetansen på alle nivåer, enten det er i politiet eller i påtalemyndigheten.

Behovet for kompetanse innenfor fagfeltene knyttet til IKT-kriminalitet endres i takt med den teknologiske utviklingen. Det samme gjør forståelsen av IKT-kriminalitet som fenomen.

Prioritering av saker som gjelder IKT-kriminalitet utfordres av at utsikten til oppklaring og iretteføring er lav. Politiets prioritering av IKT-kriminalitet vil avhenge av at perspektivet, etterforskningsformålet, antakeligvis må ses i et større perspektiv enn iretteføring av en straffbar handling. Internasjonalt samarbeid og forebygging vil stå sentralt.

[1] Rundskriv nr. 1/2021 side 12
[2] Brev av 27.9.2021, ref. 21/1971/1/OHT002

Det samme gjelder andre saker hvor databevis eller elektroniske spor utgjør informasjonsteknologi er en sentral del av bevisbildet.

2 Sammendrag

2.1 Hovedfunn

Våre hovedfunn kan oppsummeres slik:

- ✓ Avsnitt for digitale vurderes å ha høy kompetanse innenfor sikring av databevis, elektroniske spor, men opplyser å ha et stort behov for kompetanseutvikling.
- ✓ Avsnitt for digitale spor har kompetanse innenfor IKT-kriminalitet i form av datainnbrudd, men har ikke personell med spesialisering innenfor etterforskning av denne type kriminalitet. Kompetansen vurderes som ikke tilstrekkelig til å møte fremtidige forventninger.
- ✓ Antall ansatte ved Avsnitt for digitale spor er uendret siden 2019.
- ✓ Det er fagkontakter i alle driftsenheter og ved alle tjenesteenheter med ett unntak. Fagkontaktene er faglig underlagt Avsnitt for digitale spor, men administrativt underlagt tjenesteenhetsleder.
- ✓ Kompetansen til Fagkontaktene er varierende.
- ✓ Fagkontaktene har som hovedregel rollen i tillegg til andre funksjoner ved egen tjenesteenhet. Kapasiteten til den enkelte kan utfordres av andre tjenesteoppdrag.
- ✓ Påtalejuristenes digitale kompetanse er varierende.
- ✓ Politidistriktet har ikke påtalejurist med særlig fagansvar for IKT-kriminalitet og digitale spor på linje med andre fagområder som for eksempel org.krim, familievold mv.
- ✓ Avsnitt for digitale spor driver kompetanseutvikling innenfor eget avsnitt, overfor fagkontaktene og har planer om kompetanseutvikling for påtalejuristene. Tilbudet kommer i tillegg til tilbudet fra PHS.
- ✓ Politidistriktet er avhengig av at PIT tar en mer sentral rolle for infrastrukturen knyttet til digitalt politiarbeid. Behovet er spilt inn til Politidirektørens nasjonale ledergruppe.
- ✓ Politidistriktet har ikke programvare til etterforskning av kryptovaluta og live-streaming.
- ✓ Samhandlingen med Kripos/NC3 er utfordrende fordi retningslinjer for grensesnittet knyttet til samhandling og kompetanse ikke foreligger.
- ✓ Samhandlingen mellom Avsnitt for digitale spor og driftsenhetene/tjenesteenhetene følger godt etablert praksis og synes å fungere godt.
- ✓ Samhandlingen mellom Avsnitt for digitale spor og påtalejuristene er godt, men preges av noe manglende kompetanse hos juristene.
- ✓ Det er behov for bevisstgjøring om betydningen av bevissikring av digitale spor og betydningen for om/hvordan beviset kan benyttes i retten.

Vi finner særlig grunn til å fremheve Avsnitt for digitale spor sitt arbeid for kompetanseheving blant egne ansatte, fagkontaktene og påtalejuristene. Dette bidrar til økt kompetanse på ulike nivåer og er meget positivt.

Det er også grunn til å fremheve politidistriktets innsats i etterforskningen av dataangrepet mot Østre Toten kommune som illustrerer at politidistriktet har gitt etterforskning av IKT-kriminalitet høy prioritet.

2.2 Forslag til tiltak

Vi vil foreslå at politimesteren vurderer/følger opp følgende tiltak:

- ✓ Mulighet for fagansvarlig påtalejurist innenfor IKT-kriminalitet/digitalt politiarbeid
- ✓ Kompetansehevende tiltak innenfor IKT-kriminalitet/digitalt politiarbeid for påtalejuristene
- ✓ Mulighet for for spesialist innen IKT-kriminalitet
- ✓ Oppmerksomhet mot retningslinjene for grensesnittet mellom NC3 og politidistriktene når disse foreligger
- ✓ Aktiv bruk av distriktets næringslivskontakt for å forebygge alvorlige dataangrep

2.3 Betydningen for statsadvokatenes fagledelse

Hedmark og Oppland statsadvokatembeter gjennomfører årlige samarbeidsmøter med Avsnitt for digitale spor. Møtet inngår som en del av embetets fagledelsesplan. Tilsvarende møter gjennomføres for de øvrige avsnittene under Seksjon for etterforskning.

Møtet er en viktig arena for informasjonsutveksling mellom fagavsnittet og statsadvokatene. Agenda for møtet 13.12.2021 var:

- ✓ Status ved avsnittet – oppgaver og kapasitet
- ✓ Samhandling med GDE'ene
- ✓ Faglig nytt – metoder og muligheter
- ✓ Bevissikring, utarbeidelse av rapporter og bevispresentasjon i retten
- ✓ Saker og særskilte problemstillinger

Det skrives referat fra møtet som sendes politidistriktets ledelse og statsadvokatene. Møtene vurderes å gi god oversikt over avsnittets kapasitet, arbeidsoppgaver og faglige utfordringer.

Videre har sikring og bruk av digitale bevis vært tema på påtalemøtene ved flere anledninger med forskjellige innfallsvinkler. Siste gang var høsten 2021 hvor krav til å opprettholde tilliten til politiets bevissikring ble satt på agendaen. Med utgangspunkt i dette vil fagledelsen i fortsettelsen ha særlig fokus mot bevissikring, utarbeidelse av rapporter (notoritet) og bruk av bevisene i retten.

For å styrke fagledelsen av politiets innsats mot alvorlige dataangrep, datainnbrudd og annen IKT-kriminalitet vil vi ta initiativ til evaluering av etterforskningen i Østre Toten kommune-saken, blant annet med utgangspunkt i funnene i denne rapporten og Riksrevisjonens rapport. Evalueringen er av sentral betydning for læring, identifisering av behov for forbedringer og vil bidra til å heve kompetansen både hos statsadvokatene og i politiet.

En økning av statsadvokatenes fagledelse innenfor disse nokså spesialiserte feltene er krevende. Fagledelsen kan naturligvis ikke rettes mot teknologisk kompetanse, infrastruktur eller programvare. Statsadvokatenes fagledelse må derimot rettes mot *om* politidistriktet har tilstrekkelig kapasitet og kompetanse til at etterforskning og iretteføring av alvorlige dataangrep, datainnbrudd og annen IKT-kriminalitet utføres med den kvalitet og prioritet som forventes.

Fordi riksadvokaten har stilt krav om at politiets innsats mot alvorlige dataangrep, datainnbrudd og annen IKT-kriminalitet skal intensiveres, vil vi prioritere å øke vår egen kompetanse på feltet for å kunne utøve målrettet, fagledelse, tilpasset politidistriktets nødvendige behov for faglig oppfølging.

3 Noen utgangspunkter

3.1 Bakgrunnen for tilsynet

Riksrevisjonen foretok i tiden 2016-2019 undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT. Undersøkelsen ble publisert 2. februar 2021[3].

Riksrevisjonen har arbeidet ut fra følgende problemstillinger i sin undersøkelse[4]:

1. Hvilken oversikt har politiet over IKT-kriminaliteten?
2. Etterforsker og oppklarer politi- og påtalemyndigheten IKT-kriminalitet?
   2.1. Blir IKT-kriminalitet etterforsket?
   2.2. Blir anmeldt IKT-kriminalitet oppklart?
3. Hvilke faktorer hindrer oppklaring av IKT-kriminalitet?
   3.1. Har politi- og påtalemyndigheten tilstrekkelig kapasitet og kompetanse til å avdekke og oppklare IKT-kriminalitet?
   3.2. Hvordan bidrar støttesystemer til å avdekke og oppklare IKT-kriminalitet?
   3.3. Sørger organiseringen og ansvarsdelingen i distriktene og nasjonalt for effektiv avdekking og oppklaring av IKT-kriminalitet?
   3.4. Bruker politiet internasjonalt samarbeid til å avdekke og oppklare IKT-kriminalitet?
4. Hvordan ivaretas styring og oppfølging av politiets innsats mot IKT-kriminalitet?
   4.1. Ivaretar Justis- og beredskapsdepartementet sitt overordnede ansvar for styring og oppfølging av arbeidet med IKT-kriminalitet?
   4.2. Ivaretar Politidirektoratet sitt ansvar for styring og oppfølging av IKT-kriminalitet?

Tre områder er valgt ut i undersøkelsen:

- ✓ internettrelaterte seksuelle overgrep
- ✓ økonomisk IKT-kriminalitet i form av bedragerier og identitetskrenkelser
- ✓ «ren» IKT-kriminalitet i form av datainnbrudd og uberettiget befatning med tilgangsdata

Hovedkonklusjonene i Riksrevisjonens rapporten er:

- ✓ Politiets evne til å avdekke og oppklare IKT-kriminalitet har klare svakheter som samlet sett er alvorlige.
  - Politiet mangler kompetanse innenfor etterforskning av IKT-kriminalitet.
  - Tiltakene for å styrke politiets kapasitet til etterforskning av IKT-kriminalitet holder ikke tritt med utfordringene.
  - Svakheter ved støttesystemer fører til ineffektiv ressursbruk og manglende oppklaring av IKT-kriminalitet.
  - Manglende samordning mellom distrikter gir utfordringer for oppklaring av IKT-kriminalitet.
  - Utfordringer ved internasjonalt samarbeid bidrar til lav oppklaring av IKT-kriminalitet.
- ✓ Politiet mangler oversikt over IKT-kriminalitet.
- ✓ Politiet prioriterer i liten grad etterforskning og oppklaring av ren IKT-kriminalitet.
- ✓ Tips og etterretning om internettrelaterte seksuelle overgrep øker og utfordrer politiets kapasitet.

[3] Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT, Dokument 3:5 (2020-2021)
[4] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 7

- ✓ Politiet mangler kapasitet til å møte utviklingen innenfor økonomisk IKT-kriminalitet.
- ✓ IKT-kriminalitet har i liten grad vært prioritert av Politidirektoratet og Justis- og beredskapsdepartementet.

Deler av Riksrevisjonens kritikk retter seg mot Justis- og beredskapsdepartementet og Politidirektoratet. Rapporten omtaler likevel flere forhold som er av betydning for både prioritering av og kvaliteten i etterforskningen som utføres i politidistriktene. Begge deler ligger innenfor statsadvokatenes fagledelse å følge opp.

Siden det ikke går et skarpt skille mellom det som kan kalles "ren" IKT-kriminalitet og andre former for kriminalitet hvor digitale spor har betydning, kan ikke statsadvokatenes fagledelse uten videre avgrenses til IKT-kriminalitet som sådan.

En viktig del av oppgavene til politidistriktets Avsnitt for digitale spor er knyttet til andre straffbare forhold enn "ren" IKT-kriminalitet. Fagledelsen må derfor også ha for øye politidistriktets behandling av digitale spor med tanke på etterforskningsformålet som fremgår av straffeprosessloven § 226, særlig med tanke på bruk av etterforskningsresultatet i retten.

3.2 Definisjoner – noen utgangspunkter knyttet til prioritering

3.2.1 Begrepet IKT-kriminalitet

Riksrevisjonens utvalg av områder for undersøkelsen viser at selve begrepet "IKT-kriminalitet" favner nokså vidt. I rapporten påpekes det at begrepet "IKT-kriminalitet" brukes i sentrale strategier og rapporter, men forstås ulikt[5]. I det daglige brukes begrepet gjerne både om dataangrep, datainnbrudd og andre straffbare handlinger hvor (bruk av) IKT er et vesentlig eller sentralt element.

Riksrevisjonen har benyttet følgende definisjon i sin undersøkelse[6]:

> IKT-kriminalitet er IKT-relaterte handlinger og hendelser som er kriminalisert etter norsk lov, og dekker i utgangspunktet to innganger til kriminalitet:
>
> - ✓ kriminalitet som retter seg mot datasystemer og teknologi. Eksempler kan være hackerangrep, datainnbrudd, dataangrep, sabotasje, industrispionasje, og blokkering av internett-tjenester. Det er dette som ofte omtales som «ren» datakriminalitet.
>
> - ✓ kriminalitet der vesentlige/sentrale deler av den kriminelle handlingen og hendelsesforløpet skjer ved hjelp av datasystemer, utstyr eller nettverk. Straffbare forhold som tidligere ble begått i det fysiske rom skjer nå via internett. Eksempler kan være kjøp og salg av narkotika, deling av overgrepsmateriale, ID-tyverier, bedragerier og krenkelser av privatlivets fred.

[5] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport kap. 5.1
[6] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 6

I intervju med Riksrevisjonen har riksadvokaten reist spørsmål om hvor godt egnet begrepsdefinisjonen "IKT-kriminalitet" er for å gjøre gode og riktige analyser av kriminalitetsbekjempelsen på området ettersom den omfatter alle lovbrudd hvor det er benyttet IKT-verktøy[7].

Det er en risiko for at det skapes en kunstig avstand mellom IKT-kriminalitet og andre straffbare handlinger, selv om det i mange tilfeller kan være snakk om overtredelser av samme straffebud. Eksempelvis er det voldtekt å tvinge noen til å utføre seksuell omgang med seg selv[8] helt uavhengig av om det har skjedd over nett, eller ved fysisk nærhet. Et enkeltstående tilfelle vil neppe betraktes som IKT-kriminalitet selv om definisjonen ovenfor også omfatter dette. Et annet eksempel er Innlandet politidistrikts sak kalt "OP-Victoria"[9] som gjaldt omfattende finansbedragerier mv. hvor aktiviteten nesten utelukkende har foregått ved bruk av en eller annen form for informasjonsteknologi. Saken ble vurdert som en grov økonomisk straffesak/bedragerisak.

Det er måten det straffbare forholdet er forøvet på – eller rettere sagt *midlet* den straffbare handlingen er forøvet med som forsøkes definert gjennom begrepet IKT-kriminalitet – uten at det nødvendigvis er en egen *kriminalitetsform*. Det er i det hele tatt svært få straffbarhetsområder som defineres ut fra midlet de straffbare handlingene er forøvet med. Vi er derfor enig med riksadvokaten i at det er grunn til å reise spørsmål ved om begrepsdefinisjonen er egnet til å gjøre gode og riktige analyser av kriminalitetsbekjempelsen, jf. ovenfor. Spørsmålet er derfor like aktuelt i fagledelsesperspektivet.

3.2.2 Prioritering av IKT-kriminalitet

Etterforsking av alvorlig IKT-kriminalitet har over tid hørt til kategorien *Sentrale prioriteringer* i riksadvokatens årlige mål- og prioriteringsrundskriv[10].

Riksadvokaten har fremhevet at oppklaring er særlig viktig for kriminelle handlinger som inkluderer bruk av IKT-verktøy eller tjenester eller som er direkte rettet mot teknologi eller datasystemer[11]. Under henvisning til Riksrevisjonens undersøkelse, uttaler riksadvokaten i mål- og prioriteringsrundskrivet for 2021:

> "Politiets innsats mot *alvorlige dataangrep, datainnbrudd* og annen *IKT-kriminalitet* skal intensiveres. Denne kriminaliteten er sterkt økende i omfang og kompleksitet, men relativt få lovbrudd straffeforfølges. For å kunne avdekke flere alvorlige straffbare forhold, er det nødvendig å legge til rette for mer samarbeid mellom politidistriktene, Kripos, Økokrim og næringslivet. Sakene krever høy teknologisk kompetanse. Politiet må rette oppmerksomhet mot sikring og bruk av digitale bevis."

[7] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 22
[8] Straffeloven § 291 bokstav c
[9] Saksnummer hovedsak + saksnummer i tingretten
[10] Se for eksempel rundskriv nr. 1/2021 side 8 og Riksrevisjonen Dokument 3:5 (2020-2021) Rapport side 15
[11] Rundskriv nr. 1/2021 side 4

Sitatet reiser spørsmål knyttet til prioritering og hvor langt etterforskningsplikten rekker, særlig for dataangrep som har sitt utspring fra andre land og som rammer mer eller mindre tilfeldig her i landet.

Politiet vil ofte stå i en vanskelig avveining mellom prioriterte saksområder. Når det kommer til spørsmålet om prioritering av kriminalitetsområder som er sentralt prioritert, har riksadvokaten i Kvalitetsrundskrivet[12] uttalt:

> Ved ressursknapphet kan det være forsvarlig og nødvendig å prioritere innsats mot organiserte kriminelle miljøer som begår alvorlig kriminalitet som tradisjonelt ikke anmeldes, selv om dette i perioder kan lede til at den generelle oppklaringsprosenten synker og saksbehandlingstiden øker ved et politidistrikt.

Etterforskning av alvorlige dataangrep og datainnbrudd, særlig i form av såkalte "PYSA-angrep"[13], er svært krevende. Oppklaringspotensialet er beskjedent og utfordrer både ressurser og kompetansen i et politidistrikt. Det som er typisk for slike angrep er at programvare mer eller mindre tilfeldig søker/skanner etter objekter med sikkerhetshull/-brister i for eksempel brannmurer. Deretter har man tatt seg inn i datasystemene og installert såkalt "PYSA-ransomware" som blant annet krypterer informasjonen i virksomhetens egne servere og datasystemer med krav om løsepenger "ransom" for å låse opp informasjonen. Det kan være mangelfull IKT-sikkerhet, eller skjulte sikkerhetsbrister i datasystemer hos bedrifter eller offentlige virksomheter som gjør disse til ofre for slike dataangrep.

Det må legges til grunn at ikke alle slike angrep anmeldes til politiet. Anmeldelse kan føre til negativ publisitet. En annen årsak kan være at det er en utbredt oppfatning at politiet i liten grad prioriterer og/eller oppklarer slike saker. Enkelte virksomheter vil da heller se seg tjent med å benytte private firmaer som har dette som spesialområde.

IKT-kriminalitet i form av datainnbrudd, dataangrep mv. er svært samfunnsskadelig. Informasjon som er beskyttelsesverdig kan komme på avveie og personer kan bli utsatt for ID-tyverier. Store verdier kan komme på avveie og kostnadene ved å reparere skader/gjenopprette data kan være formidable.

Riksadvokaten har fremhevet at manglende oppklaring av saker som inkluderer bruk av IKT-verktøy eller tjenester, eller som er direkte rettet mot teknologi eller datasystemer, kan gå ut over tilliten og troverdigheten til politiets evne til effektiv kriminalitetsbekjempelse[14].

Det er imidlertid vanskelig å se for seg at politiet vil komme til å ha den kapasiteten det krever for å etterforske alle lovbrudd mot IKT-systemer eller annen kriminalitet med digitale åsteder. Forventningene til politiets innsats mot IKT-kriminalitet er derfor avhengig av hvilket perspektiv man velger for å ha, altså hvilket formål skal etterforskningen skal tjene.

Det er grunn til å reise problemstillingen. Etterforskningen av dataangrepet mot Østre Toten kommune er illustrerende. Dataangrepet er svært omfattende. Det er teknisk komplisert og

[12] Rundskriv nr. 3/2018 kap 4.2.1
[13] Forkortelse for **P**rotect **Y**our **S**ystem **A**migo
[14] Rundskriv nr. 1/2021 Del IV 1.

involverer etterforskning ved innhenting av informasjon fra servere i flere land. I alt 7 personer er knyttet til etterforskningen fra eget distrikt, fra NC3 og fra påtale. Straffesaksansvarlig i GDE Vest har gitt uttrykk for at man har kunnet prioritere etterforskningen høyt fordi man ikke har hatt andre svært alvorlige saker med høyere prioritet. Hvilken intensitet og prioritet etterforskningen kan gis fremover vil avhenge av om det dukker opp nye saker som har samme eller høyere prioritet.

Etter vårt skjønn bør forventningene til politiets innsats ha et videre perspektiv enn utelukkende iretterføring av en straffbar handling. Selv om etterforskning av kriminelle handlinger som er direkte rettet mot teknologi eller datasystemer kan være utfordrende å oppklare og iretteføre overfor de ansvarlige, vil etterforskningen likevel kunne gi gevinster på sikt. Politiet vil bygge kompetanse og bli bedre rustet i kriminalitetsbekjempelsen. Informasjon som innhentes vil kunne være nyttig i et større perspektiv for eksempel gjennom informasjonsutveksling i politiet og gjennom internasjonalt politisamarbeid. Erfaringene fra etterforskningen vil videre kunne benyttes i politiets forebyggende arbeid, for eksempel i samarbeid med Nasjonal sikkerhetsmyndighet.

3.3 Gjennomføring av tilsynet

I brev av 20. oktober 2021 ble Innlandet politidistrikt bedt om å oversende redegjørelse og relevante dokumenter knyttet til:

- ✓ Organiseringen og bemanningen på avsnitt for digitalt politiarbeid, DPA,
- ✓ Organiseringen og bemanningen i GDE'ene med kompetanse innenfor DPA
- ✓ Politidistriktets digitale kompetanse, herunder
  - Sentralt på DPA
  - DPA-kontakter i GDE'ene
  - Påtalejuristene
- ✓ Politidistriktets digitale kapasitet knyttet til IKT-etterforskning, herunder
  - Sentralt DPA
  - DPA-kontakter i GDE'ene
  - Infrastruktur
  - Programvare
- ✓ Politidistriktets vurdering av behov for å styrke kapasitet, herunder
  - Kompetanseutvikling
  - Infrastruktur (internt i distriktet og nasjonalt)
  - Programvare
- ✓ Samhandling/grensedragning med Kripos/NC3
- ✓ Politidistriktets prioritering av IKT-relatert kriminalitet
- ✓ Redegjørelse for saker som har vært særlig utfordrende både teknisk, kapasitetsmessig og eventuelt samhandling med andre etater/organisasjoner.

I samme brev ble politiet orientert om at vi også fokus på politidistriktets behandling av digitale spor med tanke på bruk av etterforskningsresultatet i retten. Det gjaldt både bevissikring, utarbeidelser av rapporter og presentasjon av dette i retten. viktig å få belyst om behandlingen av digitale spor er enhetlig, og hvordan samhandlingen mellom DPA og GDE'ene fungerer.

Innlandet politidistrikt besvarte henvendelsen i rapport av 12. november 2021.

Det ble avholdt møte mellom Innlandet politidistrikt og statsadvokatene 3. desember 2021. I tillegg har statsadvokatene innhentet informasjon fra straffesaksansvarlige ved GDE Øst og GDE Vest og fra tre fagkontakter DPA.

4 Organiseringen av digitalt politiarbeid i Innlandet politidistrikt

En av Riksrevisjonens hovedkonklusjoner er at det er klare svakheter ved politiets evne til å oppklare IKT-kriminalitet, herunder at tiltakene for å styrke politiets kapasitet ikke holder tritt med utviklingen.

I lys av Riksrevisjonens konklusjoner og riksadvokatens formål om å legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet, har vi sett på hvordan Innlandet politidistrikt er organisert.

4.1 Avsnitt for digitale spor

Avsnittet er organisert under Seksjon for etterforskning som igjen hører under Felles enhet for etterretning og etterforskning (FEE).

Avsnittet omfatter til sammen 10 ansatte, inkludert leder, og er fordelt på lokasjonene Hamar, Gjøvik og Lillehammer. Mannskapene består av polititeknikere, etterforskere med spesialisering på elektroniske spor og spesialetterforskere. Stillingen som avsnittsleder er lyst ledig og avsnittsleder vil bli ansatt tidlig i 2022. For tiden fungerer spesialetterforsker Ståle Gulbrandsen som leder. Fungerende leder har kontorsted på Hamar. Kapasiteten har vært redusert siste halvår 2021 grunnet vakanser og sykemeldinger.

Avsnittet har ikke såkalt "sakstrekk" og etterforsker derfor ikke egne saker. Det gir bistand til etterforskningsseksjonene innenfor et vidt spekter innenfor digitale spor uavhengig av om det er kriminalitet rettet mot datasystemer eller andre lovbrudd. Avsnittet samhandler med fagkontaktene ved geografiske driftsenheter. Avsnittet er også kontaktpunkt mot Kripos og NC3.

Innenfor rammen av dette tilsynet er det ikke mulig å foreta verken kvalitative eller kvantitative vurderinger om bemanningen er korrekt. Antall ansatte på Avsnitt for digitale spor er det samme som politidistriktet har hatt siden 2019 som er rapportert inn til Riksrevisjonen[15]. Samtidig må det understrekes at Innlandet politidistrikt den gangen fremsto som nokså godt bemannet sammenlignet med andre politidistrikter. Vi har ikke kjennskap til eventuelle endringer i andre politidistrikter etter 2019.

[15] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 53

4.2 Fagkontakter ved geografiske og funksjonelle driftsenheter

Politidistriktet er organisert i tre geografiske driftsenheter (GDE): Øst, Midt og Vest. Ved tjenesteenhetene er det i alt 16 personer som har rollen som Fagkontakt DPA. For tiden er tre av disse ikke besatt med en i GDE Vest og to i GDE Øst.

Fagkontakter er politiansatte som har fått opplæring i sikring og håndtering av elektroniske spor. Fagkontaktene gir råd om håndtering av elektroniske spor innen den enheten de arbeider, og er faglig kontaktledd mellom egen enhet og enhet for digitalt politiarbeid[16].

Det er opplyst at fagkontaktene er underlagt Avsnitt for digitale spor i faglige spørsmål, mens de administrativt er de underlagt tjenestestedsleder. De færreste fagkontaktene har digitalt politiarbeid som eneste oppgave, eller hovedoppgave. De fleste etterforskerne har rollen som fagkontakt som en tilleggsfunksjon. Flere av fagkontaktene går på integrert liste som ikke bare fører til fravær, men som også innebærer at andre arbeidsoppgaver som knytter seg til vakt- og beredskap kan bli gitt høyere prioritet.

Avsnitt for digitale spor opplever forskjeller i hvordan fagkontaktenes ressurser utnyttes.

Det er ikke utarbeidet egne instrukser for samhandlingen mellom etterforsker og lokal fagkontakt, eller mellom fagkontakt og Avsnitt for digitale spor. Verken avsnittsleder eller de straffesaksansvarlige i GDE'ene har gitt uttrykk for et slikt behov. Det har etablert seg en samarbeidsform som fungerer. Fra straffesaksansvarlige i GDE'ene har vi fått opplyst at man søker å utnytte ressursene på fagkontaktnivået selv om fagkontaktene er lokalisert på forskjellige steder. Det er opplyst at tjenesteenhetene bistår hverandre og at GDE'ene også bistår hverandre.

Vi bemerker at antallet fagkontakter ved tjenesteenhetene er det samme som ved Riksrevisjonens undersøkelse i 2019[17]. Samtidig må det understrekes at Innlandet politidistrikt også her fremsto som godt bemannet sammenlignet med andre politidistrikter. Heller ikke her har vi kjennskap til om det har vært endringer i andre politidistrikter, eller hvordan endringene er.

Kapasiteten til fagkontaktene er først og fremst ikke knyttet til etterforskning av IKT-kriminalitet i form av dataangrep eller andre omfattende saker hvor bruk av informasjonsteknologi står sentralt. Fagkontaktenes rolle er å gi bistand til bevissikring av elektroniske spor i mer ordinære saker.

[16] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 11 fotnote 23
Se også Rammer og retningslinjer for etablering av nye politidistrikt versjon 1.2 (16.7.2017) side 103
[17] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 62, figur 13

4.3 Oppsummering

Så vel Riksrevisjonen som riksadvokaten har pekt på at politiet har kapasitetsutfordringer når det kommer til bekjempelse av IKT-kriminalitet.

Sammen med Avsnitt for digitale spor utgjør fagkontaktene politidistriktets basiskompetanse knyttet til fagfeltet. Det gjelder ikke bare IKT-kriminalitet, men etterforskning som sådan hvor digitale spor kan ha betydning som bevis.

Selv om Avsnitt for digitale spor og fagkontaktene i all hovedsak synes å oppfylle roller og hovedansvar som fremgår av Rammer og Retningslinjer for etablering av nye politidistrikter[18] bør statsadvokaten ha fokus på politidistriktets kapasitet som en del av fagledelsen, ettersom dette kan gi uttrykk for distriktets prioritering av fagfeltet. Det gelder ikke bare Avsnitt for digitale spor, men også fagkontaktene. Riksrevisjonen har pekt på en rekke utfordringer knyttet til bruken av fagkontakter[19]. Deres rolle og samhandling med etterforskere, påtaleansvarlige og Avsnitt for digitale spor vil bli viet oppmerksomhet gjennom fagledelsen.

[18] Rammer og retningslinjer for etablering av nye politidistrikter versjon 1.2 (16.7.2017) side 101-103
[19] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 61 flg. avsnitt 9.2.2

5 Digital kompetanse i Innlandet politidistrikt

En av årsakene til Riksrevisjonens hovedkonklusjoner om klare svakheter ved politiets evne til å oppklare IKT-kriminalitet er at politiet mangler kompetanse innenfor etterforskning av IKT-kriminalitet. Dokument 3:5 (2020-2021) Rapport kapittel 9 beskriver politiets og påtalemyndighetens kompetanse til å oppklare IKT-kriminalitet.

I lys av Riksrevisjonens konklusjoner og riksadvokatens formål om å legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet, har vi bedt Innlandet politidistrikt beskrive distriktets digitale kompetanse.

Utdanning innenfor IKT-kriminalitet og digitalt politiarbeid ved Politihøgskolen som en del av grunnutdanningen, er ikke en del av dette tilsynet. Det bør imidlertid nevnes at digitalt politiarbeid og IKT-kriminalitet er en sentral del av politiutdanningen slik at kompetansen i "førstelinjen" er økende. I tillegg tilbys etter- og videreutdanning innenfor fagfeltet.

5.1 Avsnitt for digitale spor

Den totale digitale kompetansen for Avsnitt for digitale spor fremstår som høy slik vi kan vurdere det. Avsnittet har både teknisk kompetanse og etterforskningskompetanse. Beskrivelsen svarer til Riksrevisjonens kartleggingsundersøkelse blant DPA-ledere. Riksrevisjonen viser til at DPA-lederne anser at de ansatte har grunnleggende/god kompetanse innen de fleste områder, med unntak av forebygging, etterforskning og analyse i datakriminalitetssaker (datainnbrudd, dataskadeverk osv.).

Innlandet politidistrikt har opplyst at Avsnitt for digitale spor ikke har spesialist med særskilt kompetanse på etterforskning av IKT-kriminalitet slik som alvorlige dataangrep mv.

Dataangrepet mot Østre Toten kommune etterforskes ved GDE Vest med to etterforskningsledere: Politifaglig etterforskningsleder med kompetanse som fagkontakt fra lokalt tjenestested, i samarbeid med etterforskningsleder fra Kripos NC3. Avsnitt for digitale spor bistår GDE Vest i etterforskningen. Gjennom analyse av informasjon mottatt blant annet fra utlandet, har avsnittet, gjennom NC3 og internasjonalt politisamarbeid bidratt til at virksomheter utenfor Norge har kunnet beskytte seg mot tilsvarende angrep.

Politidistriktet benytter utdanningsmodulene som tilbys gjennom Politihøgskolen, *Nordic Computer Forensic Investigators,* som er modulbasert utdanninger/kurs på et høyt faglig nivå.

Samtidig beskriver Avsnitt for digitale spor at flere av analysesystemer/-programmer krever programspesifikke utdanninger. Det opplyses at man mangler tilstrekkelig kompetanse/sertifisering og spesialisering innenfor flere av fagfeltene til avsnittet. Det gjelder særlig på analysesystemer hvor kompetanseheving er tidkrevende og kostnadskrevende. Det er beskrevet et etterslep på kompetansen på 5-8 år.

Avsnittet bruker mye tid og ressurser på kompetansebygging internt i politidistriktet. Selv om dette er resurskrevende har man tro på at det skaper fremtidige gevinster.

Avsnittet driver opplæring av fagkontaktene i tillegg til den utdanningen som kan tas på Politihøgskolen. Opplæringen er nettbasert og utviklet av Avsnitt for digitale spor. Opplæringen er nettbasert på plattformen Moodle og består går over 23 kursdager.

Det er beskrevet at manglende dedikert påtale for datakriminalitet og kompetanse er en medvirkende årsak til lengre saksbehandlingstid ved avsnittet. Det arbeides imidlertid med å utvikle en egen opplæringsmodul for påtalejuristene. Målet er å øke politijuristenes "bestillerkompetanse" til fagkontaktene og Avsnitt for digitale spor under etterforskningen og håndteringen av dette under iretteføringen.

Politidistriktet har satt av 400 000 kr til kompetanseheving innenfor digitalt politiarbeid. Midlene vil først og fremst bli benyttet kurs og sertifiseringer innenfor analyseverktøyene som brukes ved Avsnitt for digitale spor. En ser for seg at deler av midlene kan benyttes til kurs og sertifisering innen IKT-kriminalitet. Kompetansehevingen vil foregå i løpet av første halvår 2022.

I tillegg er det bevilget 100 000 kr til kompetanseutvikling/-heving innen IKT-kriminalitet relatert til etterforskningen og påtalebehandlingen av dataangrepet mot Østre Toten kommune.

5.2 Fagkontakter ved tjenesteenhetene

Politidistriktet har opplyst at kompetansen til fagkontaktene varierer. Det er pekt på særlig to faktorer: Erfaring og interesse. Enkelte av fagkontaktene er erfarne og har hatt funksjonen helt siden rollen ble opprettet, mens andre er ferske og er under opplæring.

Fagkontaktens rolle er ikke rettet inn mot IKT-kriminalitet ut over å ha fenomenforståelse. Ved etterforskning av IKT-kriminalitet vil rollen først og fremst være bistand til taktisk etterforskning fremfor teknisk etterforskning.

Riksrevisjonen har vist til faggrupperapporten om datatekniske undersøkelser og internettrelatert etterforskning fra 2019[20] hvor utfordringene ved måten politidistriktene har tatt i bruk fagkontaktrollen for digitalt politiarbeid på, oppsummeres slik:

- ✓ Bruken av rollen fagkontakt varierer fra ett distrikt til et annet.
- ✓ Det er ikke satt krav eller gitt råd om hvilken kompetanse fagkontaktene skal ha.
- ✓ Det er ikke satt krav eller gitt råd om hvilke oppgaver en fagkontakt kan bistå med / utføre.
- ✓ Det er uklarhet rundt hva forskjellen er på en dataetterforsker og en fagkontakt.
- ✓ Dataetterforskeren skal stå for opplæring av fagkontakt, men kompetansekravene til begge roller er like.

Som nevnt i avsnittet ovenfor, er det Avsnitt for digitale spor som forestår utdanningen av fagkontaktene. Politihøgskolens kurs NCFI Core tilbys fagkontaktene, men oppleves som

[20] Politidirektoratet (2019) *Status fagområde datatekniske undersøkelser og internettrelatert etterforskning*, faggrupperapport utarbeidet av en arbeidsgruppe på oppdrag fra Politidirektoratet, datert 9. september 2019.

teknisk utfordrende. Innlandet politidistrikt ved Avsnitt for digitale spor har derfor utviklet en opplæringsmodul i Moodle som går over 23 kursdager. Opplæringen tar sikte på å være målrettet mot oppgaveløsningen innenfor hovedoppgaver og ansvar som følger av rollen som fagkontakt DPA. Opplæringsmodulen vil bli videreført, men er under revidering.

Som følge av dette har Innlandet politidistrikt skilt mellom kompetansekravene til dataetterforsker ved Avsnitt for digitale spor og fagkontakt DPA ved tjenesteenhetene.

Innlandet politidistrikt er ifølge Riksrevisjonen ett av tre politidistrikter hvor Avsnitt for digitale spor kvalitetssikrer fagkontaktenes arbeid.

5.3 Påtalejuristene

I sitt skriftlige svar har Innlandet politidistrikt vist til at distriktet mangler dedikert påtaledd i digitalt politiarbeid. I Rammer og retningslinjer for etablering av nye politidistrikter har Politidirektoratet lagt til grunn at:

> Særskilt avgitt påtalekompetanse for digitalt politiarbeid er avgjørende for å ivareta effektivitet, kvalitet, resultatoppnåelse og rettssikkerhet.

Med "særskilt avgitt påtalekompetanse" menes politiadvokater dedikert til fagfeltet digitalt politiarbeid[21].

Påtalemyndigheten i Innlandet politidistrikt har ingen opplæringstilbud innenfor IKT-kriminalitet tilpasset rollen som påtaleansvarlig eller aktor. Det finnes heller ingen opplæring knyttet til generell forståelse av digitale spor ut over at politijuristene kan benytte Politihøgskolens tilbud.

Politidistriktet har beskrevet at politijuristene er avhengige av kompetansen til spesialister eller fagkontakter for å føre digitale spor som bevis i retten. Enkelte påtalejurister har skaffet seg god kompetanse, men på grunn av stor turn-over har kompetansen blitt redusert. Kompetanseheving beskrives som tidkrevende.

Beskrivelsen samsvarer nokså godt med Riksrevisjonens funn[22].

Det arbeides med å utvikle en egen opplæringsmodul for påtalejuristene for bedre å forstå IKT-kriminalitet og digitale spor. Målet er å øke politijuristenes "bestillerkompetanse" til fagkontaktene og Avsnitt for digitale spor under etterforskningen og håndteringen av dette under iretteføringen.

Ansvaret for kompetanseheving i påtalemyndigheten er delt mellom Politidirektoratet og riksadvokaten for hhv. påtalejuristene og Den høyere påtalemyndighet. Riksrevisjonen har vist

[21] Rammer og retningslinjer for etablering av nye politidistrikter versjon 1.2 (16.7.2017) side 102, og fotnote 26
[22] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 67 avsnitt 9.4.1

til Påtaleanalyseutvalget[23] sin utredning hvor det konkluderes med at dagens kompetansetilbud til statsadvokatene og politijuristene ikke er godt nok[24].

5.4 Oppsummering

Innlandet politidistrikt Avsnitt for digitale spor fremstår etter vår vurdering med høy kompetanse. Avsnittet har vist å ha kompetanse til å foreta etterforskningsskritt innenfor alvorlig IKT-kriminalitet i samarbeid med NC3, selv om avsnittet ikke har spesialist innenfor IKT-kriminalitet. At politidistriktet ikke har spesialist innenfor IKT-kriminalitet gjør samhandlingen med NC3 krevende[25].

Samtidig rapporteres det om etterslep på kompetanseutvikling. Det er satt av midler til kompetanseheving innenfor analyseprogrammer og IKT-kriminalitet.

Vi ser det som svært positivt at Avsnitt for digitale spor driver opplæring av fagkontakter, spisset mot hovedoppgaver og ansvar som følger av rollen som fagkontakt. At det arbeides for en opplæring rettet mot juristene, vurderes som svært positivt og viktig for å styrke kompetansen som etterforskningsledere.

Kompetansen i politiets "førstelinje" vil øke etter hvert som nyutdannede kommer i arbeid. Det er bekymringsfullt at erfaringslæring er den eneste måten for kompetanseheving for politijuristene.

Med utgangspunkt i Riksrevisjonens funn om manglende kompetanse hos så vel politiet og påtalemyndigheten i alle ledd, bør statsadvokatene ha særlig fokus på *om* politidistriktet har tilstrekkelig kompetanse til etterforskning og iretteføring av IKT-kriminalitet og andre saker hvor digitale spor har betydning som bevis.

Vi mener at politidistriktet bør har en eller flere politiadvokater særskilt fagansvar for IKT-kriminalitet og digitale spor på lik linje med det som er etablert for metode, familievold, overgrep mot barn, menneskehandel mv.

[23] NOU 2017: 5 En påtalemyndighet for fremtiden
[24] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 67-68 avsnitt 9.4.2
[25] Se kap. 7 nedenfor

6 Innlandet politidistrikt sin digitale kapasitet knyttet til IKT-etterforskning og vurderinger av behov for å styrke kapasiteten

To ytterligere årsaker til Riksrevisjonens hovedkonklusjoner om klare svakheter ved politiets evne til å oppklare IKT-kriminalitet, er at tiltakene for å styrke politiets kapasitet på etterforskning av IKT-kriminalitet ikke holder tritt med utfordringene og at det er svakheter i støttesystemer som fører til ineffektiv ressursbruk og manglende oppklaring.

I lys av Riksrevisjonens konklusjoner og riksadvokatens formål om å legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet, har vi bedt Innlandet politidistrikt beskrive distriktets digitale kapasitet knyttet til IKT-etterforskning og behovet for å styrke den.

6.1 Avsnitt for digitale spor

Innlandet politidistrikt beskriver sin egen kapasitet som for lav til håndtering av IKT-kriminalitet. Årsakene er sammensatt.

Det pekes på manglende kompetanse som nevnt ovenfor under kapittel 5.1 med blant annet manglende spesialisering innenfor alvorlig datakriminalitet. Videre pekes det på bemanningen som nevnt under kapittel 4.1. Innkomne saker brukes dels til opplæring av personell på avsnittet, noe som går ut over kapasiteten på avsnittet som sådan.

De utfordringene som beskrives må også ses i sammenheng med hvilke forventninger som stilles til politidistriktets kompetanse i de sakene hvor NC3 bistår[26].

Økningen i andre prioriterte sakstyper som for eksempel overgrep mot barn og befatning med overgrepsmateriale utfordrer kapasiteten til avsnittet. Antallet anmeldelser øker og politiet er i større grad i stand til å identifisere personer og/eller nettverk som produserer, dvs. utfører overgrep, for eksempel live-streaming, deling av overgrepsmateriale mv. Særlig fremhevet er tjenestetilbyderes (for eksempel Facebook Snapchat, Kik mv.) sitt fokus på avdekking og anmeldelse av deling av overgrepsmateriale innenfor deres tjenester, de såkalte "NCMEC-sakene"[27].

Avsnitt for digitale spor fremhever også at det er en økning i profittmotivert IKT-kriminalitet som følge av Covid-19-pandemien. Det antas at tendensen vil fortsette og vil fremstå som mer organisert enn tidligere. Teknologi og programvare for å utføre denne type kriminalitet er lettere tilgjengelig, blant annet på "Det mørke nettet".

Det er opplyst at kapasiteten ved Avsnitt for digitale spor utfordres av etterforskningskapasiteten i distriktet for øvrig. Avsnitt for digitale spor bruker tid på oppgaver

[26] Se kap. 7 nedenfor
[27] NCMEC – National Center for Missing Exploited Children, www.missingkids.org

som skulle ligget på etterforskningsseksjonene. For å unngå tap av tid, særlig i fristsaker, blir ofte den etterforskningstaktiske gjennomgangen av beslag gjort ved avsnittet fremfor på etterforskningsseksjonene.

I samtale med en påtaleavsnittsleder og en straffesaksansvarlig fra GDE'ene har vi fått opplyst at man for ofte opplever at det kommer rapporter med ytterligere opplysninger til de rapportene som er utarbeidet når det nærmer seg hovedforhandling. Rapportene revideres av vitnet fra Avsnitt for digitale spor når vitnet forbereder seg til sin egen forklaring. Ofte må det lages tilleggsbevisoppgave til retten.

Fra påtale uttrykkes det at avsnittet fremstår som underdimensjonert. Påtale opplever dessuten å bli lite involvert i diskusjoner om målretting av beslagsgjennomgang, utarbeidelser av rapporter, analyser mv.

6.2 Fagkontakter ved tjenesteenhetene

Det er opplyst at kapasiteten til fagkontaktene er lavere enn ønskelig. Dels er ikke alle funksjonene besatt, dels er funksjonene lagt til operativt personell som går på tjenesteliste. Seksjon for etterforskning, FEE, og Avsnitt for digitale spor opplever at det er variasjoner mellom GDE'ene hvordan funksjonen prioriteres.

Det er videre anført at det har vært frafall og utskifting av fagkontakter. Det er opplyst at det ikke er knyttet noen incentiver til å påta seg rollen som fagkontakt. Opplysningene samsvarer med funn i Riksrevisjonens undersøkelse hvor flere DPA-ledere svarer at fagkontaktrollen er sårbar. Den kommer i tillegg til andre oppgaver og kan være krevende for DPA å følge opp, på grunn av høy gjennomtrekk, manglende økonomiske incentiver, og på grunn av påkrevd opplæring og oppfølging.

Fra påtale får vi opplyst noe av det samme. Rollen som fagkontakt er ofte en tilleggsoppgave. Enkelte har liten erfaring og kan fremstå som usikre i retten.

6.3 Infrastruktur og programvare

Avsnitt for digitale spor har opplyst at infrastruktur for håndtering av større saker som krever samhandling lokalt og nasjonalt er en av de største utfordringene politidistriktet har.

Det arbeides med å implementere DSB[28] i Innlandet. Dette vil forbedre samhandlingen mellom Avsnitt for digitale spor på den ene siden og fagkontakter og etterforskere på den andre. Per nå må disse reise til en av lokasjonene i Hamar, Lillehammer eller Gjøvik for gjennomgang av digitale beslag. Det forventes at DSB er implementert tidlig i 2022.

[28] DSB – Det Sentrale Beslagsnett

Politidistriktet erfarer at PIT ikke har satt av ressurser til å bistå politidistriktene i implementeringen. Implementeringen blir derfor svært ressurskrevende for politidistriktet. Politidistriktet vil løfte problemstillingen opp i Nasjonal ledergruppe.

Avsnitt for digitale spor opplyser at det har vært nødvendig å utvide serverkapasiteten som følge av dataangrepet mot Østre Toten kommune. I tillegg har politidistriktet bevilget midler for å øke den generelle serverkapasiteten ved Avsnitt for digitale spor. Dette forventes å gi raskere behandling av sakene.

Drift, vedlikehold og utvikling av avsnittets systemer gjøres internt på avsnittet. Etter politidistriktets syn er dette et ansvar som bør ligge sentralt hos PIT i tett dialog med Avsnitt for digitale spor.

I svaret fra politidistriktet er det opplyst at det ikke finnes analyseverktøy som er spesialisert for analyse av saker som gjelder IKT-kriminalitet.

Det pekes også på at bruk av kryptovaluta øker. Innlandet politidistrikt har pr. d.d ikke analyseverktøy for kryptovaluta og må hente bistand fra Økokrim, slik som i OP Victoria.

6.4 Politidistriktets forslag for å styrke kapasiteten

6.4.1 Kompetanse

Et gjennomgående trekk ved politidistriktets svar er mangelen på eller utilstrekkelighet hva gjelder kompetanse. Det pekes på behov for spesialisering, særlig innenfor alvorlig datakriminalitet.

Politidistriktet har planer for kompetanseutvikling. Svaret fra politidistriktet knyttet til IKT-kriminalitet og etterforskning av digitale spor forstås slik at planene ikke er tilstrekkelige for akkurat dette feltet. Det pekes på behov for langsiktige planer som er tilstrekkelig fleksible til å møte den raske teknologiske utviklingen innenfor fagfeltet.

For å oppnå en god kompetanseutvikling mener politidistriktet at det er nødvendig med involvering fra flere deler/enheter i distriktet.

- ✓ Avsnitt for digitale spor
- ✓ Felles straffesaksinntak
- ✓ Felles enhet for påtale
- ✓ Avsnitt for økonomisk kriminalitet og miljøkriminalitet
- ✓ Avsnitt for skjult etterforskning og organisert kriminalitet
- ✓ Seksjon for etterretning
- ✓ Felles enhet for forebygging

I svaret fra politidistriktet er det tatt til orde for en faggruppe bestående av representanter fra disse enhetene for å foreta innledende vurderinger og kunne bistå i saker som gjelder IKT-kriminalitet.

I tillegg tas det til orde for etablering av en nasjonal arena – for eksempel forankret hos NC3 – for utveksling av informasjon, særlig for å styrke kompetansen til fagkontaktene.

6.4.2 Infrastruktur og programvare

DSB forventes implementert fra årsskiftet 2021/2022. Dette vil lette arbeidet mellom lokasjonene i Hamar, Lillehammer og Gjøvik. Det vil også lette samhandlingen med tjenesteenhetene, både fagkontakter og etterforskere.

I svaret fra politidistriktet er det imidlertid pekt på behovet for at PIT tar en mer sentral rolle i drift og vedlikehold av systemer innenfor digitalt politiarbeid. Dette strekker seg ut over DSB. Behovet er ikke nødvendigvis relatert til maskinvare ut over det som er nevnt knyttet til serverkapasitet i omfattende saker.

Det vises heller til behov for programvare relatert til kryptovaluta og sikringsverktøy knyttet til deling av overgrepsmateriale, live-streaming mv.

6.5 Oppsummering

Innlandet politidistrikt sin beskrivelse av kapasitetsutfordringene samsvarer med de funn som Riksrevisjonen har gjort. Det vises her til oppsummeringene som er gjort i Riksrevisjonens merknader i kapitlene 2.1.1, 2.1.2 og 2.1.3[29].

Funnene ved dette tilsynet indikerer at Innlandet politidistrikt har de samme kapasitets-, kompetanse- systemutfordringer som Riksrevisjonens rapportdokument, kapitlene 8, 9 og 10[30] har påpekt.

[29] Riksrevisjonen Dok. 3:5 (2020-2021) side 5-8
[30] Riksrevisjonen, Dok. 3:5 (2020-2021) Vedlegg 3 Rapport side 50-75

7 Samhandling/grensedragning med Kripos/NC3

Riksrevisjonen har i kapittel 2.1.4 anset det som alvorlig at politiet ikke har bedre nasjonal samordning og koordinering av politidistriktene[31]. Det er anført at politiet ikke ser saker i sammenheng, og dermed ikke ser alvorlighetsgraden ved store sakskomplekser. Saker kan dermed henlegges på feilaktig grunnlag.

Med utgangspunkt i hovedformålet om å legge grunnlag for større aktivitet på fagledelsessiden rettet mot IKT-kriminalitet anser vi det som mest hensiktsmessig å se på hvordan samhandlingen fungerer med Kripos/NC3.

Nasjonalt cyberkrimsenter, NC3, er organisert som en avdeling i Kripos. NC3 ble offisielt åpnet 25. januar 2019 for å bekjempe IKT-kriminalitet gjennom etterretning, metodeutvikling, forebygging, etterforskning, sikring av digitale spor samt patruljering på nett. Senteret skal sikre en nasjonal, robust kapasitet på bekjempelse av IKT-kriminalitet og internettrelaterte seksuelle overgrep mot barn[32].

I Kontroll- og konstitusjonskomiteens behandling av Riksrevisjonens rapport er det blant annet vist til at Politidirektoratet vil "- *tydeliggjøre grensesnitt mellom Kripos/politiets nasjonale cyberkrimsenter (NC3) og politidistriktene.*"[33]. Fristen er første tertial 2021.

Innlandet politidistrikt har i sin redegjørelse 12.12.2021 uttalt at grensedragningen mot NC3 er utfordrende, blant annet fordi det mangler overordnede føringer for grensesnittet mellom NC3 og politidistriktene. På direkte oppfølgingsspørsmål er man ikke kjent med overordnede føringer.

I praksis handler dette om hvilken kompetanse et politidistrikt minst må besitte for å kunne ha en effektiv samhandling i saker hvor NC3 bistår under etterforskningen. Uten overordnede føringer for grensesnittet mellom politidistriktene på den ene siden og NC3 på den andre, vil det lett kunne føre til et kompetansegap dersom henholdsvis politidistriktene og NC3 utvikler kompetansen i ulik takt.

Innenfor rammene av dette tilsynet, hvor formålet er å legge til rette for større aktivitet på fagledelsessiden innenfor IKT-kriminalitet, har vi vurdert at det ikke er nødvendig å innhente Kripos/NC3 sine synspunkter. Vi vil ta initiativ til evaluering av etterforskningen av dataangrepet mot Østre Toten kommune, hvor flere av de punktene som Riksrevisjonen har pekt på vil bli belyst, herunder samhandlingen med NC3.

Vi forventer dessuten at det vil komme nasjonale føringer slik som bebudet i Kontroll- og konstitusjonskomiteens innstilling.

---

[31] Riksrevisjonen, Dok. 3:5 (2020-2021) side 9
[32] Nasjonalt cyberkrimsenter – Politiet.no
[33] Innst. 260 S (2020-2021) side 10 venstre spalte

8 Innlandet politidistrikts behandling av digitale spor

Det går ikke et skarpt skille mellom det som kan kalles "ren" IKT-kriminalitet og andre former for kriminalitet hvor digitale spor har betydning. Denne delen har ikke vært hovedfokuset i tilsynet, men vi vil likevel bemerke at statsadvokatenes fagledelse i praksis ikke kan avgrenses til IKT-kriminalitet (datakriminalitet). En viktig del av oppgavene til politidistriktets Avsnitt for digitale spor og fagkontaktene er knyttet til andre straffbare forhold hvor digitale spor har betydning som bevis i større eller mindre grad.

Riksadvokaten har – i forbindelse med beskrivelse av en av kvalitetsmarkørene – uttalt at «[f]or å opprettholde nødvendig tillit til etterforskingsarbeidet må det ikke etterlates tvil om bevis er innhentet og oppbevart på en korrekt måte»[34]. Hensynet til bevisets integritet er således bærende for all bevissikring[35].

Vår erfaring er at politiet, herunder påtalejuristene i politiet, har for liten bevissthet knyttet til sikring av data som bevis og dokumentasjon av spor. Eksempelvis er fotografering av skjermbilder fra en telefon feilaktig benevnt som "sikring". Kvaliteten i politiets arbeid i så måte vil ofte kunne måles ut fra om bevissikringen/dokumentasjonen lar seg etterprøve.

Temaet var en av postene i vårt påtalemøte i august 2021 og i professor Inger Marie Sundes foredrag på statsadvokatmøtet i Hamar 2021. professor Sundes utredning til Justis- og beredskapsdepartementet 18.6.2021[36] er også sentral.

8.1 Bevissikring

Innlandet politidistrikt har svart at man gjennom fagkontaktene søker å sikre digitale spor i straffesaker på mest mulig enhetlig måte. Avsnitt for digitale spor mener at bevissikringen har blitt bedre og at bevisstheten rundt korrekt sikringsmetode har blitt bedre. Fagkontaktenes tilgjengelighet skal gjøre det lettere å be om bistand til bevissikring lokalt, eventuelt videre kontakt med Avsnitt for digitale spor.

Det erkjennes imidlertid at det velges lettvinte løsninger som ikke i tilstrekkelig grad sikrer etterprøvbarhet og som i verste fall kan føre til at data går tapt.

8.2 Utarbeidelse av rapporter

Innlandet politidistrikt har pr. i dag ingen felles mal for rapport om sikring eller gjennomgang av digitale spor. Politidistriktet har en mal for gjennomgangsrapport som benyttes av analytikere, men vurderes av Avsnitt for digitale spor som mindre egnet.

---

[34] Riksadvokatens rundskriv nr. 3/2018 kap. 4.11.3
[35] Se for eksempel Inger Marie Sunde, Bevis i straffesaker (2015) side 599 flg.
[36] Inger Marie Sunde, "Effektiv, tillitvekkende og rettssikker behandling av databevis", En straffeprosessuell utredning om ransaking, sikring og beslag i data, avgitt til Justis- og beredskapsdepartementet 18.6.2021.

Avsnittet har som mål i 2022 å utarbeide bedre og mer enhetlige rapporttyper til bruk i politidistriktet:

- ✓ Sikringsrapport – Avsnitt for digitale spor og fagkontakter
- ✓ Gjennomgangsrapport – Avsnitt for digitale spor, fagkontakter og etterforsker
- ✓ Analyserapport – Avsnitt for digitale spor

Formålet er å få en grunnstruktur på rapportene slik at relevant informasjon blir lettere tilgjengelig for etterforskere og påtale samt andre aktører i straffesakskjeden.

8.3 Presentasjon i retten

Den kanskje største utfordringen knyttet til presentasjon av digitale bevis for retten, er å gjøre dette på en tilstrekkelig pedagogisk måte og at rettssikkerheten ivaretas.

Politidistriktet peker på at det er potensial for forbedringer når det gjelder samhandlingen mellom påtaleansvarlig/aktor og etterforsker/fagkontakt/spesialist.

Avsnitt for digitale spor har utviklet en presentasjonsform på video hvor elektronisk kommunikasjon mellom to parter dels leses inn og dels vises i presentasjonen. Presentasjonen imiterer kommunikasjonen slik den vil se ut på en mobiltelefon. Løsningen har vært benyttet i flere saker med gode tilbakemeldinger. Metoden er under stadig videreutvikling.

8.4 Oppsummering

Statsadvokatenes fagledelse har som et av formålene å heve kvaliteten på straffesaksbehandlingen i politiet, jf. riksadvokatens fagledelsesrundskriv[37].

Kravet til kvalitet i straffesaksbehandlingen har vært fulgt opp i samarbeidsmøtene med Avsnitt for digitalt politiarbeid, i påtalemøtene og i fagledelsen for øvrig. Med utgangspunkt i dette vil fagledelsen i fortsettelsen ha særlig fokus mot bevissikring, utarbeidelse av rapporter (notoritet) og bruk av bevisene i retten.

Hedmark og Oppland statsadvokatembeter 7. januar 2022

Iris Øsp Lydsdottir Storås

Thorbjørn Klundseter

[37] Riksadvokatens rundskriv nr. 3/2020