



POLITIET
KRIPOS

Politiets trusselvurdering 2023



Forord

Politiet skal bidra til redusert kriminalitet og økt trygghet for innbyggerne. Forebygging er et av våre viktigste strategiske virkemidler. Samarbeid med andre aktører, både offentlige og private, er viktig for å redusere kriminelle handlinger og uønskede hendelser. Dette vil også redusere skadevirkninger og hindre gjentakelse.

God kunnskap om samfunns- og kriminalitetsutviklingen, og om årsaker til kriminalitet og uønskede hendelser, er viktig. Gjennom politiets trusselvurdering deler vi vår strategiske kunnskap om de største kriminalitetstruslene. Formålet er å sette både politiet og andre i stand til å iverksette tiltak for å bidra til et trygt samfunn med redusert kriminalitet.



Benedicte Bjørnland
Politidirektør

Innhold

5 Introduksjon

6 Innledning

8 Sammendrag

10 1. FAKTORER SOM PÅVIRKER KRIMINALITET

12 2. Særlig alvorlige kriminalitetstrusler

- 13 2.1. Kriminelle spesialister selger tjenester til kriminelle aktører
- 13 2.2. Kriminelle aktører styrer sin virksomhet fra utlandet
- 14 2.3. Konfliktbildet innen kriminelle gjenger
- 15 2.4. Kriminelle nettverk benytter kryptovaluta til bedrageri og hvitvasking
- 16 2.5. Løsepengevirus mot privat og offentlig sektor
- 16 2.6. Datatyveri fra private og offentlige virksomheter
- 17 2.7. Arbeidslivskriminalitet i varetransportbransjen
- 17 2.8. Vold begått av personer med alvorlige psykiske lidelser

19 3. Situasjonsbeskrivelser

- 20 3.1. Trusler mot offentlig ro, orden og demokratiske verdier
- 21 3.2. Trusler mot alminnelig trygghet i samfunnet
- 23 3.3. Trusler mot liv, helse og personlig integritet
- 25 3.4. Trusler mot økonomi og arbeidsliv
- 27 3.5. Trusler mot miljø, ressursgrunnlag og dyrevelferd
- 29 3.6. Trusler mot IKT-sikkerhet og digital infrastruktur
- 32 3.7. Trusler mot grensesikkerhet og indre sikkerhet



INTRODUKSJON

Innledning

Politiets trusselvurdering (PTV) 2023 beskriver utvalgte særlig alvorlige kriminalitetstrusler som faller inn under politiets ansvarsområde, og gir en fremtidsrettet vurdering av disse. PTV skal bidra til en felles situasjonsforståelse av de kriminalitetstruslene samfunnet står overfor, og danne grunnlag for forebyggende samhandling med private og offentlige aktører. Rapporten må ses i sammenheng med øvrige nasjonale trusselvurderinger fra ulike virksomheter.

PTV er utarbeidet av Kripas på oppdrag fra Politidirektoratet, og bygger på politiets samlede etterretningsproduksjon. Samtlige politidistrikter og særorgan har bidratt med informasjon, analyser og fagkompetanse innen sine ansvarsområder. I tillegg bygger rapporten på informasjon fra nasjonale og internasjonale kilder, som forskningsrapporter og rapporter fra ulike samarbeidspartnere.

Denne trusselvurderingen løfter frem kriminalitetstrusler som er vurdert som spesielt alvorlige, og hvor det forventes en særlig negativ utvikling. Disse er blant annet vurdert på bakgrunn av kriminaliteten aktørene utfører og hvilken trussel kriminaliteten utgjør mot individ og mot sentrale verdier i samfunnet.

Rapporten er utarbeidet i henhold til prinsippene i Etterretningsdoktrine for politiet.¹ Den gir korte beskrivelser av hvordan kriminalitetstruslene har utviklet seg det siste året, samt sentrale premisser for vurderinger om det kommende

året. Ettersom PTV inneholder fremtidsrettede vurderinger, gir ikke disse sikker kunnskap. Satt inn i en kontekst vil de likevel gi bedre innsikt og forståelse, og bidra til å redusere usikkerhet om fremtidig utvikling.

Rapportens oppbygning

Årets PTV er tredelt. Etter et sammendrag, beskrives generelle faktorer nasjonalt og internasjonalt som påvirker, eller kan påvirke, kriminalitetsutviklingen i Norge på kort og lengre sikt. Den neste delen fremhever særlig alvorlige kriminalitetstrusler som truer verdiene politiet er satt til å beskytte. I årets PTV har det vært ekstra fokus på å fremheve kriminalitetstrusler som rammer samfunnet og fellesskapet spesielt.

Trender og forventet utvikling er vurdert på tvers av kriminalitet mot de ulike verdiene politiet er satt til å beskytte. Flere av de særlig alvorlige kriminalitetstruslene som framheves i denne rapporten berører ulike former for kriminalitet. Det er vurdert flere trusler enn de som omtales i denne rapporten. Truslene som er beskrevet i kapittel 2 er basert på de innrapporterte alvorligste truslene fra politidistrikt og særorgan, og en endelig overordnet vurdering av disse. Kriminalitetstruslene er ikke rangert og står beskrevet i tilfeldig rekkefølge.

Den siste delen av årets PTV beskriver bredden i kriminalitetsutviklingen på tvers av politiets samfunnsoppdrag. Verdiene politiet er satt til å beskytte er definert ved

¹ Politidirektoratet (2020) Etterretningsdoktrine for politiet. Oslo: Politidirektoratet.

syv kategorier, som gir retning til politiets samlede etterretningsproduksjon. Kapittel 3 er inndelt etter beskrivelser av utviklingen innen kriminalitetstrusler mot følgende verdier:

- Offentlig ro, orden og demokratiske verdier
- Alminnelig trygghet i samfunnet
- Liv, helse og personlig integritet
- Økonomi og arbeidsliv
- Miljø, ressursgrunnlag og dyrevelferd
- IKT-sikkerhet og digital infrastruktur
- Grensesikkerhet og indre sikkerhet

Fremtidsrettede vurderinger vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte er det benyttet sannsynlighetsord. Avsnittene med sannsynlighetsord i denne rapporten er i sin helhet kursivert for å synliggjøre fremtidsrettede vurderinger. Formålet med standardiserte sannsynlighetsord er å kommunisere sannsynlighet på en lik måte som reduserer uklarheter og misforståelser. Begrepene og de tilhørende beskrivelsene av begrepenes betydning er utarbeidet i et samarbeid mellom politiet, Politiets sikkerhetstjeneste og Forsvaret.

Nasjonal standard	Beskrivelse	NATO-standard
Meget sannsynlig	Det er meget god grunn til å forvente...	Highly likely (>90 %)
Sannsynlig	Det er grunn til å forvente...	Likely (60-90 %)
Mulig	Det er like sannsynlig som usannsynlig...	Even chance (40-60 %)
Lite sannsynlig	Det er liten grunn til å forvente...	Unlikely (10-40 %)
Svært lite sannsynlig	Det er svært liten grunn til å forvente...	Highly unlikely (<10 %)

Sammendrag

Gjenåpning etter koronapandemien og økt mobilitet i verden – i tillegg til krigen i Ukraina – er fremtredende faktorer som har preget situasjonsbildet det siste året, og som påvirker kriminalitetsutviklingen. Overordnet er imidlertid kriminalitetsbildet i Norge foreløpig lite påvirket av krigen i Ukraina. Krigen har ytterligere forsterket og komplisert trusselbildet i det digitale rom, men har også ført til at andre kriminelle aktører har fått større handlingsrom og nye muligheter innen en rekke kriminalitetstyper.

Videre er en profesjonalisering av kriminaliteten og tilknytning til utlandet – med komplekse strukturer og samarbeid på tvers av landegrenser – likhetstrekk som går igjen i flere av kriminalitetstruslene i årets PTV. Dette tydeliggjør at kriminalitetsbildet i Norge påvirkes av faktorer og kriminalitet også utenfor landets grenser.

Kriminelle spesialister selger tjenester til kriminelle aktører

Markedet for kjøp og salg av kriminelle tjenester, såkalt kriminalitet som en tjeneste, har fått økt utbredelse blant kriminelle nettverk. Et ekspanderende marked innen kjøp og salg av kriminelle tjenester er kapabilitetsfremmende, og det er meget sannsynlig at det øker handlingsrommet til etablerte kriminelle nettverk. Det er sannsynlig at utviklingen vil føre til at den organiserte kriminaliteten blir mer uoversiktlig og får et mer profesjonelt preg.

Kriminelle aktører styrer sin virksomhet fra utlandet

Flere bakmenn og sentrale aktører innen organisert kriminalitet styrer sin kriminelle virksomhet fra utlandet. Utviklingen er en del av en større internasjonal trend. Det er meget sannsynlig at kriminelle nettverk som styres av aktører i utlandet vil dominere markedet for innførsel av narkotika.

Konfliktbildet innen kriminelle gjenger

Gjenger og gjengrelaterte nettverk er mest synlige i og rundt storbyene, med det sentrale Østlandet som den viktigste arenaen. En fellesnevner for gjengene er at de er involvert i narkotika-, trussel- og voldskriminalitet som i mange tilfeller foregår i det offentlige rom. Det siste året har aktiviteten fra svenske gjengkriminelle på norsk jord blitt synlig. Trusselbildet knyttet til kriminelle gjenger vil til enhver tid følge spenningsnivået i gjengmiljøene. Det vil si at konfliktbildet vil variere mellom rolige og anspente perioder. Det er sannsynlig at det også vil være voldshendelser med potensielt dødelig utfall som et resultat av gjengenes interne konflikter i 2023.

1 % MC-klubbene er etablert både i rurale og urbane strøk i alle landets politidistrikter. Flere kriminelle 1 % MC-klubber synes å være i en ekspansjonsfase. Samtlige klubber har medlemmer med kriminelle kapabiliteter innen narkotika, våpen, og vold. Det er sannsynlig at 1 % MC-klubbene vil opprettholde sine ekspansjonsaktiviteter.

Kriminelle nettverk benytter kryptovaluta til å begå investeringsbedrageri og hvitvaske utbytte fra kriminalitet.

Kryptovaluta benyttes av kriminelle til å overføre store beløp på tvers av landegrenser. Videre kan kryptovaluta fremstå som en attraktiv investering for mange. Falske handelsplattformer fremstår som seriøse, bedragerne er ofte svært profesjonelle og bedrageriene genererer høy profitt. Det er sannsynlig at omfanget av investeringsbedrageri med kryptovaluta vil øke og at kryptovaluta i økende grad vil bli brukt til hvitvasking.

Løsepengevirus mot privat og offentlig sektor

Løsepengevirus rettet mot bedrifter og virksomheter anses som den største kriminalitetstrusselen mot IKT-sikkerhet og digital infrastruktur. Dette begrunnes med mange hendelser, stort skadepotensial og mulighet for høy profitt for gjerningspersonene, samt liten fare for identifisering og straffeforfølgelse. Det er sannsynlig at virksomheter med samfunnskritiske funksjoner vil rammes av løsepengevirus, og at kriminalitet mot datasystemer motivert av Russlands krig mot Ukraina vil fortsette.

Datatyveri fra private og offentlige virksomheter

Datainnbrudd uten påfølgende bruk av løsepengevirus utgjør også en alvorlig trussel mot norske virksomheter, særlig ved tyveri av data. Aktører kan i tillegg manipulere eller sabotere data. Det er sannsynlig at bedrifter

med roller i kritiske samfunnsfunksjoner, og virksomheter med betydelige kompetanse- og bransjefordeler, i økende grad vil bli utsatt for slik kriminalitet.

Arbeidslivskriminalitet i varetransportbransjen

Omfanget av lovbrudd innen varetransportbransjen fremstår å være økende. Kriminalitet i varetransportbransjen truer konkurransegrunnlaget i næringen, og påfører virksomheter og næringslivet økonomiske tap. Handlingsrommet for kriminelle aktører i bransjen har vært stort, som følge av at bransjen stiller få krav til kompetanse, har lave etableringskostnader og at næringen i liten grad har vært regulert. Det er sannsynlig at kriminalitet i varetransportbransjen vil fortsette ved at aktørene begår skattesvik, hvitvasking, sosial dumping, svart avlønning og andre arbeidsmiljølovbrudd.

Vold begått av personer med alvorlige psykiske lidelser

De fleste politidistriktene rapporterer om vold begått av personer med alvorlige psykiske lidelser som en vedvarende alvorlig kriminalitetstrussel. Enkelte aktører kan også knyttes til konspiratorisk tankegods og ekstremisme. Det er meget sannsynlig at vold begått av personer med alvorlige psykiske lidelser og problematisk rusmiddelbruk vil fortsette å utgjøre en betydelig trussel, hvor enkelte hendelser vil medføre tap av liv.

1.

FAKTORER SOM PÅVIRKER KRIMINALITET

Ulike faktorer virker sammen på tvers av flere kriminalitetstrusler og påvirker kriminalitetsutviklingen på kort og lengre sikt. Internasjonale trender, teknologisk utvikling, ettervirkninger etter koronapandemien, og krigen i Ukraina, er eksempler på slike faktorer. Blant annet gir krig og konflikt økt handlingsrom for kriminelle nettverk til å utvide kriminell virksomhet, særlig knyttet til salg av ulovlige våpen, menneskesmugling og -handel. Gjenåpning av grenser etter pandemien og økt mobilitet i verden har normalisert handlingsrommet for kriminelle aktører til å operere i Norge igjen.

Norge har høy levestandard og et godt utbygd velferdssystem. Norsk økonomi i sin helhet ble relativt lite påvirket av koronapandemien, men ettervirkninger av pandemien og krigen i Ukraina skaper økonomisk usikkerhet for både næringsliv og enkeltindivider. Norge og Europa har blant annet opplevd høye strømpriser det siste året, som har blitt ytterligere forsterket av krigen. Renteøkninger, økte matvarepriser og øvrige effekter av økt inflasjon i den globale økonomien vil også påvirke næringslivets og enkeltindividers økonomi. På tross av en usikker situasjon har høy norsk økonomisk velstand – i kombinasjon med behov for utenlandsk arbeidskraft og en forverret økonomisk situasjon ellers i Europa – ført til at Norge fortsatt er et attraktivt mål for aktører som vil begå en rekke ulike typer kriminalitet.

Tilliten til norske myndigheter er høy, og det norske samfunnet kjennetegnes av en stor grad av trygghet, blant annet fordi det ikke er områder i Norge med vedvarende høyt konfliktnivå blant kriminelle. Økt konfliktnivå mellom kriminelle

aktører og nettverk påvirker likevel tryggheten i lokalsamfunn negativt i kortere perioder.

Digitaliseringen i Norge fortsetter å øke både i offentlig og privat sektor. Det har gitt kriminelle et økt handlingsrom, eksempelvis for å utnytte barn og unge på nett eller drive narkotikasalg via sosiale medier. Deling av vold på sosiale medier gir volden økt oppmerksomhet blant enkelte unge, og fungerer som en driver til utøvelse av mer vold. Kryptovaluta, anonymiseringstjenester, kryptering og nye betalingstjenester legger til rette for hvitvasking og annen kriminalitet. I tillegg er det digitale rom en hovedarena for hatefulle ytringer og radikalisering. Videre har økt netthandel gitt større handlingsrom for aktører i transportbransjen som utnytter arbeidstakere og begår annen økonomisk kriminalitet.

Sammenhengen mellom naturødeleggelser, tap av biologisk mangfold og klimaendringer blir stadig tydeligere, og konsekvensene av klimaendringer er mer fremtredende i nyhetsbildet. Økt klima- og miljøfokus kan påvirke en rekke områder. Det kan føre til muligheter i form av teknologiske nyvinninger og nye arbeidsplasser, eller begrensninger i form av forbud eller utfasing av miljøfiendtlig teknologi og arbeidsplasser. Dette kan skape nye handlingsrom for kriminelle og nye arenaer for aktivisme.

Ulike politidistrikter beskriver en opplevelse av økt aksept for bruk av narkotika i samfunnet, spesielt i møte med unge. Dette er en erfaring som også ble omtalt i fjorårets PTV.

2.

SÆRLIG ALVORLIGE KRIMINALITETSTRUSLER

2.1. Kriminelle spesialister selger tjenester til kriminelle aktører

Et ekspanderende marked innen kjøp og salg av kriminelle tjenester er kapabilitetsfremmende, og det er meget sannsynlig at det øker handlingsrommet til etablerte kriminelle nettverk. Det er sannsynlig at utviklingen vil føre til at den organiserte kriminaliteten blir mer uoversiktlig og får et mer profesjonalisert preg. Det er sannsynlig at nye og/eller mindre sofistikerte kriminelle aktører får økt måloppnåelse og flere muligheter til å begå kriminalitet som følge av kriminalitet som en tjeneste, særlig i det digitale rom.

Ifølge Europol har den kriminelle forretningsmodellen "crime-as-a-service" (kriminalitet som en tjeneste), forkortet CaaS, fått økt utbredelse blant kriminelle nettverk. Disse setter i større grad bort ulike oppdrag til kriminelle aktører som har spesialisert seg på en kriminell tjeneste, eller som har særskilt kompetanse. Dette bidrar til at den organiserte kriminaliteten blir mer uoversiktlig. De kriminelle spesialistene fyller viktige funksjoner som pengevekslere, torpedoer, dokumentforfalskere, transportører og tilbydere av cyberkriminelle varer eller tjenester.

De kriminelle spesialistene fremstår som profittmotiverte og omsetter egne kapabiliteter, som ressurstilgang, teknisk tilgang, tillatelser, eller nødvendig utstyr, for å tilrettelegge for andre aktørers kriminelle måloppnåelse. I noen tilfeller er slike tilretteleggere en del av nettverket. I andre tilfeller opererer aktørene uavhengig og tilbyr sine tjenester til flere kriminelle nettverk.

Tilbydere av transport- eller hvitvaskingtjenester har ofte en kritisk rolle i forbindelse med narkotikainnførsler. Noen hvitvaskingsaktører bruker sofistikerte teknikker innen pengeoverføring og hvitvasking. Modus operandi

er ofte komplisert og forutsetter at nettverkene samarbeider med profesjonelle aktører, som revisorer og advokater. Blant de viktigste hvitvaskingsaktørene finnes det imidlertid også aktører som har bygget opp en effektiv kriminell tjeneste basert på enkle og tradisjonelle metoder for valutauførsler. På europeisk nivå estimeres det at kun én prosent av utbyttet fra kriminelle aktiviteter blir konfiskert.

Kriminelle nettverk produserer, stjeler, omsetter og bruker både falske og ekte ID-dokumenter. For å produsere forfalskninger av god kvalitet kreves høy kompetanse og spesialutstyr, da dokumentenes sikkerhetselementer blir stadig vanskeligere å forfalske. Ekte og falske dokumenter, herunder norske pass, omsettes åpent på internett.

Alle former for cyberkriminelle verktøy og tjenester kan kjøpes på det åpne eller det mørke nettet. Slike verktøy og tjenester tilbys ikke bare til andre etablerte kriminelle aktører, men øker også kapabiliteten til uerfarne og mindre sofistikerte aktører. Man kan for eksempel bestille et tjenestenektangrep som andre utfører, eller kjøpe tilgang til skadevare for å gjennomføre phishing eller et datainnbrudd selv. Erfarne kriminelle aktører tilbyr også opplæring i cyberkriminalitet. Noen kriminelle aktører selger løsepengevirus og tilgang til kompromitterte bedriftsnettverk til andre aktører, som gjennomfører utpressingen.

2.2. Kriminelle aktører styrer sin virksomhet fra utlandet

Det er meget sannsynlig at kriminelle nettverk som styres av aktører i utlandet vil dominere markedet for innførsel av narkotika. Dette underbygges av aktørenes handlingsrom i tredjeland, evne til å geografisk distansere seg fra kriminaliteten, økt handlingsrom som følge

av mer samarbeid med kriminelle spesialister (CaaS), og rask erstatning av eventuelle tapte mottaker- og distribusjonsnettverk i Norge.

Flere bakkmenn og sentrale aktører innen organisert kriminalitet styrer sin kriminelle virksomhet fra utlandet. Tredjeland som Marokko, Tyrkia og, i økende grad, De forente arabiske emirater (spesifikt Dubai), er attraktive tilholdssteder for kriminelle aktører. Disse kommer i tillegg til typiske transittland for innførsel av narkotika til Norge, som land på Vest-Balkan, Spania, Nederland, Tyskland, Danmark og Sverige. Utviklingen er en del av en større internasjonal trend, som også inkluderer at kriminelle migrerer fra det europeiske kontinentet til Latin-Amerika.

Migrasjonen til tredjeland knytter seg hovedsakelig til erfarne kriminelle, i mange tilfeller tidligere gjengkriminelle og aktører i det øvre sjiktet av den kriminelle næringskjeden. Mange har allerede bodd i utlandet over flere år, hvor de har fjernstyrt den kriminelle virksomheten. Aktørene er i mange tilfeller knyttet til narkotikainnførsel og økonomisk kriminalitet. Mange er etterlyst og domfelt, eller siktet/tiltalt i norske straffesaker. Aktørene kjøper seg trygghet ved å investere penger i landene de migrerer til – de investerer i eiendom og luksusvarer, og bestikker personer i ulike nøkkelposisjoner.

Det fremstår som at kriminelle nettverk som styres fra utlandet raskt klarer å erstatte personer i mottaks- og distribusjonsleddet når disse stoppes av politiet.

2.3. Konfliktbildet innen kriminelle gjenger

Trusselbildet knyttet til kriminelle gjenger vil til enhver tid følge spenningsnivået i gjengmiljøene. Det vil si at konfliktbildet vil

varierte mellom rolige og anspente perioder. Det er sannsynlig at det også vil være voldshendelser med potensielt dødelig utfall som et resultat av gjengenes interne konflikter i 2023. Det er videre sannsynlig at 1 % MC-klubbene vil opprettholde sine ekspansjonsaktiviteter i 2023.

Kriminelle gjenger forstås som selvdefinerte og eksternt definerte grupper som utviser evne til å operere sammen over tid, og med en orientering mot alvorlig kriminalitet. Gjengene er ofte knyttet til et geografisk område og aktørene bruker gjerne symbolske uttrykk for gruppetilhørighet. I gjengforståelsen inkluderes også såkalte 1 % MC-klubber. Disse klubbenes overordnede mål er å leve på siden av det lovlydige samfunnet med egne lover og regler, derav uttrykket "1 %", som betegner den ene prosenten som står utenfor samfunnet. Lojalitet til klubben er grunnleggende for 1 % MC-klubber.

Kriminelle gjenger er mest synlige i og rundt storbyene. Det sentrale Østlandet er fremdeles den viktigste arenaen for aktører tilknyttet kriminelle gjenger. Oslo er kjerneområdet til flere kriminelle gjenger og det største narkotikamarkedet i Norge. Samtidig er særlig Øst politidistrikt et viktig transittsted for innførsel og distribusjon av narkotika til kriminelle gjenger og andre mottaks- og distribusjonsnettverk i Norge. En fellesnevner for gjengene er at de er involvert i trussel- og voldsbasert kriminalitet, ofte knyttet til salg og distribusjon av narkotika. Kriminaliteten foregår i mange tilfeller i det offentlige rom, noe som kan påvirke trygghetsfølelsen negativt. Det siste året har aktiviteten fra svenske aktører tilknyttet kriminelle gjenger i Norge blitt mer synlig, blant annet gjennom voldsoppdrag.

Konfliktbildet varierer i intensitet, og konflikter har tidligere eskalert raskt, med stort voldspotensial. Faktorer som reduserer faren for voldelige

sammenstøt er blant annet fengsling av sentrale aktører i konfliktlinjene, avverging av hendelser, samt økt tilstedeværelse av politi i aktuelle områder. Faktorer som øker faren for nye voldelige konfrontasjoner er løslatelse av sentrale aktører som er involvert i konflikt og forekomst av voldshendelser som ikke er blitt hevnnet. Andre drivere for konflikt er interne ran av narkotika i kriminelle miljø, eller voldshandlinger i forbindelse med gjeldsinnkreving. Ekspansjon og tilfeldige sammenstøt, for eksempel i utelivet, vil også kunne utløse eller forsterke konflikter.

1 % MC-klubbene er etablert både i rurale og urbane strøk i alle landets politidistrikter. Politiet har over tid observert en utvikling der flere internasjonale 1 % MC-klubber synes å være i en nasjonal ekspansjonsfase. I flere europeiske land, blant annet i Danmark, ser man et økt konfliktnivå mellom enkelte 1 % MC-klubber. Samtlige klubber i Norge har medlemmer med kriminelle kapabiliteter innen narkotika, våpen, og vold. For å begrense handlingsrommet til kriminelle nettverk vedtok Stortinget i 2021 en lovendring som gir muligheter til å kriminalisere deltagelse i og rekruttering til kriminelle nettverk. Erfaringen med kriminalisering av 1 % MC-klubber i andre land er at klubbene fortsatt er aktive, men at aktørene bevisst holder en lavere profil.

2.4. Kriminelle nettverk benytter kryptovaluta til bedrageri og hvitvasking

Kryptovaluta er en attraktiv investering for mange. Falske handelsplattformer markedsføres aggressivt og fremstår som seriøse. Bedragerne er ofte svært profesjonelle, og bedrageriene genererer høy profitt. Dette er faktorer

som gjør det sannsynlig at omfanget av investeringsbedrageri med kryptovaluta vil øke. Det er sannsynlig at kryptovaluta i økende grad vil bli brukt til hvitvasking.

Kryptovaluta muliggjør overføring av store beløp på tvers av landegrenser, som regel med lave gebyrer. I likhet med ordinær valuta, benyttes kryptovaluta både som betalingsmiddel og investeringsobjekt. Kryptovaluta benyttes av kriminelle i profittmotivert kriminalitet for å skjule transaksjoner i forbindelse med hvitvasking eller kjøp og salg av ulovlige varer. Andre elementer knyttet til kryptovaluta, som global dekning, miksetjenester,² useriøse vekslingstjenester og desentralisering, gjør kryptovaluta egnet for kriminelle.

I Norge har det de siste årene vært en økning i bedragerier hvor fornærmede forledes til å investere i kryptovaluta. Metodene er mange. Én handlemåte innebærer at man blir forledet til å investere i prosjekter eller produkter som er verdiløse eller ikke-eksisterende. Dette kan inkludere opprettelse av falske handelsplattformer på nett, gjerne kombinert med en aggressiv markedsføring i sosiale medier. Fornærmede kan også motta fiktive kvitteringer og dokumentasjon på investering og gevinst, som igjen brukes for å manipulere fornærmede til å gjøre ytterligere investeringer.

Organiserte kriminelle i utlandet har egne bedrifter som utelukkende driver med investeringsbedrageri som forretningsmodell. Disse har flere ansatte og egne callsentre. Det er en økende trend innen investeringsbedrageri at fornærmede blir lurt flere ganger. Først blir de manipulert til å investere penger, deretter betaler de for hjelp til å få tilbake pengene, uten å innse at det er de samme bedragerne som lurer dem på nytt. Flere advarer også om at

² En miksetjeneste blander kryptovaluta med andre personers kryptovaluta og benyttes for å skjule hvor pengene kommer fra.

investeringsbedragere rekrutterer ofre via datingapper.

Kryptovaluta benyttes også som betalingsmiddel ved andre typer bedrageri og løsepengevirus, ved at de fornærmede blir bedt om å kjøpe kryptovaluta som oppgjør. Kryptovaluta blir også i økende grad benyttet som betaling mellom kriminelle for ulovlige varer og tjenester, slik som kjøp, salg, innførsel og utførsel av narkotika, våpen og andre ulovlige varer, i tillegg til menneskehandel. I tillegg benyttes kryptovaluta til hvitvasking av utbytte fra kriminalitet.

2.5. Løsepengevirus mot privat og offentlig sektor

Norske bedrifter og offentlige virksomheter vil fortsatt utsettes for løsepengevirus. Det er sannsynlig at virksomheter med samfunnskritiske funksjoner vil rammes av dette. Det er sannsynlig at kriminalitet mot datasystemer motivert av Russlands krig mot Ukraina vil fortsette. Effekten av tjenestenektangrep har så langt vært liten. Det er dermed mulig at politisk motiverte trusselaktører vil forsøke å benytte andre virkemidler, som datainnbrudd, løsepengevirus og datatyveri.

Løsepengevirus rettet mot bedrifter og virksomheter anses som den største kriminalitetstrusselen mot IKT-sikkerhet og digital infrastruktur. Dette begrunnes med mange hendelser, stort skadepotensial, mulighet for høy profitt for gjerningspersonene, samt liten fare for identifisering og straffeforfølgelse. Aktørene har det siste året i økende grad benyttet dobbel utpressing. Det vil si at de stjeler data i tillegg til å kryptere, og truer med publisering på det mørke nettet. Det er også observert aktører som benytter seg av trippel utpressing, ved at

de i tillegg til trusler om publisering truer med tjenestenektangrep.

Aktørene oppnår tilgang ved bruk av blant annet phishing, utnyttelse av lekkede eller svake passord, kjøp av stjalne tilganger til systemer og utnyttelse av sårbarheter i programvaren eller nettverkene til offeret. De opererer i flere tilfeller fra Øst-Europa.

Bedrifter og virksomheter med tidskritiske prosesser er utsatte mål, fordi nedetid kan være svært kostbart. De kriminelle aktørene regner med at dette øker betalingsviljen og muligheten for at de lykkes. Løsepengevirus medfører økonomiske tap for bedrifter og virksomheter, men kan også medføre at kritisk infrastruktur blir satt ut av funksjon.

Russlands pågående krig mot Ukraina har motivert hacktivistene til å begå kriminalitet mot datasystemer i land som støtter Ukraina, blant dem Norge. Disse aktørene har så langt benyttet tjenestenektangrep som virkemiddel.

2.6. Datatyveri fra private og offentlige virksomheter

Norske bedrifter og offentlige virksomheter vil utsettes for datainnbrudd, datatyveri og datamanipulasjon. Det er sannsynlig at bedrifter med roller i kritiske samfunnsfunksjoner, og virksomheter med betydelige kompetanse- og bransjefordeler, i økende grad vil bli rammet.

Datainnbrudd uten påfølgende bruk av løsepengevirus utgjør en alvorlig trussel mot norske virksomheter, særlig ved tyveri av data. Aktører kan i tillegg manipulere eller sabotere data. Motivasjonen for kriminelle aktører er hovedsakelig økonomisk vinning. Målet kan

oppnås ved direkte utpressing av offeret, eller ved å selge stjålet informasjon eller ulovlige systemtilganger til andre kriminelle eller statlige aktører. Den stjålne informasjonen kan blant annet være sikkerhetsgradert informasjon, brukernavn og passord, bedriftshemmeligheter eller personsensitive opplysninger. Betaling er ingen garanti for å få disse tilbake.

Det foregår mange phishing-kampanjer og annen kriminell aktivitet mot norske virksomheter generelt. Kritisk infrastruktur og sentrale offentlige virksomheter er utsatt for datainnbrudd. Trusselen mot offentlig sektor vedvarer. Dette er en skjerpende faktor som indikerer at kriminelle aktører ser et potensial i å utnytte det norske samfunnets avhengighet av slike sentrale offentlige funksjoner i vinnings hensikt.

2.7. Arbeidslivskriminalitet i varetransportbransjen

Det er meget sannsynlig at aktører som begår arbeidslivskriminalitet vil fortsette å ha store markedsandeler i varetransportbransjen. Kriminaliteten i varetransportbransjen truer konkurransegrunnlaget i næringen, og påfører virksomheter og næringslivet økonomiske tap.

Omfanget av kriminelle forhold i varetransportbransjen fremstår som økende. Økt netthandel og tilbud om hjemkjøring av varer har ført til stor etterspørsel etter varetransport. Transportbransjen er i liten grad regulert, har lave etableringskostnader og stiller få krav til kompetanse. Som en respons på disse utfordringene lanserte regjeringen høsten 2022 en handlingsplan mot sosial dumping i transportsektoren. Flere politidistrikter rapporterer om utstrakt bruk av underleverandører, svart avlønning, omfattende arbeidsmiljølovbrudd og trygdesvindler i varetransportbransjen. Bruk av

underleverandører gjør at kostnadene holdes nede. Det virker også konkurransevridende, slik at mange etablerte transportselskaper ender opp med å benytte seg av underleverandører som i realiteten driver ulovlig.

Mange underleverandører som benyttes bruker bevisst enkeltpersonforetak for å unndra seg arbeidsgiveransvar. I tillegg begås det grove skattesvik, svart avlønning, grov økonomisk utroskap og grov hvitvasking, uten at oppdragsgiver kan knyttes direkte til den kriminelle aktiviteten. Det foreligger også rapporteringer om at arbeidsgivere bevisst holder nede driftskostnadene sine til et kunstig lavt nivå, slik at underleverandørene presses til å bryte regler knyttet til kjøre- og hviletid.

Aktørene har god tilgang på arbeidskraft og er organisert i etablerte nettverk. Varebiler er det eneste utstyret man må ha tilgang på for å kunne gjennomføre kriminaliteten. Det er heller ikke krav til løyve for å operere i bransjen.

Aktørenes motivasjon er økonomisk profitt. Ytre forhold, som lav oppdagelsesrisiko og manglende regulering av bransjen, bidrar til at kriminelle transportforetak kan betale sjåførene sine svart, unndra skatter og avgifter, hvitvaske inntjeningen og utsette sjåførene for urimelige arbeidsforhold og sosial dumping.

2.8. Vold begått av personer med alvorlige psykiske lidelser

Det er meget sannsynlig at vold begått av personer med alvorlige psykiske lidelser og problematisk rusmiddelbruk vil fortsette å utgjøre en betydelig trussel, hvor enkelte hendelser vil medføre tap av liv.

De fleste politidistriktene rapporterer om vold begått av personer med alvorlige psykiske lidelser som en vedvarende alvorlig kriminalitetstrussel. Trusselen er ikke knyttet til bestemte deler av landet. Enkelte aktører kan også knyttes til konspiratorisk tankegods og ekstremisme. Dette fører også til at politiet, PST og helsetjenestene vil komme i kontakt med personer med indikasjoner på både alvorlige psykiske lidelser og ekstremistisk tankegods i det daglige.

I oktober 2021 ble fem personer drept på Kongsberg av en gjerningsperson som senere ble dømt til tvungent psykisk helsevern. Videre har det etter skyteepisoden i Oslo 25. juni 2022 blitt stilt spørsmål ved gjerningspersonens tilregnelighet.

Kvinnelige gjerningspersoner forekommer, men mest typisk beskrives menn i alderen 20–50 år med alvorlige psykiske lidelser, ofte med symptomer på psykose og problematisk rusmiddelbruk. Gjerningspersonene i de alvorligste sakene har ofte vært i kontakt med politi- og helsetjenestene før voldsutøvelsen. En betydelig andel er så syke at det tilsynelatende ikke ligger noen kriminell intensjon bak voldsutøvelsen, og det stilles i ettertid ofte spørsmål om gjerningspersonenes tilregnelighet. Noen har tidligere vært underlagt tvungent psykisk helsevern. Noen har voldshistorikk, og noen opplever ved gjerningstidspunktet en livskrise og en forverring av sykdomsbildet. Forskning viser at alvorlige psykiske lidelser alene ikke er sterkt knyttet til vold, men at de utgjør en risikofaktor i samspill med for eksempel relasjonsbrudd, voldsutsatthet, økonomiske kriser eller problematisk bruk av alkohol eller andre rusmidler.

Flere politidistrikter peker også på mulige årsaker til voldsutøvelsen. Individuelle årsaker kan være psykose og sykdomsforverring, rusbruk, livskriser, misnøye med myndigheter eller hjelpeapparat. Årsaker i samfunnet kan være manglende hjemmel til tvangsbruk og manglende kapasitet i helsetjenestene, eller ettervirkninger etter koronarestriksjoner.

De som rammes av volden kan være gjerningspersonens foreldre eller partner, bekjente, tilfeldige i det offentlige rom eller offentlige ansatte. Andre mulige utsatte for vold eller trusler er ansatte i barnevern, helsetjenestene, NAV, utlendingsforvaltningen og politiet.

Trusler eller vold i akutte situasjoner med psykose eller ruspåvirkning synes å være vanligst, men det forekommer også rapporteringer om personer med alvorlige psykiske lidelser som knyttes til hatefulle ytringer, konspiratorisk tankegods, radikaliserings og ekstremisme. Forskning på voldelig radikaliserings underbygger at voldelig ekstremisme og alvorlige psykiske lidelser ikke er gjensidig utelukkende fenomener.

Tilfeldig bruk av kniv og grov vold er vanligst blant de mest alvorlige forholdene. Noen av disse har resultert i drap.

Det har vært en økning i vold begått av personer med alvorlige psykiske lidelser de siste fem årene.³ Når det gjelder drap og drapsforsøk er samtlige saker fra 2022, og de fleste fra 2021, fortsatt under etterforskning. Flere av sakene venter på rettspsykiatrisk erklæring om gjerningspersonens psykiske helse.

3 Se Kripos (2022) Vold begått av personer med alvorlige psykiske lidelser. Oslo: Kripos.

3.

SITUASJONSBESKRIVELSER

3.1. Trusler mot offentlig ro, orden og demokratiske verdier

Med trusler mot offentlig ro, orden og demokratiske verdier menes kriminalitet som skaper utrygghet i det offentlige rom. Kriminaliteten truer både ytringsfriheten og individets bevegelses- og handlefrihet. Dette omfatter hatkriminalitet og aktivisme hvor vold eller sivil ulydighet kan inntreffe.

Digitale flater fungerer som arena for hatefulle ytringer og radikaliserings

Trusler og hatefulle ytringer rettet mot politikere, samfunnsdebattanter og øvrige påvirker både enkeltindivider og samfunnet. Flere politikere og privatpersoner har uttrykt at hatefulle ytringer fører til at de vegrer seg for å delta i debatter og diskusjoner, eller modererer sine ytringer. Enkelte avstår også fra å delta. Mange av ytringene fremsettes på digitale flater, hvor anonymitet legger til rette for ytringer som normalt ikke ville vært fremsatt i det offentlige rom. Det som oppleves som hatefulle ytringer, eller omtales som det i sosiale medier, er sjeldent straffbart.

Lukkede digitale arenaer fungerer som ekkokamre og bidrar til polarisering. Det digitale rom er også en hovedarena for radikaliserings. Politiet mottar bekymringsmeldinger om enkeltpersoner knyttet til radikaliserings innen både venstre- og høyreorienterte ytterliggående ideologier, samt bekymringer om religiøs radikaliserings eller antistatlige ideologier. Flere av aktørene er unge og fremstår ofte som psykisk syke.

Fysiske markeringer kan være polariserte og utløse voldelige konfrontasjoner

Debattklimaet under fysiske markeringer er tidvis polarisert og preget av steile fronter, og alvorlige ordensforstyrrelser og vold forekommer under enkelte markeringer. Særlig utsatt er innvandrings- og religionskritiske

markeringer. Markeringene, som har inkludert brenning av koranen, oppleves som hatefulle av motdemonstranter. Dette har utløst støy, aggressiv atferd og vold fra motdemonstranter. I sitt arbeid med å legge til rette for ytringsfrihet og opprettholde offentlig ro og orden, har politiet ved flere anledninger blitt oppfattet som partiske av både demonstranter og motdemonstranter. Dette har utløst vold mot politiet. Voldelig aktivisme har primært funnet sted på Østlandet.

De to siste årene har det vært gjennomført flere markeringer mot myndighetenes håndtering av pandemien, og vaksinemotstandere har forsøkt å ta seg inn på vaksinesenter for å fjerne vaksiner. Budskapene har til dels vært preget av konspirasjonsteorier. Markeringene har tiltrukket seg personer med antistatlige holdninger og personer tilhørende ytre høyre. Erfaringsmessig tiltrekker dette personer fra ytre venstre, som har ytre høyre i sitt fiendebilde. Antallet markeringer har gått ned siden restriksjoner opphørte, men engasjementet rundt vaksinemotstand og lignende er fortsatt aktivt på internett.

Etter Russlands invasjon av Ukraina har det vært gjennomført markeringer til støtte for begge parter. Det har kun vært enkelttilfeller av ordensforstyrrelser i forbindelse med disse.

Utstrakt bruk av ikke-voldelig sivil ulydighet blant klima- og miljøaktivister

Klima- og miljøaktivisme har det siste året vært preget av utstrakt bruk av ikke-voldelig sivil ulydighet. Motstanden rettes både mot konkrete utbygginger i naturområder og mot klima- og miljøpolitikk generelt, både lokalt og nasjonalt. Aktørene i Norge er stort sett løst organisert, og enkelte har knytninger til internasjonale, desentraliserte klima- og miljøvernorganisasjoner.

I løpet av 2022 har klima- og miljøaktivister gjennomført flere aksjoner hvor de har sperret

motorveier i rushtiden på ulike steder i landet. Det har også vært flere aksjoner hvor det har blitt begått skadeverk. Klima- og miljøaktivister har blitt innbragt og bøtelagt for å ikke etterkomme politiets pålegg gjentatte ganger.

Klima- og miljøaktivisme engasjerer stort, også internasjonalt. Utenlandske aktivister deltar på sivile ulydighetsaksjoner i Norge, og norske aktivister deltar i utlandet. Aksjoner i utlandet har vært større i omfang og varighet enn i Norge, og har involvert aktivitet med større konsekvenser for omgivelsene, som å ta seg ut på rullebanen på flyplasser.

3.2. Trusler mot alminnelig trygghet i samfunnet

Med trusler mot alminnelig trygghet i samfunnet menes i denne sammenhengen kriminalitet begått av kriminelle nettverk. Dette er et samlebegrep for miljøer, gjenger, grupperinger eller sett av individer som er knyttet sammen gjennom kriminalitet. Begrepet er en paraplybetegnelse som dekker alt fra organiserte kriminelle grupper til kriminelle ungdomsgrupperinger.

Kriminalitet som inngår i trusler mot alminnelig trygghet kan være menneskehandel, gjengrelatert vold og konflikter, samt innførsel, produksjon og omsetning av narkotika. Andre eksempler er ulovlig omsetning, erverv eller besittelse av skytevåpen og eksplosiver, mobil vinningskriminalitet og grove ran av eksempelvis ur- og gullforretninger, finansinstitusjoner eller verditransporter.

Kriminelle nettverk har økt profesjonalisering
Organisert kriminalitet foregår i det skjulte, og aktiviteten påvirker ikke folk flest i hverdagen. Likevel er organisert kriminalitet en av de største

kriminalitetstruslene mot samfunnsstrukturer, økonomi og næringsliv samt den alminnelige trygghet. Ifølge Europol har trusselen aldri vært høyere. Bakgrunnen for dette er at forretningsmodellen til kriminelle nettverk blir stadig mer kompleks, med hyppig utskiftning av samarbeidspartnere og økt profesjonalisering. Svært forenklet kan den kriminelle organiseringen beskrives som løst sammenkoblede nettverk av profesjonelle kriminelle, der grensekryssende samarbeid foregår både flytende og systematisk. Profittmotivet er styrende for hvordan kriminelle nettverk dannes, hvordan de driftes, hvilke handlemåter som benyttes og hvilke samarbeid som oppstår.

Kriminelle nettverk er omgitt av en rekke tilbydere av kriminelle tjenester. Disse tilretteleggerne selger sine tjenester innen blant annet transport og logistikk, banktjenester, kryptert kommunikasjon, falske dokumenter, hvitvasking og torpedovirksomhet. Når kriminelle spesialister selger sine tjenester til andre kriminelle, omtales forretningsmodellen som "crime-as-a-service" (CaaS).

Kriminelle nettverk involverer seg i ulike typer kriminalitet. Grov narkotikakriminalitet er fremtredende, men også hvitvasking, bedragerier, menneskehandel, arbeidslivskriminalitet, voldskriminalitet og smugling av avgiftsbelagte varer, med mer. Kriminelle aktører tilpasser seg endringer i markeder og handlingsrom. Krigen i Ukraina er en relevant endringsfaktor som gir økte muligheter for menneskehandel, våpensmugling og annen profittmotivert kriminalitet. Per desember 2022 er det imidlertid ikke avdekket høyere enn normalt aktivitetsnivå blant kriminelle nettverk, eller tydelig endring i fokus fra kriminelle aktører i Norge, som følge av krigen i Ukraina. Politiet er kjent med at enkeltpersoner knyttet til kriminelle nettverk i Norge har reist til Ukraina for å delta i krigen. Allerede før krigen ble det illegale

våpenmarkedet i Ukraina regnet som et av de største i Europa. Ifølge Europol er det mange personer som forsøker å reise fra Ukraina med våpen, primært håndvåpen, men det finnes også eksempler på at tyngre militære våpen blir forsøkt smuglet ut.

Kriminelle bruker ofte krypterte kommunikasjonskanaler

Kommunikasjonen mellom de kriminelle foregår ofte på krypterte kommunikasjonskanaler. Plattformene sørger for at de kriminelle kan fortsette å planlegge og gjennomføre nye kriminelle opplegg i et tempo, og med en rekkevidde, som ikke er mulig ved tradisjonelle walk-and-talk-møter. Ved bruk av krypterte kommunikasjonsplattformer kan de kriminelle enkelt knytte kontakt med personer som har ønsket kriminell kompetanse.

Økt tilgjengelighet av narkotika

Narkotikamarkedet er i endring og har blitt enda mer digitalisert i løpet av pandemien. Bruk av apper, sosiale medier og krypterte tjenester framstår som mer vanlig i distribusjon og salg av narkotika.

Narkotikasituasjonen i Europa preges av økt tilgjengelighet og større mangfold i brukermønster, ifølge EUs narkotikabyrå (EMCDDA). I 2021 ble det satt beslagsrekord for kokain i Europa. Også i Norge var de totale mengdene beslaglagt kokain blant de største noen gang. Norge er blant landene i Europa med høyest konsum av MDMA per innbygger, basert på vannprøveundersøkelser i europeiske storbyer.

Legemiddelforbruket i Norge er også økende, og i 2021 var det flere som døde ved misbruk av andre opioider (morfin, kodein, oksykodon) enn heroin. Det er imidlertid ikke kjent i hvilken grad stoffene som forårsaket dødsfallene ble kjøpt illegalt, eller om de ble foreskrevet av lege.

Fortsatt nedgang innen tyveri og vinningslovbrudd

Omfanget av registrerte tyverier og andre vinningslovbrudd fortsetter å gå ned, i tråd med en langvarig nedadgående trend. Nedgangen gjelder både tyverier fra person, bolig og fritidsbolig samt ulike former for ran. Økt aktivitet fra mobile vinningskriminelle (MVK) forventes som følge av oppheving av indre grensekontroll i Schengen, økt reisevirksomhet og økt etterspørsel av varer som følge av den sikkerhetspolitiske situasjonen i Europa. Aktørene retter seg mot lett omsettelige varer, som biler, båter, verktøy og utstyr som ekkolodd, katalysatorer og GPS-enheter i traktorer og anleggsmaskiner.

Ukrainske flyktninger befinner seg i en sårbar situasjon for menneskehandel

Som følge av krigen i Ukraina er ukrainske flyktninger sårbare for utnyttelse til menneskehandel. Ukrainske borgere var også før krigen regelmessig omhandlet som potensielle ofre for menneskehandel til prostitusjon og tvangsarbeid. Grupper på sosiale medier – med frivillige som vil hjelpe flyktningene – kan bli brukt av kriminelle aktører til å identifisere potensielle ofre for menneskehandel.

Det er indikasjoner på at ukrainske flyktninger blir lokket inn i utnyttelsesforhold av kriminelle nettverk på sosiale medier før de forlater Ukraina. Nettverkene tilbyr for eksempel organisering av flukt og transport ut av landet mot avtale om prostitusjon i Norge og andre land i Europa. Kriminelle aktører kan også bruke det å tilby hjelp i form av husly som et handlingsrom for å sette flyktninger i takknemlighetsgjeld eller andre sårbare situasjoner.

Bakmenn tilrettelegger for menneskehandel til prostitusjon og tvangsarbeid

Det er avdekket at kriminelle nettverk driver

rekruttering, transport og organisering av utenlandske kvinner for utnyttelse til prostitusjon i Norge. Majoriteten av potensielle ofre for menneskehandel til prostitusjon er utenlandske kvinner som har bakmenn eller tilretteleggere som tar en større andel av fortjenesten, fasiliterer med leiligheter, kontrollerer annonser på eskortesider og/eller har kommunikasjon med kunder.

Indikasjoner på menneskehandel til tvangsarbeid er blant annet observert i bransjer som bilverksted/bilpleie, bygg og anlegg, fiskerinæringen, dagligvare, restaurant, transport og sesongarbeid i landbruket. Arbeidsgiverne har i mange tilfeller enten samme etniske bakgrunn som arbeidstakerne, eller en ansatt som fungerer som en tilrettelegger. Tilretteleggeren mottar noe høyere lønn, og har samme nasjonalitet eller snakker samme språk som arbeidstakerne som blir utnyttet.

Majoriteten av arbeidstakerne som blir utnyttet er utenlandske statsborgere. Utnyttelsesforholdene kjennetegnes ofte av manglende arbeidskontrakter, ingen HMS-kort, lønn som ikke rapporteres, utilstrekkelig verneutstyr og uverdige boforhold. Trusler om bruk av vold, represalier, oppsigelse og kontroll av arbeidstakernes ID-dokumenter er eksempler på aktørenes kontrollmetoder.

3.3. Trusler mot liv, helse og personlig integritet

Med trusler mot liv, helse og personlig integritet menes i denne sammenhengen vold og seksuelle overgrep mot barn og voksne. Vold og seksuelle overgrep begås både i det offentlige og private rom, fysisk og over internett. Trusler mot personlig integritet omfatter også krenkelser av identitet og verdighet.

Skyteepisoder i det offentlig rom utgjør også en trussel mot tredjepersoner

Mellom høsten 2021 og høsten 2022 ble 33 personer drept av 26 gjerningspersoner. Seks av ofrene er drept med skytevåpen. Dette er innenfor normal variasjon sammenliknet med de fem siste årene. Antallet personer registrert som fornærmet i en drapsforsøkssak i samme periode er imidlertid betydelig høyere, sammenlignet med tidligere rapporteringer. Dette skyldes primært hendelsen i Kongsberg 13. oktober 2021 og skytingen utenfor London Pub i Oslo 25. juni 2022. I tillegg har det vært flere skyteepisoder i Oslo det siste året. Flere tilfeller skjedde i det offentlig rom, med mulighet for at tredjepersoner kunne bli rammet. De fleste hendelsene var knyttet til ulike kriminelle miljøer. Flere av skyteepisodene hadde ingen sammenheng med hverandre, men fremstod tilfeldig i samme tidsperiode.

De siste årene har det skjedd flere alvorlige voldshendelser der det har blitt stilt spørsmål om alvorlig psykisk lidelse hos gjerningspersonen, inkludert de ovennevnte hendelsene i Kongsberg og Oslo. Politidistriktene rapporterer om vold begått av personer med alvorlige psykiske lidelser som en vedvarende og alvorlig kriminalitetstrussel.

Vedvarende høyt antall partnerdrap og vold i nære relasjoner

Av drapssaker mellom høsten 2021 og høsten 2022 ble nesten 30 prosent av ofrene drept av partner eller ekspartner. Utviklingen knyttet til vold i nære relasjoner varierer mellom politidistriktene, men overordnet er omfanget stabilt. Vold i nære relasjoner utgjør en vedvarende alvorlig kriminalitetstrussel.

I årsrapporten fra Kompetanseteamet mot tvangsekteskap, kjønnslemlestelse og negativ sosial kontroll kommer det frem at de fleste slike forhold gjelder trusler om vold for å ivareta eller

gjenopprette familiens ære. Majoriteten av henvendelsene gjelder jenter, men det er en viss økning i henvendelser knyttet til bekymring for utsatte gutter. Det er flest forhold med familier med landbakgrunn fra Syria, Pakistan og Somalia. Spesielt utsatt er ungdom som har sin oppholdstillatelse basert på et krav om å bo med en forelder. En partner kan bryte ut av forholdet med voldsutøver og likevel få oppholdstillatelse. En voldsutsatt ungdom har ikke den samme rettigheten, og en del velger å bli værende i en voldelig relasjon for å ikke miste oppholdstillatelsen.

Trusselen knyttet til omfanget av seksuallovbrudd er stabilt høy

Antallet anmeldte voldtekter og andre typer seksuallovbrudd har variert de siste årene, men de registrerte endringene i antall skyldes trolig i liten grad en tilsvarende reell økning eller nedgang. Spesielt når det gjelder voldtekter påvirkes statistikken av at politiet noen år, som for eksempel i 2021, etterforsket enkelte gjerningspersoner som hadde begått svært mange voldtekter. Direkteoverførte bestillingsovergrep og seksuell utpressing på internett er eksempel på en type modus operandi der en gjerningsperson kan ramme mange sårbare ofre med lav anmeldelsestilbøyelighet. Når det gjelder seksuallovbrudd generelt mottar politiet stadig flere tips fra tjenestetilbydere, noe som gir mulighet for opprettelse av flere straffesaker innen seksuallovbrudd. Trusselen knyttet til omfanget av seksuallovbrudd kan derfor ikke leses ut av den registrerte kriminaliteten, men må ansees som stabilt høy.

I forbindelse med krigen i Ukraina har flere norske seksualforbrytere vært involvert i frivillig arbeid knyttet til blant annet transport og husly for ukrainske flyktninger. Det er registrert få hendelser der uønskede seksuelle handlinger

har funnet sted i Norge, men handlingsrommet vil være større så lenge det kommer ukrainske flyktninger til landet.

Stadig yngre barn deler egenprodusert overgrepsmateriale

Truslene knyttet til seksuelle overgrep mot barn på internett har vært relativt stabile det siste året. Selv om det er registrert flere faktorer som påvirker utvikling innenfor kriminalitetstrusselen, er det ikke avdekket betydelige endringer.

Andelen egenprodusert overgrepsmateriale fortsetter å øke som følge av at barn selger, frivillig deler eller presses til å dele overgrepsmateriale av seg selv. Europol rapporterer om at egenprodusert materiale i økende grad viser stadig yngre barn. Voksne som kjøper mindreåriges egenproduserte seksualiserte materiale er en vedvarende kriminalitetstrussel. I Norge har det de siste årene blitt rapportert om stadig yngre barn som selger egenprodusert overgrepsmateriale, og det er registrert tilfeller med barn ned i elleveårsalderen. Politiet har de siste årene også sett stadig yngre barn dele bilder og videoer av seg selv der de er nakne, eller annet seksualisert innhold, på internett, uten at de har blitt oppfordret eller truet til å gjøre dette av andre. Noen barn som har filmet seg selv nakne har vært så unge som fem år. Barn som deler overgrepsmateriale av andre barn uten samtykke, er en vedvarende trend. Delingen skjer på digitale plattformer, både mellom enkeltpersoner og i grupper.⁴

Når det gjelder seksuell utpressing, blir de fleste fornærmede presset til å dele mer og grovere seksualisert materiale. Rundt en tredjedel av de fornærmede presses for penger ved at de må betale for at det seksualiserte materialet gjerningspersonen allerede besitter ikke skal deles videre. Ofrene for seksuell utpressing er

4 Kripos (2022) Ungdom henges ut på nett: deling av ulovlig og bekymringsverdig materiale av barn og ungdom. Oslo: Kripos.

ofte i tenårene, men det er også registrert tilfeller med barn ned i elleveårsalderen. Jenter utsettes i større grad for seksuell utpressing med seksuelt motiv, mens ofrene for seksuell utpressing med økonomisk motiv er gutter. De fornærmede som utsettes for seksuallovbrudd med økonomisk motiv har tidligere blitt omtalt som unge voksne menn, men det siste året har også flere barn tidlig i tenårene blitt utsatt for dette. Det er en økende trend at gjerningspersonen utsetter ofrene for seksuell utpressing etter innledningsvis å ha kjøpt seksualisert materiale.

Globale reiserestriksjoner under pandemien førte til en reduksjon av seksuelle overgrep mot barn i utlandet begått av reisende seksualforbrytere. De fleste land har i løpet av 2022 åpnet opp for innreise. Dette gjelder også for land der det er stor tilgang på sårbare barn og oppdagelsesrisikoen er lav, noe som øker norske reisende seksualforbryteres handlingsrom til å begå overgrep mot barn i utlandet. Norske gjerningspersoner som begår direkteoverførte bestillingsovergrep mot barn i utlandet, er en vedvarende trussel.

Økt distribusjon av overgrepsmateriale på krypterte nettverk

Norsk politi har de siste årene sett en økt rapportering knyttet til bruk av krypterte digitale plattformer til en-til-en distribusjon og deling av overgrepsmateriale i grupper.

Deling og distribusjon av overgrepsmateriale foregår på en rekke arenaer, både på det åpne og det mørke nettet. Såkalte peer-to-peer ⁵ (P2P) nettverk har eksistert i mange år og er fortsatt en foretrukket arena for deling av filer med overgrepsmateriale på det åpne nettet. På det mørke nettet er TOR-nettverket det mest kjente for deling av overgrepsmateriale. Omfanget av

nordmenn på overgrepssider på TOR-nettverket er vanskelig å anslå, men de største forumene for overgrep har flere hundre tusen brukere internasjonalt.

Bruk av bitcoin til kjøp av overgrepsmateriale er ikke et nytt fenomen, men det er usikkerhet rundt omfanget, både nasjonalt og internasjonalt. Ifølge rapporter fra Europol økte omsetningen til overgrepssider som tar betaling i kryptovaluta i årene mellom 2017 og 2020. Etter 2020 har omsetningen til de samme sidene sunket. Det er usikkert om den rapporterte endringen gjenspeiler en reell endring.

3.4. Trusler mot økonomi og arbeidsliv

Med trusler mot økonomi og arbeidsliv menes kriminalitet som rammer både næringslivet, privatpersoner og velferdssamfunnet ved å forårsake økonomiske tap og undergrave legale strukturer, opparbeidede rettigheter i arbeidslivet og et fritt og rettferdig marked. Dette omfatter fiskerikriminalitet, arbeidslivskriminalitet, bedrageri, hvitvasking og korrupsjon.

Fiskerikriminalitet i hele verdikjeden

Fiskerikriminalitet er profittmotivert og konkurransevidende. Kriminaliteten har en negativ effekt på ressursforvaltningen.

Handlingsrommet for under- og feilrapportering er stort, blant annet fordi det er vanskelig å kontrollere næringen både til havs, ved mottakene og ved eksport. Politiet er kjent med at det forekommer under- og feilrapportering av fisk. Lovbruddene begås enten i samarbeid mellom fiskemottak og fiskere, eller ved at mottakene underslår fangst eller fangstverdi

⁵ P2P ("likemannsnettverk") er en ressursdelingsform mellom datamaskiner i et nettverk hvor ressursene er distribuert over hele nettverket, i motsetning til strukturer med en sentral maskin som styrer tilgangen til ressursen og tjener de andre maskinene. Ressursene kan være filer, overføringskapasitet, lagringsplass eller utregningskraft.

for fiskerne. Både mottak og fartøy kan tjene på dette samarbeidet – mottaket får mer råstoff, og fartøyer kan fiske mer enn kvoten tilsier. Under- og feilrapporteringen kamuflerer dermed ofte ulovlig fiske over kvote.

I tillegg til under- og feilrapportering blant yrkesfiskerne, omsetter også fritidsfiskere og yrkesfiskere betydelige mengder fisk og skalldyr svart i Norge. Selve omsetningen foregår enten direkte mellom fisker og konsumenter, eller via digitale markedsplasser. Politiet erfarer også at turistfiskere smugler ut fisk og skalldyr i store kvanta, slik at ressursuttaket fra havet er betydelig høyere enn kvoten på 18 kilo.

Arbeidslivskriminalitet begås av enkeltaktører og kriminelle nettverk

Arbeidslivskriminalitet begås over hele landet av alt fra enkeltaktører i små virksomheter til kriminelle nettverk med knytninger til alvorlig organisert kriminalitet. Unndragelse av skatter og avgifter, brudd på arbeidsmiljøloven og tilhørende forskrifter, samt bruk av svart eller ulovlig arbeidskraft, kjennetegner kriminaliteten. Kriminelle aktører benytter ofte stråpersoner i formelle roller for å skjule at de reelt sett drifter foretak. Profesjonelle aktører benyttes som tilretteleggere for å kamuflere kriminalitet.

Arbeidslivskriminalitet innebærer ofte et element av utnyttelse av sårbare utenlandske arbeidstakere. Utnyttelse til arbeid kan blant annet være lønnstyper, ulovlig overtid, uforsvarlig sikring og direkte farlige arbeidsplasser, og ellers stor grad av kontroll over arbeidstakerens livssituasjon. Sårbare utenlandske arbeidstakere benyttes ofte til sesongbasert arbeid i landbruks- og fiskerinæringen, og innen byggebransjen, varetransport og bilpleie.

Bruk av ulovlig arbeidskraft var ved utgangen av 2022 på tilnærmet samme nivå som før koronapandemien. Enkelte ukrainske asylsøkere har blitt forsøkt rekruttert til ulovlig arbeid i arbeidsintensive bransjer før de har fått innvilget kollektiv beskyttelse.

Mange virksomheter oppsøker privatpersoner i vår- og sommersesongen og tilbyr vedlikeholdsarbeid som maling og utbedring av hus og hager. Flere slike virksomheter knyttes til skatte- og avgiftskriminalitet, brudd på arbeidsmiljøloven, trusler, bedragerier og hvitvasking.

Økning i antall bedragerisaker

Den profittmotiverte vinningskriminaliteten har blitt mer digitalisert. I 2022 økte antallet anmeldelser av bedrageri med nærmere 22 prosent sammenlignet med året før. Banker rapporterer imidlertid om en ekstrem økning i antall bedragerier de seneste årene. Diskrepansen mellom politiets tallmateriale og bankenes rapporter indikerer at få velger å anmelde forholdet til politiet, og at mørketallene er store.

Bedragerier tilfører de kriminelle enorme økonomiske gevinster. I Sverige estimeres utbytte fra bedragerier å utgjøre over to milliarder svenske kroner årlig, tilsvarende utbyttet fra narkotikaomsetning på gateplan. Beløpet inkluderer ikke det man i Sverige kaller velferdsbedrageri. Bedrageri har blitt en så viktig inntektskilde for flere kriminelle nettverk at svensk politi mener det påvirker voldsutviklingen.

Ved bedrageri av foretak er det i hovedsak to modus operandi som går igjen – direktørbedrageri⁶ og fakturabedrageri.⁷

6 Direktørbedrageri: Den kriminelle aktøren skaffer informasjon om nøkkelindivider i en organisasjon og utnytter informasjonen ved å utgi seg for å være en leder/direktør for å få overført en større sum penger.

7 Fakturabedrageri: Mottaker av en faktura forledes til enten å betale for en vare eller tjeneste de ikke har bestilt, eller til å endre mottakers kontonummer ved e-post med oppdatert betalingsinformasjon.

Bedragerne er mer sofistikerte og målrettede i sine angrep, og er i mange tilfeller organisert i profesjonelle internasjonale kriminelle nettverk. Gjerningspersonene identifiserer det optimale tidspunktet for angrepet og bruker riktig språk. Det finnes tilfeller hvor norske foretak har tapt mer enn 100 millioner kroner.

Sosial manipulering via e-post, telefon eller SMS benyttes ofte ved bedrageri. Såkalt spoofing⁸ er utstrakt ved bedragerier av privatpersoner. Aktørene forleder fornærmede ved å, for eksempel, si at uautoriserte personer har fått tilgang til deres bankkonto, og at de skal bistå med å rette opp i dette. Deretter manipuleres fornærmede til å gi fra seg kontroll over nettbanken, og aktørene tapper bankkontoen for penger. De fornærmede er ofte personer i aldersgruppen 50–85 år.

Profesjonelle aktører tilbyr hvitvasking for å omgå regelverk

Profesjonelle hvitvaskere tilbyr ekspertise for å omgå regelverk, og omfatter alt fra enkeltaktører til løsere og mer organiserte nettverk. De kriminelle aktørene utarbeider skreddersydde hvitvaskingsoperasjoner, og er sjelden involvert i primærkriminaliteten. Det er ofte tette bånd mellom de profesjonelle aktørene og sentrale aktører i kriminelle miljøer. Bekjentskapet går ofte langt tilbake i tid, og samarbeidet har vart over flere år.

Kriminelle nettverk hvitvasker utbytte fra kriminalitet ved bruk av tilretteleggere som bistår med investering i eiendom og varer med høy verdi. Flere foretak eies også av, eller knyttes til, kriminelle aktører. Disse gir aktørene muligheter til å hvitvaske penger gjennom omsetning, vare- og transaksjonsflyt.

Bruk av såkalte pengemuldyr er et økende problem i Norge. Unge og sårbare personer er blant de som rekrutteres. Disse forledes til å stille kontoen sin til disposisjon og overfører penger for å kamuflere knytningen til den kriminelle aktøren.

3.5. Trusler mot miljø, ressursgrunnlag og dyrevelferd

Med trusler mot ressursgrunnlag og miljø menes kriminalitet som truer natur, dyr, miljø og kulturminner. Dette omfatter for eksempel ulovlig utslipp og avfallshåndtering, ødeleggende inngrep i naturen, forurensning, handel med truede arter, dyrevelferd og ulovlig uttak av verdifulle naturressurser.

Det er et økende omfang av flere former for miljøkriminalitet hvor sakene i seg selv ikke fremstår som alvorlige, men som i sum likevel har store konsekvenser på kort og lang sikt. Miljøkriminalitet går utover fellesskapet, og har ofte ikke en tydelig fornærmet.

Forsettlig og systematisk avfallskriminalitet er økonomisk motivert

Ulovlig avfallshåndtering representerer en kompleks og økende trussel. Ifølge Europol er dokumentforfalskning et sentralt virkemiddel for kriminelle nettverk som er involvert i avfallskriminalitet i Europa. Forfalskede dokumenter, tillatelser og analyseresultater benyttes for å skjule det reelle innholdet i forsendelser, og for å omgå tollkontroll ved grensepasseringer. Kriminaliteten er grensekryssende når avfall blir sendt ulovlig til land med lavere krav til avfallshåndtering.

Avfallsmengden fra norske husholdninger er stor. Når større mengder avfall blir håndtert i strid med lovverket, saboterer det for gjenvinningstiltak og

⁸ Spoofing innebærer at bedragerne kan sørge for at den som blir oppringt ser det nummeret angriper ønsker.

virker konkurransevridende. Avfallskriminalitet er økonomisk motivert, forsettlig og systematisk, og kan pågå over lang tid før skaden eller forurensningen materialiserer seg. Når forurensningen først avdekkes, kan den allerede ha forårsaket konsekvenser for mennesker og omkringliggende natur og dyreliv.

Norske virksomheter står ansvarlig for forurensning og ulovlig deponering av avfall. Deponeringen foregår på land og i vann, for eksempel i forbindelse med byggevirksomhet eller produksjon, og kan generere betydelig økonomisk gevinst.

Ulovlig eksport av elektrisk eller elektronisk avfall

Elektronikk inneholder tungmetaller og organiske miljøgifter som kan være svært forurensende og helseskadelige. Det er et stort miljøproblem at EE-avfall eksporteres ulovlig til land som mangler regelverk, myndigheter og en fungerende avfallsbransje som kan håndtere avfallet forsvarlig. Nordmenn er i verdenstoppen når det gjelder forbruk av elektriske eller elektroniske produkter (EE). Det tilrettelegger for tyveri og ulovlig eksport av EE-avfall. Slik kriminalitet øker i Norge og begås av både enkeltaktører og nettverk som motiveres av høy fortjeneste og lav oppdagelsesrisiko. Aktører driver til dels organisert virksomhet med tyveri av avfall fra EE-forhandlere, og avfallet eksporteres til land med lite utviklet avfallshåndtering.

Uopprettelige inngrep i naturområder

Kriminalitet som truer ressursgrunnlag kan omfatte ulovlig uttak av naturressurser, utslipp av skadelig væske eller gass til luft, vann eller grunn samt ødeleggende aktivitet i sårbart terreng. Kriminaliteten rammer bredt. Konsekvensene er ofte ikke synlige før lenge etter at overtredelsen fant sted, og kan da være uopprettelige.

Næringslivsaktører, grunneiere og kommuner begår ulovlige terrenginngrep i sårbare naturområder i Norge. Slike inngrep, i form av fjerning av vegetasjon, utfylling av masser og etablering av konstruksjoner, forringer naturen og er blant de alvorligste truslene mot miljø og ressursgrunnlag. Nylige straffesaker favner mange ulike, og i noen tilfeller svært grove, overtredelser av regelverket.

Ulovlig motorferdsel i utmark setter menneskeliv og natur i fare

Motorferdsel i utmark er forbudt, med enkelte unntak, som for eksempel nytteferdsel eller ferdsl i merkede løyper. Utmarkskjøring og barmarkskjøring kan gi store skader på natur samt forstyrre dyre- og fugleliv. I ytterste konsekvens har denne typen aktivitet også ført til skader og dødsfall, som følge av ferdsl med snøskuter og andre terrengkjøretøy.

Ulovlig organisert jakt på truede arter

Sårbare naturområder og dyrearter utsettes for økt press fra flere hold, og en vedvarende trussel er ulovlig jakt. Ulovlig jakt på sterkt truede arter som bjørn, jerv, gaupe og ulv er alvorlig, da det kan sette artens overlevelsessevne i fare. Jakten foregår primært i rurale områder, noe som reduserer oppdagelsesrisikoen. Jakten involverer brutale fellingsmetoder og utsetter dyrene for store lidelser.

Dyrevelferd

Det er årlig flere tilfeller av dyretragedier der produksjonsdyr vanskjøttes og utsettes for langvarige lidelser, slik at de dør eller må avlives. Dyreholdet kan bestå av flere hundre produksjonsdyr. Felles for flere av aktørene er at de har helseutfordringer og funksjonssvikt grunnet rusavhengighet, alder, psykiske lidelser eller annen sykdom.

Politiet mottar også informasjon om, og anmeldelser av, vold og mishandling av kjæledyr over hele landet.

Ulovlig innførsel av dyr kan bringe med seg smitte. Dette kan være en alvorlig fare for mennesker og natur. I Norge har prisen for hunder økt betydelig de senere år, og dette kan være en driver for ulovlig innførsel.

3.6. Trusler mot IKT-sikkerhet og digital infrastruktur

Med trusler mot IKT-sikkerhet og digital infrastruktur menes kriminalitet mot datasystemer, som datainnbrudd, datatyveri og løsepengevirus. Slik kriminalitet begås først og fremst for økonomisk vinning, men også for å skade maskinvare eller digitale tjenester, eller for å få urettmessig tilgang til sensitiv eller annen informasjon.

Trusselbildet i det digitale rom blir stadig mer komplekst. Koronapandemien var med på å øke digitaliseringen av det norske samfunnet. Den pågående russiske krigføringen i Ukraina har ytterligere forsterket og komplisert trusselbildet i det digitale rom, og gitt vinningskriminelle og andre kriminelle trusselaktører større handlingsrom. Landegrenser har ingen begrensende innvirkning på utøvelsen av kriminaliteten. Aktørene spenner fra opportunister og småkriminelle til organiserte kriminelle og statlige aktører.

Flere aktører har blitt dyktige til å skjule egne digitale spor, blant annet ved å kryptere data og å benytte anonymiseringstjenester. Dette vanskeliggjør avdekking og etterforskning av den kriminelle aktiviteten og identifisering av de som utfører den.

Skillene mellom mandatene til henholdsvis politiet, Politiets sikkerhetstjeneste, Etterretningstjenesten og Nasjonal sikkerhetsmyndighet utfordres av glidende overganger mellom statlige aktører og kriminelle nettverk i det digitale rom. Kriminelle nettverk kan operere på vegne av, eller med varierende grad av støtte eller tillatelse fra, statlige aktører. Krigen i Ukraina har ytterligere aktualisert dette ved at aktører innen kriminalitet mot datasystemer tar side i konflikten. Skadevare, metoder og sårbarheter som utvikles og utnyttes av statlige aktører, blir også tatt i bruk av kriminelle når de blir kjent.

Sosial manipulasjon er sentralt

Sosial manipulasjon av mennesker utnytter menneskelig kontakt og sosiale mekanismer for å tilegne seg uberettiget informasjon. Phishing er en form for sosial manipulasjon hvor mottakere av elektronisk kommunikasjon blir lurt til å installere skadevare eller oppgi sensitive opplysninger, som for eksempel brukernavn og passord. Dette er en av de vanligste inngangsvektorene kriminelle aktører bruker for å få urettmessig tilgang til datasystemer. De siste årene har denne aktiviteten blitt stadig mer målrettet, og omtales da som spearphishing. Spearphishing er vanskeligere for mottaker å avdekke fordi den er spesialtilpasset den personen eller virksomheten aktøren ønsker tilgang til. Aktørene som bruker sosial manipulasjon, prøver også tilnærminger hvor de sender ut et stort antall e-poster hvor tematikken er generisk. Disse aktørene ønsker å nå bredt ut, i håp om at enkeltmottakere vil la seg forlede til å gi fra seg informasjon.

Sosial manipulasjon utføres også gjennom tekstmeldinger (smishing) og telefonsamtaler eller taletjenester (vishing). Formålet med disse metodene for sosial manipulasjon er de samme som ved phishing og spearphishing.

Datainnbrudd som forutsetning for annen kriminalitet mot datasystemer

Datainnbrudd er både et lovbrudd i seg selv og en sentral aktivitet i utøvelsen av annen alvorlig kriminalitet. Konsekvensene og alvorligheten av innbruddet vil avhenge av aktørenes intensjon og verdiene som trues. Løsepengevirus er skadevare som blir benyttet til å kryptere filer slik at de blir utilgjengelige for de rettmessige brukerne, med mindre de betaler løsepenger. Løsepengevirus kan føre til store tap og kostnader for å gjenopprette driften. Datainnbrudd med andre formål kan også medføre store økonomiske tap og gjøre at sensitiv informasjon kommer på avveie, for eksempel som ledd i industrispionasje eller sabotasje. Handlemåtene varierer fra enkle og lett tilgjengelige metoder til sofistikerte metoder som krever spesialkompetanse.

Flere norske offentlige og private virksomheter ble utsatt for datainnbrudd og datainnbrudd med løsepengevirus i 2022. Konsekvensene har vært til dels alvorlige, med potensielt store mengder personopplysninger på avveie.

Utnyttelse av sårbarheter i programvare – Log4shell

En kritisk sårbarhet i det Java-baserte loggverktøyet Log4j fra Apache Software Foundation ble offentlig kjent 9. desember 2021. Programvaren benyttes av mange programvareselskap og netjtjenester. Sårbarheten kan gi trusselaktører full tilgang til datasystemene til både bedrifter og privatpersoner. Sårbarheten er kjent som Log4shell.

I 2022 ble Log4shell-sårbarheten utnyttet for å få tilgang til datasystemer hos flere norske bedrifter og virksomheter. På tross av oppdatering av systemer, så kan trusselaktører fortsatt benytte seg av Log4shell hvis aktøren allerede har etablert et fotfeste innenfor et

nettverk. Det rapporteres fortsatt om skanning fra trusselaktører etter Log4shell-sårbarheten over hele verden. Det er i tillegg rapportert om sårbarheter med lignende egenskaper som Log4shell i 2022, som aktivt blir forsøkt utnyttet av trusselaktører. Det foreligger informasjon om at Log4shell ble brukt til å installere såkalte kryptominere⁹ i systemene til bedrifter i Norge.

Kriminelle tjenester øker mengden kriminalitet mot datasystemer

Alle former for cyberkriminelle verktøy og tjenester kan kjøpes på det åpne eller det mørke nettet. Slike verktøy og tjenester øker kapabiliteten til uerfarne og mindre sofistikerte aktører, og fører til mer kriminalitet mot datasystemer. Man kan for eksempel bestille et tjenestenektangrep som noen andre gjennomfører, eller kjøpe tilgang til skadevare for å selv gjennomføre phishing eller et datainnbrudd. Erfarne og sofistikerte kriminelle aktører tilbyr også opplæring i cyberkriminalitet. Noen kriminelle aktører selger løsepengevirus og tilgang til kompromitterte bedriftsnettverk til mindre kompetente aktører, som så gjennomfører utpressingen. Andre kriminelle hvitvasker løsepengene gjennom mange ledd av vekslertjenester, noe som ytterligere vanskeliggjør straffeforfølgelse.

Tjenestenektangrep mot bedrifter og virksomheter forekommer ofte

Tjenestenektangrep har som formål å forhindre eller forringe tilgangen til en tjener, tjeneste eller et nettverk. Aktørene utnytter nettverk av allerede kompromitterte datamaskiner og andre enheter som en desentralisert ressurs til å overvelde målet med nettverkstrafikk. Tilgang til slike allerede kompromitterte nettverk selges gjerne av aktører med ekspertkompetanse som en tjeneste til mindre sofistikerte aktører.

⁹ Kryptominere brukes til å utvinne kryptovaluta ved å bruke datakraften til en datamaskin.

Tjenestenektangrep er et enkelt og lett tilgjengelig angrepsmiddel. Middelet benyttes av et bredt spekter av aktører, som kan være både økonomisk og politisk motiverte. Sistnevnte kalles ofte hacktivist.

Tjenestenektangrep skjer hele tiden. De aller fleste tjenestenektangrep i Norge blir avverget av automatiserte sikkerhetsløsninger. Etter et tjenestenektangrep vil de aller fleste tjenere, tjenester og nettverk driftes som normalt, uten behov for videre tiltak. Internasjonalt har tjenestenektangrep blant annet vært rettet mot børser, regjeringer, politi, valg, flyplasser og helseinstitusjoner.

Kriminelle aktører som støtter Russland har utført tjenestenektangrep mot både statlige og private institusjoner i forskjellige europeiske land. Disse gruppene er hovedsakelig profittmotiverte, og er en vedvarende trussel mot virksomheter globalt. Disse gruppene retter tjenestenektangrep mot virksomheter, ofte etterfulgt av utpressing. I mange av disse tilfellene har ofrene i forkant mottatt e-post fra gjerningspersonene med et økonomisk krav og trussel om nye og større tjenestenektangrep dersom ikke kravet betales. De økonomiske kravene har variert fra små summer til flere millioner norske kroner. Aktørene krever betaling i kryptovaluta.

I juni 2022 ble en rekke norske nettstedene utsatt for tjenestenektangrep fra den cyberkriminelle grupperingen Killnet. Natt til 29. juni 2022 la grupperingen ut en liste med norske mål som utover dagen ble angrepet. Målene var blant annet nettsidene til politiet, UDI, BankID og NAV. Flere av nettsidene ble ustabile eller sluttet helt å svare i kortere perioder. Angrepene hadde totalt sett liten effekt. Åpne kilder tilsier at motivasjonen for angrepet på generell basis skyldtes Norges støtte til Ukraina og et norsk nei til transport av varer over Storskog for videre frakt til Svalbard.

I dagene etter angrepet la tilsvarende russiskvennlige grupperinger ut lister med flere mål. Killnet er en av flere cyberkriminelle grupperinger som siden Russlands invasjon har stått bak tjenestenektangrep mot land som støtter Ukraina. Gruppen legger ut målene for angrep på sin Telegram-kanal og ber følgerne angripe målene. Killnet er en av flere grupper som begår hacktivism, og tjenestenektangrep er ofte brukt som metode.

Et mål ved tjenestenektangrep, som beskrevet over, kan være å skremme, skape splid eller øke bekymring i samfunnet. Dette kan forsterkes av medias dekning av slike typer hendelser, som i enkelte tilfeller i 2022 beskrev tjenestenektangrep som mer omfattende og alvorlig enn de var. I ytterste konsekvens kan tjenestenektangrep derfor medføre at samfunnet får svekket tillit til statens evne til å beskytte borgerne.

Lekkasjer gir innblikk i cyberkriminelles organisering

Russlands krig mot Ukraina har skapt ringvirkninger globalt, også i det digitale rom. En av disse ringvirkningene er en informasjonslekkasje assosiert med det kriminelle nettverket knyttet til løsepengeviruset Conti. Åpne kilder indikerer at lekkasjen har funnet sted på grunn av interne uenigheter om gruppens støtte til Russlands krigføring i Ukraina. Informasjonen er lekket i flere faser, og inneholder blant annet interne chatter som avslører gruppens indre liv. Dette er blant annet internstyring, informasjon om vellykkede datainnbrudd og kode til skadevare. Med bakgrunn i lekkede chatter har nøkkelmedlemmer og deres funksjon i organisasjonen blitt kartlagt. Medlemmene innehar definerte roller innen logistikk, rekruttering og utvikling av teknikker brukt i deres kriminelle virksomhet.

3.7. Trusler mot grensesikkerhet og indre sikkerhet

Med trusler mot grensesikkerhet og indre sikkerhet menes kriminalitet som truer indre og ytre Schengen-grenser og tryggheten på territoriet. Dette omfatter blant annet ID-misbruk og grenserelatert kriminalitet, som smugling av varer og migranter, i tillegg til ulovlige grensepasseringer, misbruk av legale migrasjonskanaler og ulovlig opphold.

Økt migrasjonspress og asylankomster til Norge og Europa

Det siste året har migrasjon og den grensekryssende kriminaliteten vært preget av grensekontroll og reiserestriksjoner som følge av koronapandemien. Videre har konflikter og sosioøkonomiske utfordringer i tredjeland og i enkelte land i Europa – i kombinasjon med økt mobilitet – ført til økt migrasjonspress mot Europa og Norge. Antallet ulovlige grensepasseringer i EU+¹⁰ har økt i 2022 sammenlignet med de tre siste årene, og er nå høyere enn i 2019, som regnes som forrige normalår før koronapandemien. Videre er antallet asylsøknader på et høyt nivå.

Til tross for lavere mobilitet i deler av perioden, som følge av koronarestriksjoner, har menneskesmuglingsnettverk opprettholdt sin kapabilitet og etablert nye ruter gjennom pandemien. Den kommersielle trafikken har gradvis tatt seg opp. Flytrafikken til Norge er økende og på tilnærmet samme nivå som før koronapandemien.

I 2022 har over 35 000 ukrainere søkt om beskyttelse i Norge. Majoriteten av disse har søkt om kollektiv beskyttelse. Noen av disse har ankommet over Storskog, men antallet over Storskog er lavt sammenlignet med det totale antallet.

Asylankomstene til Norge har økt og er på et høyere nivå enn i 2019. Syrere og afghanere utgjør fortsatt majoriteten av nye asylsøkere til Norge. De mest fremtredende endringene er økningen i antallet enslige mindreårige asylsøkere, særlig fra Afghanistan, og økningen av asylsøkere fra Latin-Amerika.

Aktører i Norge deltar i menneskesmugling

Majoriteten av migranter som reiser irregulært til EU+ har benyttet seg av smuglertjenester tilbudt av kriminelle nettverk på én eller flere etapper av reisen. Europol vurderer menneskesmugling blant de mest alvorlige kriminalitetstruslene. Videre viser Europol til at menneskesmugling er en sentral aktivitet for kriminelle aktører, og de forventer at etterspørselen av smuglertjenester til Europa vil øke.

I Europa og tredjeland utviser nettverkene stor intensjon og kapabilitet til å gjennomføre menneskesmuglingen, blant annet ved å frakte migranter i overfylte båter, lastebiler eller andre fremkomstmidler som ikke er egnet for persontransport. Dette kan potensielt sette sårbare mennesker i livsfare, krenke personlig integritet og true menneskeverdet.

Menneskesmuglingsnettverkene utgjør en trussel mot samfunnsstrukturer. Gjennom å smugle migranter til Norge, bidrar også de norske aktørene til å legge til rette for ulovlig innreise og sekundærbevegelser i EU+. Dette utgjør en trussel mot grensesikkerheten til både Norge og EU+. Menneskesmuglingsaktører utviser høy grad av tilpasningsdyktighet for å omgå kontrolltiltak. En viktig motivasjon er profitt. Det utvises kynisme ved å tjene penger på andres nød.

Økning i avdekket misbruk av ID-dokumenter

ID-misbruk muliggjør ulike typer grensekryssende kriminalitet, lik som menneskesmugling og

¹⁰ EU+ inkluderer EU- og Schengen-landene.

menneskehandel, samt smugling av narkotika, våpen og stjålne kjøretøy. Ifølge Europol tilrettelegger ID-misbruk for økonomisk kriminalitet, ulovlig handel med kunst- og kulturminner, vinningskriminalitet og terrorisme.

Det har vært en økning i avdekket misbruk av ID-dokumenter, sammenlignet med samme tid i fjor. Hovedvekten er totalforfalskede eller forfalskede dokumenter. Økningen var forventet, ettersom misbruk av ID-dokumenter har vært sterkt påvirket av reiserestriksjoner. Avdekket dokumentmisbruk blant såkalte impostere har gått ned. Dette er personer som utgir seg for å være noen andre, eksempelvis ved å benytte identitetsdokumenter som tilhører andre. Andelen dokumenter misbrukt av impostere sammenlignet med falske/forfalskede dokumenter er lavere i Norge enn det som rapporteres i Europa.

Krigen i Ukraina har skapt et handlingsrom for både ID-misbruk og misbruk av legale ordninger som ikke har eksistert tidligere. Det er avdekket

forsøk på å utnytte ordningen med kollektiv beskyttelse, og det har vært en økning i bruken av uriktige ukrainske ID-dokumenter i EU+ som følge av krigen. Dette inkluderer ekte dokumenter utstedt på uriktig grunnlag, falske og forfalskede dokumenter, og dokumenter misbrukt av impostere.

Misbruk av asylinstituttet og andre legale migrasjonskanaler forekommer i stort omfang blant flere grupper. Det har vært en økning i antallet migranter som har misbrukt visumordningen ved å søke om asyl. Det er også avdekket flere tilfeller av forsøk på å tilegne seg visum, arbeidstillatelse eller oppholdstillatelse på uriktig grunnlag. I tillegg avdekkes det fortsatt at oppholdstillatelser og statsborgerskap er blitt innvilget på uriktig grunnlag og uriktig identitet.

Politiets trusselvurdering 2023

Utgitt: 2023

Utgiver: KRIPOS

Forsidebilde: Shutterstock.com