ØKOKRIM

TRUSSEL-VURDERING 2024

– Den kriminelle økonomien

Trusselvurdering 2024, Økokrim
Grafisk formgivning: Økokrim
Opplag og trykk: 500x, Aksell

Foto: Unsplash

Forord

Norsk politi har over flere år arbeidet for å møte trusselen fra organisert kriminalitet gjennom en nasjonal satsing mot kriminelle nettverk. Fra 2024 og fremover styrkes dette arbeidet betydelig. Ved siden av den mer tradisjonelle hvitsnippkriminaliteten er Økokrim også tungt involvert i dette arbeidet. Nettverkene utgjør en betydelig kriminalitetstrussel og det er derfor også naturlig at Økokrim vier dette stor oppmerksomhet. Denne trusselvurderingen har fokus på de mer finansielle og økonomiske aspektene av den profittmotiverte kriminaliteten til nettverkene.

I den kriminelle økonomien omsettes ulovlige varer og det jobbes svart. Kontanter er utbredt, men også desentraliserte betalingsløsninger og kryptovaluta benyttes. Samtidig blir kriminelt utbytte reinvestert i den legale økonomien. Skillet mellom kriminelle nettverk og legalt næringsliv blir derfor gradvis visket ut. Profesjonelle tilretteleggere og innsidere selger sine tjenester til kriminelle aktører, og bidrar dermed til å tilsløre og tilrettelegge for kriminell virksomhet.

Norge er et lite og tillitsbasert samfunn og vi har generelt et høyt velferdsnivå. Åpenhet er et grunnprinsipp for det norske demokratiet og viktig for at befolkningen skal ha tillit til myndighetene. Samtidig er åpenhet og tillit faktorer som er sårbare for utnyttelse fra både kriminelle og statlige aktører. Utstrakt utnyttelse av velferdsordningene uten at kontrollorgan evner å stoppe dette, kan redusere befolkningens tillit til myndighetene.

Den kriminelle økonomien har innslag av trusler, vold og sosial manipulering. Aktørene blir også stadig mer profesjonelle. Dette stiller høye krav til tverrfaglig kompetanse, evne til prioritering og samarbeid internt i politiet, i tillegg til samhandling med andre kontrolletater og med næringslivet. Økokrim har en sentral rolle i dette arbeidet. Vi ønsker at denne trusselvurderingen skal bidra til å gi et oppdatert og samstemt situasjonsbilde slik at vi sammen kan iverksette risikoreduserende tiltak.

Pål K. Lønseth // *Sjef for Økokrim*

Innhold

Innledning

Økokrims trusselvurdering utarbeides hvert annet år. Formålet med trusselvurderingen er å presentere kriminalitetstrusler Økokrim mener vil medføre de mest alvorlige konsekvensene for samfunnet vårt de neste to årene.

I denne trusselvurderingen har vi fokus på den kriminelle økonomien og kriminelle nettverk som begår økonomisk kriminalitet. Miljøkriminalitet og dyrevelferdskriminalitet er viet mindre oppmerksomhet, men ansees fortsatt som en alvorlig trussel med store konsekvenser for både dyr og mennesker, natur og miljø.

Økonomisk kriminalitet og den kriminelle økonomien er i stor grad usynlig for folk flest. Det økonomiske tapet rammer ofte befolkningen indirekte, som ved bedrageri av velferdssystemene våre og unndragelse av skatt. Økonomisk kriminalitet kamufleres også ofte blant legale aktiviteter og i den legale vare- og pengeflyten, noe som gjør det vanskelig selv for myndighetene å avdekke hva som foregår.

Ofre som rammes direkte økonomisk, som ved bedrageri, oppfatter ikke alltid at de er utsatt for kriminalitet på grunn av manipulasjon. På samme måte kan foretak som utkonkurreres i anbudsprosesser være offer for korrupsjon uten at de vet det.

Rapportens oppbygning

Innledningsvis i rapporten presenteres de mest alvorlige truslene innen økonomisk kriminalitet de neste to årene. Deretter beskrives sårbarheter, anbefalinger og faktorer i samfunnet som påvirker kriminaliteten. I rapporten fremheves sentrale elementer og utviklingstrekk innen den kriminelle økonomien, som tilretteleggere for økonomisk kriminalitet og sammenblandingen av statlig virksomhet og kriminalitet. Vi trekker også frem to kriminalitetstrusler som rammer samfunnet og miljøet vårt på ulikt vis: bedrageri og arbeidslivskriminalitet.

Rapporten er basert på politiets informasjonskilder, inkludert hvitvaskingsregisteret, samt åpne kilder.

Hovedutfordringer

Nedenfor presenteres truslene innen økonomisk kriminalitet som Økokrim forventer vil være de mest alvorlige de neste to årene. Truslene er tett sammenvevd, påvirker hverandre og forekommer i alle deler av næringslivet.

Organiserte kriminelle aktører integrerer kriminalitet og utbytte i legal virksomhet
De senere årene har vist at økonomisk kriminalitet og organisert kriminalitet er tett sammenvevd. Europol erfarer at mer enn 80 prosent av kriminelle nettverk i Europa misbruker legale selskapsstrukturer, og at to tredjedeler aktivt benytter korrupsjon.[1]

Kriminelle nettverk i Norge har blitt en integrert del av den legale økonomien. Nettverkene oppretter foretak hvor det innberettes fiktive ansatte og fiktive lønninger, som legges til grunn for bedrageri, og de begår arbeidslivskriminalitet. Utbytte fra lovbrudd investeres i eiendomsmarkedet, legal og illegal virksomhet blandes, og det benyttes stråpersoner i formelle roller i foretak for å skjule reelt eierskap. Kriminelle utnytter også velferdsordninger og mottar ulike ytelser fra det offentlige samtidig som de profitterer på kriminell virksomhet.

Løst sammensatte nettverk med tilgang på kompetanse
Mye av den alvorlige økonomiske kriminaliteten i dag er preget av ad hoc-basert samarbeid tuftet på hvilke oppgaver som til enhver tid skal utføres og hvilke tjenester det er behov for. Både varigheten på samarbeid og sammensetning av aktører varierer følgelig.

Kriminelle aktører og nettverk benytter profesjonelle tilretteleggere for at kriminaliteten skal fremstå legal og bli mer utfordrende å oppdage for kontrollmyndighetene. Teknologiske tjenester er også sentrale i gjennomføringen av alvorlig profittmotivert kriminalitet og hvitvasking. Personer med teknologisk kompetanse utvikler og tilbyr tjenester spesielt for dette formålet. Enkelte av disse tjenestene er brukervennlige også for personer med gjennomsnittlig teknologisk kompetanse, noe som bidrar til at digital kriminalitet kan utføres av stadig flere.

1 Europol, «Serious and organised crime threat assessment (SOCTA)», 2021.

Sammenblanding av statlig aktivitet og økonomisk kriminalitet
Den sikkerhetspolitiske situasjonen blir stadig mer tilspisset. Særlig russiske og kinesiske aktører utnytter konfliktlinjer i vestlige samfunn og tar i bruk ulike sammensatte virkemidler for å fremme sine lands interesser på bekostning av andre land.[2] I Sverige har Iran benyttet svenske kriminelle nettverk til å utføre voldshandlinger for seg.[3]

Stater Norge ikke har et sikkerhetssamarbeid med benytter seg av virkemidler som kan fremstå som kriminelle handlinger, og verktøy som fremstår som lovlig forretningsvirksomhet. Også attentat, som ser politisk motivert ut, kan være utført av kriminelle nettverk på vegne av andre stater. Politiet må derfor håndtere en rekke hendelser hvor aktørenes motiver ikke er kjent.

Fordekte transaksjonsstrømmer kan være en indikasjon på både sanksjonsomgåelser, terrorfinansiering og hvitvasking. På tilsvarende måte kan påvirkningsoperasjoner igangsatt av en statlig aktør, benytte de samme virkemidlene som benyttes i bedrageri – forledelse og manipulasjon.

Bruk av trusler og vold i økonomisk kriminalitet
Økonomisk kriminalitet har tradisjonelt ikke vært forbundet med høyt konfliktnivå og voldsutøvelse. Tvert imot har den i stor grad vært utøvd skjult for allmennheten. Dette er nå i endring.

Flere former for bedrageri kombineres nå med fysisk oppmøte hjemme hos ofrene. Manipuleringen både i forkant av og under møtet med fornærmede er også blitt mer kynisk. Det er eksempler på at fornærmede blir bedt om å forflytte seg til et sted bestemt av bedragerne og ikke kan kontakte andre i tiden bedrageriet pågår.

Flere norske aktører som er involvert i narkotikakriminalitet er også involvert i utøvelsen av bedrageri eller den etterfølgende gevinsthåndteringen. Dette har bragt med seg et noe høyere konfliktnivå i utøvelse av den økonomiske kriminaliteten med mer bruk av trusler og vold.

2 NSM, «Sammensatt virkemiddelbruk og påvirkning», hentet 02.10.2024.
3 NRK, «Justisministeren: - Iran bruker svenske kriminelle», hentet 09.10.2024.

Sårbarheter

Sårbarheter

Økonomisk kriminalitet er ikke tilstrekkelig prioritert i politiet
De siste fem årene har politiet henlagt i snitt 62 prosent av alle saker om økonomisk kriminalitet. En stor del av disse sakene er anmeldelser fra andre offentlige etater hvor det foreligger grundig dokumentasjon på alvorlige lovbrudd.[4]

Samtidig var inndragningstallene i 2023 omtrent på samme nivå som for 25 år siden til tross for et uttalt ønske om å prioritere inndragning av verdier som er brukt til, eller tilegnet gjennom kriminalitet.[5] De høye henleggelsestallene og lave inndragningstallene er et uttrykk for at økonomisk kriminalitet ikke oppnår tilstrekkelig prioritert blant politiets mange oppgaver.

Åpenhet og tillitsbaserte systemer
Åpenhet og tillit er viktige verdier i det norske samfunnet og ligger til grunn for flere av våre offentlige systemer og register. Mye informasjon om både privatpersoner og foretak ligger derfor offentlig tilgjengelig, også for kriminelle aktører.

Kriminelle innhenter slik offentlig tilgjengelig informasjon om for eksempel selskaper og ansatte. Denne informasjonen gir bedragerne innsyn i reelle hendelser i sanntid, som for eksempel kjøp, salg og endringer i registerinformasjon, noe de utnytter til kriminelle formål for å fremstå som troverdige. Ny teknologi vil gi kriminelle muligheter til å automatisere denne innhentingen ved hjelp av kunstig intelligens (KI) og eksempelvis kombinere informasjon fra flere kilder.

Påliteligheten til registerinformasjon som legges til grunn i offentlig forvaltning, velferdsytelser og finans utgjør også en sårbarhet. Opplysninger som enten er feilregistrert eller fiktive i et register blir ofte benyttet av andre offentlige etater og i finansnæringen. Manglende kvalitetssikring av informasjon og/eller korreksjon av opplysninger muliggjør at kriminelle kan fordekke eierskap ved bruk av stråpersoner og stråselskap. Kriminelle har også overtatt eierskap i foretak uten at reell eier har godkjent det, og manipulerer informasjonen i offentlige registre slik at de eksempelvis får foretak til å fremstå lønnsomme og ha fiktive ansatte.

Politiet henger etter teknologisk
Kriminelle tar raskt i bruk ny teknologi. Politiet må imidlertid forholde seg til lover, regler og retningslinjer før ny teknologi kan tas i bruk. Dermed øker gapet mellom de kriminelles og politiets bruk av teknologi, noe som gir de kriminelle økt handlingsrom i utøvelsen av kriminalitet. Dette fører også til at politiets arbeid med å identifisere, analysere og respondere på kriminalitetstrusler begrenses, og at politiets kunnskap om aktører, modus og omfang av kriminaliteten svekkes.

Manglende informasjonsdeling
I et totalforsvar mot økonomisk kriminalitet bidrar både offentlig og privat sektor i kriminalitetsbekjempelsen. Uten tidsriktig deling av informasjon om pågående modus, antatte gjerningspersoner og foretak som er implisert, vil ikke verken offentlige etater, næringsaktører eller finansinstitusjoner ha mulighet til å iverksette forebyggende tiltak.

I offentlig sektor har lovverk i noen grad blitt tilpasset for å lette informasjonsdeling, men like fullt deles det lite informasjon mellom etater. Etatene har ikke samme regelverk og de juridiske vurderingene knyttet til om informasjon kan deles gjøres ulikt i forskjellige offentlige etater. For politiet er det en særlig utfordring at andre offentlige etater i liten grad deler informasjon om personer og foretak som kan knyttes til lovbrudd. I tillegg gjøres vurderingen manuelt i hvert enkelt tilfelle. Dette gjør deling av informasjon ressurskrevende og terskelen for å dele høy.

Manglende informasjonsdeling kan også føre til at registre inneholder uriktige opplysninger. For å avdekke feilregistreringer og fiktive opplysninger, som ofte benyttes i kriminalitetsutøvelsen, må etatene dele oppdatert informasjon fra sine registre med andre etater.

4 Meld. St. 15 (2023-2024) «Felles verdier – felles ansvar».
5 Politihøgskolen, «Inndragning: en satsing uten resultater?», 2023.

Anbefalinger

Oppdatere rapporteringsplikten
En av de store utfordringene i kampen mot økonomisk kriminalitet er at mange sentrale aktører som håndterer kontanter i Norge ikke er underlagt rapporteringsplikt i henhold til hvitvaskingsloven. Rapporteringsplikten bør utvides til å inkludere flere aktører, som operatører av minibanker, pengetransportører, og forhandlere av verdigjenstander. Disse aktørene spiller en viktig rolle i den kriminelle økonomiske infrastrukturen.

Ved å pålegge alle aktører som håndterer store mengder kontanter å rapportere om mistenkelige transaksjoner og kundeforhold, kan Norge forbedre sin evne til å spore penger som stammer fra kriminalitet og forhindre hvitvasking.

Investere i teknologi og kompetanse
Kriminelle aktører utnytter raskt ny teknologi til sin fordel. For å holde tritt med truslene, må myndigheter og næringsliv investere i teknologiske løsninger som sikrer en robust digital infrastruktur og muliggjør analyse av store datamengder.

Det er også avgjørende å styrke kompetansen om IT-sikkerhet og om relevant teknologi som tas i bruk blant både privatpersoner og i næringslivet, som kunstig intelligens. Det bør også kontinuerlig vurderes om teknologi kan tas i bruk for å tette sårbarheter og sikkerhetshull. Et eksempel på dette er flerfaktorautentisering som bør implementeres bredt for å hindre kriminelle i å misbruke personlige opplysninger for å få tilgang til sensitive tjenester og informasjon.

Utvikle et totalforsvar på tvers av offentlig og privat sektor
Politiet kan ikke bekjempe økonomisk kriminalitet alene. Den kriminelle økonomien blandes med den legale økonomien og eroderer tilliten i finanssektoren, næringslivet og til myndighetene. Både politi, kontrolletater og privat sektor har et ansvar for å bekjempe kriminelle som utnytter de legale strukturene i samfunnet.

Dette inkluderer å utveksle tidsriktig informasjon om trusler, sårbarheter og endringer i kriminalitetsbildet slik at hver sektor er bedre i stand til å forebygge, respondere på og stanse kriminalitet.

Styrke og effektivisere samarbeid på tvers av landegrenser
Økonomisk kriminalitet er en global utfordring. Både private og offentlige norske aktører er derfor avhengige av dialog med internasjonale samarbeidspartnere.

Norsk politi deltar i en rekke internasjonale aktiviteter hvor fokus er å forebygge kriminalitet blant annet ved å dele relevant informasjon til andre lands myndigheter. Ved å intensivere norsk deltakelse i disse foraene, vil vi kunne styrke våre relasjoner og i større grad utveksle informasjon med andre land i forebyggende og avvergende øyemed.

Foto: iStock

Faktorer som påvirker kriminaliteten

Kriminalitetsutviklingen påvirkes av en rekke faktorer. Faktorene kan være både samfunnsmessige, teknologiske, økonomiske, miljømessige og politiske. Enkelte av faktorene påvirker kriminaliteten langsomt over tid, mens andre som teknologi og nyoppståtte politiske konflikter, kan endre kriminalitetsbildet i Norge relativt raskt.

I dette kapittelet fremheves enkelte faktorer som vil kunne påvirke økonomisk kriminalitet og den kriminelle økonomien de neste årene.

Økonomisk og sikkerhetspolitisk utfordrende tider

Samtiden preges av sikkerhetspolitisk usikkerhet og maktkamper om global økonomisk innflytelse. Verdens demografiske, militære og økonomiske tyngdepunkt forskyves fra Nord-Atlanterregionen til Indo-Stillehavsregionen. Både Russland og Kina investerer i handels- og sikkerhetsavtaler i områder som er rike på naturressurser eller som er av militær interesse. Begge land bruker også sin innflytelse i Midtøsten for å utfordre Vesten.[6] Konflikten mellom Russland og NATO forventes å bli langvarig. Russland vil trolig bruke virkemidlene de har tilgjengelig for å skape splittelse og utfordringer i vestlige samfunn, og NATO-land spesielt.[7] Nordkalotten har fått økt strategisk betydning etter innlemmelsen av Sverige og Finland i NATO, og nordisk forsvars- og sikkerhetssamarbeid forventes å øke. Både Svalbard og grenseområdene i Finnmark er av strategisk betydning for Russland.

6 Etterretningstjenesten, «Fokus 2024», 2024.
7 Den norske Atlanterhavskomité, «Krigen, bjørnen, dragen og nasjonens sikkerhet», hentet: 18.03.2024.

Samtidig ønsker også Kina økt kontroll over forsyningskjeder og å posisjonere seg i Arktis.[8] Det har blitt avslørt flere tilfeller der virksomheter med kjente knytninger til statlige aktører har forsøkt å investere i strategisk viktige virksomheter og eiendom i Norge. Slike investeringer kan også benyttes for å omgå sanksjoner, eller av kriminelle aktører for å kamuflere eller hvitvaske utbytte fra kriminalitet. Formålet med investeringene kan være vanskelig å avdekke.

Fra 2020 har verdensøkonomien blant annet blitt påvirket av en langvarig internasjonal pandemi og et sikkerhetspolitisk bilde i endring. Pandemiens restriksjoner, Russlands invasjon av Ukraina og den tilspissede konflikten i Midtøsten har medvirket til økte drifts- og levekostnader i hele verden. De økonomiske ettervirkningene forventes å ha betydning i flere år fremover.[9] Økonomiske utfordringer kan bidra til at både privatpersoner og virksomheter begår ulike typer kriminalitet for å sikre egen økonomi. Det kan bli mer konkurskriminalitet i enkelte bransjer, blant annet byggebransjen og restaurantbransjen, som følge av økonomiske nedgangstider.

Kriminelle nettverk opererer internasjonalt

Alvorlig organisert kriminalitet vurderes å være den største interne sikkerhetstrusselen mot EU-land, sammen med terrorisme. Halvparten av de største kriminelle nettverkene i Europa spesialiserer seg på digitale bedrageri og opererer på tvers av landegrenser. 76 prosent av de europeiske kriminelle nettverkene som utgjør størst trussel mot EU, er aktive i to til syv EU-land samtidig.

Flere av de kriminelle aktørene som hvitvasker utbytte fra kriminalitet og begår organiserte bedrageri i Norge oppholder seg i andre land i Europa eller i andre verdensdeler.

Ifølge Interpol er hovedårsakene til økningen i digitale bedrageri mer tilgjengelig og brukervennlig KI, desentraliserte betalingsløsninger og profesjonaliseringen av nettverk som spesialiserer seg på teknologisk kriminalitet som handelsvare (KSH)[10]. Bruken av KSH har økt blant kriminelle nettverk de siste årene. Politiet erfarer at også kriminelle nettverk i Norge kjøper tjenester og teknologiske løsninger, noe som gir økt evne til å gjennomføre kriminalitet mer effektivt.

8 Forsvarsdepartementet, «Prop. 87 S – Langtidsplan for forsvarssektoren 2025-2036», 2024.
9 Statistisk sentralbyrå (SSB), «Økonomiske analyser 4/2023», 2023.
10 Interpol, «Interpol Global Financial Fraud Assessment», 2024. Omtales på engelsk som crime-as-a-service (CaaS).

Rask teknologisk utvikling og tilpasning

Den teknologiske utviklingen går raskt. Det samme gjør tilpasning av ny teknologi. I 2022 ble generativ kunstig intelligens (KI) allemannseie. KIs påvirkning sammenlignes med introduksjonen av trykkpressen, dampmotoren, elektrisiteten, datamaskinen og internett.

KI har åpnet for utviklingen av verktøy som gjør det lettere å skape digitalt innhold. Samtidig utfordrer det vår evne til å skille ekte fra kunstig innhold. KI gjør det også mulig for kriminelle uten programmeringserfaring å utvikle eller kjøpe programvare som fremmer ulovlige aktiviteter.[11] På kort sikt forventer Økokrim at KI vil føre til at flere bedrageriforsøk blir vellykkede.

Avanserte språk- og bildegenererende modeller, såkalt deepfake-teknologi, benyttes til å lage realistiske bilder, videoer og lydopptak som på en overbevisende måte kan etterligne ekte personer og hendelser.[12] Ved hjelp av generativ KI kan bedrageriaktører tilpasse innhold i bedragerikampanjer for å nå ut til målgrupper presist og effektivt. Deepfake er rapportert benyttet til bedrageri i flere land. Kriminelle vil også kunne bruke generativ KI og anbefalingssystemer for å gjennomføre bedrageri av både privatpersoner og næringslivsaktører. Samme teknologi kan bli benyttet av statlige aktører for å manipulere og feilinformere.[13, 14]

I Norge har vi kommet langt i å tilpasse oss en digital hverdag. Nesten alle har tilgang til smarttelefon, og ni av ti bruker sosiale medier styrt av anbefalingssystemer som er designet for å påvirke oss. Næringslivet blir også mer app-basert. Flere selskaper tilbyr leveringstjenester via appløsninger, som persontransport og levering av mat. Det er flere eksempler på at sårbare arbeidstakere utnyttes i denne typen tjenesteyting.

Digitale tjenester og automatiserte prosesser kan gjøre innbyggernes kontakt med offentlige etater enklere og effektivisere arbeidet til offentlig ansatte. Digitaliseringen skaper imidlertid et stort handlingsrom for kriminelle aktører. Både offentlige og kommersielle tjenester kontakter eksempelvis innbyggerne digitalt via SMS-er. Kriminelle utnytter den digitale kommunikasjonen ved å sende egne SMS-er med falske lenker. Årlig får kriminelle stort utbytte fra denne typen bedrageri, såkalt smishing.

11 Europol, «Spotlight, Online Fraud Schemes: A Web Of Deceit», 2023.
12 Europol, «Facing reality? Law enforcement and the challenge of deepfakes», 2022.
13 DNB, «Finansiell trygghet i en usikker verden», 2024.
14 Europol, «Tech Watch Flash – The Impact of Large Language Models on Law Enforcement», 2023.

Foto: iStock

Nye digitale bankløsninger og virtuell valuta muliggjør raske overføringer av penger på tvers av landegrenser. Anonymiteten og hastigheten på internasjonale digitale overføringer vanskeliggjør sporing av pengestrømmer. Dette gjør digitale overføringer egnet til hvitvasking. Kriminelle aktører bruker digitale overføringer å skjule grensekryssende transaksjoner, samt inntekt, eierskap og formue utenlands.

I eksisterende nettbaserte spillverdener og i fremvoksende metavers finnes det virtuelle valutaer, økonomier og tjenester for omsetning av virtuelle eiendeler. Omsetningen i metaverset utgjorde ca. 900 milliarder kroner i 2023, og enkelte forventer at det øker til nærmere 10 000 milliarder kroner innen 2030.[15] Metaverset er i stor grad uregulert og det er allerede eksempler på at grove tyverier har funnet sted. Det forventes at metaverset vil tiltrekke seg ytterligere kriminalitet.

Et klassedelt samfunn

Fattigdom er en stor utfordring for personene som rammes, og legger press på velferdsstatens støtteordninger. Norske husholdninger har historisk sett hatt høy gjeld, samt at rentenivået og levekostnadene har økt de siste årene.[16] Samtidig står rundt 20 prosent i yrkesaktiv alder utenfor arbeid eller utdanning.[17] Inntektsforskjellene har økt, og en av fem nordmenn anses nå å ha en sårbar økonomi. Lavinntektshusholdninger med barn er mest utsatt for økonomiske vansker.[18] Oppvekst i familier med vold og rusmisbruk, og foreldre med lite utdanning og lav inntekt er eksempler på fellestrekk hos barn og unge som begår kriminalitet.[19] Disse kan være sårbare for rekruttering til kriminelle nettverk som følge av et ønske om tilhørighet, vennskap, beskyttelse eller økonomiske muligheter. Eldre kriminelle aktører som åpent viser frem dyre eiendeler, samt oppfatningen om at kriminalitet er en mulighet til å tjene penger virker forlokkende på unge. Ønsket om lettjente penger kan også føre til at unge lar seg rekruttere som pengemuldyr, selge narkotika eller utfører voldshandlinger for kriminelle nettverk.

15 Statistia, «Metaverse market revenue worldwide from 2022 to 2030», hentet: 27.03.2024.
16 Statistisk sentralbyrå (SSB), «Fakta om norsk økonomi», hentet: 05.04.2024.
17 NAV, «1 av 5 står utenfor arbeidslivet», hentet: 21.08.2024
18 Statistisk sentralbyrå (SSB), «En av fem nordmenn har sårbar økonomi», 2023.
19 Politiet & Oslo kommune, «Barne- og ungdomskriminaliteten i Oslo (SaLTo rapporten)», 2023.

Foto: iStock

Informasjon, kompetanse og anonymitet til salgs

Flere kriminelle nettverk i dag preges av ad-hoc samarbeid og løs tilknytning mellom aktørene. En av grunnen til dette er at både kriminelle nettverk og tilretteleggere i det legale næringslivet tilbyr tjenester og teknologiske løsninger som benyttes i kriminalitetsutøvelsen.

Kriminelle kan derfor, på samme måte som næringslivsaktører, sette ut deler av virksomheten og kjøpe tjenester fra inn- og utland. Dette kan blant annet være vold, stjålet informasjon, teknologiske verktøy, hvitvaskingstjenester, ekspertkunnskap og anonymiseringstjenester. Denne typen forretningsmessige relasjoner åpner også opp for spesialiserte aktører som selger sin kompetanse eller sine tjenester til en rekke andre kriminelle aktører.

Slike tjenester omtales gjerne som kriminalitet som handelsvare. Dersom aktørene som tilbyr tjenestene utøver rollen i kraft av stilling, verv eller oppdrag i offentlig og privat sektor og mottar bestikkelser gjør de seg skyldig i korrupsjon. Slike tilretteleggere bidrar til å kamuflere og legitimere kriminalitet og fungerer nærmest som en bro mellom den kriminelle økonomien og den legale økonomien.

Profesjonelle tilretteleggere

Profesjonelle tilretteleggere er personer som i kraft av sin profesjon og kompetanse medvirker til kriminalitet, eller sørger for at kriminaliteten tilsløres. Eksempler på profesjonelle tilretteleggere er advokater, regnskapsførere, revisorer og ansatte innen eiendom, bank, finans eller IT som bistår kriminelle.

Personer i slike stillinger spiller en viktig rolle i å beskytte økonomien og ivareta viktige rettsprinsipper i samfunnet vårt. Når profesjonelle tilretteleggere utfører tjenester for kriminelle i kraft av sin posisjon, kan det regnes som korrupsjon. Handlingene undergraver tilliten til viktige profesjoner, rettsstaten og det økonomiske markedet. Profesjonelle tilretteleggere tilpasser drift og rapportering til regelverket, og får selskapsstrukturer hvor det begås kriminalitet til å fremstå som legal næringsvirksomhet.[20] Ifølge Europol blir profesjonelle tilretteleggere benyttet av 60 prosent av kriminelle nettverk som opererer i EU.[21] Det er imidlertid avdekket få slike saker i Norge.

Advokater

Samfunnet har generelt høy tillit til advokatstanden, og advokaters klientkonto har høy legitimitet. Det har imidlertid vært flere tilfeller hvor advokater har misbrukt sin klientkonto til for eksempel å la klienter disponere midler der. Klientkontoer misbrukes til blant annet å unndra kreditorgjeld, begå bedrageri og til hvitvasking.

Politiet har også informasjon om enkelte advokater som har utlevert taushetsbelagt informasjon til mistenkte i straffesak og tilrettelagt for at innsatte i fengsel urettmessig får mulighet til å kommunisere med omverdenen.

> En advokat har stilt klientkonto til disposisjon for en rekke personer dømt for alvorlig økonomisk kriminalitet. Det mistenkes at vedkommende i praksis har bedrevet hvitvasking og ulovlig betalingsformidling, inkludert overføringer av kryptovaluta.

20 OECD, «Ending the shell game – Cracking down on the professionals who enable tax and white collar crimes», 2021.

21 Europol, «The Other side of the Coin – Analysis of Financial and Economic Crime», 2023.

Informasjon, kompetanse og anonymitet til salgs

Regnskapsførere

Enkelte regnskapsførere tilrettelegger for skatte- og avgiftsunndragelser, samt hvitvasking, ved å tilsløre reelle rettighetshavere og midlers opprinnelse gjennom kompliserte foretaksstrukturer. Regnskapsførere bistår særlig med dette i virksomheter som er forbundet med arbeidslivskriminalitet.

Kriminelle som benytter foretak til å gjennomføre bedrageri benytter gjerne regnskapsførere til å manipulere regnskapet slik at likviditetsgraden og lønnsomheten ser bedre ut enn hva som er reelt. Det manipulerte regnskapet kan deretter benyttes for å ta opp lån på uriktig grunnlag.

Regnskapsførere kan også bistå med å tilsløre fiktiv fakturering, for eksempel ved at et selskaps skattemeldinger leveres med for lave inntektsbeløp og for store fradrag i inngående merverdiavgift. På den måten kan betydelige skatte- og avgiftsmidler unndras, samtidig som selskapet får tilbakebetalt merverdiavgift på uriktig grunnlag. Regnskapsførere kan også bistå kriminelle ved at de ikke etterprøver og kontrollerer informasjon de mottar i tilstrekkelig grad.

Enhver som i næring påtar seg å føre regnskap for andre skal være autorisert av Finanstilsynet. Det er imidlertid flere eksempler på at regnskapsførere som har mistet autorisasjonen fortsetter å utføre sitt virke.

Det eksisterer også regnskapsforetak som påfallende ofte er regnskapsfører for firmaer som begår ulike former for økonomisk kriminalitet. For enkelte av disse regnskapsforetakene fremstår det som at deres forretningsmodell er å tilrettelegge for økonomisk kriminalitet.

> Et regnskapsforetak skal blant annet bistå næringsdrivende med kunnskap om hvordan de kan tappe verdier fra selskaper og begå konkurskriminalitet.
>
> Et annet foretak er regnskapsfører for flere firmaer som driver sosial dumping, lønnstyveri og andre former for arbeidslivskriminalitet.

Foto: iStock

Innsideaktører som tilrettelegger for kriminelle

Innsidere er personer som i kraft av sin stilling tilrettelegger for kriminalitet på vegne av en tredjepart. Dette gjøres ved å gi kriminelle tilgang til og kunnskap om en virksomhet som innsideren er ansatt i.[22] Innsideaktører kan tilrettelegge for kriminalitet med overlegg, uten å være klar over dette selv, eller som følge av press eller trusler. Det er ikke en forutsetning at en innsider har spesialist- eller profesjonskompetanse på samme måte som en profesjonell tilrettelegger.

Informasjon som kan være av verdi for kriminelle er selskapsstrukturer og daglige rutiner, planløsninger og saksbehandlingsrutiner. Fordi bankene har blitt bedre på cybersikkerhet og deteksjonssystemer for transaksjoner, kan bankansatte være særlig utsatt for bestikkelser, press eller trusler fra kriminelle aktører for å utføre tjenester. Flere bankansatte i ulike banker på Østlandet er per tid under etterforsking for korrupsjon etter å ha innvilget lån på uriktig grunnlag. Det er identifisert at enkelte av de bankansatte har direkte eller indirekte knytninger til kriminelle aktører.

Tilgang til ansatte i logistikkvirksomheter som transporterer eller tar imot varer er også av verdi for kriminelle. Europol har konkludert med at det er helt avgjørende for kriminelle nettverk å ha et kontaktnett ved europeiske havner som kan bistå med ulike tjenester, som eksempelvis smugling. Slike innsidenettverk består av havnearbeidere og sikkerhetsvakter, men også ansatte i logistikkselskaper og offentlige etater. Hovedsakelig bestikkes innsiderne, med opptil flere hundre tusen euro,[23] men også vold og trusler blir brukt for å forsikre videre medgjørlighet. I 2023 avslørte danske medier at en rekke Hells Angels-medlemmer var ansatt ved Aarhus havn i Danmark. Havnen har blant annet blitt benyttet til å smugle kokain inn til Europa.[24]

22 Nasjonal Sikkerhetsmyndighet, «Temarapport – Innsiderisiko», hentet 23.08.2024.
23 Europol, «Criminal networks in EU ports. Risks and Challenges for law enforcement», hentet 02.10.2024
24 Finans «Afsløring - Rockere huserer i landets største erhvervshavn», hentet: 19.08.2024.

Teknologitjenester som handelsvare

Teknologi er i dag sentralt for å gjennomføre flere typer alvorlig profittmotivert kriminalitet og hvitvasking. Kriminelle har behov for anonymitet og operasjonssikkerhet, samtidig som de har behov for sensitiv informasjon for å begå eksempelvis bedrageri. Dette har skapt et eget marked hvor teknologiske tjenester og verktøy selges til kriminelle formål. Politiet har tidligere påpekt at dette markedet er stort og økende, og at teknologiske nyvinninger raskt kommer ut på det kriminelle markedet.[25]

Flere av disse verktøyene er brukervennlige også for personer med gjennomsnittlig teknologisk kompetanse. Det bidrar til at digital kriminalitet, som bedrageri, kan utføres av stadig flere. Bedragere kjøper tilgang til verktøyene de benytter i det ordinære markedet og på kriminelle markedsplasser. Dette inkluderer blant annet kapasitet til spoofing av telefonnumre og verktøy til administrering av phishing-kampanjer. Med proxytjenere og VPN-løsninger tilsløres bedragerens IP-adresser og krypterte kommunikasjonsapper skjermer kommunikasjonen mellom de involverte.

Kriminelle som begår datatyveri selger også stjålet påloggingsinformasjon og data fra kompromitterte brukerkontoer til bedragere. Kripos har registrert en økning av slike opplysninger på digitale kriminelle markedsplasser.[26]

Statlige aktører kan også kjøpe tjenester fra de samme tilbyderne. Et godt utbygd system med tilbud av tjenester til kriminelle kan lette statlige aktørers virksomhet. Samtidig har politiet sett at kriminelle har lykkes i å anskaffe avansert programvare utviklet av statlige aktører for bruk til kriminelle formål.[27]

25 Politiet, «Politiets trusselvurdering 2023», 2023.
26 Kripos v/NC3, «Cyberkriminalitet 2024», 2024.
27 Politiet, «Politiets trusselvurdering 2023», 2023.

Pengemuldyr

Såkalte pengemuldyr bistår kriminelle ved at de mottar penger som er ulovlig ervervet på egne konti, for deretter å flytte disse videre. De kan også låne ut bankkortene sine. Ofte overføres pengene fra muldyrenes bankkonti til norske og utenlandske bankkonti, som disponeres av kriminelle aktører. I noen tilfeller overføres pengene til ulike kryptovalutabørser for kjøp av kryptovaluta. Politiet mottar jevnlig rapporter om unge mennesker som mottar bankoverføring fra bedrageriofre, og som deretter benytter pengene til blant annet kjøp av kostbare klokker og elektronikk.

I 2023 var det flere eksempler på at pengemuldyr ble utsatt for trusler og vold dersom utbyttet de skulle overføre gikk tapt, for eksempel ved at beløpet ble stanset av banker. Den siste tiden kan aktørene se ut til å ha endret modus fra å bruke trusler mot pengemuldyr, til å benytte personer som er villig til å stille sin bankkonto til disposisjon i bytte mot betaling.

Bruk av pengemuldyr i hvitvaskingsoperasjoner er en økende utfordring i mange land inkludert i Norge.[28] Totalt mottok Enheten for finansiell etterretning (EFE) ved Økokrim over 2 014 rapporter om pengemuldyr i 2023, mot 599 i 2020. Økningen kan ses i sammenheng med at digital kriminalitet har økt, særlig bedrageri.[29] Politiet har i tillegg informasjon om at norske pengemuldyr brukt i forbindelse med bedrageri også kan knyttes til narkotikakriminalitet.

Økokrim har informasjon om at personer også benyttes som «telemuldyr», ved at de mottar penger for å bruke sine mobilabonnement til å sende ut svindel-SMSer.

28 National Crime Agency (NCA), «National Strategic Assessment of SOC», 2021.
29 Europol, «Money muling», 2021.

Foto: iStock

Utbyttehåndtering og hvitvasking

For at kriminelle skal kunne benytte fortjenesten fra kriminalitet uten å vekke mistanke, må utbyttets opprinnelse tilsløres, samt at pengene må plasseres og integreres i den legale økonomien. Dette omtales gjerne som hvitvasking.

Stadig mer av kriminaliteten og utbyttet som genereres, skjer i det digitale rom. Dette medfører vekst i hvitvasking i det digitale domenet, for eksempel ved bruk av neobanker, allerede nevnte pengemuldyr og kryptovaluta. De fleste kryptovalutaer har full åpenhet om transaksjoner, adresser (tilsvarende bankkontoer) og innestående beløp på de ulike adressene. Hvem som er reell eier av adressene er imidlertid ofte ukjent. Beløpsgrenser, global dekning, miksetjenester, useriøse vekslingstjenester og desentralisering gjør kryptovaluta velegnet for kriminelle.

Selv om samfunnet digitaliseres, viser etterforskninger og etterretningsbildet for øvrig at kontanter fremdeles benyttes i stor grad som betalingsmiddel mellom kriminelle. De kriminelle konverterer også fortjeneste fra kriminalitet til verdigjenstander.

Misbruk av selskapsstrukturer

Mer enn 80 prosent av de kriminelle nettverkene undersøkt av Europol benytter legale selskapsstrukturer i kriminalitetsutøvelsen, enten ved å opprette egne selskaper eller ved å infiltrere eksisterende selskaper.[30] Selskapene benyttes til å utføre profittmotivert kriminalitet og til hvitvasking.

Politiet mottar jevnlig informasjon om at det hvitvaskes penger gjennom kapitalintensive foretak. Bransjer det er særlig mye informasjon om er restaurantbransjen, bygg- og anleggsbransjen og transportbransjen. Her fordekkes svarte betalinger eller utbytte fra kriminalitet i mengden av daglige transaksjoner, innkjøp og kundebesøk. Verdier unndras fra regnskap, samtidig som ansatte lønnes svart.

En annen fremgangsmåte for hvitvasking gjennom selskapsstrukturer er å fakturere foretak for tjenester som aldri er utført, såkalt fiktiv fakturering. Faktureringen gir grunnlag for pengeoverføringer hvis egentlige formål er å skjule inntekter fra svart arbeid. I mange tilfeller er foretakene stråselskaper, gjerne enkeltpersonsforetak, uten reell drift. Underleverandører benyttes også i denne sammenhengen som rene stråselskap.

Selskapsstrukturer gir en legitim fasade og skaper avstand mellom den kriminelle handlingen og gjerningspersonene. For å tilsløre de kriminelles tilknytning til virksomhetene benyttes stråpersoner i sentrale roller som eier eller daglig leder. Selskapsstrukturen gjøres kompleks og det foretas hyppige eierskifter. Dette vanskeliggjør myndighetens arbeid med å kontrollere opplysninger og dermed muligheten for å avdekke og iretteføre kriminalitet. Ved å blande legal inntekt med utbytte fra kriminalitet blir det enklere å tilsløre de ulovlige midlenes opphav. I tillegg vil større internasjonale pengeoverføringer fremstå mer troverdig hvis disse gjøres fra et selskap, enn hvis de gjøres via bankkonto tilhørende en privatperson, da et selskap normalt sett har større kapitalflyt.[31, 32]

30 Europol, «Serious and organised crime threat assessment (SOCTA)», 2021.
31 OECD, «Ending the shell game – Cracking down on the professionals who enable tax and white-collar crimes», 2021.
32 Europol, «The other side of the coin – An analysis of financial and economic crime», 2023.

Utbyttehåndtering og hvitvasking

Utbytte fra kriminalitet investeres i eiendom

Kriminelle aktører benytter eiendomsmarkedet til hvitvasking av fortjeneste fra arbeidslivskriminalitet, narkotikakriminalitet og økonomisk kriminalitet. Aktørene investerer i privatboliger og næringsbygg, både i Norge og utlandet.

Hvitvasking gjennom eiendomsmarkedet er attraktivt fordi det er kapitalintensivt, som muliggjør hvitvasking av større beløp, i tillegg til at det er en investering som kan gi god avkastning. Hvem som er den reelle eieren av eiendommen kan skjules på flere måter, blant annet via bruk av stråpersoner og blanco skjøte, samt eierskap via sekretessejurisdiksjoner og kompliserte selskapsstrukturer.[33]

Boliger kan også rehabiliteres med bruk av svarte midler som stammer fra kriminelt utbytte. Det er en effektiv måte å konvertere kontanter til en eiendel som vil gi verdiøkning. Eiendommer kan også selges til over- eller underpris for å legitimere pengestrømmer. En annen sårbarhet er at fiktive verdivurderinger kan legges til grunn for såkalt svingdørsalg hvor samme eiendom omsettes hyppig og med unormal prissetting.

Informasjon om eiendomsmarkedet i Dubai har vist at nordmenn kjøper eiendom i utlandet med penger de har tjent på kriminalitet. Utveksling av informasjon knyttet til eiendom er sjelden del av internasjonale utvekslingsavtaler. Myndighetene har derfor mindre mulighet til å avdekke eierskap i eiendom i utlandet.[34] Geografisk avstand mellom den kriminelle handlingen og investeringen bidrar også til å gjøre det vanskeligere å oppdage pengenes opprinnelse.

Det er ikke lovpålagt å tinglyse eierskap til eiendom i Norge. Særlig næringseiendom eies ofte gjennom aksjeselskap og eierskap tinglyses ikke.[35] Selv der hvor det er åpenhet om hvilket selskap som eier en eiendom, kan reell rettighetshaver endres ved salg av eierandeler i selskapet uten at dette fremkommer i eiendomsregisteret. Ved salg av aksjeselskap kan det være utfordrende å ettergå verdien på enkelteiendommer da det er selskapet som helhet som er verdisatt. Eierskap gjennom aksjeselskap kan derfor gjøre det lettere både å skjule reelle rettighetshavere og manipulere eiendomsverdien.

33 Transparency International Norge, «Hvem eier Oslo? Hvitvaskingsrisiko i eiendomsmarkedet», 2021.
34 Alstadsæter, Annette; Planterose, Bluebery; Zucman, Gabriel & Økland, Andreas «Who owns offshore real estate? Evidence from Dubai», EU Tax Observatory Working Paper No. 1, 2022.
35 Henning Lauridsen, «Kjøp av eiendom i Norge må tinglyses», blogg, Eiendom Norge, 2021.

Foto: iStock

Kontanter og verdigjenstander

Kontanter er spesielt egnet til hvitvasking fordi midlene og betalingspartene er vanskelig å spore. Norges kontantbeholdning har vært stabil på rundt 40 milliarder siden midten av 1990-tallet til tross for at de fleste i dag benytter seg av digitale betalingsløsninger. Det er grunn til å tro at en stor andel av denne kontantbeholdningen benyttes i den kriminelle økonomien, som betalingsmiddel mellom kriminelle og ved hvitvasking av utbytte.[36]

I mange år har mellom syv og åtte milliarder norske kroner i kontanter årlig blitt fraktet ut av landet. Som følge av høy hvitvaskingsrisiko ble banker mer restriktive med å kjøpe tilbake norske kontanter fra utlandet våren 2023. Etter at restriksjonene ble innført har mengden kontanter som deklareres inn til Norge fra utlandet blitt kraftig redusert. Det registreres nå at kontanter i større grad veksles inn i andre verdier før det forlater Norge.

Fysiske varer, eiendeler og tjenester benyttes fremdeles i stor utstrekning for å hvitvaske utbytte fra kriminalitet. Varer som er kostbare, lett omsettelige og vanskelig å verdisette, slik at prisen kan manipuleres til å overdrive eller underdrive markedspris, er spesielt attraktive til hvitvasking. Eksempler på egnede gjenstander er smykker, klokker, kunst, og samlegjenstander. Også varer som gull, fisk, elektronikk, biler og byggevarer kjøpes for penger ervervet på kriminalitet.

Kjøp og salg av kostbare klokker blir ofte benyttet for å hvitvaske utbytte fra narkotikakriminalitet, bedrageri og arbeidslivskriminalitet. Klokkene kjøpes gjerne med kontanter, stjålne bankkort eller gavekort. Det rapporteres jevnlig om unge mennesker som mottar bankoverføring fra bedrageriofre og deretter benytter pengene til blant annet kjøp av kostbare klokker eller elektronikk.

36 Økokrim, «Nå er det NOK – kontanter i den kriminelle økonomien», 2023.

Underground banking og ulovlig hawalavirksomhet

Underground banking er et begrep som dekker alle typer uregulerte bankaktiviteter som foregår utenfor det formelle finansielle systemet. Verdioverføringer gjøres ofte ved bruk av metoder som for eksempel hawala eller andre uformelle verdioverføringssystemer.

Flere aktører som driver ulovlig hawalavirksomhet i Norge tilbyr hvitvaskingstjenester til kriminelle, blant annet ved mottak og forflytning av kontanter. Transaksjoner gjennomført i hawala-systemet er nærmest umulig å spore, og er derfor attraktive for aktører som ønsker å tilsløre sine transaksjoner. Hawala benyttes derfor til hvitvasking av penger og finansiering av terror.

Hawala-virksomhetene består ofte av et større antall aktører som utfører ulike oppgaver knyttet til kontanthåndteringen. Aktørene har ulik grad av tilknytning til selve virksomheten, og noen utfører kun enkle ad hoc-oppgaver i en tidsbestemt periode.

Pågående voldelige konflikter internasjonalt, samt restriksjoner på innførsel og veksling av norske kontanter fra utlandet, aktualiserer uregulerte banktjenester.

Hawala er et uformelt system for betaling og pengeoverføring over landegrenser basert på tillit og personlige forbindelser. Det anvendes oftest når betalingsmottakerne bor i land uten normalt fungerende bankvesen. Virksomheten er lovlig så lenge de har konsesjon fra Finanstilsynet og etterlever regnskap- og revisjonsplikt samt hvitvaskingsreglene.

- Det overleveres et kontantbeløp til en hawala-virksomhet i Norge
- Hawala-virksomheten tar kontakt med en annen hawala-virksomhet i det landet hvor mottakeren befinner seg
- Den utenlandske hawala-virksomheten utbetaler et tilsvarende beløp i lokal valuta til mottakeren

Pengene trenger ikke å krysse landegrensene, da hawala-virksomhetene gjør opp seg imellom.

Kriminelle i grålånsmarkedet

Det grå lånemarkedet er lovlig, men ikke regulert av myndighetene. Aktørene er i hovedsak privatpersoner. Advokater og private meglere benyttes imidlertid ofte som mellomledd. Lånevilkårene blir avtalt individuelt og det er eksempler på at privatpersoner har lånt 30 millioner kroner til 40 prosent rente. Utlån i grålånsmarkedet kan derfor gi høy profitt.

Grålån er en mulighet for kriminelle til å få avkastning på utbytte fra kriminalitet. Flere kriminelle, som blant annet har begått alvorlig narkotikakriminalitet, driver lånevirksomhet i grålånsmarkedet med skyhøye renter og svært kort nedbetalingstid. Enkelte långivere har stor tilgang på kontanter fra eksempelvis prostitusjon og omsetning av svarte varer, som deretter reinvesteres i pengeutlånsvirksomhet.

Egenskapene til grålån gjør de attraktive for hvitvasking og oppgjør i den kriminelle økonomien. Kontrakten kan være falsk i den forstand at lånet aldri blir utbetalt og at tilbakebetaling av lånet er oppgjør for annen kriminalitet.[37]

Dersom låntager ikke klarer å gjøre opp for seg, kan lånet bli videresolgt til kriminelle miljøer med voldskapabilitet I disse tilfellene kan låntager bli utsatt for trusler og tvunget til å utføre tjenester for de kriminelle.

Det er også eksempler på at det som fremstår som et lån for låntaker, i realiteten er et forsøk på å lure fra vedkommende større verdier. Et eksempel er en långiver som gjør seg utilgjengelig for låntaker når lånet skal betales, og på denne måten kan overta pantet som er verdt mer enn lånet.[38]

37 SKUP, «Metoderapport: Hvitvasking», 2016.
38 SKUP, «Metoderapport: Lånehaien», 2014.

Foto: iStock

Korrupsjon og utnyttelse av posisjoner

Det er straffbart både å tilby og gi bestikkelser i anledning utøvelse av stilling, verv eller oppdrag i både offentlig og privat sektor. Korrupsjon svekker borgernes tillit til myndighetene og undergraver demokratiet og rettsstaten. I tillegg er korrupsjon et hinder for rettferdig konkurranse og effektiv utnyttelse av ressurser. Som følge av de særlig skadelige konsekvensene, straffes korrupsjon strengere enn annen økonomisk kriminalitet.

I Norge er det avdekket flere tilfeller av korrupsjon i offentlig sektor. Erfaringsmessig er det forhøyet korrupsjonsrisiko i forvaltningen av verdifulle naturressurser og i saker som avhenger av offentlige tillatelser eller lisenser for å få tilgang til marked, som kjøp av eiendom og byggetillatelser. Offentlige anskaffelser fremheves ofte som et område som er særlig utsatt for korrupsjon. Bestikkelser kan føre til at beslutninger blir tatt på uriktig grunnlag. I tillegg kan bestikkelser gi leverandørene mulighet til å få innpass i markeder, samt opprettholde markedsposisjon og ekspandere sin virksomhet på bekostning av andre.

Enkeltpersoner kan være mål for korrupsjon som følge av innflytelsen en stilling gir eller fordi de besitter relevant informasjon. Dette gjelder på alle nivå i offentlig og privat virksomhet.[39]

Det er vanskelig å anslå hvor stort problem korrupsjon er i Norge. En av årsakene er at både giver og mottaker har en felles interesse av å holde korrupsjon skjult. I 2023 kom Norge på fjerdeplass på Transparency International sin liste over verdens minst korrupte land.[40] Like fullt ble flere korrupsjonssaker rettskraftig i domstolene i 2023.

39 Økokrim, «Korrupsjon – typetilfeller og indikatorer», 2022.
40 Transparency International, «Corruption Perceptions Index 2023», hentet: 26.08.2024.

Foto: Overvåkningskamera/Økokrim

Statlig etterretning eller kriminalitet?

Russiske og kinesiske myndigheter utnytter splittelse og konfliktlinjer i vestlige samfunn på flere måter. I tillegg registrerer PST at økonomisk motiverte kriminelle utfører terrorangrep mot jødiske og israelske mål i Europa på vegne av andre stater.[41] For politiet kan det være utfordrende å vite om det man observerer er organisert kriminalitet eller statlige aktørers etterretningsvirksomhet.

I mange tilfeller kan virkemidlene som benyttes av statlige aktører ligne på bedrageres forsøk på forledelse og manipulasjon. Begge benytter eksempelvis falsk og villedende informasjon til å påvirke beslutninger og adferd.[42]

Det har vært flere tilfeller der ansatte i virksomheter av interesse for utenlandske etterretningstjenester har blitt utsatt for forsøk på såkalt spear phishing, det vil si et målrettet angrep mot vedkommende via for eksempel falsk lenke i en e-post.[43] Lignende modus observeres i bedrageriforsøk rettet mot styremedlemmer i aksjeselskap, ofte i sammenheng med en reell hendelse i selskapet.

Russlands og Kinas etterretningsvirksomhet innebærer at bestikkelser kan benyttes som del av deres aktivitet i Norge.[44, 45] Ansatte i både offentlige og private virksomheter antas å være mål for slike tilnærmelser.

Uklarheter rundt aktørenes motiver bidrar til at politiet og sikkerhetstjenestene må håndtere et stadig mer komplekst trusselbilde. Eksempelet på neste side illustrerer hvor utfordrende det kan være å skille mellom statlig aktivitet og kriminalitet.

41 Politiets sikkerhetstjeneste (PST), «Trusselvurdering – økt terrortrussel i Norge», hentet 08.10.2024.
42 Den norske Atlanterhavskomité, «Krigen, bjørnen, dragen og nasjonens sikkerhet», hentet 18.03.2024.
43 Nasjonal sikkerhetsmyndighet (NSM), «Risiko 2024», 2024.
44 Etterretningstjenesten, «Fokus 2024», 2024.
45 Politiets sikkerhetstjeneste (PST), «Nasjonal trusselvurdering 2024», 2024.

IMSI-fanger brukt til bedrageri

I 2023 pågrep og siktet Politiets sikkerhetstjeneste (PST) en malaysisk borger for å ha drevet ulovlig signaletterretning i Norge. Siktede hadde kjørt rundt i Oslo og Bergen med en IMSI-fanger i bilen. Bruken av IMSI-fanger ble avdekket av Nasjonal Sikkerhetsmyndighet (NSM).

PST frafalt siktelsen for spionasje og overlot saken til Økokrim, som siktet den pågrepne for grovt bedrageri med bruk av IMSI-fanger. Etterforskningen avdekket at mannen samarbeidet med aktører som ikke befant seg i Norge, blant annet en som fungerte som teknisk tilrettelegger.

Mannen brukte IMSI-fangeren som en falsk basestasjon. Telefoner som ble koblet til den falske basestasjonen, ble utsatt for nettfiske gjennom tilsendte tekstmeldinger som inneholdt lenker til nettsider kontrollert av bedragerne.

Ved å gå utenom tjenesteleverandørenes mobilnettverk omgikk han teleoperatørenes deteksjon og sikkerhetsmekanismer. Det er første gang denne typen bedragerimodus er avdekket i Norge.

Tekstmeldingene som ble sendt ga uttrykk for å være fra kjente merkenavn som Bank Norwegian, DHL og DNB og la seg i samme meldingstråd som legitime tekstmeldinger fra dis se selskapene. De fornærmede ble bedt om å oppgi bankkortinformasjon på de falske nettsidene.

Mannen ble dømt til 4,5 års fengsel for bedrageriforsøk mot nær 245 000 personer, 103 fullbyrdede bedrageri, og for ulovlig bruk av IMSI-fanger.[46]

Samme modus har blitt benyttet i flere andre land.

Eksempel på SMS sendt fra gjerningspersonene.

46 Borgarting lagmannsrett dom 21. mars 2024 (sak nr. 24-014600AST-BORG/03).

Foto: KI-generert Økokrim

Strategisk eierskap

Kunnskap om og kontroll over verdikjeder og infrastruktur i Norge, vil ha betydning for Russland og Kina fremover. Kina har over en lengre periode hatt fokus på å oppnå kontroll over viktige verdikjeder globalt, og å være en nøkkelspiller innen infrastruktur og logistikk. For Russland har sanksjonene gjort det vanskeligere å få tilgang til vestlige verdikjeder. En måte å løse dette på er å få tilgang til en verdikjede via små underleverandører.[47]

De siste årene har vi sett at statlige og kriminelle aktører har forsøkt å få innpass i norsk næringsliv. Bergen Enginessaken, utvisningen av mistenkte spioner fra norske universiteter, og organiserte kriminelle som investerer i norsk næringsliv er eksempler på dette.

Kinesiske selskap har over lang tid vist interesse for å delta i anbudsprosesser for blant annet bygging av infrastruktur i Norge.[48] Flere kinesiske selskap har vist interesse for å investere i Kirkenes havn og i Narvik havn. Dette skal være begrunnet med at havnen ligger svært strategisk til for Kinas uttalte plan om en nordlig sjørute, «den arktiske silkeveien», mellom Europa og østkysten av Asia.

Flere norske havner er også sentrale militære mottakshavner for NATO, og med Finland og Sverige som nye NATO-medlemsland, er funksjonen mer aktuell enn tidligere.[49] Kjennskap eller eierskap til disse havnenes infrastruktur kan gi statlige aktører tilgang til verdifull informasjon. Den samme informasjonen og tilgangen til havnene kan også være nyttig for aktører innen organisert kriminalitet som driver med eksport og import av ulovlige varer.

47 Nasjonal sikkerhetsmyndighet (NSM), «Risiko 2024», 2024.
48 Etterretningstjenesten, «Fokus 2024», 2024.
49 Forsvarets Forskningsinstitutt (FFI), «Norske havner - hvor viktige er de for forsvaret av Norden?», hentet: 16.04.2024.

Sanksjonsomgåelser

Norge har sluttet seg til nær alle EUs innførte restriktive tiltak (sanksjoner) mot Russland, med noen få nasjonale tilpasninger. Formålet er å gjøre det mer utfordrende for Russland å fortsette finansieringen av angrepskrigen mot Ukraina. Sanksjonene blir stadig strengere og handelsmulighetene med Russland er nå sterkt innsnevret og innebærer høy risiko.[50]

Enhver norsk statsborger, juridisk person, enhet eller organ plikter å etterleve sanksjonene mot Russland. Utgangspunktet er at både brudd på, og omgåelse av, sanksjonene er straffbart. Dette stiller høye krav til norske bedrifter når det gjelder å undersøke om deres forretningsvirksomhet er berørt av gjeldende sanksjoner.[51]

Økokrim mottar stadig informasjon om potensielle omgåelser av gjeldende sanksjoner mot Russland. Informasjonen omhandler både enkeltpersoner, foreninger og foretak med nasjonal og internasjonal forretningsvirksomhet. Informasjonen indikerer at enkeltpersoner bistår listeførte sanksjonerte objekter, samt bryter forbudet mot å selge, levere, overføre eller eksportere visse typer valuta og varer.

I næringslivet er det aktører som driver handel med sanksjonsbelagte varer eller tjenester via tilslørte selskapsstrukturer i ikke-sanksjonerte tredjeland. Transaksjonsstrømmer tilsløres via ett eller flere tredjeland. Økokrim er kjent med enkeltsaker som innbefatter totalbeløp på flere hundre millioner norske kroner innen bransjer som shipping- og fiskerinæringen.

Fordekte transaksjonsstrømmer kan være en indikasjon på både sanksjonsomgåelser og hvitvasking i ett og samme forhold. Tilsløringen kan benyttes for å skjule formålet bak en transaksjon, skjule sluttdestinasjonen til transaksjonen, hvem som reelt sett er de involverte partene, og opphavet til midlene som sendes.

50 Regjeringen, «Ny runde med sanksjoner innført mot Russland», hentet: 19.04.2024.
51 Regjeringen, «Veileder om sanksjoner som svar på Russlands militære aggresjon mot Ukraina», hentet: 12.08.2024.

Terrorfinansiering

Etterretningstjenesten anser ekstreme islamistiske organisasjoner og deres sympatisører som den største globale terrortrusselen. Fraværet av etablerte globale høyreekstreme organisasjoner begrenser høyreekstreme sin evne til å koordinere mer komplekse angrep. Dyrtid og økende polarisering kan imidlertid bidra til økt støtte til høyreekstreme organisasjoner, noe som utgjør en potensiell økt trussel på sikt dersom disse får større oppslutning.[52]

Det er også disse to aktørgruppene PST forventer vil utgjøre de mest alvorlige terrortruslene i og mot Norge.[53] PST forventer videre at det kontinuerlig foregår innsamlingsaksjoner på forskjellige nettfora til støtte for ekstremister og terrorgrupper, og at norske ekstreme islamister vil fortsette å støtte globale terrororganisasjoner og ekstremister i regionale konflikter de selv har en tilknytning til.

Terrorfinansiering har både likheter med, og forskjeller fra, annen økonomisk kriminalitet. I likhet med eksempelvis hvitvasking av kriminelt utbytte, vil terrorfinansiering bli forsøkt tilslørt. Den viktigste forskjellen er at det er fokus på transaksjonenes destinasjon i stedet for opprinnelse. Summene det er snakk om er heller ikke avgjørende. Samtidig utelukker ikke dette at midlenenes opphav også kan stamme fra kriminalitet, som for eksempel salg av antikke gjenstander som er plyndret fra konfliktområder.

Et skjerpet trusselbilde fra økt rekruttering og støtte til ekstremistiske grupperinger kan føre til flere tilfeller av terrorfinansiering. Penger rutes inn mot områder aktuelle for terrororganisasjoner. Dette er ofte land i Afrika, Midtøsten og Sør-Asia med lengre pågående konflikter. Flere av områdene har behov for nødhjelp, og er land som også familie og sympatisører i Norge sender penger til. Det kan derfor være utfordrende å identifisere hva som er terrorfinansiering, og hva som er legitime overføringer. Økt bruk av kryptovaluta gjør dette enda mer utfordrende.

52 Etterretningstjenesten, «Fokus 2024», 2024.
53 Politiets Sikkerhetstjeneste (PST), «Nasjonal trusselvurdering 2024», 2024.

Utvalgte kriminalitets-utfordringer

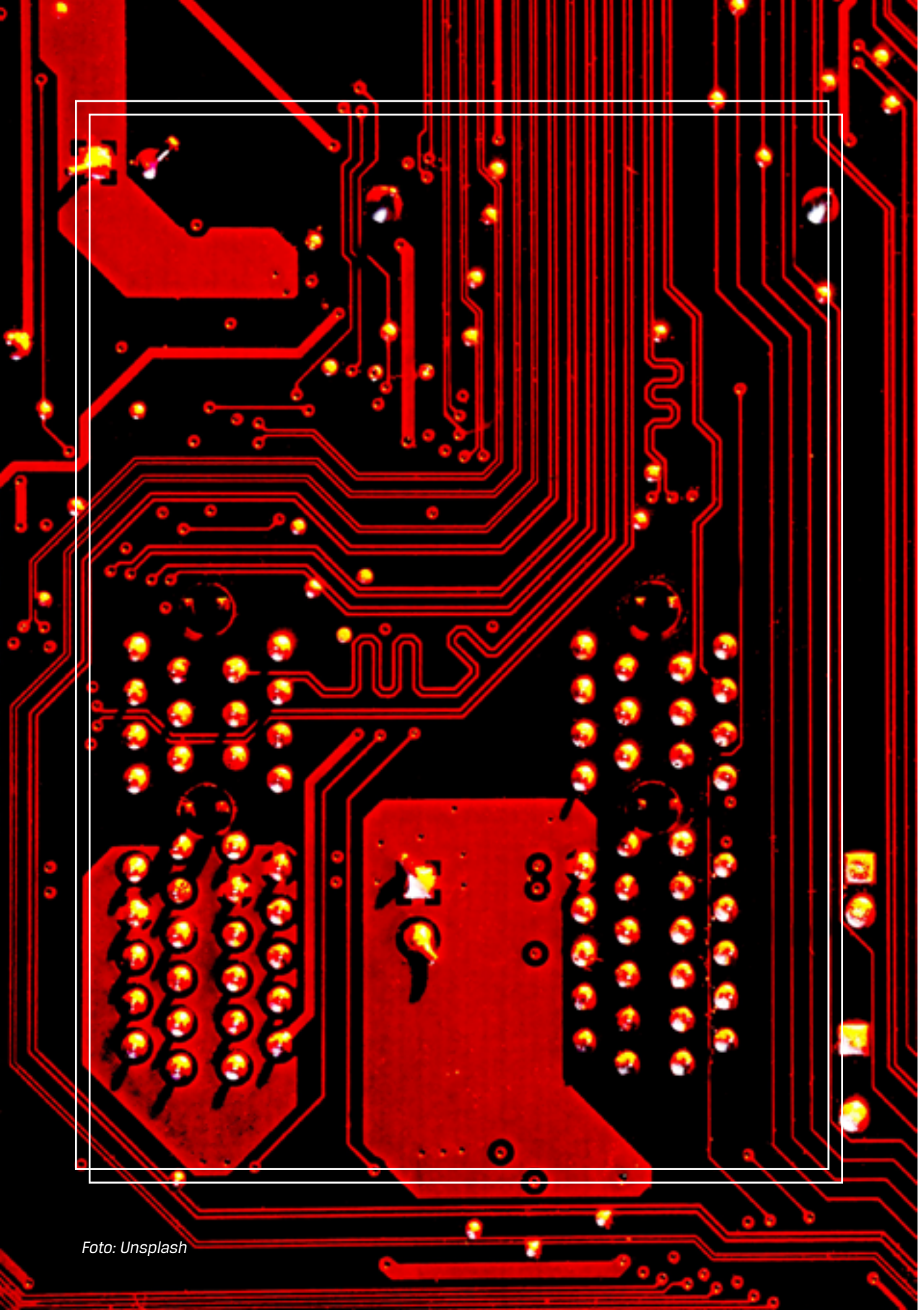

Foto: Unsplash

Økning i digitale bedrageri

I 2023 ble det anmeldt nærmere 26 000 bedrageri i Norge. Det tilsvarer en økning på 13 prosent fra året før. 73 prosent av bedragerianmeldelsene omhandlet digitale bedrageri. I politiets innbyggerundersøkelse fra 2023 er bedrageri og identitetstyveri det som bekymrer befolkningen mest ved bruk av digitale tjenester.[54]

Betalingstjenestetilbydere rapporterte bedragerirelaterte tap på totalt 928 millioner kroner for 2023. Det betyr at bedragere tilegnet seg nærmere en milliard kroner gjennom bedrageri i Norge.[55] Mørketallene relatert til bedrageri, det vil si forskjellen mellom den anmeldte og den faktiske kriminaliteten, antas imidlertid å være betydelig. Det er derfor grunn til å tro at det reelle utbyttet som bedragere tilegner seg er høyere. I tillegg er det indikasjoner på at utbytte fra bedrageri finansierer annen kriminalitet, som alvorlig narkotikakriminalitet.

Aktørene inkluderer både utenlandske borgere som begår bedrageri fra utlandet, samt norske og nordiske borgere som opererer både i eget land og på tvers av landegrenser innad i Norden. Enkelte opererer alene, som ved nett-handel-bedrageri, mens andre er del av kriminelle nettverk.[56]

Digitale bedrageri evner å ramme mange mennesker på kort tid. Ofte utføres bedrageriene ved bruk av såkalt vishing eller smishing, som på kort tid kan nå flere hundre tusen mennesker i et svindelforsøk. Ved slike massebedrageri taper ofte de fornærmede et mindre beløp, men summen av mange slike bedrageri genererer betydelig inntekt for kriminelle nettverk.[57]

Det begås også mer målrettede bedrageri der gjerningspersonene i større grad selekterer ofrene. For eksempel innhenter bedragere person- og selskapsinformasjon fra offentlige registre eller kjøpe stjålne datapakker. Det er også blitt mer vanlig at ofre for bedrageri blir bedratt på nytt.

54 Politidirektoratet, «Politiets innbyggerundersøkelse 2023», 2024.
55 Finanstilsynet, «Risiko- og sårbarhetsanalyse (ROS) 2024», 2024.
56 Økokrim, «Nordic threat assessment on online fraud 2024», 2024.
57 Polisen, «Bedrägerier och penningtvätt», 2022.

Bedrageriofre utsettes for manipulasjon og vold

Økokrim registrerer en bekymringsfull utvikling der bedrageri, trussel- og voldshandlinger samt narkotikakriminalitet sammenveves. Flere norske aktører som er involvert i narkotikakriminalitet, er også involvert i gjennomføring av bedrageri eller den etterfølgende gevinsthåndteringen. Det siste året har det vært en økning av tilfeller der bankbedrageri begås med fysisk oppmøte hjemme hos fornærmede. Det har også vært tilfeller hvor eldre kvinner blir frihetsberøvet eller manipulert til å oppholde seg på et sted utpekt av bedrageren i flere dager. Bedragerne utgir seg for å være politi og pålegger de fiktiv taushetsplikt for å unngå at de kontakter andre. Under oppholdet blir bankkontoene deres tappet for penger.[58]

Manipuleringen av bedrageriofrene kan være av en slik art at de får psykiske plager. I flere tilfeller har bedragerne lange telefonsamtaler med ofrene der de utgir seg for å være fra banken eller politiet. I etterkant opplever ofrene frykt for å svare på telefon, gå ut av boligen eller samhandle med andre privatpersoner, offentlige instanser og privat næringsliv.

Enkelte bedrageriofre blir redd for å svare politiet som etterforsker saken av frykt for å bli bedratt på nytt.

I forbindelse med lånebedrageri er det eksempler på at gjerningspersoner truer ofre, blant annet med kniv, til å ta opp lån hos finansinstitusjoner. Lånet utbetales deretter til bedragerne. Utøvere av lånebedrageri gjør en kynisk utvelgelse av målobjekt, og utnytter blant annet sårbare utenlandske personer. De forledes til å oppgi personalia i tro om at de skal få hjelp til å søke skoleplass, opprette bankkonti eller annet de trenger når de ankommer landet.

Internasjonalt er det flere eksempler på at ofre for bedrageri og seksuell utpressing tar sitt eget liv som følge av det de er utsatt for.[59, 60] I Norge erfarer politiet at bedrageri får så store konsekvenser for ofre at både familie og omgangskrets blir bekymret for deres liv og helse.

58 NRK, «Eldreran: 'Politi' lurte eldre kvinne til isolasjon i flere døgn», hentet: 08.10.2024.
59 The straits times, «The painful cost of scams suicide and self harm», 2023.
60 CNN, Killed by a scam: A father took his life after losing his savings to international criminal gangs. He's not the only one, hentet: 14.10.2024.

Bedrageri rammer norsk næringsliv og det offentlige

I næringslivets egne undersøkelser oppgir nærmere en tredel av små og mellomstore bedrifter at de har vært utsatt for svindelforsøk og digitale angrep.[61] Bedrageri anmeldes sjelden til politiet, noe som blant annet skyldes manglende tiltro til at politiet vil respondere, eller frykt for å skade eget omdømme.

I Sverige er det estimert at såkalte BEC-bedrageri mot bedrifter genererte 329 millioner svenske kroner til kriminelle aktører i 2023.[62] BEC-bedrageri er en forkortelse for Business email compromise og er en fellesbetegnelse for blant annet direktørbedrageri og fakturabedrageri mot bedrifter. Det er flere eksempler på at norske bedrifter er blitt svindlet for beløp på flere titalls millioner kroner i slike bedrageri.

Låne- og kredittbedrageri er også en trussel. Ved utnyttelse av samtykkebasert lånesøknad (SBL), opprettes det ansettelsesforhold hvor det innberettes feilaktige opplysninger om lønn til myndighetene. Opplysningene benyttes deretter til å søke lån på uriktig grunnlag.

Manipulerte foretaksregnskap som gir uttrykk for en bedre økonomi enn hva som er reelt, benyttes også til å kjøpe kostbare varer på kreditt uten å betale for varene.

Ved bruk av manipulert dokumentasjon og systematisk utnyttelse av tillitsbaserte ordninger, forledes Skatteetaten og NAV til å refundere merverdiavgift eller utbetale NAV-ytelser. Ifølge NAV feilutbetaler de minst fem milliarder kroner årlig.[63] Til sammenligning rapporteres det i Sverige om tap i størrelsesorden 13–16 milliarder svenske kroner gjennom misbruk av velferdsordninger.[64]

61 SMB Norge, «Kriminalitet mot næringslivet må tas på større alvor», hentet: 26.06.2024.
62 Polisen v/Nationellt bedrägericentrum, «Brottsvinsterna for bedrägeribrottsligheten 2023», 2024.
63 NAV.no «Innsats mot trygdesvindel», hentet: 26.06.2024.
64 Polisen v/Nationellt bedrägericentrum, «Brottsvinsterna for bedrägeribrottsligheten 2023», 2024.

Grove bedrageri av nordmenn begått fra utlandet

I 2023 startet Økokrim etterforskning av en rekke grove bedrageri etter anmeldelse fra Statens Vegvesen. To rumenske menn ble i 2024 dømt for ID-tyveri og for å ha bedratt 423 nordmenn fra Romania.[65]

Gjerningspersonene rettet bedrageriene hovedsakelig mot norske brukere av Statens vegvesens selvbetjeningsportal for kjøp og salg av kjøretøy. Personer som nylig hadde fått godkjent sin salgsmelding for kjøretøy i selvbetjeningsportalen, mottok en SMS der det stod at salgsmeldingen måtte godkjennes på nytt via tilsendt lenke.

Ved bruk av spoofing fremstod det som at SMS-ene var sendt fra Statens Vegvesen. Dersom fornærmede tidligere hadde mottatt SMS fra Statens Vegvesen, la den falske SMS-en seg inn i den eksisterende meldingsrekken. I tillegg var SMS-ene målrettede og inneholdt fullt navn og telefonnummer til kjøper og selger, samt registreringsnummer på den aktuelle bilen. Denne informasjonen økte troverdigheten.

På nettsiden ble de fornærmede bedt om å logge inn med BankID. Samtidig som de fornærmede skrev inn sine personopplysninger på nettsiden, satt gjerningspersonene i Romania og opprettet brukere med de fornærmedes BankID. Slik fikk gjerningspersonene tilgang til skattemeldinger, nettbank og annen sensitiv informasjon.

Kjøp av hvitvaskingstjenester

Etterforskningen viser at gjerningspersonene har samarbeidet med andre aktører i forbindelse med hvitvaskingen av utbyttet. Det er beslaglagt en rekke Telegram-chatter der gjerningspersonene etterspør ulike tjenester som for eksempel opprettelse av kontoer hos ulike betalingstjenester og assistanse i forbindelse med KYC-prosesser.

Eksempel på SMS sendt fra gjerningspersonene.

65 Oslo Tingrett dom 28. juni 2024 (sak nr. 24-018855MED-TOSL/03). Saken er anket og dommen er ikke rettskraftig.

Foto: iStock

Foto: iStock

Gjengangere innen arbeidslivs-kriminalitet

Innen arbeidslivskriminalitet er det flere eksempler på gjengangere som fortsetter sin aktivitet i flere år. Noen gjengangere innen arbeidslivskriminalitet har blitt domfelt, men fortsetter sin kriminelle aktivitet kamuflert av stråpersoner i nøkkelroller.

Eksempler på slike kriminelle gjengangere er blant annet avdekket i transportbransjen, oppsøkende håndverkervirksomhet og nettverk som driver med ulike former for næringsvirksomhet og utleie av eiendom.

Gjengangerne er hovedaktører i virksomheter som utnytter sårbare utenlandske arbeidstakere og tjener godt på den kriminelle aktiviteten de styrer. Det er vanlig at gjengangere innen arbeidslivskriminalitet begår skatte- og avgiftskriminalitet og hyppig slår sine virksomheter konkurs. I tillegg benytter de fiktiv fakturering, samtidig som de sender krav om refusjon av merverdiavgift til Skatteetaten.

Utbyttet de opparbeider seg fra kriminaliteten hvitvaskes ved kjøp av formuesgoder og eiendom eller gjennom foretak. Bruk av stråpersoner tilslører reelt eierskap, slik at det kan bli vanskelig å oppdage hvem som egentlig begår kriminaliteten og hvitvasker utbytte. Underleverandører benyttes gjerne som rene stråselskap. Det er også flere eksempler på at kriminelle aktører endrer sitt eget navn. Da kan det ta tid for kontrollmyndighetene å avdekke at det er de samme personene som fortsetter sin kriminelle aktivitet i nytt navn. Det er eksempler på at de bytter bransjer og overfører sin kriminelle arbeidsstruktur til en annen næring.

Utnyttelse av sårbare arbeidstakere

Utenlandske arbeidstakere som benyttes i arbeidsintensive bransjer med høy andel ufaglærte, er mer sårbare for utnytting enn norskfødte arbeidstakere. Dette skyldes blant annet språkutfordringer, lite eller ingen utdanning, og at mange av arbeidstakerne har lite kjennskap til norsk regelverk og lovverk, rettigheter og plikter. Utnyttelse er spesielt fremtredende innen bygg og anlegg, bilpleie og -verksted, varetransport og sesongarbeid i jordbruket.

Utnyttelse kan for eksempel skje i form av lønnstyverier, misbrukte identiteter, lange arbeidsdager uten lønnskompensasjon og mangelfulle og uverdige boforhold. I 2023 ble en arbeidsgiver for første gang dømt for lønnstyveri etter at den nye loven trådte i kraft i 2022.[66] Det har vært en økning i anmeldte lønnstyveri på 59 prosent fra 95 forhold i 2022 til 151 forhold i 2023.

Det nye app-baserte næringslivet er egnet for å utnytte sårbare arbeidstakere. Enkelte selskaper tilbyr kun arbeid som frilansere og deltids-arbeidere[67] og flere av selskapene som leverer mat og transport er registrert i utlandet, noe som vanskeliggjør kontroll. Det er også ofte uklart hvem som faktisk leverer varene, da det er flere eksempler på at arbeidskontrakter deles mellom arbeidstakere og personer som benytter andres identitet. Det arbeider også personer uten arbeidstillatelse for selskaper som er app-basert.

Sesongarbeidere

Hvert år kommer sesongarbeidere til Norge, og høysesongen er fra mai til september. Fra januar til juli 2024 innvilget Utlendingsdirektoratet 3269[68] sesongarbeidstillatelser til tredjelandsborgere.[69]

Sesongarbeidere i landbruket trenger ikke formalkompetanse. Tredjelandsborgere som kommer til Norge som sesongarbeidere har ofte begrensede norsk- og engelskkunnskaper, lite utdanning og de kommer ofte fra fattige områder i hjemlandet. Disse faktorene medvirker til at de anses som sårbare for utnyttelse til arbeid. Tidligere års kontroller av sesongarbeidere har avdekket blant annet kritikkverdige boforhold, lange arbeidsdager uten lønnskompensasjon, ikke allmenngjort lønn og manglende arbeidskontrakter.

En økning i innvilgede sesongarbeidertillatelser til tredjelandsborgere, samt informasjon om at enkelte av arbeiderne aldri blir utreisekontrollert fra Norge, gir et handlingsrom for at sesongarbeidere kan bli utnyttet til både ulovlig arbeid og kriminalitet.[70]

Mange sesongarbeidere har gjennom flere år blitt rekruttert og utnyttet av tilretteleggere. Tilretteleggerne har gjerne samme etniske bakgrunn som sesongarbeiderne, og de kan være i familie med sesongarbeiderne. De organiserer reise og innkvartering, kontakt mellom arbeidsgiver, norske myndigheter og sesongarbeider, i tillegg til utbetaling av lønn.[71] I 2023 ble en tilrettelegger dømt for blant annet grov utnyttelse av 42 polske sesongarbeidere.[72]

Arbeidere som utnyttes av oppsøkende håndverkervirksomheter

Flere kriminelle nettverk står bak oppsøkende håndverkervirksomheter i Norge som bedrar nordmenn på bopelen sin. De utnytter utenlandsk arbeidskraft, begår skatte- og avgiftskriminalitet, bedrageri og hvitvasking. Gjennom flere år har de oppsøkt særlig eldre personer på bopel og tilbudt tjenester som utvendig vask og håndverkertjenester på tak og fasade, samt steinlegging. Aktørene bak de oppsøkende håndverkervirksomhetene bedrar kundene for store summer og hvitvasker utbyttet.

Arbeiderne er ofte fra Øst-Europa og snakker verken norsk eller engelsk. Deres manglende språkkunnskaper og svake kjennskap til Norge gjør dem sårbare og derfor avhengige av arbeidsgiverne. De jobber også hovedsakelig uten formelle arbeidskontrakter. Arbeidsgiverne har over lengre tid systematisk benyttet denne type arbeidskraft og profittert på underbetaling og manglende etterlevelse av sitt arbeidsgiveransvar.

Det er flere eksempler på at aktørene utnytter arbeiderne ved å misbruke identiteten deres blant annet ved å opprette foretak og bankkonti med arbeidernes identitet. I de fleste tilfellene har de ansatte verken kontroll på midlene eller virksomheten selv. Deres identitet kan derimot bli stående som eier av foretak som begår bedrageri.

66 Oslo Tingrett dom 21. september 2023 (sak nr. 23-094374MED-TOSL/01).
67 Kongsvik, T.; Moen, Ø.; Vie, O.E.; Jørgensen, R.B. & Albrechtsen, E., «Norsk arbeidsliv mot 2050. Muligheter og trusler», Fagbokforlaget, 2022.
68 Av disse var 1531 fra Vietnam, etterfulgt av 410 fra Filippinene og 333 fra Thailand.
69 UDI, «Innvilgede arbeidstillatelser for tredjelandsborgere - sesongarbeid», 2024.
70 UDI, «Statistikk innvilgede arbeidstillatelser for tredjelandsborgere», 2023.
71 Økokrim, «Tilretteleggere for sesongarbeidere», 2023.
72 Sogn og Fjordane tingrett dom 22. mars 2023 (sak nr. 22- 1 36095M E D-TSOF/TSOG).

Gjengangere i transportbransjen

Det har gjennom mange år vært flere kriminelle gjengangere i transportbransjen. Økokrim har i samarbeid med Oslo politidistrikt etterforsket et sakskompleks hvor det til sammen er avsagt fellende dom mot syv personer som var knyttet til transportvirksomheter. Personene er dømt for blant annet grov hvitvasking, grov selvvasking, grovt økonomisk utroskap, grovt underslag, grovt trygdebedrageri og grovt skattesvik.[73] Aktørene har vært aktive i mange år.

Noe av utbyttet stammet fra svart arbeid i varebilbransjen. Etterforskningen avdekket betydelig bruk av underleverandører. Underleverandørene hadde hverken kjøretøy, ansatte eller driftsmidler, noe som tilsa at det ikke var reell drift i foretakene. Det ble likevel fakturert for transporttjenester fra underleverandørene til oppdragsgiverne.

Betaling for arbeidet ble gjort til stråselskap på grunnlag av fiktive fakturaer. Samtidig har de urettmessig mottatt refusjon for merverdiavgift på bakgrunn av de fiktive fakturaene. På denne måten hvitvasket de svart betaling for utførte transportoppdrag. I den utstrekning transportoppdragene ble gjennomført, ble det benyttet svart arbeidskraft. Det meste av pengene som ble betalt til disse aktørene ble tatt ut, enten i kontanter, ved overføringer til andre virksomheter hvor pengene ble hvitvasket, eller ved pengeoverføringer til utlandet.

73 Borgarting Lagmannsrett dom 1. november 2023 (sak nr. 22-135564AST-BORG/01).

Foto: iStock

Begrepsliste

I denne rapporten benyttes det en rekke begreper. Under er de mest sentrale forklart.

Arbeidslivskriminalitet er handlinger som bryter med norske lover om lønns- og arbeidsforhold, trygder, skatter og avgifter, gjerne utført organisert, som utnytter arbeidstakere eller virker konkurransevridende og undergraver samfunnsstrukturen.

Anbefalingssystemer er algoritmer som brukes til å gi tilpassede anbefalinger til brukere basert på deres tidligere atferd og preferanser, ofte brukt i netthandel og strømmetjenester.

Business Email Compromise (BEC) er bedragerier mot bedrifter hvor målet er å stjele penger eller informasjon ved kompromittering av e-post. Det er en felles betegnelse for blant annet direktørbedrageri og fakturabedrageri mot bedrifter.

Det digitale rom er alle datamaskiner, nettverk og enheter som er koblet sammen og deler informasjon, likt hvordan vi tenker på «det offentlige rom» i den fysiske verden.

Ekstremisme er aksept for bruk av vold for å nå politiske religiøse eller ideologiske mål. En ekstremist aksepterer bruk av vold, men bruker ikke nødvendigvis vold selv.

Generativ kunstig intelligens er KI-systemer som skaper unikt innhold som tekst, bilder, lyd og video ut fra instrukser. I motsetning analyserer tradisjonell KI primært eksisterende data.

Hvitvasking innebærer å sikre utbyttet fra en straffbar handling ved å skjule knytningen til kriminalitet og få utbyttet til å se ut som det er fremskaffet på lovlig måte ved å integrere det i den legale økonomien.

IMSI-fanger er en enhet som simulerer en mobilbasestasjon for å fange kommunikasjon mellom telefoner og nettverk. Bruk er strengt regulert og ulovlig for privatpersoner.

Innsider er en nåværende eller tidligere tilknyttet person (ansatt, konsulent, kontraktør) som enten gir kriminelle tilgang til og kunnskap om virksomheten, eller som misbruker sin stilling for å skade eller påføre virksomheten tap.

Klientkonto brukes av virksomheter, eksempelvis advokat- eller eiendomsmeglerforetak, som administrerer og oppbevarer klienters midler. Virksomhetene er pliktig å holde egne og klienters midler adskilt.

Korrupsjon er misbruk av makt i betrodde stillinger for personlig gevinst. Dette kan være ved at en person mottar en bestikkelse eller en fordel ved utøvelse av stilling, verv eller oppdrag. Det er straffbart både å tilby og motta en bestikkelse.

Kriminalitet som handelsvare (KSH), omtalt som Crime as a Service på engelsk, er en forretningsmodell hvor kriminelle tilbyr kompetanse, teknologi og informasjon som tjenester eller varer. Dette inkluderer hacking, dataangrep, voldsoppdrag, salg av personinformasjon og hvitvasking, tilsvarende tjenestetilbud i den legale økonomien.

Kriminelle nettverk brukes i denne rapporten om miljøer, gjenger, grupperinger eller sett av individer som samarbeider om den kriminelle virksomheten.

Krypterte kommunikasjonsapper beskytter meldinger og annen kommunikasjon mellom brukere ved hjelp av kryptering. Dette innebærer at informasjonen kodes til et format som bare kan leses av mottakeren.

Kryptovalutabørs er en digital handelsplattform som tilrettelegger for kjøp, salg og veksling av kryptovalutaer. Plattformen muliggjør handel mellom ulike kryptovalutaer, samt konvertering mellom kryptovalutaer og tradisjonelle valutaer som euro eller amerikanske dollar.

KYC (Know your costomer eller Kjenn din kunde på norsk) er prosessen som benyttes av finansinstitusjoner og andre virksomheter for å identifisere og verifisere identiteten til sine kunder. Formålet er å forbygge blant annet økonomisk kriminalitet, hvitvasking og terrorfinansiering.

Metaverset defineres i denne rapporten som et tredimensjonalt, digitalt miljø hvor brukere, representert av virtuelle figurer, samhandler i virtuelle rom løsrevet fra fysisk virkelighet.

Pengemuldyr er enkeltpersoner som overfører ulovlig tilegnede midler på vegne av andre og dermed fasiliterer for hvitvasking for kriminelle.

Phishing (nettfisking) er en svindelmetode som bruker masseutsendelser via e-post, telefon eller meldinger som et ledd i å påvirke mottakere til å avsløre personlige data eller påloggingsdetaljer.

Spear-phishing er målrettet mot enkeltindivider, grupper og bedrifter.

Statlig aktør forstås i denne rapporten som en organisasjon, institusjon eller enhet som handler på statens vegne og som har som mål å ivareta eller fremme statens politiske, økonomiske eller militære spørsmål.

Strategisk eierskap refererer til en eierposisjon i en virksomhet som er motivert av mer enn bare finansielle hensyn. Dette kan være en aktør som har en interesse i å påvirke beslutninger eller strategi og som kan ha både forretningsmessige og politiske interesser.

Stråperson refererer til en person som stiller sitt navn eller identitet til disposisjon for å skjule den reelle eieren sin tilknytning til en virksomhet eller handling. Hensikten er å skjule kriminelle handlinger.

Stråselskap er firma som opprettes med formål å skjule reell eier eller tilsløre ulovlige aktiviteter. Slike firma har ofte ikke en reell drift, og benyttes gjerne for sanksjonsomgåelse, skatteunndragelser, MVA-bedragerier eller hvitvasking av kriminelt utbytte.

Totalforsvaret er et begrep hentet fra Forsvaret som innbefatter den gjensidige støtten og samarbeidet mellom Forsvaret, andre offentlige aktører og det sivile samfunn om både forebygging, beredskapsplanlegging og operative forhold, i møte med en ekstern trussel. I denne trusselvurderingen benyttes begrepet om en strategi for å utvikle tettere samarbeid mellom offentlige sektorer, og mellom offentlig og privat sektor, for å forebygge og bekjempe kriminalitet.

Virtuell valuta er et digitalt uttrykk for verdi som ikke er utstedt av en sentralbank eller offentlig myndighet. Virtuell valuta er ikke nødvendigvis knyttet til en offisiell valuta, men aksepteres som betalingsmiddel. Valutaen kan overføres, lagres eller handles elektronisk. Den mest kjente virtuelle valutaen er Bitcoin.

VPN (Virtual Private Network) er en teknologi som maskerer brukerens internettforbindelse og krypterer datatrafikken for økt personvern og sikkerhet.

ØKOKRIM

Postadresse: Pb. 2096 Vika, NO-0125 Oslo
Besøksadresse: C.J. Hambros plass 2 C, NO-0164 Oslo
Kontakt: 23 29 10 00 / post.okokrim@politiet.no

www.okokrim.no

Financial Intelligence Unit
Norway

Foto: KI-generert av Økokrim