POLITIET

Nordland politidistrikt

Nyhetsbrev fra næringslivskontakten

Nordland politidistrikt

Utgitt: Mai, 2026

Foto politiet

Politiets trusselvurdering for 2026
Politiets trusselvurdering er en årlig offentlig rapport som gir et helhetlig og oppdatert bilde av kriminalitetsutfordringene i samfunnet. Dette nyhetsbrevet bygger i all hovedsak på Politiets trusselvurdering for 2026 og på Nordland politidistrikts trusselvurdering for samme periode, og retter seg i særlig grad mot næringslivet i Nordland.

Kriminaliteten viser en utvikling der organiserte kriminelle profesjonaliserer sin virksomhet. Kriminelle nettverk spesialiserer seg innen ulike former for kriminalitet og kjøper tjenester fra hverandre for å skjerme seg selv og effektivisere virksomheten. Fremmede stater benytter seg også av organiserte kriminelles tjenester, og i tillegg benyttes kriminelle nettverk som stedfortreder for statlige aktører.

Nyhetsbrevet skal bidra til å øke kunnskapen om utviklingen og de utfordringene næringslivet står ovenfor når det gjelder kriminalitet. Denne kunnskapsdelingen vil således bidra til å styrke evnen til å forebygge kriminalitet rettet mot næringslivet i Nordland.

Økonomisk kriminalitet
Økonomisk kriminalitet er en lite synlig kriminalitetsform for omgivelsene, men den tapper statskassen, bedrifter og privatpersoner for enorme summer. Nesten 20 prosent av kommunene og 7 prosent av øvrige virksomheter oppgir i en kartlegging å ha hatt økonomiske tap som følge av slik aktivitet. Det direkte tapet i 2024 ble anslått til å være mellom 43 og 64 milliarder kroner. Straffesaker som går under kategorien økonomisk kriminalitet utgjør 10 prosent av den anmeldte kriminaliteten i 2025.

Hele 85 prosent av den anmeldte økonomiske kriminaliteten er bedragerier, hvor noen gjennom manipulasjon eller løgn får andre til å overføre verdier til seg selv. Bedragerier mot virksomheter kan i enkelte tilfeller komme opp i flere hundre millioner kroner. Økokrim har regnet seg frem til at norske privatpersoner og bedrifter ble bedratt for 2,1 milliarder kroner i 2024.

Næringslivet blir utsatt for ulike former for bedrageri, både av norske og internasjonale aktører. Særlig har det blitt trukket frem at norske finansforetak blir bedratt gjennom organiserte lånebedrageri ved bil- og boliglån som ikke blir tilbakebetalt. Flere norske foretak har blitt bedratt for millionbeløp gjennom direktørbedrageri over e-post eller telefon. Gjerningspersonene har utgitt seg for å være direktør, leverandør, eller en sentral person i selskapet som kan beordre en straksbetaling eller endre kontonummer. Ofte har de fått tilgang på den sentrale personens faktiske e-postadresse og skjuler korrespondansen for vedkommende.

Kunstig intelligens (KI) benyttes i økende grad i bedrageri både i Norge og internasjonalt. Verktøy for å generere kunstig tekst, bilde, lydopptak og video er svært lett tilgjengelig og det krever tilnærmet ingen bakgrunnskunnskap for å bruke. Deepfake-teknologi er bilde, video og lydopptak som har blitt manipulert for å feilaktig fremstille noe som ikke har skjedd. Samtidig blir kvaliteten på innhold som produseres bedre, og det blir stadig vanskeligere å skille mellom autentisk og kunstig innhold. Teknologien er under stadig utvikling og vil kunne kreve avanserte verktøy for å oppdages. KI vil utgjøre en økende trussel innen direktørbedrageri og ande former for bedrageri.

Foto: Kripos, KI-generert.

Grensene mellom den tradisjonelle økonomiske kriminaliteten og annen profittmotivert kriminalitet fortsetter å viskes ut ettersom organiserte kriminelle er mer involvert i økonomisk kriminalitet enn tidligere. Det er store summer å tjene på bedrageri av både statlige og private aktører. Offentlig sektor jobber med å bli mer brukervennlig for publikum, med åpenhet og digitale løsninger. Dette forenkler tilgjengeligheten for publikum, men kan også gjøre det enklere å begå kriminalitet.

Utbytte fra kriminell aktivitet blir i økende grad profesjonelt håndtert. Spesialiserte hvitvaskingsaktører har utviklet en rekke uregulerte finansielle tjenester på utsiden av den tradisjonelle finansnæringen, noe som muliggjør en parallell finansiell underverden for de kriminelle aktørene. Utbyttet tilfaller de kriminelle og kan reinvesteres i den kriminelle økonomien.

Digitale personopplysninger brukes til å begå bedragerier
Årlig blir offentlig sektor, private virksomheter og privatpersoner utsatt for ulike former for bedragerier. I 2025 ble det anmeldt bedragerier med et estimert tap på over to milliarder kroner i Norge. Til sammenligning ble tapene knyttet til bedragerier i hele Norden i 2023 estimert til 828 millioner Euro, tilsvarende om lag ni og en halv milliarder norske kroner. Det reelle tapet er antakelig betraktelig høyere. Profitten fra bedragerier kan som nevnt bidra til å finansiere nye bedragerier, men den kan også brukes også til å finansiere annen kriminell virksomhet.

Cyberkriminalitet
Cyberkriminalitet er en vedvarende trussel mot våre felles verdier og stiller store krav til samfunnets håndtering. Daglig utsettes samfunnet for angrep mot datasystemer eller ondsinnet digital interaksjon som kan ha alvorlige konsekvenser for digitale og fysiske verdier. Antallet slike angrep har økt de siste årene i både Norge og resten av Europa, og utviklingen forventes å fortsette.


Foto: Politiet.

Cyberkriminalitet er ikke lenger et avgrenset fagområde, men et gjennomgående trekk ved store deler av kriminalitetsbildet. Store deler av kriminaliteten skjer i dag i et digitalt økosystem der aktører, verktøy og tjenester henger tett sammen.

Skillet mellom det fysiske og det digitale rom viskes stadig mer ut. Nå kan mange typer kriminalitet foregå uten at offer, utøver eller samarbeidspartnere på noe tidspunkt møtes fysisk. Det siste året har politiet fått økt innsikt i ulike typer nettbaserte kriminelle samfunn. I mange av disse skapes fellesskap med en distinkt indre kultur og grenseforskyvende dynamikk. Medlemmene søker ofte intern status og forsøker å overgå hverandres prestasjoner innenfor den aktuelle kriminelle nisjen. Slike digitale samfunn gir flere aktører mulighet til å utføre kriminalitet de ellers ikke hadde hatt kompetanse eller handlingsrom til. Dette kan for eksempel skje ved at de deler kunnskap og metoder eller leier tjenester og teknisk infrastruktur.

Cyberrettet kriminalitet utføres med stor variasjon. Aktørbildet er sammensatt med et betydelig antall roller basert på ulike praktiske behov i en angrepskjede. Det finnes i dette økosystemet et stort antall uerfarne og mindre kompetente aktører som finner mål og oppnår resultater gjennom lavterskel bruk av blant annet kunstig intelligens og kommersielt tilgjengelige dataverktøy.

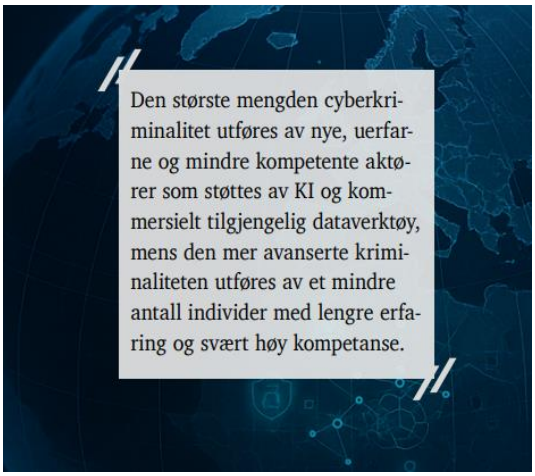

Foto: Kripos, KI-generert.

Men det er også en internasjonal trend at en mindre gruppe profesjonelle cyberkriminelle aktører benytter seg av spesialtilpassede angrep mot nøye utvalgte mål. Det skyldes at et enkelt vellykket angrep mot et verdifullt mål kan gi stor avkastning og rettferdiggjøre en betydelig investering. Et angrep er en prosess som gjerne deles inn i flere faser, der det finnes ulike roller som kan settes ut til uavhengige spesialister. Dette er en form for kriminalitet som handelsvare.

Et datainnbrudd representerer ikke bare en trussel mot den som rammes der og da, men kan også gi grunnlag for fremtidige angrep gjennom misbruk av den stjålne informasjonen. Politiet og andre samarbeidspartnere observerer jevnlig at cyberkriminelle benytter elementer fra tidligere datatyverier som grunnlag for tilgang og målutvelgelse.

Inngangsporten til nøye utvalgte mål er i mange tilfeller såkalte tilgangsmeglere. Dette brukes som en betegnelse for spesialiserte cyberkriminelle som selger forslag til mål og ulovlige tilganger til datasystemer. Når selve utvalget av egnede mål eller ofre gjøres av en kriminell spesialist, kan andre cyberkriminelle aktører fokusere sin innsats på selve angrepsutførelsen.

Fremtidsbildet innen cyberkriminalitet gir grunn til bekymring. Trusselen vurderes som vedvarende, og i økende grad kompleks, både når det gjelder metoder, aktørbilder og konsekvenser. Små gradvise endringer over tid kan gi store utslag når det gjelder cyberkriminalitet. I et stadig mer digitalisert og urolig trusselbilde er samarbeid mellom politi, myndigheter, næringsliv og sivilsamfunn avgjørende for å forebygge denne formen for kriminalitet og for å styrke samfunnets samlede motstandskraft.

NÆRINGSLIVSKONTAKTEN I NORDLAND

Næringslivskontakten i Nordland skal arbeide med å forebygge og redusere arbeidsmarkeds-kriminalitet og kriminalitet rettet mot næringslivet.

Næringslivskontakten er politidistriktets hovedkontakt med næringslivet utenom straffesakssporet, og skal gi råd og videreformidle henvendelser til rett instans.
Funksjonen skal sørge for et godt lokalt samarbeid mellom politiet, næringslivet, sikkerhetsmyndigheter og andre aktører i det sivile samfunn. Dette vil bidra til både proaktive og treffsikre tiltak i næringslivet og hos andre private aktører, og til en helhetlig og kunnskapsbasert kriminalitetsbekjempelse i politiet.

Håvard Fjærli er Næringslivskontakten i Nordland politidistrikt. Han kan kontaktes på:
Tlf. 918 83 382
E-mail: havard.fjarli@politiet.no

Kilder:

Politiets trusselvurdering for 2026.
Nordland politidistrikts trusselvurdering for 2026.
PSTs Nasjonale trusselvurdering for 2026.
NSM: Risiko 2026.
Kripos: Cyberkriminalitet 2026.
Økokrim: Årlig Esum 2025.