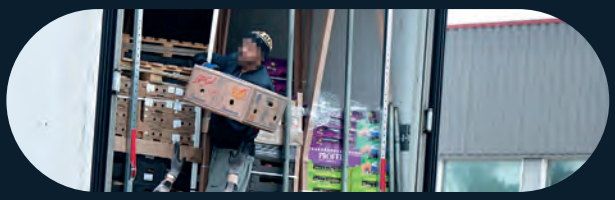
POLITIET



POLITIETS

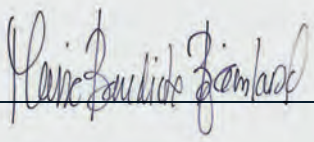
TRUSSELVURDERING 2024

FORORD

Trygghet for samfunnet og innbyggerne er kjernen i politiets samfunnsoppdrag. I en tid hvor skillene mellom samfunnssikkerhet og statssikkerhet er i ferd med å viskes ut, har politiet et ansvar for å kommunisere til politiske myndigheter og andre sentrale samfunnsaktører hvilke trusler vi kjenner til som truer eller kan true våre felles samfunnsverdier. Politiets trusselvurdering er et viktig bidrag til nettopp dette.

En rekke utviklingstrekk i samfunnet gjør ivaretagelsen av politiets samfunnsoppdrag stadig mer krevende og vi er avhengig av et godt samarbeid med andre aktører for å forebygge kriminalitet og ivareta samfunnets trygghet og sikkerhet. I tillegg blir fremtidens utfordrings- og trusselbilde trolig mer komplekst og omfattende enn i dag. Vi må forvente at kriser i større grad skjer samtidig, at de forsterker hverandre og at de treffer på tvers av sektorer. I krevende tider er prioritering nødvendig. Politiets trusselvurdering bidrar til økt kunnskap og blir et viktig grunnlag for felles prioritering og innsats mot alvorlig kriminalitet i året som kommer.

Marie Benedicte Bjørnland
politidirektør



INNHOLD

01 INNLEDNING

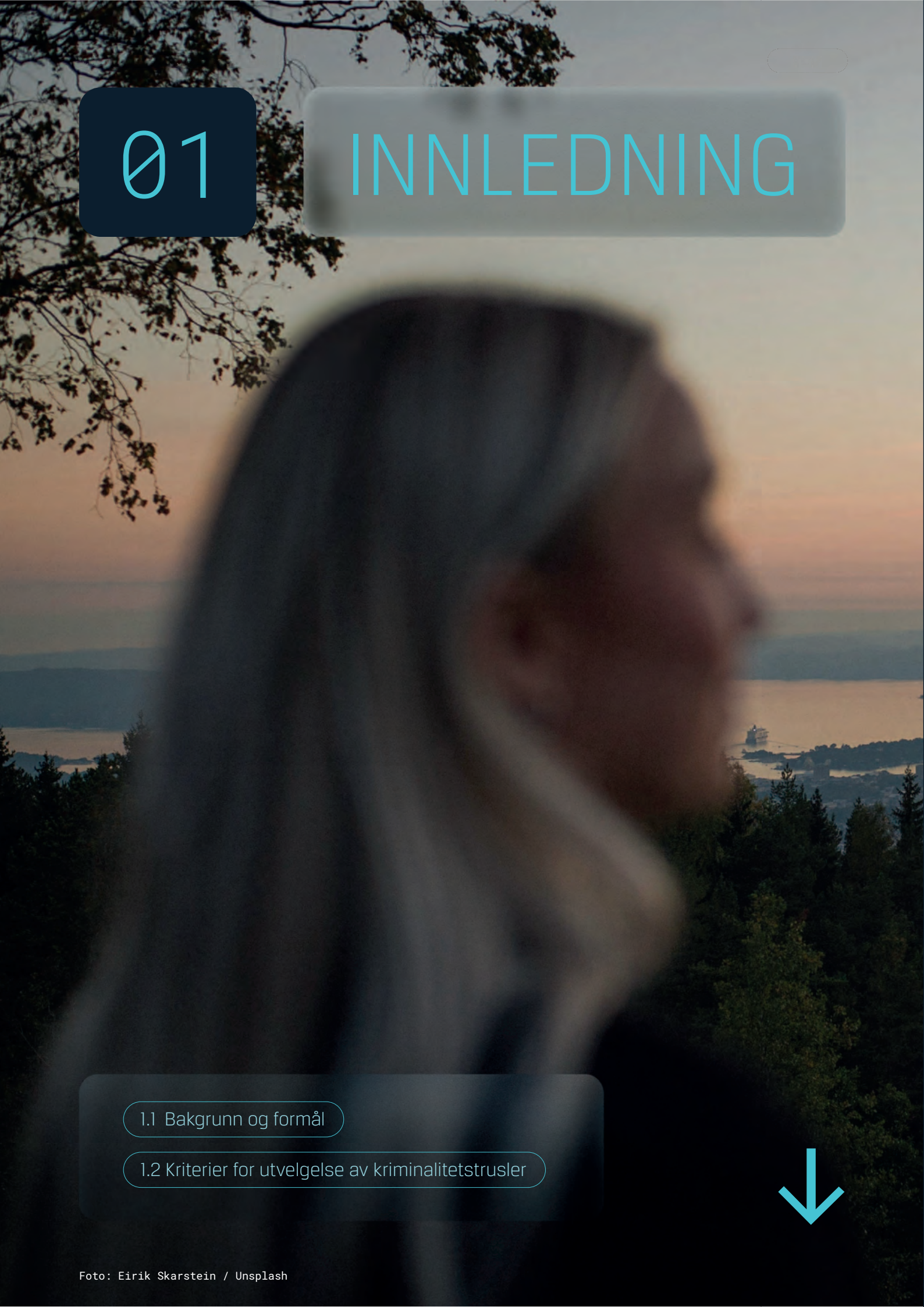


Foto: Eirik Skarstein / Unsplash

1.1

BAKGRUNN OG FORMÅL

Politiets trusselvurdering 2024 presenterer et utvalg alvorlige kriminalitetstrusler som på ulike måter truer våre felles samfunnsverdier, og som vurderes som særlig utfordrende i året som kommer. Formålet med trusselvurderingen er å bidra til en felles forståelse for det trusselbildet samfunnet står overfor, og danne grunnlag for forebyggende samhandling med private og offentlige aktører.

Trusselvurderingen er utarbeidet på bestilling fra Politidirektoratet. Den bygger på etterretning fra politidistrikt og særorgan samt rapporter fra nasjonale og internasjonale aktører både i og utenfor politiet. Analytikere fra Kripos, Økokrim, Politiets utlendingsenhet og Nasjonalt ID-senter har bidratt inn i utarbeidelsen av trusselvurderingen.

Politiets trusselvurdering 2024 føyer seg inn i rekken av tidligere års trusselvurderinger som er utarbeidet av Kripos på vegne av norsk politi. Årets trusselvurdering skiller seg imidlertid fra tidligere utgivelser, ved at den i all hovedsak fokuserer på trusler mot *samfunnet som helhet*. En av grunnene til dette er politiets bekymring for at organiserte kriminelle nettverk som er etablert i Europa, skal etablere seg i Norge på en slik måte at det kan true sentrale samfunnsinstitusjoner. En annen grunn er den endrede sikkerhetspolitiske situasjonen i Europa. I en tid hvor skillene mellom samfunnssikkerhet og statssikkerhet viskes ut, har politiet et ansvar for å kommunisere til politiske myndigheter og andre sentrale samfunnsaktører hvilke trusler vi kjenner til som truer eller kan true våre felles samfunnsverdier.

Ulikt tidligere utgitte utgaver av Politiets trusselvurdering, er ikke prediksjonene i rapporten beskrevet med bruk av sannsynlighetsord. Fremtidsrettede vurderinger er i stedet gjort rede for i forklarende tekst. Formålet med denne endringen er å bidra til en enklere og mer forståelig kommunikasjon av kriminalitetsbildet i Norge.

Rapportens oppbygning

Trusselvurderingen er delt inn i tre hoveddeler. I denne første delen gjøres det rede for formål, bakgrunn og avgrensning. Del 2 omhandler overordnet utvikling på noen sentrale kriminalitetsområder, og gir en beskrivelse av sentrale drivkrefter som kan påvirke kriminalitetsbildet i året som kommer. I del 3 presenteres et utvalg kriminalitetstrusler som på ulike måter truer våre felles samfunnsverdier. Kriminalitetstruslene er ikke rangert i prioritert rekkefølge.

1.2

KRITERIER FOR UTVELGELSE AV KRIMINALITETSTRUSLER

Kriteriet for utvelgelsen av de særskilte kriminalitetstruslene i del 3 er at de utgjør en trussel mot samfunnet som helhet. I årets trusselvurdering vektlegges kriminalitet som truer den *alminnelige tryggheten, økonomiske verdier, grunnleggende samfunnsstrukturer* og *kritisk infrastruktur og samfunnsfunksjoner*.

Trusler mot den alminnelige tryggheten forstås som kriminalitetstrusler som påvirker enkeltpersoners ferdsel i det offentlige rom, aktivitet i det digitale rom eller deltagelse i den offentlige debatten.

Trusler mot økonomiske verdier forstås som kriminalitetstrusler som medfører direkte skader og økonomisk tap, inkludert samfunnsøkonomiske tap ved unndratt beskatning, konkurransevridning i samfunnet og utkonkurrering av virksomheter.

Trusler mot grunnleggende samfunnsstrukturer forstås som kriminalitetstrusler som undergraver eller utnytter grunnleggende samfunnsstrukturer, som et rettferdig arbeidsmarked og næringsliv, rettssystemet og demokratiske prinsipper.

Trusler mot kritisk infrastruktur og samfunnsfunksjoner forstås som kriminalitetstrusler som skader eller hindrer kritisk infrastruktur og samfunnsfunksjoner. Truslene kan påvirke statens evne til å opprettholde basistjenester innen helse og omsorg, strøm, vann og finansielle tjenester.

Fokuset på kriminalitetstrusler som rammer våre felles samfunnsverdier, innebærer at trusler som i all hovedsak rammer enkeltpersoner, ikke inkluderes i årets trusselvurdering. Unntaket er tilfeller der kriminaliteten skjer i *svært stort omfang*, og der den derfor vurderes som en større, samlet samfunnstrussel. Dette gjelder for eksempel kriminalitet som omhandler barn som utsettes for seksuallovbrudd via digitale plattformer, eller bedragerier der omfanget er så stort at det grenser til å være et problem for samfunnssikkerheten.

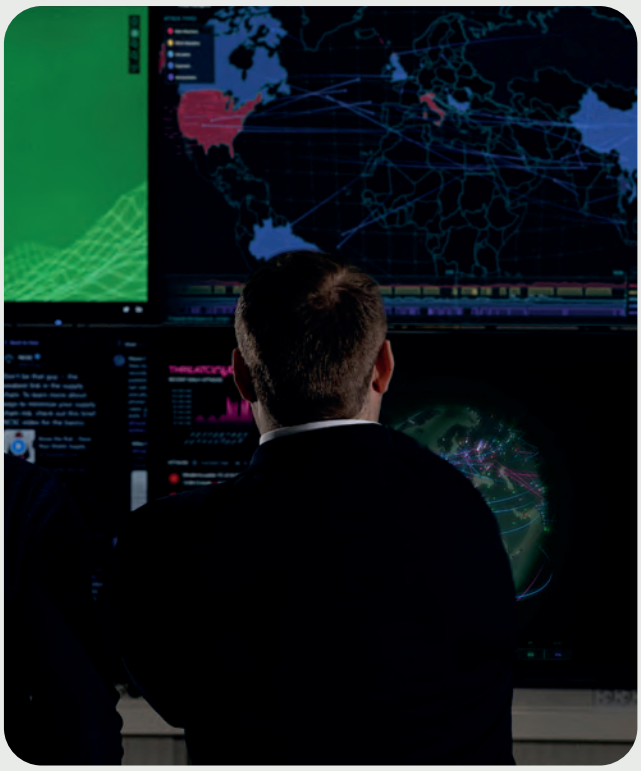


Foto: Politiet

02 ENDRINGER I KRIMINALITETSBILDET

Endringer i kriminalitetsbildet i Norge kommer til uttrykk både i analyser av den registrerte kriminaliteten og i politiets beskrivelser og vurderinger av ulike kriminalitets-trusler som rammer samfunnet.

I denne delen av politiets trusselvurdering ser vi innledningsvis på utviklingen i den registrerte kriminaliteten i Norge, basert på politiets straffesakstall per 31.12.23. Deretter presenteres overordnede vurderinger av samfunnstrusler innenfor organisert kriminalitet, cyber-kriminalitet og økonomisk kriminalitet.

Fordi samfunnet er i stadig endring, vil det alltid være knyttet usikkerhet til slike vurderinger. Avslutningsvis ser vi derfor nærmere på hvilke drivkrefter som vil kunne påvirke kriminaliteten i det kommende året. I det sistnevnte arbeidet har vi tatt utgangspunkt i det analytiske rammeverket PESTEL, som kan brukes til å identifisere og forstå politiske, økonomiske, sosiale, teknologiske, miljømessige og juridiske faktorer som kan påvirke kriminalitetsbildet.

Foto: Politiet

2.1

OVERORDNET UTVIKLING I REGISTRERT KRIMINALITET

Antall registrerte straffesaker kan gi en indikasjon på kriminalitetsbildet i Norge. Forekomst og variasjoner i den registrerte kriminaliteten påvirkes imidlertid av anmeldelsestilbøyelighet, endring i registreringspraksis og av politiets egen innsats og prioriteringer. I tillegg kan endringer i den registrerte kriminaliteten de siste årene knyttes til konsekvenser av smitteverntiltak under pandemien. Dette gjelder særlig for vinnings- og voldslovbrudd.

Den nedadgående trenden i antall registrerte saker siden 2016, ser ut til å ha snudd de siste to årene. Antallet saker i 2023 er likevel lavere enn i 2016. Vinnings- og trafikklovbrudd er kategoriene med flest anmeldte saker. Når det gjelder de ulike kriminalitetskategoriene, ser vi at antallet registrerte saker innenfor voldskriminalitet, økonomi, skadeverk og vinning var det høyeste i 2023, målt opp mot perioden 2016–2023. For vinnings- og voldslovbrudd betyr utviklingen at nedgangen man så under pandemien, er mer enn reversert.

Norge har få drap sammenlignet med flere andre land, og antallet drap har de siste ti årene holdt seg relativt stabilt. I 2023 var antallet drap imidlertid det høyeste siden 2013, med 38 ofre.[1] 17 av ofrene ble drept av en nåværende eller tidligere partner eller kjæreste. Totalt sett utgjør dette 45 prosent av alle ofrene i 2023, noe som er det nest høyeste i siste tiårsperiode. Ingen av drapene i 2023 ser ut til å være drevet frem av konfliktlinjer i kriminelle nettverk.

Når det gjelder seksuallovbrudd, omfatter denne kriminalitetskategorien både fysiske seksuelle overgrep og overgrep begått over internett, så vel som besittelse av overgrepsmateriale. Overgrep mot mindreårige utgjør en betydelig andel av sakene. Disse overgrepene er ofte digitale og kan inngå i store sakskomplekser.

Antallet registrerte seksuallovbrudd kan ha relativt stor variasjon fra år til år. Seksuallovbrudd er en kriminalitetstype der anmeldelsestilbøyeligheten er lavere enn i andre saker, overgrep blir ofte anmeldt lang tid etter gjerningstidspunktet, og politiets innsats kan være avgjørende for å avdekke saker. Disse faktorene fører til at antallet registrerte seksuallovbrudd kun delvis beskriver nåsituasjonen.

Innenfor narkotikakriminalitet har antallet registrerte saker blitt kraftig redusert de siste årene, og halvert sammenlignet med 2016. Politiet ser likevel med bekymring på tall fra Folkehelseinstituttet som indikerer at dobbelt så mange unge mellom 16 og 30 år oppgir å ha brukt kokain det siste året, sammenlignet med for 10 år siden.[2] Totalt ble det i 2023 beslaglagt mer kokain enn i løpet av de siste 22 årene til sammen.[3]

I 2023 ble det registrert det høyeste antallet straffbare forhold begått av ungdom og barn under 18 år, siden 2009. Over en tredjedel av disse forholdene ble begått av barn under 15 år. Økningen i antall saker er størst når det gjelder lovbrudd som tyveri, kroppskrenkelse, trusler og skadeverk. Politiet ser en økt forekomst av vold og annen alvorlig kriminalitet blant mindreårige. Politiet er spesielt bekymret for at det også er en negativ utvikling når det gjelder ran, ulovlig bevæpning med kniv og skytevåpen samt grov kroppskrenkelse.

2.2

OVERORDNEDE UTVIKLINGSTREKK VED SENTRALE KRIMINALITETSOMRÅDER SOM RAMMER SAMFUNNETS FELLESVERDIER

Politiet produserer jevnlig både graderte og ugraderte etterretningsrapporter innenfor en rekke ulike kriminalitetsområder. De siste to årene er det publisert flere offentlige rapporter blant annet innenfor temaene organisert kriminalitet, cyberkriminalitet og økonomisk kriminalitet.[4] Arbeidet gir politiet en bred forståelse av nåsituasjonen og utviklingstrekk ved kriminalitetsbildet.

Organisert kriminalitet

I Europa har trusselen fra organisert kriminalitet aldri vært høyere.[5] Også i Norge er trusselen fra organiserte kriminelle betydelig. Flere sterkt profittmotiverte kriminelle nettverk opererer i Norge, og mange av disse er involvert i salg, distribusjon og innførsel av narkotika.[6] Dette har blant annet blitt synlig for befolkningen gjennom de rekordstore kokainbeslagene i Norge i 2023.

Organisert kriminell virksomhet kan resultere i både konflikter og samarbeid mellom kriminelle aktører. Politiet ser at flere av de organiserte kriminelle nettverkene i økende grad samarbeider med andre kriminelle. Slikt samarbeid blir spesielt tydelig der kriminelle kjøper og selger tjenester, oppdrag og spesialisert kompetanse. Slik kompetanse kan være alt fra transport og hvitvasking til vold og pengeinnkreving. Samtidig ser politiet at den samme utviklingen kan resultere i økt konkurranse om narkotikamarkedene, noe som tidvis har resultert i voldshandlinger både i det private og i det offentlige rom.[7]

Politiets vurdering er at trusselen fra organiserte kriminelle nettverk er betydelig og økende, blant annet på grunn av økt profesjonalisering, grensekryssende samarbeid og stadig mer komplekse forretningsmodeller. I kjølvannet av dette er vi særlig bekymret for et økt konfliktnivå der trusselen fra svenske aktører er fremtredende.

Cyberkriminalitet

Cyberkriminaliteten har stor geografisk spredning og rammer bredt. Kriminaliteten rammer både enkeltpersoner, i form av eksempelvis bedragerier og seksuallovbrudd, og virksomheter, i form av eksempelvis datainnbrudd, datatyverier og løsepengevirusangrep. Verdien på stjålet informasjon vurderes som stadig økende. Små og mellomstore virksomheter er særlig utsatte.

Politiet erfarer en rekke endringer innen cyberkriminalitetsfeltet i 2023, særlig relatert til geopolitiske og teknologiske faktorer. De cyberkriminelle fortsetter å utvikle og tilpasse teknikker, metoder, verktøy og strategier, blant annet for å omgå mottiltak fra offentlige og private virksomheter. Samtidig er det observert flere likheter med foregående år, som at majoriteten av de cyberrettede kriminelle lovbruddene i 2023 er både opportunistiske og profittmotiverte.[8] Ett lovbrudd kan imidlertid ha ulik motivasjon og verdi, eksempelvis profitt og samtidig etterretningsverdi for statlige aktører.

Politiets vurdering er at trusselen fra cyberkriminelle aktører er økende. Aktørene tilegner seg stadig økende kompetanse og kapasitet til å gjennomføre kriminalitet av økt kompleksitet og skadepotensial. Seksuallovbrudd støttet av datasystemer er en vedvarende høy trussel.

Demningen i Braskereidfoss etter ekstremværet Hans. Foto: Shutterstock

Den teknologiske utviklingen bidrar til å skape et utvidet handlingsrom for cyberkriminelle aktører.

Økonomisk kriminalitet

Digitaliseringen av samfunnet og integreringen av økonomier og arbeidsmarkeder øker mulighetene for grensekryssende økonomisk kriminalitet. Politiet ser at kriminelle organiserte nettverk har direkte eller indirekte kontroll over foretak, og det benyttes profesjonelle aktører og stråpersoner for å skjule kriminelle handlinger og eierskap. Samtidig trues deler av velferdsstatens finansieringsgrunnlag gjennom arbeidslivskriminalitet. Det er et vedvarende problem med svart avlønning og skjult omsetning på tvers av bransjer i arbeidslivet.

Både politiet og bankene registrerer en voldsom økning i antall bedragerier. Politiet forventer at bedrageri vil fortsette å øke i omfang, og at folk i alle aldre og samfunnslag vil rammes i kommende år. Bedrageri genererer stort utbytte til kriminelle aktører som benyttes til å finansiere ny kriminalitet. Flere siktede i norske bedragerisaker kan knyttes til organiserte kriminelle nettverk, som også er involvert i narkotika- og voldskriminalitet.[9] Bruk av pengemuldyr i hvitvaskingsoperasjoner er en økende utfordring og har blitt en forbruksvare for kriminelle. Politiet forventer at bedrageri vil bli en viktigere inntektskilde for kriminelle miljøer, og at flere vil bli rekruttert og utnyttet som muldyr.

Miljøkriminalitet

Miljøkriminalitet er mangeartet og omfatter forurensings-, natur-, fiske- og akvakulturkriminalitet, samt andre aktiviteter som forårsaker alvorlig skade på økosystemer. Denne typen kriminalitet er ofte motivert av økonomisk gevinst eller kostnadsbesparelser, og kan involvere enkeltpersoner, næringsdrivende og kommuner.

I Norge er effekten av klimaendringer tydelige, i form av mer nedbør, flere flommer og skred, og isbreer som krymper.[10] Høsten 2023 førte ekstremværet «Hans» til store lokale utfordringer, i form av ødeleggelser både på miljø og infrastruktur.

I en tid med økonomisk utfordrende tider, er politiets vurdering at flere vil kunne begå miljøkriminalitet for å kutte kostnader. Politiet vurderer at ulovlige fysiske naturinngrep og arealendringer i naturen kan gjøre oss mindre i stand til å håndtere klimaendringene fremover, og få langt mer alvorlige og kostbare konsekvenser enn de vi allerede ser i dag.[11]

2.3

SENTRALE DRIVKREFTER FOR UTVIKLING AV KRIMINALITET

Samfunnet er i kontinuerlig endring, og det er av den grunn heftet usikkerhet knyttet til de overordnede vurderingene av kriminalitetsutviklingen beskrevet i del 2.2. Her gir vi derfor en beskrivelse av ulike drivkrefter som kan påvirke kriminalitetsbildet i året som kommer.

Kriminalitetsutviklingen i et samfunn påvirkes av både interne og eksterne drivkrefter. Mens interne drivkrefter i all hovedsak er motivasjonsfaktorer som ikke er profittdrevne, slik som hevn, sjalusi eller seksuell interesse for barn, er eksterne drivkrefter forhold i samfunnet som påvirker kriminalitetsbildet og utviklingen av dette. Under har vi identifisert ulike *eksterne drivkrefter* som vil kunne påvirke kriminalitetsbildet i Norge det neste året.

Internasjonale konflikter påvirker kriminalitetsbildet i Norge

Konfliktbildet i Ukraina og Midtøsten er to eksempler på hvordan krig og konflikt i andre land også får konsekvenser for Norges interesser, både i inn- og utland.

Som følge av Russlands angrep på Ukraina er trusselbildet mot Norge endret, og Norges sikkerhet blir utfordret på nye måter. Dette innebærer blant annet at såkalte *sammensatte trusler* utgjør en del av trusselbildet. Sammensatte trusler kan innebære både lovlig og ulovlig aktivitet. Den ulovlige aktiviteten kan for eksempel være sabotasje, skadeverk og digitale angrep. Politiet spiller derfor en sentral rolle i å oppdage og rapportere om sammensatte trusler.[12,13]

Krigen i Ukraina har ført til store flyktningestrømmer. I likhet med flyktninger fra andre land, står også ukrainske flyktninger i fare for å bli utnyttet av kriminelle aktører som profiterer på deres situasjon, gjennom menneskesmugling og menneskehandel. Det store antallet ukrainere som kommer til Norge, kan skape et økt handlingsrom for utnyttelse av arbeidskraft og utnyttelse til prostitusjon. Det finnes kriminelle nettverk i Norge som målrettet rekrutterer flyktninger inn i utnyttelsesforhold. Nettverkene tilbyr for eksempel organisering av flukt og transport ut av landet, mot avtale om prostitusjon i Norge og andre land i Europa.

Den voldelige konflikten i Midtøsten er et aktuelt eksempel på internasjonale konflikter som skaper politisk engasjement, og som kan utgjøre et potensial for sosial uro og hatefulle ytringer på internett.

Økonomiske utfordrende tider kan gjøre ungdom sårbare for å involveres i kriminalitet

2023 var et økonomisk utfordrende år, med høy prisstigning, renteøkning og høye strømpriser. Dyrtiden forsterker helsemessige, sosiale og økonomiske ulikheter, og fører til en økning i antall husstander som opplever problemer.[14]

I perioden 2020–2022 levde over 10 prosent av alle barn under 18 år i en familie med vedvarende lavinntekt.[15] Barn som vokser opp i lavinntektsfamilier, kan oppleve utenforskap og har økt fare for å oppleve dårligere levekår og livskvalitet enn andre barn.[16] Dette kan gjøre dem sårbare

for å bli involvert i profittmotivert kriminalitet og rekruttering til gjengkriminalitet. Flere studier har eksempelvis vist at det å vokse opp i en lavinntektsfamilie, øker risikoen for å bli involvert i ungdomskriminalitet.[17]

Sammenhengen mellom oppvekst i lavinntektsfamilier og risiko for senere kriminalitet er imidlertid kompleks, og forskningen peker på flere faktorer som påvirker barns livssjanser og utviklingsmuligheter. Flere studier hevder for eksempel at sammenhengen mellom lavinntekt og kriminalitet i større grad skyldes at lav inntekt påvirker familierelasjoner og nivået av stress og uro i familien – som igjen kan påvirke barns risiko for å involveres i kriminalitet.[18]

Internasjonal forskning viser også at barn og unge som vokser opp i lavinntektsfamilier, er mer utsatt for vold, overgrep og omsorgssvikt. Dette gjelder også i en norsk og nordisk kontekst.[19]

Det er usikkert hvordan den økonomiske situasjonen vil utvikle seg i 2024, og hvordan dette vil påvirke kriminalitetsbildet i Norge. Tall fra Statistisk sentralbyrå (SSB) viser imidlertid at antallet barn som lever i husholdninger med vedvarende lavinntekt, har vært nedadgående de to siste årene.[20]

Teknologisk utvikling gir et økt handlingsrom for kriminelle aktører

De siste årene har det skjedd en voldsom teknologisk utvikling, blant annet innen bruken av digitale verktøy. I dag er en stor del av både offentlige og private tjenester digitalisert, noe som gjør samfunnet sårbart for manipulasjon og utpressing. Teknologi og teknologisk utvikling er derfor en fundamental driver for cyberkriminalitet.[21] Dette krever nye mottiltak fra lovgivere, politiet samt private og offentlige virksomheter.

Utviklingen innenfor både kunstig intelligens (KI) og anonymiseringsteknologi bidrar til å skape et utvidet handlingsrom for kriminelle. KI er i kontinuerlig utvikling, og er en driver for at det blir flere kriminelle aktører på det digitale området. Aktørene tilegner seg høyere kompetanse og blir stadig mer effektive.[22] Dette gjelder både innenfor kriminalitet mot datasystemer og kriminalitet støttet av datasystemer.

KI omfatter blant annet teknologi som bidrar til å manipulere menneskers virkelighetsoppfatning. Eksempelvis gjør utviklingen av såkalte *deepfakes** det mulig å produsere svært realistiske, men falske, videoer der noen sier eller gjør noe de aldri har sagt eller gjort. Deepfakes kan blant annet brukes til utpressing, identitetstyveri, bedrageri og svindel samt manipulering og påvirkning gjennom falske nyheter og media.[23]

Videre utvikling av lett tilgjengelige og kommersielle anonymiseringsteknologier øker muligheten for at kriminelle aktører kan opptre fordekt i det digitale rom, samt at de kan operere på tvers av landegrenser og jurisdiksjoner.[24] Ende-til-ende-krypterte meldingsplattformer bidrar eksempelvis til at seksualforbrytere har lavere risiko for å bli oppdaget under seksualisert kontakt med barn, eller under kommunikasjon med hverandre.

Kriminelle aktører benytter ulike digitale økonomiske tjenester som bidrar til anonymisering. Utviklingen innenfor kryptovalutamarkedet vil påvirke kriminelle aktørers mulighet til å gjennomføre ulovlige handlinger, som for eksempel hvitvasking, seksuallovbrudd og bedragerier, eller å skjule annen kriminell aktivitet.

Hatefulle ytringer på sosiale medier utgjør en trussel mot demokratiet

Sosiale medier har bidratt til at langt flere mennesker kan ytre seg og delta i samfunnsdebatten nå enn tidligere. Muligheten til å kommunisere direkte og til alle døgnets tider har imidlertid bidratt til et hardere debattklima og en økning i hatefulle ytringer og sjikane, både mot samfunnsprofiler og mellom meningsmotstandere. Konspirasjonsteorier og falske nyheter sprer seg raskere enn noen gang før, noe som bidrar til å svekke den generelle tilliten i samfunnet.

* Deepfakes er et samlebegrep på bilder, video og lyd som er fremstilt ved hjelp av kunstig intelligens.

Flere studier har vist at norske politikere i økende grad utsettes for trusler og hatefulle ytringer.[25] Dette kan føre til at mange trekker seg fra politiske verv og deltakelse i den offentlige debatten. Slike handlinger, og en slik samfunnsmessig utvikling, kan utgjøre en trussel mot ytringsfriheten og mot demokratiet.

Klima og naturvern danner grunnlag for økt polarisering

Klimaendringer fører til store ødeleggelser for mennesker og natur, og utgjør en trussel mot vårt livsgrunnlag. Globale virkninger av klimaendringene er komplekse og usikre, og noen områder rammes hardere enn andre. Ifølge FN ble 22 millioner mennesker i 2021 fordrevet fra sine hjem på grunn av ulike følger av klimaendringene.[26] Flyktning-situasjonen skaper et handlingsrom for menneskesmugling til Norge.

I Norge vil politiske valg og prioriteringer danne grunnlag for konflikter mellom ulike aktivister innenfor klima- og naturvern og representanter for næringsinteresser og politiske vedtak. Et sterkt engasjement fra ulike grupperinger i samfunnet kan være både lovlig, positivt og ønskelig. Samtidig kan slikt engasjement også føre til økt polarisering, noe som kan komme til uttrykk gjennom ulovlige handlinger både på digitale og fysiske arenaer, for eksempel i form av økt forekomst av hatefulle ytringer.[27] Hvordan klima-endringene utspiller seg, konsekvensene av klimatiltak og aktivistenes påvirkning fra tilsvarende miljøer i utlandet, er faktorer som kan påvirke hvorvidt eventuelle protest-aksjoner vil føre til ulovlige handlinger i form av skadeverk, sabotasje eller voldelige handlinger.

Myndighetenes håndtering, for eksempel gjennom strengere klimatiltak, kan også være en driver for miljøkriminalitet. Det forventes blant annet strengere regulering av forurensningskilder og bruk av naturressurser. Økte kostnader knyttet til forsvarlig deponering av avfall, kan eksempelvis føre til at enkelte neglisjerer kravene eller oppgir uriktig informasjon for å spare utgifter.

Skolestreik for klima utenfor Stortinget i 2019. Foto: Zhyshchynskyi Vadym / Shutterstock

03 UTVALGTE KRIMINALITETSTRUSLER

Denne delen av rapporten presenterer et utvalg trusler som anses å true de fire samfunnsverdiene *alminnelig trygghet*, *økonomiske verdier*, *grunnleggende samfunnsstrukturer* og *kritisk infrastruktur og samfunnsfunksjoner*.

Samlet sett viser beskrivelsene av truslene at kriminaliteten blir stadig mer profesjonalisert, at den preges av aktører som utnytter mulighetene og handlingsrommet som skapes av teknologisk utvikling, og at de kriminelle ofte opererer sømløst på tvers av geografiske grenser. I tillegg ser vi at noen av kriminalitetstruslene oppstår i en tid preget av politisk, økonomisk og miljømessig usikkerhet.

Foto: Politiet

3.1

KRIMINALITET SOM HANDELSVARE BIDRAR TIL PROFESJONALISERING AV ORGANISERT KRIMINALITET

I en verden som blir stadig mer spesialisert og kompleks, endres også kravene til kunnskap og kompetanse hos de organiserte kriminelle nettverkene. Kriminelle nettverk som mangler tilstrekkelig kunnskap og kompetanse til å få utført spesifikke handlinger, søker i større grad denne ekspertisen hos tilbydere som blant annet er å finne på det mørke nettet. *Kriminalitet* som *handelsvare* er et begrep som i stadig større grad blir brukt for å beskrive en utvikling der tilbydere av spesifikke kriminelle aktiviteter og tjenester utvikler ekspertise innenfor handel med kriminalitet. Utviklingen bidrar til en profesjonalisering av den organiserte kriminaliteten, og fører på den måten til et økt handlingsrom for organiserte, kriminelle nettverk.

Kriminalitet som handelsvare utgjør et bredt konsept av både roller og tjenester som tilbys alle delene av kriminell aktivitet – fra produksjon og rekruttering, til logistikk og distribusjon.[28] Det knyttes særlig til cyberkriminalitet, men også til pengeinnkreving, vold, logistikk og hvitvasking. Hvitvasking og pengeoverføringer krever kompetanse og aktiviteter som kan involvere aktører i både den svarte og hvite økonomien. Ulike aktører har spesialisert seg på hvitvasking og utførsler av utbytte, på oppdrag fra kriminelle nettverk i Norge. Utførsel av kontanter og uregistrert betalingsvirksomhet er en attraktiv tjeneste for å hvitvaske og sikre verdier.

Kjøp og salg av kriminelle tjenester foregår over hele landet. Politiet registrerer en økt rapportering om dette i tilknytning til kjente kriminelle nettverk og geografisk sentrale områder. Eksempelvis har det vært flere tilfeller der svenske kriminelle aktører har utøvet vold i Norge på bestilling fra andre kriminelle aktører. Enkelte svenske kriminelle nettverk har høy volds- og fryktkapital og har bygd nettverket som en egen merkevare. Utviklingen av kriminalitet som handelsvare bidrar altså ikke bare til en profesjonalisering av den organiserte kriminaliteten, men også til at kriminaliteten blir mer alvorlig.

Kriminalitet som handelsvare innenfor cyberkriminalitet er under kontinuerlig utvikling

Cyberkriminalitet krever ofte spesiell kompetanse, noe som har skapt et eget marked hvor tjenester og verktøy selges, kjøpes eller leies ut til kriminelle formål. Politiet observerer at dette markedet er stort og økende. Nyvinninger kommer raskt ut på det kriminelle markedet. Kriminelle har vist evnen til å ta lærdom av feil og er helt i front på å utvikle og bruke verktøy.

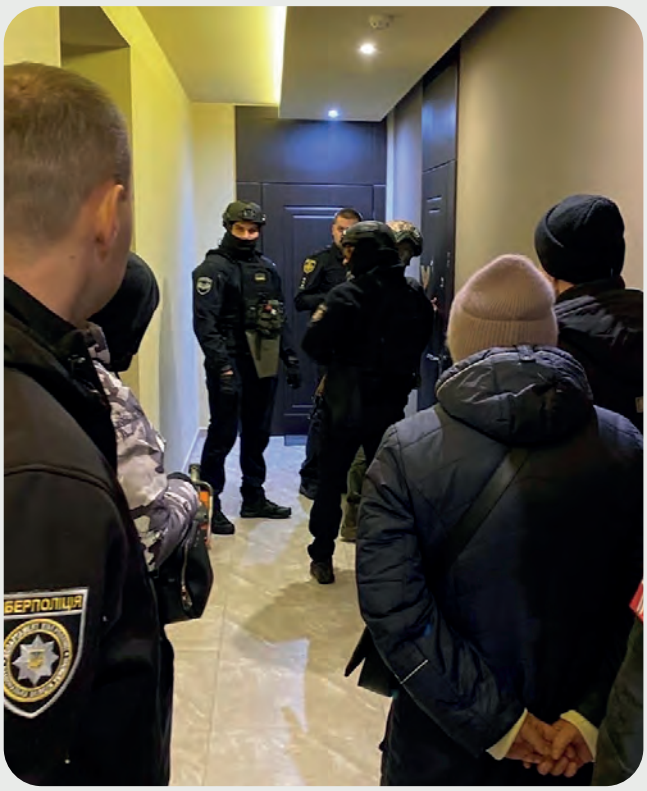
Det mest prominente eksempelet på kriminalitet som handelsvare er *løsepengevirus*. Dette har utviklet seg til å bli en av de mest alvorlige sikkerhetsrisikoene for virksomheter i både offentlig og privat sektor.[29] Løsepengevirus er skadevare som tradisjonelt sett blir benyttet til å kryptere fornærmedes data. Deretter kreves løsepenger for å låse opp datasystemene igjen. Angrepene skjer vanligvis ved at kriminelle som utvikler skadevaren, selger eller leier denne ut til andre kriminelle grupperinger, som bruker skadevaren til dataangrep mot en virksomhet. Målet er å få virksomheten som rammes, til å betale løsepenger. I tillegg settes det ofte frem trusler om å selge data og sensitiv informasjon dersom løsepengene ikke

utbetales. Til slutt hvitvaskes utbyttet av andre kriminelle aktører gjennom flere ledd av vekslertjenester, noe som gjør det vanskelig å straffeforfølge.[30]

Det reelle omfanget av løsepengevirusangrep er usikkert. De siste to årene har det imidlertid vært noen færre anmeldte løsepengevirusangrep mot norske virksomheter. De fleste slike angrep er opportunistiske og motivert av vinning, men det er likevel observert angrep i 2022 og 2023 som tyder på større grad av kartlegging og målrettethet. Bedrifter som ikke har ressurser til – eller ikke har prioritert – å beskytte sine verdier tilstrekkelig, vil være spesielt sårbare for angrep. Ofte kan dette være små eller mellomstore bedrifter. Konsekvensene ved å bli utsatt for løsepengevirusangrep for den enkelte virksomhet kan derfor være betydelige. For noen kan det bety driftsstans og i verste fall konkurs.[31]

Politiet har i 2023 observert en utvikling i utpressingsmodus blant enkelte kriminelle som har angrepet norske virksomheter. Som et ekstra ledd i utpressingen har gjerningspersoner utført datatyveri med påfølgende tjenestenektangrep (se også del 3.5). I tillegg er det observert at gjerningspersoner har tatt kontakt med virksomheten via e-post og telefon for ytterligere utpressing. Samlet omtales dette som trippel utpressing.[32]

Det er også observert at kriminelle aktører publiserer stjålne data på det åpne nettet. Dette kan utgjøre en økt risiko for gjentagende angrep, ved at den stjålne dataen er lett tilgjengelig for alle på internett og har kort nedlastingstid sammenlignet med data på det mørke nettet.



Bildet viser en pågripelse i Kiev, der norsk politi bistår ukrainsk politi. Utgangspunktet for pågripelsen er løsepengeangrepet mot Norsk Hydro i 2019. Foto: Politiet

En annen type handelsvare er *påloggingsdetaljer*. Disse er til salgs på markedsplasser på det mørke nettet, og kan brukes til datainnbrudd og annen kriminell aktivitet. Slike påloggingsdetaljer er mulig å stjele ved å bruke såkalt informasjonsstjelerskadevare*, en type skadevare som det også handles med på det mørke nettet.

* Informasjonsstjelere er skadevare som er designet for å kompromittere og stjele informasjon fra en enhet. Skadevaren kan blant annet stjele brukernavn og passord lagret i nettlesere, informasjonskapsler og nettleserhistorikk.

Et tredje eksempel på handelsvare er *nulldagssårbarheter*** som kan kjøpes og selges på det mørke nettet, hvor en symbiose av hackere, kriminelle og etterretningstjenester opererer.[33] Nulldagssårbarheter har begrenset levetid og har derfor svært høy verdi for kriminelle. Det kreves høy kompetanse og arbeid over tid for å utnytte nulldagssårbarheter, og derfor er dette også en ettertraktet handelsvare.

Det siste året har politiet sett at kriminelle aktører har lyktes i å anskaffe programvare utviklet av statlige aktører, til bruk til kriminelle formål. På den måten blir avansert teknologi utbredt i kriminelle kretser, noe som kan innebære en trussel mot kritisk infrastruktur. Eksempelvis kan kriminelle dra nytte av programvare designet for å påvirke operasjonell teknologi (OT). OT-systemer er maskinvare- og programvaresystemer som brukes til å overvåke, kontrollere og administrere kritisk infrastruktur og fysiske prosesser i flere ulike bransjer. Ved angrep på et OT-system vil kriminelle aktører kunne gjøre skade i den fysiske og digitale verden samtidig, ettersom cyberkriminalitet både har en digital og en analog slagside.

Rekruttering av personer til å gjennomføre angrep skjer hovedsakelig på forum og møteplasser på det mørke nettet. Ettertraktet kompetanse innenfor cyberkriminalitet er teknisk og språklig kompetanse, i tillegg til kompetanse innen menneskelige atferdsmønstre – fordi dette regnes som en suksessfaktor for å påvirke fornærmede. Samtidig vil kriminelle enkeltpersoner også kunne gjennomføre dataangrep uten forkunnskap om den enkelte programvaren. Informasjon om relevante verktøy kan skaffes fra meningsfeller eller ved å søke seg frem til dette selv. Verktøyene er i mange tilfeller gratis, og oppskrifter for fremgangsmåte er lett tilgjengelig – hvilket får stor påvirkning på rekrutteringen til cyberkriminalitet.

Foto: Shutterstock

** En nulldagssårbarhet er et svakt punkt i en programvare som oppdages av angripere før forhandleren har blitt klar over det.

Regnskapsførere som bistår kriminelle, utgjør en trussel mot vårt økonomiske system

Kriminelle aktører bruker regnskapsførere for å legitimere foretak som benyttes til økonomisk kriminalitet. Politiet har informasjon om at enkelte regnskapsførere tilrettelegger for blant annet hvitvasking, fiktiv fakturering, skatte- og avgiftsunndragelse og arbeidslivskriminalitet. Dette gjør de blant annet ved å opprette kompliserte foretaksstrukturer, noe som kan tilsløre reelle eiere og gjøre det vanskelig å kontrollere foretakets økonomi.

Det finnes regnskapsforetak som virker utelukkende å tilby sine tjenester til kriminelle aktører *(kriminalitet som handelsvare)*. Eksempler på slike tjenester kan være å bistå næringsdrivende i hvordan de kan gå frem for å manipulere regnskap, unndra midler og slå et firma konkurs.

Kriminelle aktører som gjentagende utnytter selskaper og slår dem konkurs, fører til en uheldig konkurransevridning og betydelige samfunnsøkonomiske tap. Å gi kreditt til næringslivet er en viktig hjørnestein i vårt økonomiske system, men innebærer en risiko for de som låner ut penger og investerer i virksomheter. Dersom kredittgivere ikke har tillit til at det gis korrekt og fullstendig informasjon om en virksomhets reelle økonomiske stilling, kan det føre til at færre skyter inn kapital eller gir kredittytelser. Konkurskriminalitet utgjør dermed en vesentlig trussel for vårt økonomiske system.

DATAANGREP MOT OT- OG IT-SYSTEMER

I november 2023 ble Australias største havneoperatør, DP World, utsatt for et omfattende dataangrep. På bakgrunn av angrepet måtte DP World ta ned datasystemene sine, og Australia måtte stenge viktige storhavner som står for rundt 40 prosent av alle varer og produkter til og fra Australia.

Datasystemene til DP World ble koblet fra internett, og havneoperatøren hadde svært begrenset kapasitet til å flytte containere og frakt ved havnene. Dette er et realistisk eksempel i norsk kontekst, og illustrerer hvordan et dataangrep kan ramme både OT- og IT-systemer i Norge.

Melbourne, Australia. Foto: Aerometrex Ltd / Getty

3.2

KRIMINALITET SOM UTNYTTER LEGALE STRUKTURER

Gjennom å utnytte legale strukturer for næringsliv eller offentlig virksomhet, kan organiserte kriminelle aktører lettere plassere profitt fra kriminell aktivitet og øke den økonomiske vinningen. Ved å integrere den kriminelle virksomheten i den legale økonomien vil de kriminelle virksomhetene også kunne oppnå økt anerkjennelse og legitimitet.

Eiendomssektoren og fiskerinæringen er to eksempler på bransjer der organiserte kriminelle aktører benytter seg av legale strukturer som et ledd i å utføre økonomisk kriminalitet. Se også del 3.4 for hvordan legale strukturer utnyttes i varetransport.

Foto: Jacek Dylag / Unsplash

Eiendomssektoren vil fortsatt være en attraktiv sektor for hvitvasking

Kontantintensive bransjer gir ofte en god mulighet til å kombinere både lovlig og ulovlig utbytte.[34] Eiendomssektoren er et godt eksempel på en slik bransje. Verdistigning og god avkastning over mange år har gjort sektoren til et attraktivt sted å plassere både norsk og utenlandsk kapital. Det gjør at kriminelle aktører kan investere store beløp i eiendom, som dermed integreres i den legale økonomien.[35] Beløpene kan være utbytte fra ulike typer kriminalitet, for eksempel narkotika- eller arbeidslivskriminalitet.

Fremgangsmåten er ofte å kjøpe boliger ved å bruke kriminelt utbytte. Bruk av stråselskap og stråpersoner bidrar til å tilsløre midlenes opprinnelse. Deretter rehabiliteres boligene ved å bruke ulovlig arbeidskraft, og arbeiderne blir betalt kontant. Materialene betales med kontanter som er skaffet gjennom straffbare handlinger. Slik hvitvaskes utbyttet gjennom svart avlønning til arbeiderne. I tillegg får boligen en verdiøkning som igjen gir et utbytte til de kriminelle. Kriminalitetstrusselen kan også føre til samfunnsøkonomiske tap gjennom skatteunndragelse, konkurransevridning i samfunnet og utkonkurrering av legale virksomheter.

Fiskerikriminalitet undergraver en bærekraftig fiskeriforvaltning

Norsk sjømat er å regne som en av landets viktigste handelsvarer. I 2022 ble det fra fiskeri- og havbruksnæringen eksportert 2,9 millioner tonn norsk sjømat til en verdi av 151,4 milliarder kroner.[36] I bransjen forekommer det

imidlertid omfattende *fiskerikriminalitet*, et begrep som omfatter både miljøkriminalitet, økonomisk kriminalitet og arbeidslivskriminalitet. Fiskerikriminalitet er profittmotivert og konkurransevridende, og utgjør en trussel mot velferdsstaten gjennom blant annet unndratte skatteinntekter. I ytterste konsekvens kan den ulovlige virksomheten også ramme matsikkerhet og være en trussel for liv og helse. Fiskerikriminalitet foregår i hele verdikjeden, fra hav til bord.

Overfiske, kvoteovertredelser og feilrapportering undergraver en bærekraftig forvaltning og skader det marine økosystemet.[37] Kvoteovertredelser og feil- og underrapportering av fangst fører også til reduserte skatteinntekter. Feilrapporteringer foregår hovedsakelig i transaksjonen mellom fiskeren og fiskemottaket, enten gjennom samarbeid mellom aktørene, eller ved at mottaket underslår fangsten eller fangstverdien fra fiskeren, uten at fiskeren er involvert.[38] Enkelte markedsledende aktører har innlemmet fiskerikriminalitet som en del av virksomheten i flere ledd i verdikjeden.

Både yrkesfiskere og fritidsfiskere omsetter norsk sjømat svart til privatkunder og restauranter. Omsetningen foregår enten direkte mellom kjøper og selger, eller via digitale markedsplasser. Smugling av fangst fra fisketurisme og svart omsetning av eksempelvis kongekrabbe kan bidra til konkurransevridning i markedet.[39] Ulovlig omsetning av sjømat er også en trussel mot matsikkerheten, fordi det ikke er mulig å sikre at hygienen er tilstrekkelig ivaretatt ved håndtering, transport og oppbevaring.

Foto: Piola666 / Getty

I fiskerinæringen forekommer det også arbeidslivskriminalitet og utnyttelse av sårbare arbeidstakere. Dette gjelder hele verdikjeden. Eksempler er lønnstyverier, uforsvarlig innkvartering eller arbeidsmengde, bruk av ulovlig arbeidskraft eller brudd på kjøre- og hviletidsbestemmelser.

3.3

KRIMINALITET I EN TEKNOLOGI-STYRT HVERDAG

Norge har utviklet seg til å bli et av verdens mest digitaliserte land. I likhet med mange private tjenester er også offentlige tjenester innen eksempelvis skatt, helse og trygdeytelser digitalisert. De siste årene har vi også sett hvordan utviklingen av digitale plattformer gjør det mulig å skape nye forretningsmodeller som kobler kunder og leverandører sammen, som for eksempel person- og flyttetransport og renhold. Slike forretningsmodeller kan skape en lettvint hverdag for forbrukere. Samtidig åpner det for arbeidsmarkedskriminalitet, ved at arbeidsgiver-ansvaret blir pulverisert og at skatte- og avgiftsinnbetalinger ikke innbetales.[40]

I denne teknologistyrte hverdagen skapes et nytt handlings-rom for kriminelle aktører. Befolkningen settes på prøve når de må navigere i digitale henvendelser som potensielt kan være profesjonelle forsøk på bedrageri. De kriminelle aktørene benytter mange ulike fremgangsmåter og utviser stor kreativitet i sine bedrageriforsøk. Utviklingen og bruken av KI vil bidra til å øke trusselen ytterligere i 2024.

Den teknologistyrte hverdagen preger også i stor grad unge mennesker og deres hverdag. Dette kapittelet viser hvordan utviklingen innenfor både KI og anonymiserings-teknologi bidrar til å skape et utvidet handlingsrom for kriminelle. Kapittelet viser også hvordan den digitale delingskulturen som har utviklet seg de siste årene, har sine negative sider – gjennom deling av digitalt materiale som viser grov vold og seksuelle overgrep. Slik deling kan få svært alvorlige følger for dem som blir utsatt.

Kunstig intelligens kan føre til at flere barn og unge utsettes for seksuell utpressing med økonomisk motiv

Barn og unge utforsker i dag mye av sin seksualitet på internett, noe som gjør dem særlig sårbare for å bli utsatt for ulike typer seksuelle overgrep. En type overgrep som politiet ser stadig flere rapporterte tilfeller av, er seksuell utpressing med økonomisk motiv. Det er i tillegg grunn til å tro at mørketallene på dette området er betydelige.[41] Samlet sett utgjør denne type utpressing en trussel for barn og unges trygghet i det digitale rom.

Seksuell utpressing med økonomisk motiv utføres ofte av profesjonelle kriminelle aktører som befinner seg i utlandet. Blant annet er det avdekket godt organiserte call-sentre som opererer på et globalt nivå. Utpressingen skjer gjennom bruk av falske kontoer, der fornærmede blir forledet til å ta nakenbilder eller filme seg selv mens de utfører seksuelle handlinger. Fornærmede presses deretter til å betale for at gjerningspersonen ikke skal dele materialet med eksempelvis fornærmedes venner, familie eller følgere i ulike sosiale medier. Det er eksempler på gutter og unge menn som har betalt flere tusen kroner som følge av utpressingen. Pengekravene varierer i hovedsak fra 5000 til 20 000 kroner, og i flere tilfeller bes det om betaling i kryptovaluta. De som har betalt, har som regel fått nye pengekrav, og i noen tilfeller er materialet delt til tross for at betalingen er gjennomført. Politiet ser også at trusselen om å dele materialet er gjennomført i flere tilfeller hvor fornærmede ikke har betalt pengekravet.

Politiet ser at utpressingen blir mer aggressiv og pågående, og at det benyttes stadig nye og mer kyniske metoder. Pengekravene gjelder større summer, og de siste par årene har de utsatte blitt yngre. Det er rapportert om fornærmede helt ned i 13–14-årsalderen. Majoriteten av de som utsettes, er gutter og unge menn mellom 15 og 25 år, men også jenter har blitt utsatt. Utpressingen foregår på de fleste sosiale medier hvor unge befinner seg. Snapchat, Instagram og Discord er noen av plattformene som oftest benyttes.

Den kontinuerlige teknologiutviklingen innenfor KI gjør at trusselaktørenes handlingsrom utvides. For det første vil kriminelle aktører kunne bruke vanlige bilder av fornærmede til å produsere falske nakenbilder. Det er derfor ikke lenger nødvendig å vinne fornærmedes tillit for å skaffe seg nakenbilder som de senere kan bruke til utpressing.[42] Politiet har også informasjon om at KI blir brukt til å generere seksualisert materiale, med intensjon om å drive utpressing med økonomisk motiv.

For det andre kan KI benyttes til å velge ut potensielle ofre på en mer effektiv og målrettet måte, der hensikten er videre utpressing. Ved å bruke oversettelsesverktøy kan hvem som helst kommunisere på alle språk og tilpasse språkbruken til ofrenes alder. Internasjonalt rapporteres det også om tilfeller der KI er benyttet til å etablere kontakt og drive utpressing av mindreårige.[43]

For det tredje kan KI føre til at også aktører som ikke er profesjonelle og organiserte, i større grad begår denne type kriminalitet. Eksempelvis så man nylig i Spania et tilfelle hvor unge gutter manipulerte bilder av unge jenter i alderen 11–17 år ved hjelp av KI-program, for så å spre falske nakenbilder av jentene med blant annet WhatsApp og Telegram.[44]

Bruk av KI vil føre til at flere barn og unge kan bli utsatt for seksuell utpressing med økonomisk motiv. Slik utnytting er svært belastende for den som rammes, og er forbundet med mye skyld og skam.[45] I flere land, inkludert Norge, har personer tatt sitt eget liv etter å ha blitt utsatt for denne typen utpressing.[46]

Økt deling av grovt seksualisert materiale og voldsvideoer

De siste årene har det utviklet seg en delingskultur der mindreårige i økende grad deler grovere innhold på sosiale medier. Innholdet gjelder både grovt seksualisert materiale og voldsvideoer. Delingen skjer raskt og i stort omfang, og konsekvensene for de fornærmede kan være svært alvorlige.[47] Usikkerhet knyttet til hvor materialet har blitt delt og hvem som har sett det, kan føre til psykiske belastninger og påvirke skolegang og livet for øvrig.

Når det gjelder deling av seksualisert materiale, ser politiet at voldtekts- og samleievideoer deles hyppig i sosiale medier. Politiet mottar mange tips om unge som laster ned og/eller deler overgrepsmateriale, inkludert seksualisert materiale av andre jevnaldrende. Barn helt ned i 11–12 årsalderen deler eller opplever at bilder av dem blir delt. Både gutter og jenter deler seksualisert materiale, men gutter er oftere representert. De som deler, har en relasjon til hverandre, enten gjennom skole eller på andre måter. I flere tilfeller har de som deler seksualisert materiale, selv filmet det og er også selv en del av materialet.

De siste årene har det i økende grad blitt opprettet såkalte *exposed-kontoer*, det vil si lukkede kontoer der det deles bilder og video som ofte er innsendt av kontoens følgere. Disse kontoene er mest utbredt på Snapchat, men finnes også på andre sosiale medier, som for eksempel TikTok og Instagram. Det er også mindreårige blant dem som følger og/eller oppretter slike kontoer.

Exposed-kontoer har i hovedsak blitt brukt til ryktespredning, hetsing og lignende, men brukes også til å dele pornografi og overgrepsmateriale.[48] Over tid har andelen av materiale som deles, blitt grovere. Eksempler på innhold som deles, er private bilder av mindreårige med ulik grad av nakenhet, barn i seksualiserte situasjoner, og mennesker som utfører seksuelle handlinger på dyr. Exposed-kontoer brukes også til å dele videoer som viser voldtekter og grove seksuelle overgrep mot barn.

Når det gjelder deling av voldsvideoer, skjer også dette blant annet via slike exposed-kontoer. Unge over hele landet filmer og deler voldshandlinger i sosiale medier, noe som både kan normalisere vold og fungere som en driver for voldshandlinger.[49] Flere steder i landet registrerer politiet en økt voldstilbøyelighet blant stadig yngre personer. I enkelte miljøer er tersklene for å bruke vold lave, og enkelte voldshandlinger er begrunnet i ryktespredning, provoserende atferd og uenigheter.

Politiet forventer at delingskulturen kan resultere i en økt normalisering av voldsbruk og at flere og mer alvorlige voldshendelser vil bli begått både av og mot unge. Alvorlige voldshendelser har ikke bare konsekvenser for den som selv blir utsatt, men kan også påvirke den alminnelige tryggheten i samfunnet.

Når det gjelder deling og økt eksponering for grovere seksualisert materiale, kan dette bidra til holdningsendringer og normalisering av seksuelle overgrep blant unge. Utviklingen kan på den måten fungere som en driver for nye seksuallovbrudd.[50,51]

Kriminelle med internasjonale knytninger begår bedrageri av norske borgere

Både politiet og bankene registrerer en voldsom økning i antall bedragerier. Omfanget er nå så stort at det grenser til å være et samfunnssikkerhetsproblem. Både privatpersoner, organisasjoner og bedrifter lider store økonomiske tap. Politiet, banker og IKT-sikkerhetsavdelinger må bruke betydelige ressurser på å avdekke bedragerier.[52]

Gjerningspersonene opererer med ulike fremgangsmåter og med ulik grad av organisering. Bedrageriene er ofte svært profesjonelt utført, der bedragerne har ulike funksjoner som de har spesialisert seg på.

Særlig utbredt er fremgangsmåten der bedragerne ringer med spoofet telefonnummer* og utgir seg for å være enten banken eller politiet. Også SMS misbrukes for å få tilgang til fornærmedes nettbank eller bankkortopplysninger. Ofte vil SMS-en legge seg inn i eksisterende meldingshistorikk på fornærmedes mobiltelefon, noe som gjør at flere lar seg forlede. Denne typen utnyttelse av sårbarheter i telekominfrastrukturen kan svekke befolkningens tillit til private og offentlige instanser og deres bruk av digitale sikkerhetsløsninger.

De siste årene har flere av gjerningspersonene i bedragerisaker vært knyttet til annen alvorlig kriminalitet og kriminelle nettverk, slik som narkotika- eller voldskriminalitet. Enkelte av de sentrale aktørene er også involvert i saker som gjelder ran og ulovlig befatning med våpen. I tillegg er det åpenbare paralleller mellom bedragerier begått i Norge og i Sverige. Bedrageri via billån og usikret kreditt involverer transnasjonale kriminelle miljøer som også kan knyttes til narkotika- og menneskesmugling.[53]

INVESTERINGS- OG KJÆRLIGHETSBEDRAGERI

Mange nordmenn utsettes for investerings- og kjærlighetsbedragerier. Investeringsbedrageri regnes for å være den mest alvorlige bedrageriformen mot privatpersoner, og skjer gjerne ved at personer blir lurt til å investere i tilnærmet verdiløse aksjer eller kryptovaluta. Ved kjærlighetsbedragerier blir personer forledet til å overføre penger eller stille kontoen sin til disposisjon til en person de har fått en relasjon til, for eksempel gjennom datingapper.

I løpet av første halvår i 2023 registrerte politiet tap på over 150 millioner kroner knyttet til investerings- og kjærlighetsbedragerier. Gjerningspersonene ved både investerings- og kjærlighetsbedrageri knyttes ofte til utlandet.

* Spoofing innebærer at den som blir oppringt, ser det nummeret angriper ønsker.

BRUK AV DEEPFAKE I BEDRAGERIER

Mange assosierer deepfaketeknologi primært med visuell forfalskning, men teknologien kan også brukes til å forfalske lyd. En utfordring som trolig vil bli mer aktuell fremover, er kombinasjonen av automatisering og skreddersydde angrep.

Et tenkt eksempel på en kombinasjon av automatisering og skreddersydde angrep vil være et callsenter som består av datamaskiner som driver med automatisk oppringning. Datamaskinen ringer opp en privatperson for å gjøre opptak av vedkommendes stemme, for eksempel under dekke av å gjennomføre en spørreundersøkelse. Deretter brukes datalekkasjer fra sosiale medier til å kartlegge personens vennekrets. Datamaskinen ringer så opp personens venner ved hjelp av spoofingteknologi, slik at det ser ut som at samtalen kommer fra personen det er gjort opptak av. I tillegg benyttes KI for å få stemmen til å høres ut som vennen. I realiteten snakker da den oppringte med en datamaskin som forsøker å få ut personopplysninger. Denne fremgangsmåten gjør de kriminelle i stand til å nå ut til flere potensielle bedrageriofre på kortere tid. Det er også observert at bedragere har begynt å bruke verktøyet ChatGPT, og at interessen blant kriminelle er økende. Dette vil i så fall føre til betydelig flere bedrageriforsøk.

I starten av januar 2024 florerte det kompromitterende deepfakes av artisten Taylor Swift på nettet.

Foto: Brian Friedman / Shutterstock.

3.4

KRIMINALITET KJENNER INGEN GRENSER

Norges landegrenser er i overkant av 250 mil, hvorav 20 mil også er Schengens yttergrense mot Russland. I tillegg utgjør den norske sjøgrensen også Schengens yttergrense. Dette kapittelet handler om hvordan Norge utfordres av organiserte transnasjonale kriminelle nettverk som relativt sømløst samarbeider på tvers av landegrenser og kontinenter. Slike nettverk utgjør en trussel mot Europa, som ifølge Europol aldri har vært høyere.[54]

De kriminelle nettverkene involverer seg i ulike typer kriminalitet. Grov narkotikakriminalitet er fremtredende, men de er også involvert i voldskriminalitet, menneskehandel, arbeidslivskriminalitet, bedragerier, hvitvasking og smugling av både lovlige og ulovlige varer. I flere deler av landet er politiet også kjent med kriminelle aktører som er involvert i import og distribusjon av ulovlige skytevåpen til Norge. I mange av tilfellene styres nettverkene av bakmenn og lederskikkelser som befinner seg i utlandet – inkludert land uten utleveringsavtale med Norge, eller som ikke utleverer egne borgere.

Organisert kriminalitet foregår i all hovedsak i det skjulte. Allikevel regnes organisert kriminalitet som en av de største kriminalitetstruslene mot samfunnssikkerheten.[55] Dette skyldes for det første at forretningsmodellene til kriminelle nettverk blir stadig mer komplekse, med økt profesjonalisering og hyppig utskiftning av samarbeidspartnere. Svært forenklet kan det kriminelle landskapet beskrives som et kriminelt økosystem, eller et løst sammenkoblet nettverk av profesjonelle kriminelle, der grensekryssende samarbeid foregår både flytende og systematisk. For det andre kan den organiserte kriminaliteten true den alminnelige tryggheten gjennom voldshandlinger i det offentlige rom, slik en har sett i blant annet Sverige, Nederland og Belgia.

Kriminelle nettverk vil i økende grad bruke Norge som transittland for narkotika

Kriminelle nettverk involvert i narkotikasmugling har tradisjonelt benyttet godstrafikk langs landeveien for å føre inn narkotika til Norge. I 2023 har imidlertid politiet registrert en økning i narkotikabeslag i forbindelse med godstransport på skip. Tre rekordstore kokainbeslag på til sammen to tonn* ble alle innført via skipscontainere med opprinnelse i Sør-Amerika. I alle tilfellene benyttet de kriminelle nettverkene seg av legale strukturer for matvaretransport, ved at de forsøkte å skjule innførslene i regulær godstransport. I tillegg ble det i april 2023 beslaglagt over 100 kilo kokain som var festet på skroget til et skip som lå til kai på Vestlandet. Også dette beslaget hadde opprinnelse i Sør-Amerika.[56]

Norges kystlinje er spesielt lang og uoversiktlig. Store avstander, lange fjordarmer og mange anløpsmuligheter gjør maritim kontroll til en ressurskrevende og vanskelig oppgave. Norske havner fremstår derfor som attraktive innførselspunkter for kriminelle nettverk som vil smugle kokain i containere og fraktskip fra Sør-Amerika.[57]

Det å være et attraktivt innførselspunkt fører til potensielle trusler, både mot den alminnelige tryggheten og mot sentrale samfunnsstrukturer. Havnebyene Antwerpen og

* Henholdsvis 712 kg, 803 kg og 503 kg

Rotterdam, som er Europas mest populære transittpunkter for transatlantisk kokainsmugling,[58] har for eksempel sett en økning i vold (inkludert bruk av skytevåpen og eksplosiver) i forbindelse med kriminelle nettverks rivalisering om narkotikamarkedet.[59] Dette har ført til skader og drap på uskyldige – som for eksempel i Nederland, der kriminelle nettverk involvert i kokainsmugling målrettet har drept uskyldige tredjepersoner for å hindre vitnemål i en rettssak.[60] Andre trusler inkluderer korrupsjon av havnearbeidere, skipsmannskap, tolltjenestemenn, politi og andre myndigheter.[61] Dette er potensielle trusler og sårbarheter som anses som relevante også i norsk og nordisk sammenheng.[62]

NARKOTIKABESLAG I 2023

I 2023 var det 7 prosent flere saker der det ble gjort beslag av narkotika, sammenlignet med året før. Dette skjer etter at antallet saker har vært nedadgående helt siden 2014. Mengden beslaglagt kokain er flere titalls ganger større enn normalt, og styrkegraden i kokainen er svært høy. Det er også gjort flere beslag av svært potente syntetiske opioider i 2023, inkludert nitazener og fentanyl. Slike syntetiske stoffer er ofte svært sterke, noe som øker risikoen for overdoser.[63] Parallelt med at nye syntetiske opioider når det norske narkotikamarkedet, har den internasjonale produksjonen av heroin falt drastisk. Taliban nedla i 2022 et forbud mot all opiumsproduksjon i Afghanistan. Ettersom Afghanistan utgjør kilden til nesten all heroin i Europa, kan dette føre til at konsumenter av heroin og andre opioider tyr til de syntetiske opioidene som erstatning.[64]

Narkotiske stoffer har generelt hatt en høy verdi på det ulovlige narkotikamarkedet. Politiet estimerer at markedsprisen på 1 kg kokain ligger et sted mellom 300 000 - 500 000 kr, 1 kg heroin på 100 000 - 250 000 kr og 1 kg marihuana på 50 000 - 100 000kr. Til sammenligning er det anslått at innkjøpsprisen på 1 kg kokain i opprinnelseslandene i Sør-Amerika ligger på inntil 30 000kr,[65] altså drøye 10 prosent av prisen på det norske markedet. Dette tydeliggjør hvorfor narkotika kan være svært lukrativt for kriminelle organisasjoner.

MARKEDSPRIS I NORGE:

1 KG KOKAIN
300 000 – 500 000

1 KG HEROIN
100 000 – 250 000

1 KG MARIHUANA
50 000 – 100 000

TRANSNASJONALE KRIMINELLE NETTVERK I NORGE

Trusselen fra transnasjonale kriminelle nettverk som opererer i eller mot Norge, vil materialisere seg på ulike måter i 2024. Marokkanske kriminelle nettverk vil utgjøre en betydelig trussel innen innførsel og distribusjon av cannabis og kokain til Norge. Albanskspråklige kriminelle nettverk forventes å utgjøre en betydelig trussel innen innførsel og distribusjon av kokain. Litauiske kriminelle nettverk tilbyr viktige transport- og logistikktjenester for andre kriminelle nettverk i Europa og Norden, og vil fortsette å transportere store mengder narkotika til Norge.

Norsk politi er kjent med at noen narkotikakriminelle nettverk som opererer mot Norge, har transatlantiske forbindelser som blant annet gir dem direkte adgang til produksjonsledd for kokain i Sør-Amerika. Blant de store nettverkene i Europa har særlig albanske og marokkanske aktører direkte forbindelser til Sør-Amerika. Disse nettverkene sitter på store deler av verdikjeden fra det produksjonsstyrende leddet til distribusjons- og omsetningsleddet i europeiske byer. Denne lukrative handelen domineres av noen av Europas største kriminelle nettverk, inkludert nettverk fra Italia, Marokko og land på Balkan.

Kriminelle nettverk og aktører vil i hovedsak samarbeide med andre der dette fører til profitt, uavhengig av forskjeller i nasjonalitet, etnisitet og kulturell eller religiøs tilhørighet. Kriminelle nettverk opererer i en kriminell næringskjede som ligner legale forretningsmodeller. Fra det øverste organisatornivået hos narkotikakriminelle nettverk i Colombia, Italia, Albania og Marokko til narkotikaselgere i Norge, styrer profittmotivet både drift, handlemåter og den stadige skiftende konteksten for hvem som velger å samarbeide med hvem. Selv om trusselen fra transnasjonale kriminelle nettverk primært foregår i det skjulte, er størrelsen på verdiene som omsettes av en slik orden at den truer samfunnssikkerheten i Europa.


NORGE
LITAUEN
ITALIA
ALBANIA
MAROKKO

Økt aktivitet fra svenske kriminelle nettverk i Norge kan føre til flere voldshendelser

De siste årene har Sverige i økende grad opplevd alvorlige og dødelige voldshendelser som følge av kriminelle nettverks rivalisering innenfor narkotikakriminalitet. Enkelte av nettverkene har høy volds- og fryktkapital og har bygd nettverket som en egen merkevare.

I 2023 har samtlige politidistrikter i Norge registrert aktivitet knyttet til svenske kriminelle aktører. Aktiviteten handler i all hovedsak om narkotikavirksomhet og innpass på det norske narkotikamarkedet. Graden av aktivitet i de ulike distriktene varierer. Enkelte svenske kriminelle nettverk har hatt narkotikavirksomhet i Norge i flere år og har gode relasjoner til norske kriminelle nettverk. I andre tilfeller er det svenske kriminelle nettverk eller aktører som er i en etableringsfase på narkotikamarkedet i et distrikt. I noen distrikter er det kun ett enkelt narkotikabeslag som knyttes til kjente svenske kriminelle nettverk.

Det har vært flere tilfeller der svenske kriminelle aktører har utøvet vold i Norge, både på bestilling fra norske kriminelle og som ledd i egen virksomhet. Økt aktivitet i Norge kan føre til konflikt med eksisterende kriminelle nettverk i Norge, eller en forlengelse av eksisterende konfliktlinjer i Sverige.

Aktiviteten fra svenske kriminelle aktører i Norge vil øke i det kommende året, primært innen narkotikavirksomhet. Norge fremstår som et attraktivt marked for disse aktørene på grunn av allerede etablerte relasjoner i Norge og muligheter for større profitt som følge av høyere gate-salgspris.[66] Gitt siste års utvikling og medieoppmerksomhet knyttet til gjengkriminalitet i Sverige, kan tilstedeværelsen av svenske kriminelle aktører i Norge påvirke den opplevde tryggheten i befolkningen.

I kampen om markedsandeler og territoriell kontroll i Sverige har de kriminelle nettverkene bevisst brukt uerfarne ungdommer under kriminell lavalder til å begå drap og alvorlige voldshandlinger. Rekrutteringen har foregått på sosiale medier og krypterte kommunikasjonsplattformer. Det er ikke observert en slik kynisk og målrettet rekruttering

Overlevering av narkotika. Foto: Politiet

av barn til å utføre voldshandlinger i Norge. Samtidig gjør den tilsynelatende økende normaliseringen av vold og rus, sammen med tilgjengelighet via sosiale medier, at ungdom kan være mer sårbare for slik rekruttering.

Kriminelle nettverk utnytter legale strukturer til å smugle personer inn i landet

De to siste årene har det vært en økning i antall personer som har blitt smuglet til Norge, blant annet ved hjelp av kriminelle nettverk. Flere norske nettverk har over tid blitt mer profesjonelle, ved at de eksempelvis benytter legale strukturer, som norske firmaer, for å gjennomføre menneskesmuglingen. Enkelte av nettverkene har vært involvert i menneskesmugling over flere år og har vist stor tilpasningsevne som respons på tiltak fra politi- og kontrollmyndigheter.

Menneskesmugling er en lukrativ virksomhet, der prisen til Norge varierer mellom 50 000 og 250 000 kroner per person. Nettverkene som smugler personer inn til Norge for at de skal søke asyl, bruker flere fremgangsmåter. Det vanligste er at ID-dokumenter misbrukes for å smugle migranter med fly fra Sør-Europa, eller at migrantene blir transportert landeveien.

Nettverkene som tilrettelegger for å legalisere opphold for arbeid, gjør dette gjennom å bruke falske dokumenter som bekrefter utdanning eller arbeidserfaring. Søknad om oppholdstillatelse for arbeid krever omfattende dokumentasjon av identitet og utdanning, i tillegg til blant annet et konkret tilbud om arbeid fra en arbeidsgiver i Norge. Nettverkene opererer i flere bransjer, og aktører både i utlandet og i Norge er involvert i de ulike prosessene. Kriminaliteten er en trussel for liv og helse, ved at personer uten nødvendig kompetanse utfører arbeid, blant annet i bilverksteder og i bygg- og anleggsbransjen. Det er også et potensial for at de som smugles, utnyttes i arbeidslivet etter ankomst til Norge.

Noen av menneskesmuglingsnettverkene kan også knyttes til annen alvorlig organisert kriminalitet, blant annet narkotika-, økonomisk- og arbeidslivskriminalitet. De opererer hovedsakelig fra Østlandet, men de er også etablert i andre deler av landet.

Ulovlig inn- og utførsel av kontanter, dyr og varer kan true folkehelsen og finansiere kriminalitet

Politiet har informasjon som tilsier at ulovlig inn- og utførsel av kontanter og varer kan kobles til internasjonale kriminelle nettverk.[67] Smugling av ulovlige eller udeklarerte varer fører til tapte skatteinntekter og kan utgjøre en fare for befolkningens liv og helse.

Årlig deklareres det inn mellom åtte og ti milliarder kroner i kontanter til Norge, mens beløpet som deklareres ut, er betydelig lavere. Store deler av denne differansen smugles ut av Norge. Sirkulasjonen av norske kontanter over landegrensen involverer flere ulike aktører. Transporten skjer eksempelvis gjennom pengekurérer på fly eller i vogntog, sammen med annen legal varetransport, eller i personbiler.[68] Aktørene som frakter kontanter ut av Norge, er ofte del av et større internasjonalt vekslernettverk som samarbeider om overføringer ved behov. Formålet kan være å benytte kontanter som oppgjør for illegale varer, hvitvaske penger eller finansiere terror.

Ulovlig import av matvarer fører til en betydelig trussel mot matsikkerheten i Norge. Dette skyldes en risiko for at matvarene ikke har vært håndtert og oppbevart på riktig måte, og at det er vanskelig å spore hvor matvarene faktisk kommer fra. Dette er spesielt alvorlig ved ulovlig omsetning av kjøttvarer, ost og sjømat. Hygienekravene til merking, håndtering og oppbevaring er strenge for å sikre forbrukerne mot sykdom.

Ulovlig innførsel av kjæledyr og truede arter utgjør en risiko for folkehelsen.[69,70] Dyr som innføres ulovlig til Norge, kan være bærere av sykdommer og parasitter som er potensielt dødelige for både mennesker og dyr, slik som rabies og bendelorm.[71] Nettverkene som smugler kjæledyr og truede arter, er tilsynelatende ofte også innblandet i annen kriminalitet.

Det er avdekket flere tilfeller der norske aktører som også er kjent for annen kriminalitet, importerer og videreselger falske merkevarer i Norge, også omtalt som *IPR-kriminalitet*. Typiske varer som importeres, er dyre merkeklær, kosmetikk og husholdningsvarer. I EU er det et kjent problem at IPR-kriminalitet benyttes av organiserte kriminelle nettverk for å finansiere annen alvorlig kriminalitet.[72] Det er ikke kjent hvorvidt IPR-kriminalitet benyttes til å finansiere annen organisert kriminalitet i Norge.

MISBRUK AV NORSKE BORGERES IDENTITET

Hvert eneste år meldes i overkant av 30 000 norske pass tapt. Noen av passene blir stjålet gjennom målrettede tyverier av turister i europeiske storbyer. Dette, i kombinasjon med en stor kriminell industri som produserer falske dokumenter, gjør at kriminelle har enkel tilgang på identiteter de kan benytte for å gjennomføre ulike former for kriminalitet.

Stadig flere norske borgere får sin digitale identitet misbrukt. Store mengder personopplysninger som tilhører norske borgere, ligger tilgjengelig for salg på det mørke nettet og på ende-til-ende-krypterte meldingsplattformer. Kriminelle kan bruke slike opplysninger til å skjule kriminell aktivitet. Eksempler kan være å opprette kontoer for krypto-valuta for å skjule pengespor eller å opprette mobil-abonnement for å skjule kommunikasjon.

Ifølge Europol går pengene fra denne kriminelle industrien til å finansiere og styrke komplekse organiserte kriminelle nettverk. Disse innbefatter blant annet økonomisk svindel, narkotika, menneskehandel og terrorisme.

Bryggen i Bergen. Foto: Politiet

3.5

KRIMINALITET I USIKRE TIDER

Ved overgangen til 2024 står vi både politisk, økonomisk og miljømessig i en mer usikker og uforutsigbar verden enn på lenge. Dette kapittelet handler om kriminalitet som helt eller delvis kan sies å være et resultat av disse usikre tidene. Kriminaliteten kan true felles samfunnsverdier, som for eksempel ytringsfrihet, alminnelig trygghet i det offentlige rom og bevaring av natur som et vern mot effekten av klimaendringer. En av truslene som trekkes frem i kapittelet viser også hvordan aktivisme kan arte seg i en digital verden, herunder hvordan politisk motiverte grupperinger gjennomfører digitalt skadeverk ved bruk av tjenestenektangrep.

Trusler og hatefulle ytringer kan føre til polarisering og begrense deltakelsen i den offentlige debatten

Ytringsfriheten står sterkt i Norge, sammenlignet med de fleste andre land i verden.[73] Ytringsfrihet er et avgjørende prinsipp i norsk rett, og selv om straffeloven forbyr noen typer alvorlige hatytringer, er de aller fleste ytringer tillatte.

Trusler og hatefulle ytringer rammer bredt og har en negativ innvirkning på både samfunnet og enkeltpersoner, uavhengig av om de er straffbare eller ikke. De kan bidra til eksklusjon, økt polarisering og til å begrense deltakelsen i den offentlige debatten. Slik kan trusler og hatefulle ytringer bidra til å undergrave demokratiet.

Det ble registrert i overkant av 400 anmeldelser av hatefulle ytringer i 2023. Majoriteten av disse er rettet mot hudfarge eller etnisitet. De to siste årene, og særlig etter terrorangrepet 25. juni 2022, har politiet imidlertid sett en økning i anmeldelser av hatefulle ytringer rettet mot skeive. Det er uvisst om dette skyldes en reell økning, eller om flere er tilbøyelige til å anmelde. Økningen har vedvart i 2023.

De hatefulle ytringene rammer også transpersoner, der det offentlige ordskiftet fremstår svært polarisert. Det har vært en eksplosiv økning i antall twittermeldinger om transpersoner de siste årene, fra om lag 1500 i 2018 til nær 24 000 i 2022. Nesten halvparten av meldingene hadde en kritisk tilnærming. Både transpersoner og Pride ble omtalt stadig mer kritisk på både Twitter og Facebook i denne perioden.[74]

Også mange politikere blir utsatt for hatefulle ytringer og/eller trusler. Dette skjer hovedsakelig via sosiale medier. En nylig publisert kartlegging av omfanget av hatefulle ytringer og trusler mot lokalpolitikere, viser at over 40 prosent av de som har opplevd dette, har endret adferd, for eksempel i form av selvmoderering. Godt over halvparten av denne gruppen har vurdert å slutte som politiker.[75]

Styrket samarbeid mellom politisk motiverte kriminelle grupperinger kan øke trusselen mot Norge

Tjenestenektangrep* er et angrepsmiddel som er enkelt og lett tilgjengelig, og som oftest benyttes av politisk motiverte kriminelle grupperinger som opererer på internett – såkalte *hacktivister*.** Slike angrep regnes som digitalt skadeverk, dog med begrenset skadeeffekt, fordi angrepene

* Tjenestenektangrep utføres oftest ved å overbelaste nettverkskapasitet eller andre ressurser, eller ved å blokkere en tjeneste eller funksjon.

** Eksempelvis KillNet, Anonymous Sudan og REvil.

som regel er ment for å påvirke politiske prosesser og rammer nettsider som ikke er direkte koblet til drift eller en virksomhets interne systemer.[76]

I løpet av det siste året er det observert at hacktivist-grupperinger i økende grad søker å samarbeide. Denne typen samarbeid kan utvide grupperingenes samlede kompetanse og kapasitet og øke evnen til å gjennomføre mer kompleks og skadelig cyberkriminalitet – for eksempel datainnbrudd, datatyveri og digitalt skadeverk. Nasjonal Sikkerhetsmyndighet (NSM) rapporterer om en bekymring for at angrepsformen er i utvikling, ved at mer sofistikerte teknikker tas i bruk og kan rettes mot sårbare punkter i virksomheters nettverk. NSM viser også til at erfaringen fra utlandet er at angrepene blir mer sofistikerte og vanskeligere både å oppdage og beskytte seg mot.[77]

Økt samarbeid mellom hacktivistgrupperinger kan utgjøre en økt trussel for Norge, fordi det nettopp er slike grupperinger som ofte står bak tjenestenektangrep. Politiet ser at det har vært en massiv økning i slike typer digitale skadeverk det siste året, utført av ulike politiske grupperinger. Angrepene har typisk vært rettet mot høyteknologi, næring og offentlig forvaltning, men det siste året har det særlig vært en økning i prorussiske aktører som har angrepet virksomheter i transport-, finans- og helsesektoren. De sistnevnte er sektorer som ikke har vært typiske mål tidligere.[78] Det er antatt at vestlig støtte til Ukraina har ført til økt samarbeid og styrket samhold blant disse grupperingene.

En mulig årsak til økningen i tjenestenektangrep mot norske mål kan være Norges tydelige støtte til Ukraina. Ettersom Norge spiller en sentral rolle, både ved å sende militært utstyr til frontlinjen og gjennom politiske prosesser tilknyttet NATO, bidrar dette til å sette Norge på kartet for politisk motiverte kriminelle.

Spenningsnivået i diasporamiljøer kan føre til flere voldelige konfrontasjoner

I løpet av det siste året har flere markeringer og demonstrasjoner i det offentlige rom resultert i vold mellom partene. Disse har i all hovedsak hatt bakgrunn i konflikter mellom eller innad i diasporagrupperinger i Norge. Enkelte av de involverte har også rettet aggresjon mot norsk politi, noe som har skjedd spontant under markeringene.

De til dels voldelige markeringene har ofte funnet sted i forbindelse med andre grupperingers lovlige sammenkomster eller demonstrasjoner. Ved å forsøke å hindre ytringsfriheten til grupperinger de er motstandere av, truer demonstrantene ved slike motmarkeringer demokratiske prinsipper, som forsamlings- og ytringsfrihet. Tilsvarende utvikling ser vi også i andre europeiske land, om enn med enda mer voldsbruk. Det har også der blitt rettet voldelig aggresjon mot landets politi.

Det rapporteres også om alvorlige trusler innad i diasporamiljøer, uten at disse nødvendigvis blir politianmeldt. Årsaken til at truslene ikke blir anmeldt, kan være språkbarrierer og manglende tillit til myndighetene.

Konfliktnivået i disse miljøene har potensial til å utløse ytterligere voldshendelser i kommende konfrontasjoner.

Potensiell høy fortjeneste og lav oppdagelsesrisiko fører til ulovlige naturinngrep og arealendringer

Ulovlige naturinngrep og arealendringer forekommer i hele Norge. Overtredelsene skjer blant annet på privat eiendom, i naturreservater, på fjellet, i våtmark, i skog og i strandsonen. De omfatter ulovlige byggetiltak, etablering av veier, graving og sprengning, uttak- og oppfylling av masser i naturen, terrengendringer og hogst. Det er stor variasjon i overtredelsene, både i type og alvorlighetsgrad. I mange tilfeller ødelegges natur og økosystemer permanent eller for veldig lang tid. I tillegg rammes et bredt spekter av sårbare naturtyper og dyre- og plantearter. Få saker politianmeldes.

Inngrepene begås av privatpersoner, næringsdrivende og kommuner. Mange av inngrepene skjer i tilknytning til, eller i nærheten av, eksisterende bebyggelse eller i forbindelse med annet anleggsarbeid. Saker som omhandler ulovlig

oppfylling av masser og ulovlig bruksendring av bygg, kan utgjøre en fare for menneskers liv og helse. I 2022 ble flere kommuner anmeldt for overtredelse av plan- og bygningsloven. Som ansvarlig planmyndighet behandler kommunen de fleste søknader om byggetillatelse. Dobbeltrollen som oppstår når kommunen «sitter på begge sider av bordet» i en planprosess, øker trolig risikoen for overtredelser. Det kan svekke den allmennpreventive effekten når den ansvarlige myndigheten selv blir anmeldt for lovbrudd, noe som kan bidra til å undergrave samfunnsstrukturer og demokratiske prinsipper. Ulovlige naturinngrep og arealendringer skjer også i sammenheng med andre typer kriminalitet. Blant annet er det etterforsket korrupsjonssaker i kommunale etater.[79]

Majoriteten av de anmeldte er privatpersoner som begår lovbrudd på egen eiendom. Ulovlige inngrep og bygging kan gi økonomisk gevinst gjennom at eiendommen øker i verdi, og ved at man sparer tid og utgifter knyttet til søknadsbehandling. I flere saker viser gjerningspersonene gjentakelse og forsett, noe som kan skyldes at potensialet for kostnadsbesparelser og fortjeneste er betydelig, og at oppdagelsesrisikoen er lav. Dispensasjon anses av enkelte som en formalitet, og noen satser trolig på at det er lettere å be om tilgivelse enn tillatelse. Lovbrudd som avdekkes, får ofte minimale konsekvenser.[80]

Klimaendringer kan forverre konsekvensene av ulovlig hogst

Klimaendringer i form av økt nedbørsmengde og mer ekstremvær kan gi store skader på samfunnets infrastruktur og i verste fall sette liv og helse i fare.[81] Skog bidrar til å regulere avrenningen fra nedbørfelt og beskytter dermed mot effektene av klimaendringer, blant annet ved å hindre flom, erosjon og skred. Til tross for at vi har ordninger som skal beskytte sårbar og viktig natur, foregår det i dag ulovlig hogst av verdifull skog. Dersom omfanget av ulovlig hogst opprettholdes, kan dette gjøres oss mindre i stand til å håndtere klimaendringene fremover. Ulovlig hogst vil dermed få langt mer alvorlige og kostbare konsekvenser enn det vi allerede ser i dag.[82]

Både skogbrukslova og naturmangfoldloven skal beskytte naturen og motvirke skadefølger av lovovertredelser. Overtredelsene omfatter blant annet hogst som er utført uten lovpålagt miljøkartlegging, og hogst som er utført til tross for at nøkkelbiotoper* er kjent og registrert ved lokaliteten.

Antallet anmeldelser er lavt, og de fleste saker som gjelder ulovlig hogst, fremstår isolert sett som lite inngripende. Samlet kan slike overtredelser likevel føre til alvorlig skade. Dette gjelder ikke minst fordi skadene i mange tilfeller er irreversible.[83] Lovbruddet får i de fleste tilfeller ingen eller minimale konsekvenser for gjerningspersonen. Mye tyder på at verken regelverket i seg selv eller myndighetenes håndheving av dette har en avskrekkende virkning. Lav oppdagelsesrisiko, kombinert med potensial for fortjeneste, er faktorer som kan bidra til at ulovlig hogst i Norge vil fortsette.

I februar 2024 anmeldte Statsforvalteren i Trøndelag ulovlig hogst i Bymarka naturreservat i Trondheim. Foto: Carina Ulsund / Statsforvalteren i Trøndelag

* Et område som er særlig viktig for bevaring av det biologiske mangfoldet.

REFERANSER

1. Kripos. 2024. *Nasjonal drapsoversikt – drap i Norge 2013-2023.*
2. Folkehelseinstituttet. 2023. *Narkotikabruk i Norge* (09.02.2023).
3. Kripos. 2023b. *Narkotika- og dopingstatistikk 2023*.
4. Kripos. 2023a. *Cyberkriminalitet 2023;* Kripos. 2023c. *Nasjonal trusselvurdering. Nasjonal operasjon rettet mot kriminelle nettverk (KN).* Offentlig versjon; Kripos. 2023d. *Generativ kunstig intelligens og cyberkriminalitet*; Økokrim. 2022a. *Økokrims trusselvurdering 2022*.
5. Europol. 2023a. *The other side of the coin. An analysis of Financial and Economic Crime*; Euronews. 2021. *Europe has reached a 'breaking point' over organised crime, says Europol* (12.04.21).
6. Kripos. 2023c.
7. Kripos. 2023c.
8. Kripos. 2023a.
9. Økokrim. 2023f. *Bedrageri – et samfunnsproblem.*
10. Klima- og miljødepartementet. 2021. *Slik kan vi tilpasse oss klimaendringene* (22.10.2021).
11. Økokrim. 2023c. *Ulovleg hogst.*
12. NOU 2023:17. *Nå er det alvor - Rustet for en usikker fremtid.*
13. NOU 2023:14. *Forsvarskommisjonen av 2021. Forsvar for fred og frihet.*
14. Helsedirektoratet. 2023. *Kunnskapsoppsummering om ulikheter i helse og livskvalitet i Norge siden 2014 – sammendrag.*
15. Statistisk sentralbyrå. 2024. *Færre barn lever i familier med lavinntekt* (18.1.24).
16. Statistisk sentralbyrå. 2023. *Hvor mange er fattige i Norge?* (14.6.23).
17. Savage. 2009. *The Development of Persistent Criminality.* Oxford University Press.
18. NOVA. 2018. *Muligheter og hindringer for barn i lavinntektsfamilier*. *En kunnskapsoppsummering.* Rapport 11-2018.
19. NOVA. 2018.
20. Statistisk Sentralbyrå. 2024.
21. Kripos. 2023a.
22. Kripos. 2023d.
23. Kripos. 2023d.
24. Kripos. 2023a.
25. Ipsos. 2020. *Hatefulle ytringer og trusler mot lokale folkevalgte. Rettslige rammer, rettspraksis og kommunesektorens praksis*; Ipsos. 2023. *Hatytringer, trusler og desinformasjon mot folkevalgte.*
26. FN. 2023. *Providing legal options to protect the human rights of persons displaced across international borders due to climate change*. A/HRC/53/34.
27. Forsvarets forskningsinstitutt. 2021. *Samfunnsutvikling frem mot 2030*. Rapport 21/01132.
28. Europol. 2021. *Serious and Organised Crime Threat Assessment (SOCTA).*
29. Norsk senter for informasjonssikring (NorSIS). 2023. *Hva er løsepengeangrep?* (02.08.2022).
30. Kripos. 2023a.
31. NSM. 2023. *Nasjonalt digitalt risikobilde 2023.*
32. Recorded Future. 2023. *Threat Analysis 2022 Annual Report.*
33. NSM. 2023.
34. Europol. 2023a.

35. Finanstilsynet. 2023. *Risikovurdering 2023. Hvitvasking og terrorfinansiering.*
36. Norges Sjømatråd. 2023. *Norge eksporterte sjømat for 151,4 milliarder kroner i 2022* (06.11.2023).
37. NOU 2019:21. *Framtidens fiskerikontroll. Nærings- og fiskeridepartementet.*
38. Politiet. 2023a. *Politiets trusselvurdering 2023.*
39. Økokrim. 2022a.
40. Økokrim. 2023a. *Status arbeidsmarkedskriminalitet juni 2023.*
41. TV2. 2023. *POLITIET ADVARER: Gutter blir lurt og presset for penger: – Alvorlig* (23.7.23).
42. ECPAT. 2023. *Då tog "hon" en screen og allt började. En rapport om sexuell utpressning av barn i ekonomiskt syfte med särskilt fokus på pojkars utsatthet.*
43. Thorn, Stroebel og Portnoff. 2023. *Generative ML and CSAM: Implications and Mitigations.* Standford: Internet Observatory. Cyber Policy Center.
44. NRK. 2023c. *Kunstig intelligens brukt til å generere falske nakenbilder av mindreårige jenter i Spania* (25.09.2023).
45. ECPAT. 2023.
46. Kripos. 2019. *Seksuell utnyttelse av barn og unge over internett.*
47. Kripos. 2022. *Ungdom henges ut på nett: Deling av ulovlig og bekymringsverdig materiale av barn og ungdom.*
48. Kripos. 2022.
49. Politiet. 2023b. *DELE=DELTA: Om deling av voldsvideoer*
50. Kripos. 2019.
51. Oslo Politidistrikt. 2018. *Trender i kriminalitet 2018-2021. Digitale og globale utfordringer.*
52. Økokrim. 2022b. *Økokrims årsrapport 2022.*
53. NRK. 2023a. *I grenseland* (22.01.2023).
54. Europol. 2021.
55. Europakommisjonen. 2021. *EU-strategi for bekjempelse av organisert kriminalitet 2021-2025.*
56. NRK. 2023b. *Slik avslørte politiet og Tolletaten rekordbeslaget* (19.11.2023).
57. Kripos. 2023c.
58. Politico. 2023a. *Europe's got a problem' – Drug violence grips Belgium's second largest city;* Euronews. 2023. *Antwerp takes over from Rotterdam as Europe's leading port for cocaine seizures (10.01.2023).*
59. Europol. 2023b. *Criminal networks in EU ports: Risks and challenges for law enforcement.* Joint report of Europol and the Security Steering Committee of the ports of Antwerp, Hamburg/Bremerhaven and Rotterdam; EMCDDA. 2022. *'Cocaine: increasingly attractive for a wide range of criminal networks'.*
60. EMCDDA. 2022.
61. Global Initiative Against Transnational Organized Crime & InSight Crime. 2021. *The Cocaine Pipeline to Europe*; Europol. 2023b.
62. Kripos. 2023c.
63. Kripos. 2023b.
64. UNODC. 2023. *Afghanistan opium cultivation in 2023 declined 95 per cent following drug ban: new UNODC survey*. Press release.
65. GI-TOC & InSightCrime. 2021.
66. Kripos. 2023c.
67. Økokrim. 2022a.
68. Økokrim. 2023b. *Nå er det NOK – kontanter i den kriminelle økonomien.*
69. Økokrim. 2022a.
70. Mattilsynet. 2022. *Mattilsynet deltar i europeisk storaksjon mot smugling av kjæledyr* (03.11.2022).
71. Mattilsynet. 2023. *Hvordan unngå å kjøpe ulovlig innført hund* (21.03.2023).
72. Europol. 2022. *Intellectual Property Crime Threat Assessment 2022.*
73. NOU 2022:9. *En åpen og opplyst offentlig samtale – Ytringsfrihetskommisjonens utredning.*
74. Analyse & Tall. 2023. *Ytringsklimaet for skeive på Twitter og Facebook.*
75. Ipsos. 2023.
76. Kripos. 2023a.
77. NSM. 2023.
78. NSM. 2023.
79. Økokrim. 2023d. *Ulovlige naturinngrep og arealendringer.*
80. Økokrim. 2023d.
81. Økokrim. 2023e. *Miljøkrim*, nr.1. 2023.
82. Økokrim. 2023c.
83. Økokrim. 2023c.

POLITIET

Politiets trusselvurdering 2024

Utgiver: Kripos

politiet.no/trusselvurdering