POLITIET
KRIPOS

Cyberkriminalitet 2024

Politiets årlige rapport om cyberrettet
og cyberstøttet kriminalitet

Cyberkriminalitet 2024, Kripos
Politiets årlige rapport om cyberrettet og cyberstøttet kriminalitet

Grafisk formgivning: Økokrim
Opplag og trykk: 400x, Aksell

Foto: Shutterstock

Forord

Trusselbildet i det digitale rom blir stadig mer komplekst. Økt samarbeid, spesialisering og kommersialiseringen av kriminaliteten, sammen med teknologisk utvikling, driver cyberkriminaliteten fremover.

Omfanget av kriminaliteten er stort. Norske virksomheter er attraktive mål for kriminelle. Samtidig rammer også cyberkriminaliteten enkeltpersoner. Truslene vi står overfor er sammensatte, og verktøyene og virkemidlene som rettes mot oss er i stadig utvikling. Kriminaliteten har i 2023 hatt stor geografisk spredning og rammet bredt.

Informasjonens allsidige bruksområde utvider de cyberkriminelles handlingsrom, og øker samtidig sannsynligheten for å oppnå de kriminelle målene. Mengden stjålne påloggingsdetaljer og data fra kompromitterte brukerkontoer økte det foregående året på kriminelle markedsplasser, og illustrerte nettopp informasjonens verdi i cyberkriminaliteten.

Cyberkriminalitet handler om gjerningspersoner med kriminelle motiv og global rekkevidde, med vilje og evne til utføre et bredt spekter av lovbrudd. Denne viljen og evnen må møtes med samlet motkraft fra det private og offentlige Norge.

Cyberkriminalitet 2024 er et nasjonalt situasjonsbilde for cyberkriminalitet, utarbeidet av Kripos, på oppdrag fra Politidirektoratet (POD). Dette er den andre årlige strategiske etterretningsrapporten om cyberkriminalitet som Kripos har offentliggjort.

Kripos ønsker med denne rapporten å bidra med vår kunnskap om cyberkriminaliteten, dens målrettethet og natur, og med begrepsapparatet vi benytter i vårt arbeid.

Kristin Kvigne
Sjef Kripos

Foto: Shutterstock

Innhold

Rapportens formål og oppbygging 8
Trussellandskapet 2023 10
- Cyberrettet kriminalitet 12
- Bedrageri 13
- Seksuelt motiv 13
- Politisk motiverte cyberkriminelle 16
- Politiets innsats 16

Cyberkriminalitet 21
Cyberkriminalitetens betingelser 23
- Tverrgående drivere 24
- Aktører 24

Om cyberkriminelle handlemåter 29
- Profittmotivert cyberrettet kriminalitet 29
- Bedrageri 37
- Direkteoverførte bestillingsovergrep 38
- Kryptovaluta 40
- Ende-til-ende-krypterte meldingsplattformer 45

Om digitale sårbarheter 49
- Skytjenester 49
- Nulldagssårbarheter 50
- Den trådløse hverdagen 52

Utviklingstrekk 55
- Leverandørkjedeangrep 55
- Utpressing i det digitale rom 56
- Påvirkningen fra kunstig intelligens 61

Den cyber-fysiske koblingen 69
Ventet utvikling 2024 75
- Trusselen mot samfunnet 75
- Trusselen mot virksomheter 76
- Trusselen mot enkeltpersoner 77

Vedlegg 79
- Sannsynlighetsord 79
- Begreper 79

Sammendrag

Det finnes per i dag ingen etablert universell definisjon av cyberkriminalitet. I rapporten *Cyberkriminalitet 2023*[1] definerte Kripos cyberkriminalitet som helheten av to kriminalitetsområder: Kriminalitet mot datasystemer, og kriminalitet støttet av datasystemer. I denne rapporten erstattes begrepene av henholdsvis cyberrettet og cyberstøttet kriminalitet[2] Meningsinnholdet er uendret.

Cyberkriminaliteten rammer bredt og har i 2023 vært økende i både volum og alvorlighetsgrad, men den nasjonale sikkerhetstenkningen er i ferd med å modnes. Det er tydelig at informasjonens verdi øker i cyberkriminelles øyne.

Både cyberkriminelle og samfunnet som må beskytte seg mot kriminaliteten opplever fortsatt stor utvikling og man ser økt samarbeid, spesialisering og eksistensen av gjensidige avhengigheter i begge grupper. Analyser viser også at begge grupper har de samme rammebetingelser for sin aktivitet i det digitale rom, og at man må benytte de samme verktøy for å oppnå sine mål. For cyberkriminelle er det særlig kommersialiseringen av kriminaliteten, sammen med teknologisk utvikling som underbygger utviklingen innenfor cyberkriminalitet.

En viktig del av samfunnets innsats i bekjempelsen av cyberkriminalitet ligger i å forstyrre kriminaliteten. Rapporten redegjør for politiets innsats i foregående år. Men det er også en erkjennelse av at mange andre aktører, som eksempelvis offentlige og private sikkerhetsorganisasjoner og produktutviklere, bedriver kontinuerlig forstyrring av cyberkriminell aktivitet. Dette har positiv effekt på bekjempelsen av kriminaliteten, men er også en drivkraft for ytterligere kriminell innovasjon. Dette vil være en evig katt-og-mus-lek.

---

1 Rapport: Kripos, Cyberkriminalitet 2023, side 10, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

2 Eng: Cyber-dependent og cyber-enabled crime. Beskrevet i IOCTA 2020, https://www.europol.europa.eu/cms/ sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

Kripos har hatt et særlig fokus på de cyberkriminelle aktørene i året som har gått. Sammenstilt med en trusselpersepsjon som ser på tvers av kriminalitetstyper, har dette resultert i en bedre forståelse som presenteres i denne rapporten. Likheten mellom tradisjonelle hierarkiske organisasjoner og den cyberkriminelle organiseringen er slående. Tilstedeværelsen av både uerfarne og spesialiserte cyberkriminelle bygger opp under den organiserte kriminaliteten, og er i seg selv viktige drivkrefter og danner rekrutteringsgrunnlaget for ny kriminalitet. Selv hos forholdsvis autonome cyberkriminelle, som eksempelvis seksualforbrytere, finnes det avhengigheter. Samtidig fremkommer det at den profesjonelle delen av cyberkriminaliteten består av langt færre aktører enn først antatt.

Den økte innsikten i det cyberkriminelle aktørgalleriet har gitt Kripos flere analytiske verktøy. Disse beskrives i rapporten, både for å skape et omforent terminologisk rammeverk, gi grunnlag for en kunnskapsbasert samfunnsdebatt og for å øke samfunnets motstandsdyktighet.

Rapporten løfter frem de fenomener som Kripos mener har størst betydning for trussellandskapet slik det er i dag og for den forventede utviklingen på mellomlang sikt. Særlig utviklingen innen skytjenester og den trådløse hverdagen, stadig mer komplekse leverandørkjeder, påvirkningen fra kunstig intelligens og cyber-fysiske systemer trekkes frem som fenomener som har avgjørende betydning for situasjonen i det digitale rom, både på taktisk, operasjonelt og strategisk nivå.

Rapporten konkluderer med at den komplekse, globale og sammensatte cyberkriminaliteten best håndteres i fellesskap gjennom samarbeid på tvers og gjensidig informasjonsdeling.

Rapportens formål og oppbygging

Dette er den andre utgivelsen i rekken av årlige strategiske etterretningsrapporter om cyberkriminalitet som blir utgitt av Kripos. Rapportserien skal øke kunnskapsgrunnlaget for hva gjelder hele kriminalitetsfeltet, både cyberrettet og cyberstøttet kriminalitet. Dette gjøres ved å beskrive dagens trusselbilde, cyberkriminalitetens betingelser og bestanddeler, i tillegg til utviklingstrekk. Denne utgivelsen bygger på rapporten *Cyberkriminalitet 2023* ved å videreutvikle begreper og analyseverktøy og oppdatere trusselvurderinger.

Datagrunnlaget for rapporten er i hovedsak fra 2022 og 2023. Norske kilder har blitt prioritert. Politiets straffesaks- og etterretningsregister har blitt benyttet. Datagrunnlaget bygger også på informasjon innhentet gjennom åpne kilder, besvarelser fra utvalgte private og offentlige samarbeidspartnere.

Trussellandskapet 2023 (s. 10) gir et tilbakeblikk på cyberkriminaliteten i året som har gått, sett fra politiets ståsted. Kapittelet fokuserer på sentrale hendelser og statistikk som har hatt en strategisk betydning for utviklingen i trussellandskapet. I kapittelet Cyberkriminalitet (s. 21) presenteres en mer grundig inndeling av begrepsapparatet for hele kriminalitetsfeltet. Redegjørelsen legger vekt på organisert og annen alvorlig kriminalitet og belyser gjennom dette Kripos' mandat i det digitale rom. Cyberkriminalitetens betingelser (s. 23) forklarer cyberkriminalitetens sammensetning gjennom analytiske rammeverk. Kripos benytter seg av rammeverkene til å fortolke og beskrive cyberkriminalitetens fenomener og utviklingstrekk, i tillegg til aktørene som utøver kriminaliteten. Med utgangspunkt i Kripos' observasjoner og erfaringer fra Trussellandskapet 2023, introduserer kapitlene Om cyberkriminelle handlemåter (s. 29) og Om digitale sårbarheter (s. 49) et utvalg fremtredelser i det cyberkriminelle økosystemet. Utvalget gjenspeiler sentrale kriminalitetstyper og nevnverdige

fenomener som er av betydning for året som har gått og Kripos' ventede utvikling i 2024. Disse to kapitlene er ment som oppslagsverk der underkapitlene kan leses adskilt uten videre kontekst eller bakgrunnskunnskaper. Utviklingstrekk (s. 55) beskriver hvordan anvendelse av ny teknologi og cyberkriminelles tilpasning vil kunne få innvirkning på cyberkriminalitetsbildet på kort og mellomlang sikt. Ventet utvikling 2024 (s. 75) oppsummerer strategiske betydninger av trusselbildet, fenomenbeskrivelser og utviklingstrekk for det norske samfunnet, norske virksomheter og norske borgere. Vurderingene kan bidra til beslutningsstøtte og utvikling av mottiltak på ulike sosiologiske nivåer.

I denne rapporten benyttes en rekke kjente begreper som kan ha ulik betydning i andre sammenhenger. For å være tydelige på hvordan Kripos anvender begrepene i rammen av denne utgivelsen, er det utarbeidet en begrepsliste som er vedlagt rapporten. Første gang et av disse begrepene nevnes i teksten er det markert med en nøkkel 🗝 som indikerer at definisjonen er beskrevet bakerst i rapporten.

Trussellandskapet 2023

Det digitale trussellandskapet formes av en rekke forhold som eksisterer i den analoge verden. Interdisiplinære faktorer som jus, økonomi, teknologiutvikling, politikk, samfunnsendringer, enkeltpersoners livssituasjon og forstyrrelser 🗝 spiller inn på hvordan cyberkriminaliteten utvikler seg. Likeså påvirker disse faktorene politiets evne til å oppdage, forebygge, etterforske og iretteføre cyberkriminalitet. Kapittelet redegjør for Kripos' forståelse av trussellandskapet i 2023 gjennom en beskrivelse av betydningsfulle hendelser 🗝 og over ordnet statistikk.

Kripos erfarte en rekke endringer i det cyberkriminelle 🗝 trussellandskapet i 2023. Dette gjaldt særlig innen geopolitikk og teknologi. Kriminaliteten har hatt stor geografisk spredning og har rammet bredt. Kripos ønsker å trekke frem Norges mange små og mellomstore virksomheter som særlig utsatte foregående år. Samtidig har cyberkriminaliteten også rammet enkeltpersoner og større virksomheter, eksempelvis flere kommuner.

Figur 1 illustrerer de observerte utviklingene for de kriminalitetstypene 🗝 som følges av Kripos. Til venstre er cyberrettet kriminalitet, som omfatter datainnbrudd, datatyveri og digitalt skadeverk 🗝. Til høyre er cyberstøttet kriminalitet, bestående av seksuallovbrudd, økonomisk kriminalitet og organisert kriminalitet. For alle praktiske formål er det mulig digitalt å understøtte det meste av kriminalitet, men oversikten avgrenses til organisert kriminalitet og annen alvorlig kriminalitet som seksuallovbrudd. Det overordnede bildet er tilnærmet entydig, ved at det er registrert en økning innen alle områder, med unntak av digitalt skadeverk som holder seg på et stabilt nivå.

Det er imidlertid større usikkerhet knyttet til mengden cyberrettet kriminalitet enn det er til cyberstøttet kriminalitet. En årsak kan være lavere anmeldelsesrate for cyberrettede kriminalitetstyper. En annen årsak kan være at lovbrudd ofte forekommer i kombinasjon, og i slike tilfeller er det som regel den cyberstøttede

Figur 1: Trender for cyberkriminalitet fulgt av Kripos. Illustrasjonen er utviklet av Kripos

kriminaliteten som fremkommer i datagrunnlaget. Når det gjelder seksuallovbrudd mot barn 🗝 på internett 🗝 er det allikevel store mørketall. Kripos er kjent med at mange barn aldri forteller om hva de har blitt utsatt for på internett.

Cyberkriminelle fortsetter å utvikle og tilpasse teknikker, metoder, verktøy og strategier. Dette gjøres for å effektivisere kriminaliteten, forfølge oppdukkende muligheter, øke gevinst 🗝 og omgå mottiltak. Dynamikken i cyberkriminaliteten reflekteres i hvilke typer data som etterspørres og omsettes på meldingstjenester og kriminelle markedsplasser. Bruken av kriminelle markedsplasser understøtter også tidligere vurderinger om at majoriteten av cyberrettet kriminalitet

er opportunistisk og motivert av profitt.

Mye av cyberkriminaliteten har de siste årene beveget seg i retning av økt samarbeid, spesialisering og gjensidige avhengigheter. Dette medvirker til et sterkere sammenkoblet kriminelt økosystem 🗝 som gir rom for at enkeltpersoner med relevant kompetanse og interesse, enklere kan ta del i kriminaliteten. Sammen med begrenset sannsynlighet for straffeforfølgelse gjennom bruk av anonymiseringsteknologier og en desentralisert økonomi, senker dette inngangsbarrieren for å ta del i cyberkriminalitet.

Cyberrettet kriminalitet

I 2023 har datatyveri fortsatt å være en vesentlig trussel for norske virksomheter. Cyberkriminelle nyttiggjorde seg i større grad informasjon i utøvelsen av cyberrettet kriminalitet, eksempelvis ved sosial manipulering 🗝 og aksessetablering, eller i utpressingsøyemed. Informasjonens allsidige bruksområde utvider de cyberkriminelles handlingsrom og øker sannsynligheten for å oppnå de kriminelle målene 🗝.

Internasjonalt er det siden 2022 observert en dobling av datatyveri.

Mengden stjålne påloggingsdetaljer og data fra kompromitterte brukerkontoer økte på kriminelle markedsplasser, og illustrerte nettopp informasjonens verdi i cyberkriminaliteten.[3]

Til tross for at det ofte er krevende å koble stjålet person- eller virksomhetsdata til påfølgende kriminelle handlinger, er det noen eksempler på dette i Norge. I 2023 ble flere kommuner i Finnmark rammet av datainnbrudd. Innbruddene ble utført med en kompromittert brukerkonto hos en tjenesteleverandør. Etterforskning viste at påloggingsinformasjonen tidligere hadde ligget til salgs på en kriminell markedsplass.

Internasjonal statistikk viser at rundt 1/5 av all cyberrettet kriminalitet starter hos en tredjepartsleverandør 🗝 I perioden 2022-2023 var offentlige virksomheter og digitale tjenestetilbydere de mest utsatte sektorene. Ut over datainnbruddene i Finnmark ble det observert ytterligere saker som kan betegnes som leverandørkjedeangrep 🗝 i Norge i 2023.

I 2023 registrerte Kripos en liten nedgang i antallet anmeldte saker med løsepengevirus. Dette til forskjell fra en økning totalt i det internasjonale trussel-

3 Rapport: Europol, IOCTA 2023, https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

landskapet. Til tross for en liten nasjonal nedgang fortsatte løsepengevirus å være en sentral trussel for samfunnssikkerheten med til tider store konsekvenser for norske virksomheter. I noen tilfeller ble tjenestenektangrep brukt som et ledd i utpressingen av fornærmede 🗝, eksempelvis i kombinasjon med løsepengevirusangrep. Kryptering av fornærmedes data forble et viktig verktøy i den cyberkriminelle verktøykassen med flere nye løsepengevirus som kom til i 2023.

Internasjonalt rapporteres det om en økning i løsepengevirusaktører som kun stjeler data til bruk i utpressing fremfor å fullstendig eller delvis kryptere systemer og nettverk. Dette samsvarer med Kripos' observasjon av enkelte cyberkriminelle grupperinger 🗝, samt utbredt bruk av informasjon i kriminalitetsutøvelse. Det ble likevel registrert få eksempler på dette mot norske virksomheter, og kombinasjonen datatyveri og kryptering var fortsatt den primære handlemåten 🗝 i 2023.

Mye av den cyberrettede kriminaliteten i 2023 illustrerer det komplekse aktørgalleriet, og hvordan ett lovbrudd kan være drevet av flere motiv 🗝 og på samme tid ha ulik verdi for flere aktører 🗝. Eksempelvis ble flere norske kommuner utsatt for cyberkriminalitet i 2023, herunder forsøk på eller faktiske datainnbrudd, både med og uten påfølgende kryptering og løsepengevirus. Fordi norske kommuner har ansvaret for- og forvalter informasjon knyttet til blant annet infrastruktur og beredskap, kan slik informasjon også ha stor etterretningsverdi, selv om motivet bak angrepene er ukjent.

Bedrageri

Bedrageriforsøk er blitt en del av hverdagen til mange nordmenn og utgjør i dag et utbredt mengdeproblem i Norge og Europa. Phishing 🗝 ble brukt i en rekke ulike bedragerier, og falske nettsider ble opprettet raskere enn man klarte å ta dem ned. De totale bedrageribeløpene utgjorde milliarder av kroner og antall fornærmede økte. Over én million bedrageriforsøk over telefon ble stanset hver måned. Politiet registrerte tap på 287 millioner kroner tilknyttet nettbank-, investerings- og kjærlighetsbedrageri i 2023.

Seksuelt motiv

Cyberstøttede seksuallovbrudd skiller seg på mange måter fra annen cyberkriminalitet, blant annet ved at seksuell tilfredsstillelse er det dominerende motivet for denne gruppen gjerningspersoner 🗝. Samtidig er også deler av denne kriminaliteten profittdrevet, og seksuallovbrytere utvikler nye teknikker og metoder slik også andre cyberkriminelle gjør.

Norske cyberkriminelle begikk i 2023 en rekke kriminelle handlinger med seksuelt motiv, fra ulike former for befatning med overgrepsmateriale 🗝 til cyberstøttede voldtekter. I 2023 ble 1230 norske gjerningspersoner anmeldt for befatning med overgrepsmateriale. Norsk politi mottok over 13 500 tips om norske gjerningspersoner fra samarbeidspartnere som National Center for Missing and Exploited Children (NCMEC).

I 2023 ble det iverksatt etterforskning mot en mann bosatt i Nordland. Han ble siktet for seksuelle overgrep mot over 250 norske barn i det som blir omtalt som en av Norgeshistoriens største overgrepssaker. Overgrepene skjedde på Omegle[4], og politiet fant skjermopptak av overgrepene på mannens digitale enheter. Arbeidet med å identifisere fornærmede pågikk fremdeles ved utgangen av året. De hittil identifiserte barna var mellom syv og tretten år gamle på gjerningstidspunktet.

I november ble Omegle lagt ned uten forvarsel. Plattformens grunnlegger erklærte i et åpent brev på internett at Omegle var blitt brukt til kriminelle handlinger, men at plattformen også hadde møtt kritikk og motstand, i en slik grad at det ikke lenger var mulig å opprettholde driften av nettstedet. Det eksisterer fremdeles en rekke plattformer som ligner Omegle, men de har hittil ikke vært like hyppig forbundet med seksuallovbrudd i Norge.

I 2023 var et vanlig virkemiddel i gjerningspersoners kontaktetablering med barn på internett å utgi seg for å være yngre enn sin faktiske alder. Andre mye brukte virkemidler var å rose og gi komplimenter, opptre vennskapelig og tillitvekkende, samt å tilby penger eller andre goder, ofte i bytte mot seksuelle tjenester. Flere gjerningspersoner benyttet seg også av andre overtalelsesteknikker. De var pågående og masete eller fremsatte trusler, gjerne for å få barnet til å dele seksualiserte bilder og videoer.

Barn helt ned i elleveårsalderen delte seksualisert materiale 🗝 av andre jevn-

4 Omegle var en amerikansk plattform og nettsted som blant annet var forbundet med digital blotting og seksuell utnyttelse av barn på internett. Mange straffesaker med norske fornærmede og gjerningspersoner hadde sitt utspring i plattformen. Plattformen hadde 18-års aldersgrense, men 13-års aldersgrense med samtykke og tilsyn fra foresatte

aldrende barn. I løpet av 2023 så man at materialet som ble delt blant barn i sosiale medier var grovere enn tidligere, i form av flere voldtekts- og samleievideoer. For eksempel ble en video av en gruppevoldtekt av ei norsk jente delt hyppig og blant mange barn i hele landet. Det var både jenter og gutter som delte videoen og delingen foregikk hovedsakelig på Snapchat.

Det ble i 2023 rapportert om flere svært unge gjerningspersoner, både under atten år og under femten år, som begikk seksuallovbrudd. Saker med gjerningspersoner under femten år blir ikke konsekvent anmeldt, og følges ofte opp utenfor straffesakssporet. Det vil derfor være mørketall i denne gruppen. Den største andelen seksuallovbrudd blant unge var cyberstøttede. Gjerningspersonene var i hovedsak gutter. Hovedandelen av de fornærmede var jenter.

De siste årene har det vært en økning i voksne som betaler barn for egenproduserte seksualiserte videoer og bilder. Deling av bilder og videoer skjedde også i 2023 på sosiale medieplattformer, mens det til betaling ofte ble brukt direktebetalingstjenester som Vipps. Selv om det i hovedsak ble utvekslet mediefiler, ble det også avdekket tilfeller der barn direkteoverførte video til gjerningspersonen.

De registrerte cyberkriminelle som kjøpte seksualisert materiale av barn var menn i alle aldre. Lavest rapporterte alder på barn som solgte slikt materiale i 2023 var ti år. Noen menn kjøpte fra flere barn, og noen av barna solgte til et stort antall menn. Beløpene varierte fra ti kroner til flere tusen kroner. De fleste barna som solgte var jenter, men også noen gutter solgte seksualisert materiale.

Kripos registrerte at mange av barna som solgte eller delte egenprodusert seksualisert materiale ikke var utsatt for press, trusler eller manipulasjon. De fleste som faller inn under denne kategorien var motivert av profitt eller anerkjennelse. Noen barn ble utsatt for seksuell utpressing etter å ha solgt nakenbilder og videoer av seg selv. Gjerningspersonene presset barna til å sende mer seksualisert innhold ved å true med å publisere allerede oversendte bilder og videoer offentlig.

Norske gjerningspersoner benyttet kryptovaluta til å kjøpe overgrepsmateriale fra det mørke nettet 🗝, også i 2023. De identifiserte gjerningspersonene var i hovedsak yngre menn med IT-kompetanse. Et fåtall var registrert som gjerningspersoner innenfor seksuallovbrudd fra tidligere. Overgrepsfora på det mørke nettet har i tillegg samlet inn penger til drift av sidene ved bruk av forskjellig

kryptovaluta. Andre aktører har tatt betalt for overgrepsmateriale med en rekke ulike betalingstjenester, blant annet betalingsformidlingstjenester[5],

Politisk motiverte cyberkriminelle

I 2023 har Norge ved flere tilfeller vært et utvalgt mål blant politisk motiverte cyberkriminelle. Ettersom Norge spiller en sentral rolle i støtten til Ukraina, både ved å sende militært utstyr til frontlinjen og gjennom politiske prosesser tilknyttet NATO, har dette bidratt til å sette Norge på kartet for politisk motivert hacktivisme.

Norske virksomheter har gjennom 2023 opplevd nedetid i drift og mistet tilgang til kritisk informasjon som følge av tjenestenektangrep 🗝. Tjenestenektangrep kan få konsekvenser for den enkelte virksomhet i form av tap av omdømme, driftsinntekter og tjenesteleveranse, men politisk påvirkning og innvirkning på samfunnskritiske funksjoner har så langt vært svært begrenset i en norsk sammenheng.

Hacktivisme blir nært assosiert med tjenestenektangrep som modus. På grunn av liten skadeeffekt har trusselen fra hacktivister 🗝 blitt nedvurdert fra et norsk ståsted. Politiet er ikke kjent med tjenestenektangrep i 2023 mot norske virksomheter som har medført særskilt teknisk skade eller langvarige konsekvenser. Enkeltgrupperingers varsling om fremtidige cyberangrep 🗝 som senere viser seg å ikke inntreffe, eller som har forårsaket mindre skade sett opp imot forventninger, er med på å ta ned den oppfattede trusselen i befolkningen, samtidig som det fører til redusert dekning i mediebildet. I likhet med andre cyberkriminelle aktører er heller ikke hacktivister bundet til én handlemåte eller et fast utvalg verktøy. Samtidig er medlemsmassen i hacktivistgrupperinger omskiftelig og deres samlede kapabiliteter 🗝 justeres med intern kompetanseheving, teknologiske fremskritt, tilegnede ressurser og endringer i medlemsmassen.

Politiets innsats

Det er flere aktører og faktorer som spiller en viktig rolle i å forstyrre det cyberkriminelle økosystemet. I dette kapittelet belyses hvordan politiets innsats i det digitale rom har bidratt til å forstyrre de kriminelles virksomhet. I løpet av 2023 har både norsk og utenlandsk politi

5 Eksempelvis Paypal og Western Union

gjennomført flere vellykkede aksjoner 🗝 mot cyberkriminelle nettverk 🗝 og enkeltpersoner. I etterkant av disse aksjonene har politiet observert at cyberkriminaliteten har forflyttet seg videre til andre plattformer og enkeltpersoner som slipper unna dukker opp med nye verktøy og aliaser. Selv om kriminaliteten fortsetter, synliggjør aksjonene politiets innsats i å forstyrre de cyberkriminelles handlingsmønstre og demonstrerer politiets evne til å bekjempe cyberkriminalitet ved bruk av ulike metoder. Dette arbeidet er tidkrevende, det krever internasjonal koordinering og samarbeid med andre offentlige og private virksomheter.

Politiet står i en særegen posisjon når det kommer til å straffeforfølge og iretteføre cyberkriminelle. Dette arbeidet gir politiet unik innsikt i kriminelles planer, intensjoner 🗝 og motivasjoner 🗝, og understøtter etterforskning og utarbeidelse av forebyggende tiltak. Etterforskning viser blant annet at iretteføring av sentrale aktører i cyberkriminelle nettverk har langtrekkende og varig innvirkning på cyberkriminaliteten. Selv om cyberkriminaliteten er sammensatt og kompleks, viser det seg at grunnleggende menneskelige mekanismer også er fellende for cyberkriminelle aktører.

Dette danner grunnlaget for at forebyggende politiarbeid og straffeforfølgelse i det digitale rom 🗝 lyktes med å skape forstyrrelser i det cyberkriminelle økosystemet i 2023. Samtidig som politiet jobber med å håndheve norsk lov i det digitale rom, er forebyggende arbeid rettet mot virksomheters sårbare digitale flater og seksuell utnyttelse av barn på internett en prioritet.

Politiet fjernet overgrepsmateriale fra internett

Kripos utviklet i 2023 en ny metode for effektivt å vanskeliggjøre deling av overgrepsmateriale på både det mørke og det åpne nettet. Store mengder overgrepsmateriale deles via kommersielle One Click Hosting (OCH)-tjenester[6]. Metoden går ut på at Kripos skaffer passord og lenke fra ulike overgrepsfora, laster ned innholdet og verifiserer at det er overgrepsmateriale. OCH-tilbyderen varsles om materialet og bes om å fjerne dette med henvisning til tilbydernes

6 OCH-tjenester gir internettbrukere muligheten til å laste opp en eller flere filer til en fildelingstjeneste, slik at filene kan deles med andre internettbrukere gjennom en lenke

egne retningslinjer.[7] Kripos kontrollerer deretter om tilbyder fjerner materialet og varsler tilbyderens domeneforhandler eller domeneregister dersom det ikke skjer.

Siden løsningen ble tatt i bruk er om lag 20 000 lenker med overgrepsmateriale fjernet fra internett. Så langt er omtrent 90 000 videoer og én million bilder sikret. Kripos ønsker å ta i bruk kunstig intelligens (KI) for å søke opp og identifisere barn i materialet som er sikret. Det vil kunne medføre at barna hjelpes ut av pågående overgrepssituasjoner.

Stadig flere norske tilbydere ønsker å følge utenlandske tilbydere i å samarbeide med politiet om rapportering av seksuell utnyttelse av barn. I 2023 inngikk Telenor et samarbeid med norsk politi om å detektere og rapportere overgrepsmateriale i sin skytjeneste «Min Sky». Telenor informerer i sine brukervilkår om at overgrepsmateriale og annet seksualisert materiale av barn vil bli rapportert til politiet eller andre relevante myndigheter og kontoen til aktuell bruker vil bli avsluttet uten forvarsel.

Hive

Norsk og internasjonalt politi iverksatte en rekke mottiltak mot cyberkriminelle nettverk i 2023. I januar 2023 tok blant annet FBI, US Secret Service og Europol ned Hive-nettverket og -tjenesten, med støtte fra norsk politi. I 2021 og 2022 ble Hive knyttet til flere vellykkede løsepengevirusangrep mot norske virksomheter. Hive var definert som løsepengevirus som handelsvare (se kapittel 6.1). Aksjonen har gitt norsk politi muligheten til å se knytninger mellom cyberkriminelle aktører i Hive og andre løsepengevirusgrupperinger.

«Splashside» av Hive-plattformen etter nedstengningen.

7 https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2023/09/25/ny-kripos-metode---vi-har-fjernet-titusenvis-av-filer-med-overgrepsmateriale/

Ny utvikling i Hydro-saken

2023 ble et godt år for etterforskningen av datainnbruddet som rammet Norsk Hydro i 2019. Som følge av en europeisk arrestordre ble en armensk statsborger, mistenkt for å ha vært en del av den cyberkriminelle grupperingen som rammet Hydro og en rekke andre virksomheter i 2019, pågrepet i Tyskland og senere utlevert til Norge for varetektsfengsling. Kripos mistenker at mannen har hatt en sentral rolle i gruppen.

Mot slutten av året deltok representanter fra Kripos under en planlagt aksjon i Ukraina, hvor også flere personer tilknyttet den samme cyberkriminelle gruppen ble pågrepet. Blant disse var en av gruppens sentrale personer. Målet med den videre etterforskningen er at disse straffeforfølges i Ukraina, Sveits, Frankrike og Norge.[8]

Norsk og ukrainsk politi under aksjon i Ukraina. Foto: Politiet

8 https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2023/11/26/kripos-flere-personer-i-kriminelt-nettverk-pagrepet/

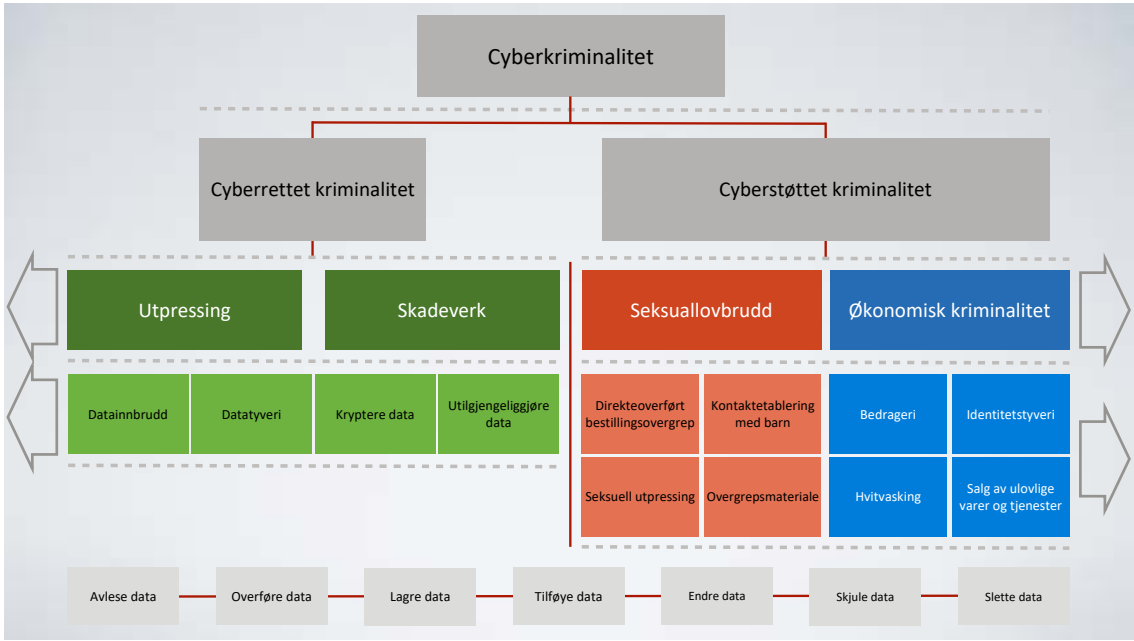
> For å lykkes med varige forstyrrelser i det cyberkriminelle økosystemet er det avgjørende å forstå cyberkriminalitetens byggeklosser og kartlegge aktørene som utøver kriminaliteten.

Foto: Laget med KI

Cyberkriminalitet

Cyberkriminalitet er helheten av kriminalitetsområdene 🗝 cyberrettet og cyberstøttet kriminalitet.

Cyberrettet kriminalitet kan ikke begås utenfor det digitale rom og kriminaliteten rammer IKT[9]-systemer direkte.
I figur 2 fremheves kriminalitetstypene *cyberrettet utpressing* 🗝 og *cyberrettet skadeverk* 🗝, som sammen utgjør den cyberrettede kriminaliteten som omtales i denne rapporten. Flere cyberkriminelle **handlinger** 🗝 kan begås innenfor hver av disse to kriminalitetstypene. Eksempler er datainnbrudd og datatyveri. Ingen av disse handlingene er utelukkende tilknyttet én kriminalitetstype. Kripos har



Figur 2: Cyberkriminalitetens inndeling. Modellen er utviklet av Kripos

9 Informasjons- og kommunikasjonsteknologi

foreløpig ingen utfyllende oversikt over alle kriminalitetstyper og handlinger som kan begås innenfor cyberrettet kriminalitet.

Cyberstøttet kriminalitet er kriminalitet som fantes før det digitale rom oppstod, men som nå også kan støttes av, eller gjøres enklere ved bruk av IKT-systemer. I denne rapporten er det kriminalitetstypene *seksuallovbrudd* og *økonomisk kriminalitet* som blir omtalt. I motsetning til den cyberrettede kriminaliteten der alle handlinger kan understøtte begge kriminalitetstyper, er det særegne handlinger som utføres innenfor hver av disse kriminalitetstypene. Eksempelvis er besittelse av overgrepsmateriale og seksuell utpressing forbeholdt seksuallovbrudd, på samme måte som bedrageri og hvitvasking er forbeholdt lovbrudd innen økonomisk kriminalitet.

Særegent for cyberkriminalitetsfeltet 🗝 er at det eksisterer et begrenset utvalg **aktiviteter** 🗝 som springer ut av et grunnleggende mulighetsrom basert på IKT. Minimum én av disse aktivitetene må utføres for å gjennomføre cyberkriminelle handlinger. Disse aktivitetene er dataavlesing, dataoverføring, datalagring, i tillegg til å tilføye, endre, skjule, ødelegge eller slette data. Kripos er ikke kjent med andre aktiviteter på samme konseptuelle nivå som kan understøtte cyberkriminelle handlinger.

Organisert kriminalitet[10] berører all cyberrettet kriminalitet som omtales i denne rapporten, samt deler av seksuallovbrudd og økonomisk kriminalitet. Det finnes cyberkriminalitet som er verken organisert eller alvorlig, og som ikke er illustrert i modellen. Alle kriminalitetstyper som faller innunder disse to kriminalitetsområdene er således ikke beskrevet i modellen.

10 Straffeloven § 79c. Fastsetting av straff ut over lengstestraffen (flere lovbrudd, gjentakelse, organisert kriminalitet)

Cyberkriminalitetens betingelser

For å lykkes med varige forstyrrelser i det cyberkriminelle økosystemet er det avgjørende å forstå cyberkriminalitetens byggeklosser og kartlegge aktørene som utøver kriminaliteten. Kripos har derfor utviklet analytiske rammeverk som bidrar til å forstå sammenhengene i det uoversiktlige, i tillegg til å identifisere sentrale innsatsområder for forebygging, avverging og etterforskning. Dette

Figur 3: Cyberkriminalitetens elleve drivere. Modellen er utviklet av Kripos.

kapittelet introduserer de gjeldende rammeverkene som benyttes for å forstå cyberkriminalitetens betingelser.

Tverrgående drivere

Det digitale trussellandskapet er både sammensatt og vidstrakt sett fra politiets ståsted. For å forstå trussellandskapet og være i stand til å vurdere sannsynlig fremtid trengs et rammeverk. Første skritt på veien kom i *Cyberkriminalitet 2023*[11], der Kripos presenterte elleve tverrgående drivere for cyberkriminalitet. Det er særlig de tre fundamentale driverne; økonomi og kostnader, lovregulering og teknologiutvikling, som spiller en sentral rolle i å forme endringer i trussellandskapet. Denne rapporten bygger ut det analytiske rammeverket ved å beskrive aktørenes sammensetning.

Aktører

Til tross for et komplekst trussellandskap, fremstår kriminelles motivasjoner som bestandige. Dette introduserer en mulighet til å rydde opp i aktørgalleriet. Med utgangspunkt i antatte motivasjoner kan Kripos skissere fem grunnleggende **roller**:

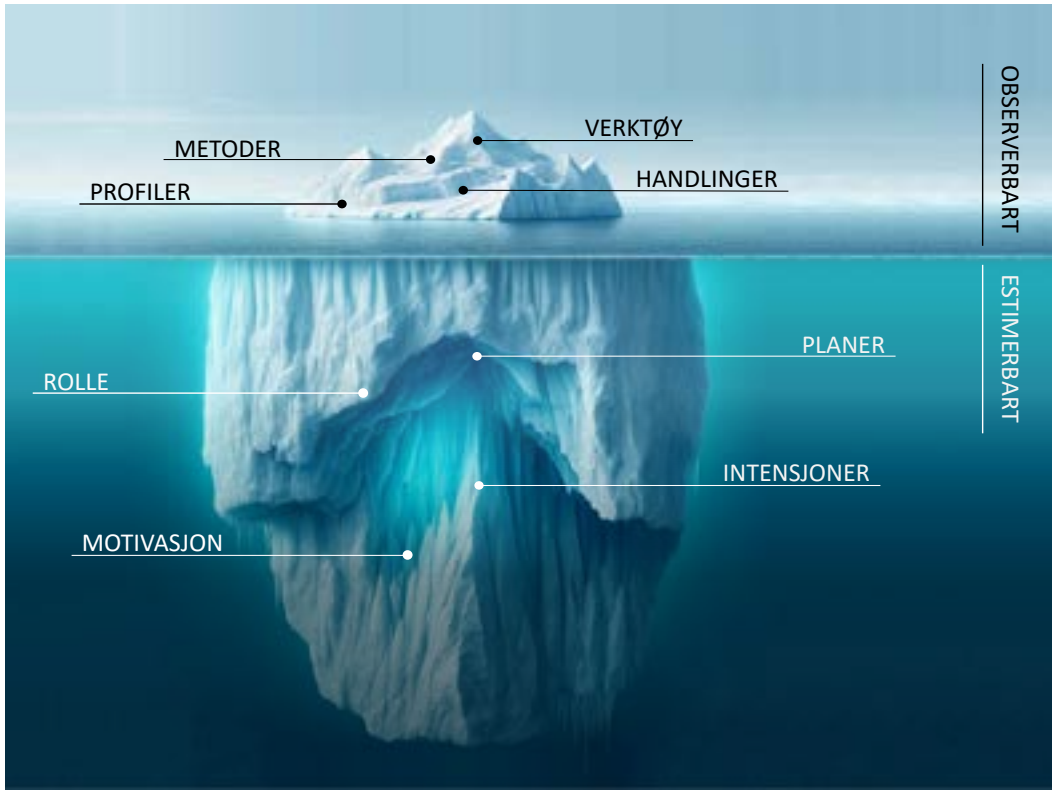
- profittmotiverte kriminelle;
- seksuallovbrytere;
- aktivister;
- statlige aktører; og
- terrorister.

Disse fem rollene representerer et sett med **motivasjoner** og **intensjoner** som er forholdsvis stabile, og som leder ut i mål. Aktørers mål kan være konkrete eller vage, og kan endre seg over tid. Mål omsettes til **planer** som videre utledes i observerbare **handlinger** og aktiviteter. **Metoder** og **verktøy** tilpasses kontinuerlig for å understøtte ulike handlinger utført av en aktør. Aktørers rolletilhørighet er domeneuavhengige[12] og stort sett vedvarende.

Basert på lignende handlemåter kan politiet opprette **profiler** som tilskrives aktører. Forskjellige roller er gjerne forbundet med et utvalg profiler, basert på handlemåter som naturlig understøtter en aktørs intensjon. I motsetning til roller som stort sett er vedvarende, kan profiler enten være skiftende, kortvarige eller uendret. Det betyr at én aktør samtidig kan beskrives med flere ulike profiler. Eksempler på slike profiler kan være

11 Rapport: Kripos, Cyberkriminalitet 2023, side 14, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

12 Her henvises det til det digitale og fysiske domenet



Figur 4: Aktørers sammensetning (teksten er lagt oppå et KI-generert bilde).
Modellen er utviklet av Kripos

skadevareutviklere, informasjonstyver, løsepengevirusgrupperinger, hvitvaskere, svindlere eller selgere av direkteoverførte bestillingsovergrep.

Profilers oppbygging er vesentlig for å forstå cyberkriminalitetens kompleksitet. I tillegg til å stå sentralt i cyberkriminalitetens tjenestemarked, bidrar profilers særegne funksjoner til å balansere det cyberkriminelle økosystemet. Verken roller eller profiler er objektive sannheter om en aktør, men er nyttige merkelapper som kan benyttes for å estimere aktørers underliggende motivasjoner og intensjoner.

Figur 4 illustrerer i hvilken grad de åtte variablene er skjult eller synlig for politiet.

Profilers betydning for det cyberkriminelle økosystemet

Som følge av at kriminelles handlemåter er i konstant endring, er tekniske og taktiske kjennetegn ved ulike aktører også skiftende. Kripos observerer at enkelte aktører bekler én tydelig profil som er forbundet med aktørens antatte rolle. Andre aktører bekler flere profiler forbundet med samme rolle, og noen aktører bekler profiler som er forbundet med ulike roller. Årsaker til sistnevnte kan eksempelvis være flerdelte motivasjoner som følge av geopolitiske forhold, seksuelle preferanser og ønske om økonomisk gevinst, eller personlige relasjoner og overbevisning. En annen årsak kan være aktører med en bevisst strategi om å utføre handlinger som ligger under terskelen for iverksettelse av mottiltak fra offentlige myndigheter. Det er eksempelvis observert, at statlige aktører, direkte og indirekte, benytter seg av cyberkriminelle med ulike roller og profiler, til å gjennomføre handlinger som understøtter egne intensjoner.[13]

Når aktørene avgrenses til det digitale rom, bestående av et felles sett med verktøy og metoder som i utgangspunktet ikke er forbeholdt én enkelt aktør, blir skillelinjene mellom ulike typer cyberkriminelle og statlige aktører ytterligere uklare. Dette til forskjell fra den analoge verdenen der det eksisterer flere identitetsmarkører og tydeligere kjennetegn, som utfordrer operasjonssikkerhet og vanskeliggjør fornektbarhet. I det digitale rom kan kjente teknikker eller metoder som tidligere er benyttet av enkelte, deles med – eller gjenskapes av – noen andre. Dette bidrar til å øke den kollektive cyberkriminelle verktøykassen, og kan føre til økt operasjonssikkerhet og fornektbarhet blant cyberkriminelle og statlige aktører i det digitale rom.

Den mulige tvetydigheten i aktørers bakenforliggende intensjon, aktørenes evne til å operere fordekt og et felles sett med digitale verktøy og aktiviteter, fører til særlige utfordringer når det kommer til etterretning, straffeforfølgning og beviskrav i retten. Uten nødvendig kontekst kan derfor rolleoverskridende handlinger oppfattes som avvik og derigjennom føre til feilaktige tolkninger, hypoteser og vurderinger. For politiet og andre offentlige myndigheter utfordrer dette evnen til å koor-

13 Ofte omtalt som proxy eller stedfortreder

dinere og håndtere cyberkriminalitet i gråsoner 🗝. Spesielt fremtvinger disse utfordringene behovet for økt informasjonsdeling og koordinering på tvers av sektorer og mellom offentlige og private virksomheter.

Samtidig ser Kripos at mange cyberkriminelle med seksuelt motiv fortsatt opptrer alene og i liten grad er avhengig av å samarbeide med andre. Flere aktører i denne gruppen samhandler allikevel med likesinnede, ikke for å benytte seg av andres kompetanse, men heller for å føle tilhørighet og oppnå seksuell tilfredstillelse ved for eksempel å utveksle fantasier. Overordnet er det lite behov for spesialisering og gjensidige avhengigheter for seksuallovbrytere som ønsker å tilfredsstille sine seksuelle behov.

> I likhet med andre cyberkriminelle aktører er heller ikke hacktivister bundet til én handlemåte eller et fast utvalg verktøy.

Foto: Laget med KI

Om cyberkriminelle handlemåter

Et pålitelig beslutningsgrunnlag forutsetter en helhetlig forståelse av trusselen. Både hvordan intensjoner henger sammen med handlinger for ulike roller og profiler, men også hvordan aktører benytter seg av teknologi for å skjule sin identitet, kommunikasjon og pengestrømmer. Det er avgjørende å tegne et tydelig og detaljrikt normalbilde for å oppdage avvik og identifisere indikatorer som kan overvåkes for hurtig reaksjon og varsling. Dette kapittelet beskriver derfor et utvalg cyberkriminelle handlemåter som har hatt betydning for utviklingen av trussellandskapet i 2023 og som Kripos følger med på for å fange opp endringer som har betydning for cyberkriminalitetsutviklingen.

Profittmotivert cyberrettet kriminalitet

Cyberkriminelle aktører har behov for tjenester i form av spesialisert kompetanse, verktøy og infrastruktur, for å drifte sin kriminelle virksomhet. Dette har skapt et eget marked hvor tjenester, tekniske verktøy og digital infrastruktur selges eller leies ut til kriminelle formål. Denne forretningsmodellen omtales som kriminalitet som handelsvare (KSH[14]) og har over tid blitt standarden innen cyberrettet kriminalitet.

Kripos har observert at flere cyberkriminelle aktører med ulike rollebeskrivelser og profiler er gjensidig avhengig av hverandre for å kunne utføre kriminelle handlinger. Profittmotiverte kriminelle utgjør en av de største bestanddelene innenfor det cyberkriminelle økosystemet.

Overordnet kan KSH betegnes som en industri der cyberkriminaliteten

14 Eng: Crime as a Service (CaaS)

kommersialiseres og det oppstår nettverk av kriminelle støttetjenester[15], Kommersialiseringen sprer både verktøy og kompetanse, og tilgjengeliggjør infrastruktur på en slik måte at kriminaliteten blir tilgjengelig for alle som ønsker å ta del i den. Den viktigste årsaksfaktoren for å ta steget inn i den kriminelle verdenen er ikke lenger relatert til kunnskap og ressurser, men primært egen motivasjon og anslått risiko for straffeforfølgelse. I *Cyberkriminalitet 2023*, vurderte Kripos KSH som en selvstendig tverrgående driver, som ville påvirke cyberkriminaliteten på både strategisk, operasjonelt og taktisk nivå (se figur 3 på side 23). Det er sett flere tilfeller av dette i 2023.

Det er observert at nyvinninger, eksempelvis bruk av generativ kunstig intelligens (GKI) til kriminelle formål, raskt kommer ut på det kriminelle markedet. Når cyberkriminelle tar i bruk et nytt verktøy eller tjeneste kan andre raskt følge etter, og slik kan nyvinningen på kort tid få stor innvirkning på cyberkriminelles kapabiliteter. Risikoeier 🗝 som beskytter digitale verdier forsøker å komme opp med mottiltak for å lukke eventuelle sårbarheter som oppstår i kjølvannet av nyvinningen, og dette beskrives gjerne som en katt-og-mus lek.

Flere aktører tilbyr verktøy sammen med opplæring, eller sin ekspertise gjennom leie- eller abonnenttjenester[16] for utførelse av cyberkriminalitet. Komplette manualer for handlinger slik som datainnbrudd, datatyveri og kryptering blir solgt på kriminelle markeder. Det forventes også at GKI vil kunne påvirke utviklingen av skreddersydde manualer på bestilling

Kripos ser en økning av både dekonstruksjon[17] og kopiering, hvor trusselaktører 🗝 gjenbruker verktøy som har vist seg å være effektfulle. En trend er at cyberkriminelle setter sammen nye løsepengevirus ved å bruke fragmenter av flere stjålne eller lekkede kildekoder.[18]

15 Eng: Network of Supporting Services

16 Eng: Subscription Services

17 Er en prosess der man forsøker å forstå hvordan noe er laget og fungerer, uten å ha direkte kjennskap til oppbygning og virkemåte. Kunnskapen skaffes ved hjelp av testing og analyse. Eng: Reverse Engineering. Store Norske Leksikon, https://snl.no/reverse_engineering

18 Eng: Franken-ransomware

Lekkasjen av Conti og LockBit[19] sine kildekoder er eksempler på dette, der kildekodene benyttes av andre for å oppdatere og tilpasse, eller for å lage helt nye skadevarer.

Cyberkriminelle grupperinger

Det mest prominente eksempelet på KSH er løsepengevirus som handelsvare (LSH)[20]. LSH-grupperinger utgjør en betydelig bestanddel innenfor KSH, ettersom det krever differensiert kompetanse, erfaring og ressurser for å utføre et vellykket løsepengevirusangrep. Dette fører til at LSH-grupperinger er blant de mest sentrale komponentene innenfor KSH-industrien.

Kripos har observert at flere cyberkriminelle er involvert i LSH, men at de bidrar i varierende grad og med ulike ferdigheter. Eksempelvis står enkelte for krypteringen av virksomheters systemer, mens andre utvikler selve skadevaren.[21]

Kripos har sett knytninger mellom cyberkriminelle som er involvert i forskjellige løsepengevirus samtidig. LSH-grupperinger og løsepengevirus avvikles og nye dukker opp. Det er observert at de samme cyberkriminelle aktørene veksler mellom nye og etablerte grupperinger. I flere tilfeller er det de samme cyberkriminelle som går igjen på tvers av straffesaker. Ut ifra dette har Kripos anslått at det er færre sentrale cyberkriminelle i LSH-nettverkene enn tidligere antatt.

Cyberkriminelle har benyttet seg av, og har tilgang på flere løsepengevirusvarianter gjennom LSH-nettverk. Samme infrastruktur, eksempelvis i form av servere som brukes til lagring av data og til å angripe virksomheter, brukes av flere aktører.

Muligheter for profitt i cyberrettede kriminelle handlinger

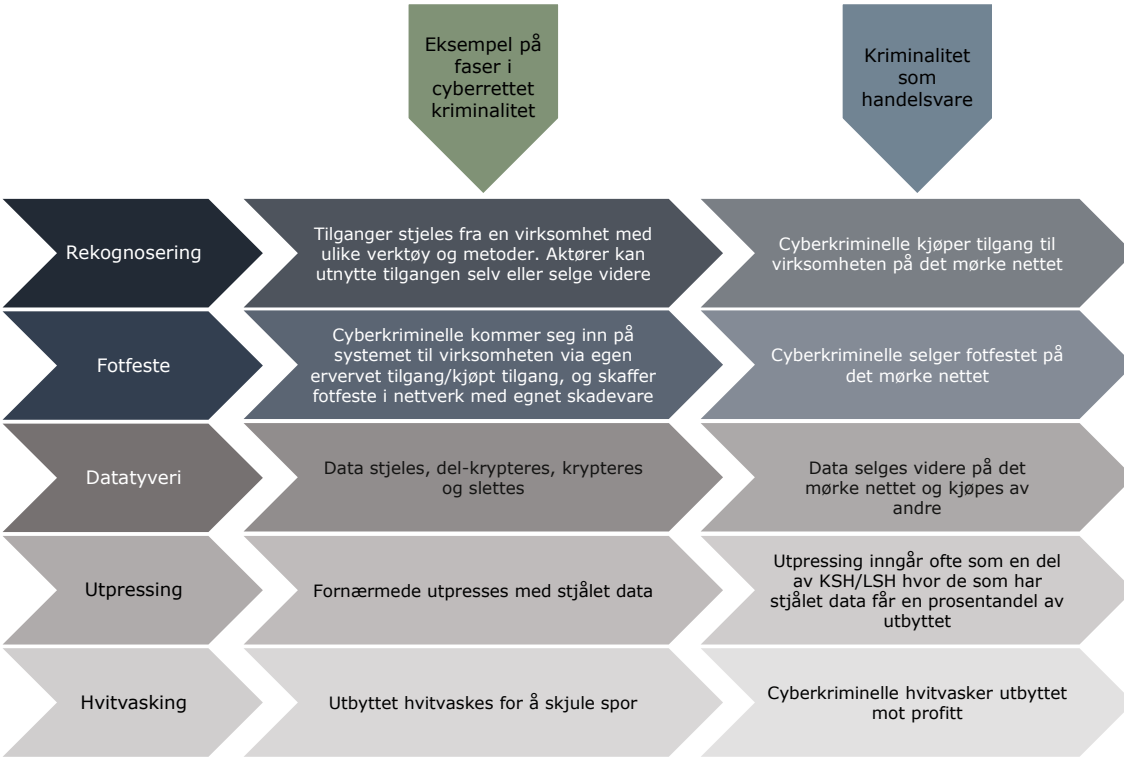
Cyberkriminelle som utfører cyberrettet kriminalitet er særlig tjent med kriminelle tjenester som selges som en handelsvare. Årsaker til dette er kriminalitetens kompleksitet, kompetansekrav og sammensatte angrepskjede 🗝.

Prosessen med å bryte seg inn og påvirke et datasystem 🗝 består av flere ulike kriminelle handlinger, inndelt i faser med innbyrdes avhengigheter. Et datatyp-

19 To kjente LSH-grupperinger som har rammet norske virksomheter

20 Eng: Ransomware-as-a-Service (RaaS)

21 Rapport: Kripos, Cyberkriminalitet 2023, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf



Figur 5: Eksempel på et utvalg faser i cyberrettet kriminalitet og muligheten for profitt gjennom hele prosessen. Modellen er utviklet av Kripos med inspirasjon fra Cyber Kill Chain®

veri er eksempelvis avhengig av erververvelse av tilgang til et datasystem, noe som kan skaffes på ulike måter. I neste steg benytter profesjonelle aktører seg av stjålet data til utpressing av fornærmede, hvor motivet er profitt. Figur 5 illustrerer denne sammenhengen. Alle fasene kan i større eller mindre grad kjøpes eller leies innenfor kriminalitet som handelsvare. Slik kan utøveren av løsepengevirusangrep velge å kun stå for koordineringen og organiseringen av selve angrepet, og heller benytte kriminalitet som handelsvare for de nødvendige fasene. Det finnes også cyberkriminelle som tilbyr å koordinere og organisere alle fasene i angrepskjeden. Cyberkriminelle som ønsker å gjennomføre løsepengevirusangrep kan i teorien kun involvere seg i oppdragsbeskrivelsen og finansieringen av de kriminelle handlingene.

Rekruttering og seleksjon

På grunn av gjensidige behov, cyberkriminalitetens flyktighet og mulighetene som KSH gir, består det cyberkriminelle

Figur 6: De ulike kategoriene i nettverket, hvor det er glidende overganger mellom kompetanse, handlinger og tjenester som tilbys. Modellen er utviklet av Kripos

økosystemet av flere nettverk. Profittmotiverte kriminelle og andre aktører samarbeider både direkte og indirekte i det cyberkriminelle økosystemet.

Kripos har gjennom 2023 erfart at noen av disse nettverkene har spesifikke organiseringsmønstre og er hierarkisk styrte. Dette er ikke nødvendigvis standarden, men det er paralleller på tvers av grupperingene som driver med cyberrettet kriminalitet.

Basert på observasjonene deler Kripos aktørene i dette nettverket inn i tre ulike kategorier basert på erfaring og kompetanse: uerfarne, spesialiserte og organiserte cyberkriminelle.

Rekruttering til cyberkriminalitet og seleksjon av ønsket personell skjer til alle disse tre kategoriene. Kripos observerer at kategoriene blant annet er avgjørende for hvilken grad av innflytelse og goder den cyberkriminelle får tilbud om. Cyberkriminelles kategoritilhørighet er ikke nødvendigvis konstant og de kan bevege seg mellom de tre kategoriene. Motivet kan være ulikt for de ulike kategoriene,

men flerparten av aktørene er motivert av økonomisk gevinst.

Uerfarne cyberkriminelle

Det er i utgangspunktet enkelt for cyberkriminelle å benytte seg av deler av KSH-markedet, hvilket gjør forretningsmodellen tilgjengelig for langt flere aktører, også de som ikke innehar særskilt teknisk kompetanse. I kategorien uerfarne cyberkriminelle finnes blant annet innsideren 🗝 og «gutteromshackeren». Den uerfarne cyberkriminelle har ikke nødvendigvis god teknisk kompetanse fra før, men har tilstrekkelig motiv og mulighet til å begå cyberkriminalitet. Gutteromshackeren har gjerne grunnleggende tekniske ferdigheter som trengs for å tilegne seg ny og relevant kunnskap, men også tilstrekkelig interesse for å søke etter tilgjengelig kildekode, oppskrifter eller manualer. Innsideren har en allerede etablert tilgang som eksempelvis kan misbrukes til å skade organisasjonen eller tilegne seg en gevinst.

Kripos har observert at enkeltpersoner som ikke har cyberkriminell erfaring benytter eksisterende programvare tilgjengelig på internett til å utføre sitt første dataangrep. Gjerningspersonen trenger ikke nevneverdig forkunnskap om den enkelte programvare og hvordan den fungerer. Det er enkelt å søke seg frem til slik programvare, samtidig som det er lett å få hjelp av meningsfeller til å finne frem. Programvaren er i mange tilfeller gratis, og oppskrifter for fremgangsmåte er lett tilgjengelige. Den uerfarne cyberkriminelle kan gjennom sine handlinger bli direkte eksponert for rekruttering fra organiserte cyberkriminelle på kriminelle forum.

Spesialiserte cyberkriminelle

Likevel er organiserte cyberkriminelle nettverk ofte avhengig av kompetente og spesialiserte cyberkriminelle som kan nyttiggjøre seg av deres tjenester og tjene inn penger til deres gruppering.

Spesialiserte cyberkriminelle innehar spesialistkompetanse innenfor et felt, eksempelvis skadevarebygging eller penetrasjonstesting, og tilbyr ofte sine tjenester innenfor kriminalitet som handelsvare.

Spesialistene rekrutteres som oftest fra eksisterende cyberkriminelle nettverk, ofte basert på bekjentskap og renommé. Det er observert at det foregår samarbeid på tvers av nettverkene, der spesialistene tilbyr sine tjenester til flere cyberkriminelle grupperinger. Selv om ett nettverk tas ned, dukker spesialistene gjerne opp i et annet, med bakgrunn i tidligere samarbeid.

Organiserte cyberkriminelle benytter tilstedeværelse og annonsering på

cyberkriminelle fora og markedsplasser for rekruttering av spesialister. Denne rekrutteringen kan være skjult eller fordekt, eller i tilfeller hvor det rekrutteres bredere har rekrutteringen foregått i det åpne. Det benyttes også lukkede kanaler på ende-til-ende-krypterte meldingstjenester som Telegram og TOX.

I denne kategorien cyberkriminelle skilles det på hvilken type erfaring og kompetanse spesialisten har. Eksempelvis er det observert at tilgangsmeglere 🗝 og hvitvaskere er en viktig del av kriminalitetsutøvelsen, men at de gjerne er lengre til venstre i illustrasjonen (se figur 6), og har mindre innflytelse i grupperingen. De skiller seg fra spesialister med teknisk kompetanse, som sitter tettere på kjernegruppen 🗝.

Organiserte cyberkriminelle

Det organiserte nivået er aktørene i den innerste kjernen. Her er grad av organisering og samarbeid tydeligere. Dynamikken fremstår som en vanlig hierarkisk organisasjon med en sentralstyrt ledelse som gir føringer til de «ansatte».

Det er eksempelvis innenfor løsepengevirus som handelsvare observert at det er behov for både ledelsesfunksjoner, rekrutteringsansvarlige og affiliert-ansvarlige 🗝. Disse kan eksempelvis styre operasjonen, utvikle skadevare og styre forhandlinger med fornærmede. Denne bestanddelen av gruppen anses som høyst profesjonelle cyberkriminelle, og er avgjørende for om en LSH-skadevare er levedyktig over tid. I sirkelen utenfor denne kjernen er gjerne nærmere tilknyttede affilierte med godt renommé eller viktig spesialistkompetanse. Disse kan gis ulike fullmakter og innflytelse, eksempelvis at de får muligheten til å foreta forhandlinger selv, eller kan rekruttere inn ny kompetanse. Utenfor denne sirkelen er løsere tilknyttede affilierte, som samarbeider med kjernegruppen ved behov (se figur 6).

Det er observert at ulike grupperinger konkurrerer med hverandre om de cyberkriminelle med mest erfaring og/eller ettertraktet kompetanse. I disse tilfellene er det sett at goder i form av en større prosentandel av utbytte og bedre rettigheter i nettverket, blir brukt i rekrutteringsøyemed.

Ettersom organiserte cyberkriminelle har behov for å påvirke mennesker, tjenester og utstyr, er det observert at teknisk og språklig kompetanse er ettertraktet innenfor mer alvorlig cyberkriminalitet. Det er også sett behov for mellommenneskelige ferdigheter, da påvirkning av fornærmede er ansett som en suksessfaktor.

Det er glidende overganger mellom de to siste kategoriene, spesialiserte og

organiserte cyberkriminelle, hvor de mest avanserte aktivitetene utøves av de organiserte cyberkriminelle. Organisering kan også forekomme blant uerfarne eller spesialiserte cyberkriminelle, men det er innenfor kategorien organiserte cyberkriminelle hvor dette profesjonaliseres.

Vurderinger

Det er *sannsynlig* at KSH er en selvforsterkende mekanisme. Ettersom cyberkriminelle bruker markedsplasser for å skaffe til veie tjenester og kompetanse, synker *sannsynlig* behovet hos enkelte for å erverve seg disse egenskapene eller ressursene over tid. Dette gir en økt etterspørsel etter cyberkriminelle tjenester, verktøy og infrastruktur, som igjen gjør det lukrativt å tilby sine varer og tjenester, som igjen fører til økt spesialisering av cyberkriminaliteten. Denne mekanismen har over tid *sannsynlig* gjort cyberkriminelle mer avhengige av KSH i utførelsen av cyberkriminaliteten.

Utviklingen går i retning av leie fremfor å eie. Det er derfor *sannsynlig* at KSH har i løpet av 2023 fått økt betydning som driver for cyberkriminaliteten.

KSH vurderes som spesielt avgjørende for de fem operasjonelle driverne for cyberkriminalitet (se figur 3), hvor markedet påvirker de kriminelles handlingsmåte. KSH påvirkes også av disse fem driverne da de legger føringer for hvordan kriminaliteten kan utøves, og det er en gjensidig avhengighet mellom driverne for at cyberkriminelle kan nå sine målsetninger.

Det ventes at manualer for delprosesser i angrepskjeden blir tilgjengelige i stadig større omfang. Det er *mulig* at dette tilbudet kan redusere behovet for enkelte tjenester på sikt, ved at også uerfarne cyberkriminelle klarer å utføre mer alvorlig cyberkriminalitet på egen hånd ved å følge oppskriften i manualen.

Det er sett at de samme cyberkriminelle går igjen i flere grupperinger, at grupperinger fragmenteres eller legges ned, men at samme skadevare dukker opp med nytt navn. Det er *sannsynlig* at det er færre sentrale aktører innen LSH enn tidligere antatt. Selv om LSH-nettverk og grupperinger blir forstyrret er det *sannsynlig* at personer og kompetanse forflytter seg til andre LSH-nettverk grunnet samarbeid på tvers. Det er *sannsynlig* at interaksjonen i utstrakt grad er transaksjonsbasert. Det er *sannsynlig* at individualisme står sterkt i miljøet, selv om samarbeid er avgjørende for suksessfull drift. Pragmatisme er *meget sannsynlig* utbredt i miljøet.

Ettersom at cyberkriminelle rekrutteres fra nettverk basert på erfaring og renommé, og at goder i form av profitt og

innflytelse i grupperingen, gis basert på kompetanse og prestasjoner, medfører dette *sannsynlig* at kompleksiteten i cyberrettet kriminalitet vil fortsette å øke, siden økosystemet drives av at erfaring og kompetanse gir cyberkriminelle nye muligheter som igjen øker kompetanse og gir erfaring.

Bedrageri

Sosial manipulering brukes gjerne i bedragerier, og kjente fremgangsmåter er eksempelvis via e-post[22], telefonoppringning[23,24], SMS[25] og falske nettsider[26]. I korte trekk handler sosial manipulering om å forlede en fornærmet til å gjøre noe vedkommende i utgangspunktet ikke ønsker. Dette kombineres gjerne med villedning, som innebærer at den cyberkriminelle utgir seg for å være en annen enn den man egentlig er.

Økonomien og betalingsevnen til mange nordmenn er fortsatt god, til tross for økte renter og inflasjon. Dette gjør nordmenn til attraktive mål for investerings- og kjærlighetsbedrageri. Tapene er ofte så store at de får betydelige konsekvenser for privatøkonomien og livet til fornærmede og deres familie. Dette kan igjen føre til belastninger utover det økonomiske.

Det rapporteres stadig oftere om investeringsbedrageri hvor den innledende kontakten mellom bedrager og fornærmet startet på ulike datingapplikasjoner. Det er en sammenheng mellom investerings- og kjærlighetsbedragerier. I tillegg hender det at fornærmede som utsettes for kjærlighetsbedrageri også blir benyttet som pengemuldyr 🗝. En vanlig form for slik muldyraktivitet er at fornærmede kjøper gavekort til gjerningspersonen med egne penger, slik at fornærmede i praksis hvitvasker det den selv blir bedratt for, eller kjøper gavekort med penger den har mottatt på bankkonto og på den måten begår heleri.

Det har blitt tydelig at flere av de cyberkriminelle i bedragerisaker kan knyttes til organisert og annen alvorlig kriminalitet. Det er åpenbare paralleller mellom bedragerier begått i Norge og

22 Eng: Phishing
23 Eng: Vishing
24 Eng: Spoofing
25 Eng: Smishing
26 Eng: Pharming

Sverige, samtidig som det er knytninger til transnasjonale kriminelle miljøer knyttet til narkotika- og menneskesmugling. Modus registreres gjerne først i Sverige før de dukker opp i Norge. Eksempler innebærer bruk av falsk dokumentasjon, oppkjøp av legitime virksomheter og bruk av stråpersoner 🗝.

Det er flere nettverk som begår bedrageri ved å få tilgang til fornærmedes bankkonto gjennom BankID. I likhet med cyberrettede kriminelle nettverk spenner aktørgalleriet seg fra løst sammensatte nettverk med en kjerne av faste deltagere, til nettverk som fremstår organiserte med et tydelig hierarki og linjeledelse på tvers av landegrenser. Basert på informasjonen om de sentrale aktørene fremstår det som at selve bedrageriene gjennomføres av et mindretall sentrale gjerningspersoner. Et gjennomgående funn er at sentrale aktører i BankID-bedrageriene i stor grad også er involvert i narkotikakriminalitet og andre typer bedrageri.

Vurderinger

Det er *meget sannsynlig* at bedrageri vil fortsette å øke i omfang, og at personer i alle aldre og samfunnslag vil rammes i av dette i løpet av 2024.

Direkteoverførte bestillingsovergrep

Direkteoverførte bestillingsovergrep (DOBO) er seksuelle overgrep mot barn som direkteoverføres med video via internett til kjøpere som bestiller og betaler for overgrepene. Kjøper kan gi instruksjoner til selger om hvordan overgrepene skal utføres. Prisen på overgrepene blir forhandlet mellom kjøper og selger og betalingen blir overført til selger via betalingsløsninger på internett. Det kreves lite teknisk kompetanse for å begå DOBO, og det fordrer kun grunnleggende engelskkunnskaper.

DOBO selges fra flere verdensdeler og land, men en uforholdsmessig stor del av kriminaliteten foregår på Filippinene. Årsaken til dette er trolig sammensatt, men kombinasjonen av høy andel engelskspråklige, god internettutbygging, fattigdom, kulturelle aspekter og god tilgjengelighet på betalingstjenester er ofte pekt på i denne sammenheng.[27]

Registrerte fornærmede for DOBO er

27 Rapport: International Justice Mission, Online Sexual Exploitation of Children in the Philippines, https://ijmstoragelive.blob.core.windows.net/ijmna/documents/Final_OSEC-Public-Summary_05_20_2020.pdf

oftest jenter i slutten av barneskolealder som ble utsatt for overgrep av foreldre, andre slektninger eller naboer. Det er vanlig at flere selgere samarbeider, blant annet ved å byttelåne barn som utnyttes til overgrep og for å byttelåne chatte- og/eller betalingskontoer. DOBO er derfor i mange tilfeller alvorlig organisert cyberkriminalitet.

Aktørene som kjøpte DOBO fra Norge var utelukkende menn. De var fra alle samfunnslag og var i liten grad registrert med seksuallovbrudd fra tidligere. Det var en overvekt av single menn og gjennomsnittsalderen på menn som kjøpte DOBO var høyere enn nordmenns gjennomsnittsalder.

Kripos anser en betydelig del av DOBO-kjøperne som situasjonelle overgripere. Situasjonelle overgripere har i utgangspunktet ikke intensjon om å begå overgrep, men ender med å begå overgrep når muligheten byr seg. Et eksempel på dette er en mann som i utgangspunktet vil ha direkteoverført seksuelt innhold med voksne, men som takker ja til DOBO etter å ha blitt tilbudt dette av selgeren.

Vurderinger

Omfanget av DOBO kjøpt av nordmenn er svært vanskelig å anslå ettersom få av forholdene anmeldes. Kripos anslår at mellom 400 og 2000 nordmenn har kjøpt DOBO i løpet av 2023. Det er *sannsynlig* at antall overgrep som er begått av nordmenn er langt høyere enn antall gjerningspersoner, da én gjerningsperson kan begå mange overgrep i løpet av et år.

Det er *sannsynlig* at den mentale terskelen for å begå voldtekt på internett er lavere enn i den fysiske verden, i tillegg til at det er praktisk enklere. Årsaker til dette kan være en større grad av opplevd anonymitet på internett og at fysisk avstand til den kriminelle handlingen gjør at den oppleves som mindre alvorlig.

Både gjerningspersonens ønske om å minimere oppdagelsesrisikoen og den teknologiske utviklingen er viktige drivere for hvordan cyberkriminaliteten vil begås i fremtiden. Det er *meget sannsynlig* at DOBO-kjøpere vil benytte sikrere plattformer og betalingsløsninger i året som kommer.

Kryptovaluta

I 2023 observerte Kripos at kryptovaluta ble benyttet av alle aktører i det cyberkriminelle økosystemet, på tvers av flere kriminalitetsområder.[28] Kryptovaluta ble også brukt på nye måter for å skjule kriminelle handlinger.

Cyberkriminelles bruk av kryptovaluta er ikke begrenset til cyberkriminalitet, men inngår nå som en komponent i alle typer profittmotivert kriminalitet.

Kripos har erfart at cyberkriminelle hvitvasker utbytte fra kriminelle handlinger gjennom bruk av såkalte miksertjenester. Det er observert en kontinuerlig fremvekst av miksertjenester drevet av cyberkriminelle aktører. Tjenester som utfører miksing av kryptovaluta blander ulike strømmer med kryptovaluta for på den måten å øke eierens anonymitet, og for å gjøre transaksjoner med kryptovaluta vanskeligere å spore. Bruk av miksertjenester skjer normalt på en av tre måter. Enten sendes kryptovaluta til en sentralisert miksertjeneste hvor kontrollen på egen kryptovaluta overgis mens miksеprosessen pågår. Alternativt kan ferdig mikset kryptovaluta tildeles når innskudd gjøres hos en miksertjeneste. En tredje mulighet er å beholde kontrollen på egen kryptovaluta og samarbeide med flere for å mikse kryptovalutaen mellom seg. Selv om miksertjenester kan fungere en periode, jobber myndigheter kontinuerlig for å finne metoder for å spore transaksjoner, stenge ned tjenesten eller straffeforfølge de involverte.

> Kryptovaluta er desentralisert og ikke under noen lands myndighetskontroll. Selvstendigheten gir muligheter for anonymisering, men risiko for enorme verdiendringer på kort tid.

Kripos har sett eksempler på at cyberkriminelle sender kryptovaluta til undergrunnsbanktjenester[29]. Disse tjenestene veksler kryptovalutaen til en spesiell kryptovaluta, som oftest låst til amerikanske dollar for å unngå verdisvingninger, og holder deretter på pengene. Kunden ber så tjenesten om å

28 Spesielt i forbindelse med kjøp og salg av illegale varer, betaling for overgrepsmateriale, hvitvasking av kriminelt utbytte og som betalingsmiddel ved løsepengekrav og bedragerier

29 Eng: Underground Banking

få ut verdien i vanlig valuta, i et ønsket land, og kan på denne måten hvitvaske kriminell gevinst.

Cyberkriminelle benytter blokkjedebaserte teknologier som kryptovaluta, med funksjoner som tilbyr anonymitet, og som er egnet til forflytning av verdier.

Tyveri av kryptovaluta har de senere år vært et økende og omfattende problem internasjonalt. I 2022 ble det stjålet kryptovaluta for 3,8 milliarder USD, noe som var en økning fra 3,3 milliarder USD året før. Mange av de større tyveriene av kryptovaluta er gjennomført via såkalte desentraliserte finanstjenester (DeFi[30]). Disse oppbevarer kryptovaluta og er særlig attraktive mål for kriminelle. Et eksempel på en slik DeFi-tjeneste er Bridges som muliggjør at man overfører kryptovaluta på tvers av blokkjeder.

Blokkjeder (Eng: Blockchain) gjør det mulig for to eller flere individer, organisasjoner eller datamaskiner, uavhengig av deres gjensidige kjennskap, å utveksle verdier i digitale omgivelser. Dette uten innblanding fra en tredjepart, som en bank.

Vurderinger

Det er *meget sannsynlig* at cyberkriminelle aktører fortsetter å hvitvaske store summer ved bruk av kryptovaluta.

Det er *sannsynlig* at cyberkriminelle aktører vil bruke blokkjeder, kryptovalutaer og tjenester som har lave krav til kundekontroll[31], er desentraliserte og har funksjoner som gir økt anonymitet. Dette gjør det lettere for cyberkriminelle å forflytte og hvitvaske kriminelt utbytte, også i Norge.

30 DeFi er en forkortelse for «desentralisert finans» og brukes som en samlebetegnelse for flere forskjellige typer prosjekter som opererer utenfor det tradisjonelle finanssystemet

31 Eng: Know Your Customer (KYC)

Cyberkriminelle ønsker å skape avstand mellom seg selv og infrastrukturen som benyttes i kriminalitet. Dette er nødvendig for å ivareta egen anonymitet. Kripos vurderer derfor at mange velger å benytte kommersielle proxy- og VPN-løsninger som lagrer minst mulig informasjon om brukerne, fremfor å selv etablere slike løsninger, da sistnevnte gjør det utfordrende å skape tilstrekkelig avstand til infrastrukturen. I tillegg er det tidkrevende og kostnadsbelastende å sette opp egen proxy- eller VPN-infrastruktur.

Proxy- og VPN-løsninger

En avgjørende faktor for mye av cyberkriminaliteten er muligheten til å kunne operere fordekt[32]. Anonymiseringsteknologier gjør dette mulig. Utviklingen av disse teknologiene drives frem av legitime personvernbehov og et ønske om frihet i det digitale rom, men kommer samtidig cyberkriminelle til gode. Som følge av dette står politiet overfor en pågående utfordring med å håndtere trusselen fra kriminelles bruk av anonymiseringsteknologier.

Blant flere anonymiseringsteknologier utgjør proxy- og VPN-løsninger 🗝 en vesentlig andel av verktøyene som cyberkriminelle benytter seg av. Ved bruk av disse teknologiene kan cyberkriminelle skjule egne IP-adresser og kryptere datatrafikk. Dette innebærer at avdekking og etterforskning av cyberkriminalitet vanskeliggjøres.

I 2023 ble det internasjonalt rapportert om at VPN var den mest brukte anonymiseringsteknologien blant cyberkriminelle.[33] Europol omtalte også VPN som en av mange krypterings- og anonymiseringsløsninger som spesielt seksuallovbrytere brukte i stor og økende grad. Samme år registrerte Kripos at omlag 40% av de som benyttet fildelingsnettverk til å laste opp og ned overgrepsmateriale benyttet seg av VPN-løsninger. Videre er det eksempler på at proxy-

32 Kripos har i Cyberkriminalitet 2023 identifisert «fordekt aktivitet» som en frittstående driver for cyberkriminalitet. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

33 Rapport : Europol, IOCTA 2023, https://europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023

servere ble benyttet som mellomlagringspunkt for overgrepsmateriale som ble delt på tvers av fildelingsnettverk.

Proxy- og VPN-løsninger som *Residential Proxy, Mobile Proxy* og *Residential Virtual Private Network* skaper særskilte utfordringer. Løsningene tilslører brukernes IP-adresser ved å benytte privatpersoners internettabonnement (IP-adresse). Det er vanskelig å avdekke at disse løsningene har vært i bruk, noe som i ytterste konsekvens kan medføre at politiet etterforsker personer for straffbare handlinger de ikke har begått.

Ordinære proxy- og VPN-løsninger kan blokkeres fra å få tilgang til nettsteder og tjenester på internett gjennom sikkerhetstiltak ment for å forhindre kriminell aktivitet.[34] For cyberkriminelle er dette et problem som kan omgås ved bruk av Residential Proxy, Mobile Proxy eller Residential VPN, som ikke like enkelt kan fanges opp av slike sikkerhetstiltak. Løsningene har derfor et kriminelt bruksområde som strekker seg forbi anonymiseringseffekten.

Selv om det er teoretisk mulig for politiet å identifisere sluttbruker av en proxy- eller VPN-tjeneste krever dette at leverandøren som leverer tjenesten både er villig og i stand til å utlevere informasjon om sluttbrukeren. Kripos erfarer at dette sjeldent er tilfelle i praksis. Flere kommersielle aktører hevder at de drifter sine tjenester på en slik måte at de ikke vil være i stand til å utlevere informasjon om sine brukere til myndigheter. Dette brukes videre av aktøren som en garanti for at nettopp deres løsning kan ivareta brukernes anonymitet.

Samlet sett spiller proxy- og VPN-løsninger en betydningsfull rolle for cyberkriminelles evne til å operere fordekt. Teknologiene bidrar til å komplisere et allerede innviklet økosystem hvor cyberkriminelle opererer på tvers av landegrenser og jurisdiksjoner. Dette stiller store krav til fremtidig kriminalitetsbekjempelse, hvor politiet må tilpasse metoder og verktøy for å håndtere den stadige utviklingen og utbredelsen av anonymiseringsteknologier.

Vurderinger

Som hovedregel senker proxy- og VPN-løsninger hastigheten på brukernes

34 Et eksempel er enkelte nettbanktjenester som bruker sikkerhetstiltak som blokkerer IP-adresser knyttet til kommersielle proxy- og VPN-tjenester, med hensikt om å verne kundene mot urettmessige innlogginger fra mistenkelige IP-adresser

> Overgrep mot barn blir normalisert i fora på det mørke nettet og i chattegrupper på ende-til-ende-krypterte plattformer. Slik normalisering kan føre til at personer som ikke har gjort det tidligere deler overgrepsmateriale eller begår egne overgrep som dokumenteres.

Foto: Shutterstock

datatrafikk. Dette kan gjøre det vanskelig å aksessere eller benytte visse tjenester på internett. Kripos vurderer at treghetene som preger proxy- og VPN-løsninger kan drive flere av dagens cyberkriminelle til å benytte andre løsninger for å være anonyme. Infrastrukturen som understøtter internett blir gradvis bedre og raskere, og disse treghetene vil på sikt forsvinne. Det er *sannsynlig* at denne utviklingen vil føre til økt bruk av proxy- og VPN-løsninger blant cyberkriminelle.

Kommersielle proxy- og VPN-løsninger gjør det *meget sannsynlig* lettere for cyberkriminelle med lav kompetanse om operasjonell sikkerhet å operere anonymt på internett.

Ende-til-ende-krypterte meldingsplattformer

Kommunikasjon er en grunnleggende driver for cyberkriminalitet (figur 3) og cyberkriminelle er derfor avhengig av å ta i bruk teknologi for å kunne kommunisere sikkert.

Ende-til-ende-krypterte meldingsplattformer 🗝 skaper en rekke utfordringer for politiet. Meldingsplattformene øker de kriminelles handlingsrom ved at de automatisk sletter data og ved å beskytte informasjonen i applikasjonene med ekstra lag av sikkerhet. Dette gjør det utfordrende for politiet i å få tilgang

Telegram er en kontroversiell ende-til-ende-kryptert meldingsplattform. Telegram har blitt omtalt som det «mørke hjørnet» av det åpne nettet, og har i løpet av de siste årene opplevd en massiv migrasjon av cyberkriminelle fra det mørke nettet.

Kriminalitetsbildet på Telegram er sammensatt og komplekst. Det foregår distribusjon av våpen og narkotika, hallikvirksomhet, høyreekstremistisk innhold, radikalisering, hacking, svindel, deling av seksualisert materiale av voksne uten samtykke, deling av overgrepsmateriale og utnyttelse av personer i sårbare situasjoner.

Kripos har gjennom patruljering på Telegram observert at mye av kriminaliteten foregår i de offentlige gruppene/kanalene. I tillegg har politiet mottatt informasjon fra ulike kilder om at de mer alvorlige kriminalitetsformene foregår i de private gruppene/kanalene.

til informasjonen, samtidig som at viktige spor kan gå tapt. Som for proxy- og VPN-tjenester drives også utviklingen av ende-til-ende-krypterte meldingsplattformer av legitime personvern- og sikkerhetsbehov. Blant annet ble kommunikasjonen i Messenger ende-til-ende-kryptert i 2023, noe som begrunnes i at det gir brukerne en sikrere og mer privat tjeneste.

Ende-til-ende-krypterte meldingsplattformer er enkle å bruke, gir de cyberkriminelle anonymisering, er stabile i drift, tilbyr en god fildelingsopplevelse og gir lav oppdagelsesrisiko. Plattformene er i tillegg lett tilgjengelige og brukeropplevelsen er som for andre sosiale medier.

Cyberkriminelle har forskjellig motiv og mål med sin kriminalitet og ende-til-ende-krypterte meldingsplattformer har følgelig varierende bruksverdi blant dem som benytter dette. For seksuallovbrytere gir teknologien mulighet til å utføre en rekke ulike seksuallovbrudd på internett, alt fra samtaler om seksuelle fantasier med andre til direkteoverføring av fysiske overgrep som voldtekt av barn.

Cyberkriminelle bruker ikke internett bare for å begå kriminalitet, men også for å kunne etablere kontakt og kommunisere med likesinnede. Overgrep mot barn blir normalisert i fora på det mørke nettet og i chattegrupper på ende-til-ende-krypterte plattformer. Slik normalisering kan føre til at personer som ikke har gjort det tidligere deler overgrepsmateriale eller begår egne overgrep som dokumenteres.

Ende-til-ende-krypterte meldingsplattformer gir mulighet for å produsere, laste ned, lagre og dele overgrepsmateriale uten at dette enkelt kan avdekkes. Deling av overgrepsmateriale krever samhandling mellom seksuallovbrytere på internett, men graden av samarbeid varierer. Ende-til-ende-krypterte meldingsplattformer krever lite organisering og administrering. Til sammenligning ser seksuallovbrytere på det mørke nettet i større grad ut til å organisere seg i forbindelse med deling av overgrepsmateriale på chattesider eller i internettfora.[35]

Kripos har det siste året observert at seksuallovbrudd som tidligere ble begått på åpne plattformer har flyttet seg til ende-til-ende-krypterte meldingsplatt-

35 Rapport: Kripos, Cyberkriminalitet 2023, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

former. Likevel er det kun observert få tilfeller av seksualisert kontakt mellom voksne og barn på slike plattformer. Slik kontakt foregår fremdeles i all hovedsak på åpne plattformer.

Vurderinger

Ende-til-ende-krypterte meldingsplattformer skaper et stort handlingsrom for cyberkriminelle. Teknologien tilbyr både anonymisering og brukervennlighet, og dekker slik behovene til både avanserte aktører og aktører med lav kompetanse. Plattformene er i tillegg en stabil faktor for kriminalitetsutvekslingen som foregår der. Det er derfor *sannsynlig* at cyberkriminelles bruk av ende-til-ende-krypterte meldingsplattformer vil øke i årene fremover. Dette vil utfordre politiets muligheter til å avdekke og etterforske cyberkriminalitet som foregår på plattformene.

Det er *meget sannsynlig* at norske gjerningspersoner deler egenprodusert overgrepsmateriale, og direkteoverfører egne fysiske overgrep mot barn i en-til-en-samtaler på ende-til-ende-krypterte meldingsplattformer. Det er *sannsynlig* at seksuallovbrytere i økende grad vil søke til ende-til-ende-krypterte meldingsplattformer da de oppleves som mer sikre og gir en bedre fildelingsopplevelse.

Det er *sannsynlig* at omfanget av seksuallovbrudd i stort begått på ende-til-ende-krypterte meldingsplattformer vil øke i årene fremover. Det er videre *sannsynlig* at seksuallovbrudd som tradisjonelt har blitt begått på andre plattformer, som sosiale medier, vil flytte seg til krypterte plattformer fremover. Det er derfor *sannsynlig* at forekomsten av kontakt mellom barn og voksne på ende-til-ende-krypterte meldingsplattformer vil øke i 2024.

Foto: Shutterstock

Om digitale sårbarheter

I likhet med cyberkriminelles handlemåter er også digitale sårbarheter avgjørende for å tegne et helhetlig bilde av trusselen. Samfunnet må bekjempe cyberkriminalitet i fellesskap. Identifisering og håndtering av digitale sårbarheter er viktig i så måte. Kripos ønsker i dette kapitellet å trekke frem noen sårbarheter som politiet mener er særlig viktig å øke kunnskapen og samarbeidet om i samfunnets kamp mot cyberkriminalitet.

Skytjenester

Virksomheter benytter seg av tjenesteutsetting, inkludert skytjenester, som ett av virkemidlene for å realisere gevinst fra teknologiutviklingen og digitaliseringen.[36]

Bruk av skytjenester kan bidra til bedre sikkerhet ved at skyleverandørene har store og effektive drifts-, sikkerhets- og utviklingsmiljøer.[37] Skytjenesteleverandørene vil kunne oppdatere systemene raskere. Dette vil være positivt der virksomheter tidligere utførte oppdateringer selv. Spesielt oppdatering av kjente og nyoppdagede sårbarheter vil kunne oppdateres hurtigere ved en løsning der skytjenesteleverandør utfører dette vedlikeholdet for en virksomhet. Fravær av systemoppdatering skaper mulighetsrom for cyberkriminelle.

Bruk av skyteknologi muliggjør rask overføring av store datamengder. Dette så vi eksempel på når ukrainske myndigheter og virksomheter ved å ta i bruk skyteknologi opprettholdt evnen til å støtte landets befolkning på tross av

36 Rapport: NSM, Risiko 2020, https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2020/skytjenester-og-tjenesteutsetting/

37 Rapport: NSM, Nasjonal skytjeneste – Konseptvalgutredning. Januar 2023 – versjon 1.0, https://nsm.no/getfile.php/1313330-1696430485/NSM/Filer/Dokumenter/Rapporter/Nasjonal%20skytjeneste%20-%20konseptvalgutredning%20-%20KVU%202023.pdf

store fysiske ødeleggelser som følge av krigen.[38]

Samtidig vil bruk av skytjenester innebære utfordringer. Informasjon og funksjonalitet er basert på infrastruktur på fysiske lokasjoner langt unna, ofte i andre land. Eierskapsstrukturer og uautorisert tilgang til informasjon kan være vanskelig å kontrollere.[39] Cyberkriminelle aktører kan benytte skytjenesteinfrastruktur til å ramme virksomheter som har plassert sine data, applikasjoner og systemer hos en skytjeneste. De kan også benytte seg av skytjenesteleverandørens infrastruktur og bygge opp systemer og applikasjoner som de cyberkriminelle anvender i sine operasjoner.

Cyberkriminelle benytter seg av legitime tjenester for å laste opp store mengder data til skytjenester.

I mange år har norsk og internasjonalt politi sett at personer med seksuell interesse for barn bruker kommersielle tilbydere for å dele overgrepsmateriale. Dette skyldes lav overføringskapasitet på det mørke nettet som gjør det uegnet for deling, og det deles derfor passord og lenker til servere på det åpne nettet i ulike fora, både på det åpne og det mørke nettet.

En generell utvikling er at virksomheter i større grad enn tidligere leier skytjenester. En antagelse er at cyberkriminelle følger eller vil følge denne utviklingen. Dersom antagelsen stemmer, vil cyberkriminelle i mindre grad trenge egen fysisk hardware.

Nulldagssårbarheter

Nulldagssårbarheter 🗝 er krevende å oppdage, og det er ofte meget kompetente aktører som klarer å avdekke disse. Å avdekke sårbarheter i en programvare som ennå ikke er kjent for leverandøren selv, har historisk krevd spesialisert kunnskap og forståelse. Nulldagssårbar-

38 Rapport: NSM, Nasjonalt digitalt risikobilde 2023, side 30, https://nsm.no/getfile.php/1313382-1697777843/NSM//Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf

39 https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2020/skytjenester-og-tjenesteutsetting/

heter selges hovedsakelig kommersielt for store pengesummer.[40]

Når en nulldagssårbarhet blir oppdaget må produsenten utvikle en sikkerhetsoppdatering 🗝 som lukker sårbarheten. Denne oppdateringen må distribueres og installeres på alle sårbare enheter. Frem til oppdateringen er installert er det mulig for de som har kunnskap om nulldagssårbarheten og har kompetanse til å utnytte den, å skaffe seg uberettiget tilgang til systemet. I løpet av 2023 ble det blant annet avdekket nulldagssårbarheter i programvare fra produsentene Citrix og Cisco.

Det er flere eksempler på straffesaker hvor cyberkriminelle har utnyttet nulldagssårbarheter for å skaffe seg uberettiget tilgang til datasystemer. Relatert til nulldagssårbarhetene i Citrix ble et norsk selskap utsatt for et løsepengevirus. Et amerikansk selskap med avdeling i Norge ble utsatt for datainnbrudd med påfølgende datatyveri av en cyberkriminell gruppe i juni 2023. I forbindelse med datainnbruddet ble en nulldagssårbarhet utnyttet. Den profittmotiverte grupperingen med bruk av løsepengevirus som modus knyttes til Øst-Europa. Det er usikkert om den cyberkriminelle grupperingen selv avdekket nulldagssårbarheten eller tilegnet seg informasjon om sårbarheten fra noen andre.

Sommeren 2023 ble Departementenes sikkerhets- og serviceorganisasjon (DSS) utsatt for et datainnbrudd, hvor det ble utnyttet en nulldagssårbarhet. Straffesaken ble først etterforsket hos politiet, men ble etter hvert overført PST. PST henla saken, men tilskrev angrepet en profesjonell cyberaktør, trolig statlig aktør 🗝.

Det finnes flere private selskaper som jobber med å avdekke nulldagssårbarheter. En av disse[41] avdekket 25 nulldagssårbarheter i 2020, 69 i 2021, 41 i 2022 og foreløpig 56 nulldagssårbarheter i 2023. Trenden er økende fra 2014.

Vurderinger

Det er *sannsynlig* at ondsinnede aktører som lykkes i å avdekke nulldagssårbar-

40 https://security.apple.com/bounty/categories/
https://zerodium.com/program.html
https://twitter.com/vxunderground/status/1562550443712352256/photo/3
https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/

41 Google Project Zero

heter jobber på vegne av en stat eller er statsstøttet.

Det er *sannsynlig* at det kreves sterke økonomiske muskler for å tilegne seg personer som har kompetanse til å avdekke nulldagssårbarheter, og det er *sannsynlig* at kun noen få cyberkriminelle grupperinger har denne kapasiteten 🗝.

Det er *sannsynlig* at jo mer penger de cyberkriminelle tjener på kriminelle handlinger, jo større muligheter har de for å tiltrekke seg aktører med riktig kunnskap og kompetanse til å avdekke nulldagssårbarheter.

Det er *sannsynlig* at tekniske svakheter, som nulldagssårbarheter og andre systemuavhengige sårbarheter, vil få økt verdi blant cyberkriminelle aktører og øke skadepotensialet ettersom flere virksomheter deler de samme sårbarhetene.

Selv om nulldagssårbarheter har stort skadepotensiale så vurderer Kripos trusselen som mindre viktig for norske virksomheter enn allerede kjente sårbarheter.

Den trådløse hverdagen

I kjølvannet av Covid-pandemien har arbeid fra hjemmekontor blitt mer utbredt i mange offentlige og private virksomheter. At arbeidsstedet har forflyttet seg utover virksomhetens tradisjonelle rammer har imidlertid medført varierte og utvidede angrepsmuligheter for cyberkriminelle. Spesielt der fjernarbeid utføres i stor skala øker sårbarhetsflatene.

I tillegg til å utvide, har bruk av hjemmekontor flyttet angrepsflatene utenfor virksomhetenes tradisjonelle beskyttelsestiltak som brannmurer og varslingssystemer. Dette er problematisk ettersom arbeidstakere som jobber hjemmefra generelt har færre sikkerhetsmekanismer tilknyttet egen internettilgang og digitale enheter. Mange har svake passord på trådløse hjemmenettverk, bruker ikke VPN-løsninger, mangler flerfaktorautentisering, utsetter viktige sikkerhetsoppdateringer og har flere usikrede digitale enheter[42] tilkoblet nettverkene sine. Dette medfører en forhøyet risiko for at arbeidstakere faller for taktikker og metoder som cyberkriminelle benytter for å bedra og forlede.

Som følge av utviklingen ligger det et større ansvar på den enkelte arbeidstaker for å bidra til å ivareta virksomhetens informasjonssikkerhet, spesielt ved arbeid utenfor arbeidsstedet.

---

42 No: «Tingenes internett»-gjenstander som for eksempel robotstøvsuger, musikkanlegg, smart-TV, etc. Eng: Internet of Things Device (IoT Device)

Den vide utbredelsen av smarttelefoner har skapt nye muligheter for cyberkriminelle som ønsker å få tak i sensitive og personlige data. Rask og uavbrutt internettilgang, samt mengder av tilgjengelige applikasjoner og tilkoblingsmuligheter, gjør mobiltelefonen til et attraktivt mål for skadevareutviklere. Det at man kan installere tredjeparts programvare åpner opp for nye muligheter og funksjonaliteter for skadevareutviklere.

Smarttelefoner kan infiseres med ondsinnet programvare på flere måter. Skadevare kan sendes via MMS eller e-post eller kan spres til telefonen gjennom tilkobling til andre kompromitterte enheter. Det vanligste er likevel at brukere av smarttelefonen selv laster ned skadevare gjennom å installere tredjepartsapplikasjoner med ondsinnet innhold. Dette skjer oftest ved at personer forledes gjennom forskjellige former for sosial manipulasjon.

Veldig mange barn har tilgang til sine foreldres enheter og kontoer på internett og i sosiale medier. Dette medfører flere sårbarhetsflater for foreldre, og er en ekstra sikkerhetsrisiko for virksomheter.

Da Kripos undersøkte forekomsten av barn under tretten år som delte seksualiserte videoer av seg selv på internett, var et av funnene at de yngste barna som delte seksualisert materiale av seg selv ofte benyttet foreldrenes brukerkontoer til delingen. Mange av delingene på YouTube som politiet fikk tips om, var med foreldrenes navn og brukerkontoer. Spesielt gjaldt dette de yngste barna ned i femårsalderen, men også i noen tilfeller der barna var ti til elleve år.[43]

43 Rapport: Kripos, Barn under 13 år som deler seksualiserte videoer, https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/kripos/seksuelle-overgrep/barn-under-13-ar-som-deler-seksualiserte-videoer.pdf

Foto: Shutterstock

Utviklingstrekk

Som en del av kriminalitetsbekjempelsen forsøker Kripos å løfte blikket og se på utviklingstrekk som vil endre kriminalitetsbildet.[44] I samfunnet er det utviklingsområder som ventes å ha fremtidig påvirkning på cyberkriminaliteten. For noen utviklingsområder har påvirkningen allerede vart en stund, mens for andre områder har man ennå ikke sett slik påvirkning. I dette kapittelet trekker Kripos frem de identifiserte utviklingsområdene som i størst grad ventes å påvirke den fremtidige cyberkriminaliteten.

Leverandørkjedeangrep

I et stadig mer globalisert og digitalisert samfunn benytter virksomheter ulike digitale tjenester og programvarer fra tredjeparter. Kostnadseffektivitet, fokus på egen kjernevirksomhet og økt produktivitet er grunner til at virksomheter benytter seg av underleverandører og slik inngår i en leverandørkjede. Dette har som beskrevet sine fordeler, men vil samtidig øke risikoen for å bli utsatt for cyberkriminalitet.

Cyberkriminelle kan utnytte dårlig sikkerhet hos underleverandører i programvare og digitalt utstyr. Skadevare kan plantes i programvare som distribueres ut til flere kunder, og på den måten kan gjerningspersonen skaffe seg uberettiget tilgang til datasystem hos et eller flere mål. Cyberkriminelle og andre trusselaktører leter etter det svakeste leddet i en slik kjede.

Norske offentlige og private virksomheter er en del av komplekse leverandør-

> Et leverandørkjedeangrep forekommer når det gjennomføres et angrep på en tredjepart, men hvor det egentlige målet er en eller flere virksomheter i samme leverandørkjede. Selv om en virksomhet har god fysisk og digital sikkerhet, kan trusselaktører utnytte underleverandører som er langt dårligere sikret for å få tilgang til sine egentlige mål.
> Rapport: NSM, Risiko 2023.

44 Eng: Horizon Scanning

kjeder hvor det er vanskelig å ha oversikt over ulike sårbarheter. Virksomheter som forvalter grunnleggende nasjonale funksjoner (GNF)[45] er også en del av de samme leverandørkjedene.[46] GNF og/eller IKT-tjenester som understøtter GNF, kan derfor rammes utilsiktet ved at de er en del av en leverandørkjede.

I januar og februar 2023 ble flere kommuner i Finnmark utsatt for et datainnbrudd i forbindelse med et leverandørkjedeangrep. Etterforskning har avdekket at innbruddene ble utført med en kompromittert brukerkonto hos en felles kommunal underleverandør.

I prinsippet er alle virksomheter i Norge et potensielt mål for leverandørkjedeangrep. Hvor utsatte virksomheter er, avhenger av hvor god styring virksomheten har på innkjøp, logistikk, sikkerhet og avhengigheter. Lovverk og reguleringer, som stiller krav til et gitt sikkerhetsnivå hos virksomheter, vil også kunne påvirke dette. Det er observert flere angrep i 2023 hvor trusselaktør retter seg mot underleverandører eller selskaper som lager programvare, for å kunne angripe deres kunder.

Vurderinger

Det er *sannsynlig* at ulik praksis i hvordan norske virksomheter praktiserer innkjøp, logistikk og sikkerhet vil medføre alvorlige sikkerhetsutfordringer for samfunnskritiske funksjoner.

Det er *sannsynlig* at innføringen av nye regelverk som ansvarlig gjør virksomheter innen krav til leverandørstyring og verdikjederisiko, vil redusere handlingsrommet cyberkriminelle har til å unytte sårbarheter i leverandørkjeder.

Utpressing i det digitale rom

Utpressing er en metode kriminelle bruker for å oppnå økonomisk utbytte. Pressmidlet varierer selv om målet er det samme. Profittmotiverte cyberkriminelle kan bruke både cyberrettet og cyberstøttet kriminalitet til å fremskaffe pressmidlet, for eksempel ved å få et

45 GNF er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser

46 Rapport: NSM, Risiko 2023, https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

barn til å kle av seg foran webkamera eller ved å begå datainnbrudd for å stjele informasjon.

Seksuell utpressing med økonomisk motiv

Fra høsten 2022 ble det registrert et økende antall tilfeller av seksuell utpressing med økonomisk motiv. Cyberkriminaliteten rettet seg mot stadig yngre norske gutter, mens den tidligere hovedsakelig har rettet seg mot voksne menn. Tendensen fortsatte inn i første tertial av 2023 med vedvarende stabil rapportering, også internasjonalt.[47] I denne perioden var de mindreårige fornærmede gutter i alderen femten til sytten år, og gjerningspersonene var organiserte,[48] ikke-identifiserte aktører som opererte fra utlandet, hovedsakelig Afrika og Asia. Kommunikasjonen mellom gjerningsperson og fornærmede var på engelsk, og gjerningspersonene benyttet falske profiler hvor de utga seg for å være utenlandske jenter frem til fornærmede hadde sendt nakenbilder og/eller -videoer av seg selv. Det ble deretter fremsatt trusler om spredning av materialet dersom fornærmede ikke betalte. I flere tilfeller ble truslene fullbyrdet og materialet spredt dersom fornærmede ikke etterkom gjerningspersonenes pengekrav. I mange av tilfellene hvor fornærmede betalte, fremsatt gjerningspersonene nye krav om ytterligere betaling. I utlandet har det også vært tilfeller der utpressingen fortsatte overfor den fornærmedes familie, etter at fornærmede tok sitt eget liv.

Fra våren 2023 ble det registrert en økende rapportering av tilfeller der norske fornærmede hadde blitt utsatt for seksuell utpressing med økonomisk motiv. Gjerningspersonene var, i likhet med tidligere, organiserte cyberkriminelle aktører, men pengekravene var høyere og de fornærmede enda yngre, barn helt ned i tretten års alder. I tillegg til et offerbilde i endring skjedde det en utvikling i de cyberkriminelles modus.

Flere gjerningspersoner laget bildekollasjer de truet med å dele, satt sammen av bilder mottatt fra fornærmede, bilder

47 https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis

48 Rapport: Kripos, Seksuell utnyttelse av barn og unge over internett 2019, https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/seksuell-utnyttelse-av-barn-over-internett.pdf

funnet i sosiale medier og/eller nakenbilder av andre personer. Kollasjene hadde påskrift med feilaktige opplysninger om at den fornærmede var etterlyst for alvorlige seksuallovbrudd mot barn med oppfordring om å la budskapet gå viralt, samt tekst som inneholdt identifiserende opplysninger om fornærmede.

En annen endring i modus er syntetisk seksualisert materiale av fornærmede. Internasjonalt ble det rapportert om tilfeller hvor kunstig intelligens er benyttet til utpressing av barn, og i juni advarte FBI allmennheten om at teknologien kan bli benyttet til å generere seksualiserte bilder av barn ved bruk av bilder som ligger tilgjengelig på internett.

Flere av de fornærmede, både voksne og barn, betalte gjerningspersonene flere tusen kroner som følge av utpressingen. Pengekravene varierte, men befant seg hovedsakelig i størrelsesordenen 5000 NOK til 20 000 NOK, selv om det i enkelte tilfeller ble fremsatt høyere pengekrav og/eller betalt høyere beløp. I flere tilfeller ble det bedt om betaling i kryptovaluta.

Mot slutten av 2023 ble det registrert tilfeller av seksuell utpressing hvor utpresser benyttet seg av norske navn og norsk språk. Dette kan være en måte å fremstå mer troverdig på, og/eller som ledd i å oppnå tillit før utpresseren gjør sin egentlige agenda kjent. Det er foreløpig ukjent for Kripos om det er de samme organiserte nettverkene som står bak, for eksempel ved å benytte GKI for å fremstå på norsk, eller om det er nordmenn som utnytter kjent modus for å tjene penger.

Seksuell utpressing er en stor mental og emosjonell påkjenning for fornærmede, og er sterkt forbundet med skyld, frykt og skam. Det antas derfor at langt flere er utsatt for seksuell utpressing enn antallet som melder ifra til politiet tilsier.

Vurderinger

Norske gutter og menn har betalt flere tusen kroner til gjerningspersoner som har utsatt dem for seksuell utpressing. Det er *meget sannsynlig* at utpressere anser nordmenn for å være velstående og med betalingsevne, og at de vil fortsette å rette seg mot norske gutter og menn i 2024.

Utpressere har vist evne og vilje til å utvikle sin modus, og metodene som benyttes blir stadig mer kyniske, blant annet ved å rette seg mot yngre gutter og kreve høyere beløp. Det er *sannsynlig* at konsekvensene av utpressingen vil være alvorlige for de som rammes av kriminaliteten, både økonomisk, psykisk og emosjonelt. Det er *sannsynlig* at enkelte

norske fornærmede vil forsøke å ta livet sitt som følge av utpressing.

Det er *sannsynlig* at cyberkriminelle vil øke bruken av GKI i saker om seksuell utpressing med økonomisk motiv i 2024 og at bruk av GKI vil medføre at flere barn vil bli utsatt for seksuell utpressing med økonomisk motiv.

Utpressingstrender innen løsepengekrav

Kripos har observert at cyberkriminelle som opererer innenfor enkelte LSH-grupperinger er tilpasningsdyktige og har et bevisst forhold til hvilke taktikker og metoder som er best egnet for utpressing av fornærmede. Normalbildet blant løsepengevirusaktører er å stjele og kryptere data, etterfulgt av utpressing. Målutvelgelsen kan være tilfeldig, så vel som målrettet. Informasjon som stjeles fra fornærmedes systemer er ofte taushetsbelagt eller annen sensitiv informasjon. Hensikten er å kunne bruke dette for å legge ytterligere press på en fornærmet for å øke sannsynligheten for betaling.

Det er i de senere år observert at få norske virksomheter betaler løsepenger til cyberkriminelle. På samme tid erfares det at cyberkriminelle går lengre i sin virkemiddelbruk for å få betaling. Kripos observerte i 2023 en endring i utpressingsteknikker blant enkelte cyberkriminelle grupperinger som har rammet norske virksomheter.

Denne observerte utviklingen illustrerer cyberkriminelles tilpasningsdyktighet og dynamiske karakter. Det er eksempelvis sett tilfeller av datatyveri med løsepengevirus, men uten at krypteringsfunksjonen aktiveres. Datatyveriet har vært etterfulgt av utpressing med den stjålne informasjonen. Datatyveri uten gjennomført kryptering endrer selve gjennomføringen av et typisk løsepengekrav, og antyder at cyberkriminelle ser en stadig større verdi i informasjon.

En annen trend som er observert er at aktørene stjeler og krypterer dataen utenfor systemene til fornærmede. Dette omtales som fjernkryptering. Deretter følger utpressing med den stjålne dataen som pressmiddel.

Etter datatyveri har gjerningspersoner i 2023 også utført påfølgende tjenestenektangrep mot virksomheter som et ekstra ledd i utpressingen. I tillegg er det observert at gjerningspersonen har tatt kontakt med virksomheten via telefon for ytterligere press. Samlet omtales dette som trippel utpressing.

Det er observert at enkelte løsepengevirusaktører publiserer stjålne data på det åpne nettet. Dette kan utgjøre en økt risiko for gjentagende cyberangrep mot

en virksomhet ved at den stjålne dataen er lett tilgjengelig for alle på internett og har kort nedlastingstid sammenlignet med data på det mørke nettet.

Det er observert at ulike løsepengevirusaktører har kontaktet virksomheter, hevdet at de har stjålet data fra systemene deres og fremsatt krav om løsepenger. Etter undersøkelser av egne systemer har det ikke vært funnet tegn på datainnbrudd eller datatyveri. Det kan være flere årsaker til dette som viser til en interessant utvikling som er verdt å merke seg.

Vurderinger

Lavere betalingsvillighet blant virksomheter som blir utsatt for løsepengevirus bidrar *meget sannsynlig* til at cyberkriminelle vil fortsette å ta i bruk nye og kreative virkemidler i sin utpressing av norske virksomheter for å øke sannsynligheten for betaling av løsepengekrav.

Det er *sannsynlig* at flere LSH-aktører har økt sin fleksibilitet når det kommer til taktikker og metoder for å hente ut data og presse fornærmede. Dette er *mulig* et resultat av økt sikkerhetskultur og -bevissthet i virksomheter, herunder bedre rutiner for sikkerhetskopiering, samt en økt forståelse for verdien av informasjon blant de cyberkriminelle. KI vil bidra til å forenkle og automatisere prosessen med å identifisere verdifull informasjon i fornærmedes systemer.

I tilfeller hvor sensitiv informasjon ikke er på avveie og kritiske prosesser forblir upåvirket av et løsepengevirus, vil bedre rutiner for sikkerhetskopiering *sannsynlig* redusere virksomheters betalingsvilje.

Løsepengevirus bygget på lekkede kildekoder, sammen med bruk av GKI, kan *mulig* indikere at det er uerfarne cyberkriminelle uten særlige forkunnskaper som står bak løsepengevirusangrepet. Det er *mulig* at disse aktørene velger nye metoder og utpressingstaktikker i mangel på teknisk kompetanse og cyberkriminell erfaring.

Utviklingen innen utpressing i LSH vil *sannsynlig* bidra til å endre behovet for verktøy og kompetansekrav for løsepengevirusaktører, fra kryptering og dekryptering til aksessetablering.

Det er *sannsynlig* at flere LSH-grupperinger har en økt bevissthet rundt hvilke mål som er mest sårbare og derfor mest lønnsomme. Bedrifter som ikke har, eller ikke prioriterer ressurser til å beskytte sine verdier, vil være spesielt sårbare for angrep. Ofte er dette små eller mellomstore bedrifter.

Påvirkningen fra kunstig intelligens

Teknologi driver frem endringer i det digitale trussellandskapet. Til tross for at utviklingen innen KI har vært under opptrapping de siste 60 årene, var 2023 året da kunstig intelligens for alvor trådte inn i det offentlige ordskiftet. Debatten har vært preget av lovnader og bekymringer knyttet til teknologiens potensial på den ene siden, og skeptikere som belyser teknologiens begrensninger på den andre siden. Diskursen har en tendens til å svekke forståelse av teknologiens kapabiliteter i dag, samt betydningen dette kan ha for fremtidige muligheter og trusler. Utviklingen de senere årene og allmenninteressen for KI utgjør en egen drivkraft som dytter teknologiselskaper, forskningsmiljøer og nettsamfunnet til nye oppdagelser. For myndigheter har dette ført til politisk enighet om sterkere regulering både nasjonalt og internasjonalt.

KI-kapabiliteter

Til tross for at dagens KI-systemer 🗝 har åpenbare begrensninger, ligger teknologiens potensial for cyberkriminalitet i dens hastighet, hukommelse og nesten ubegrensede utholdenhet. I en forestilt fremtid hvor KI-systemer ikke bare beregner, men også *forstår*,[49] vil trusselen fra teknologien utgjøre en vesen-

> Kunstig intelligens kan understøtte alle kriminalitetsområder og ramme individer, organisasjoner og stater. KI medfører en styrking og endring i utførelsen av kriminalitet. Styrkingen oppstår basert på automatisering, effektivisering og økende grad av autonomi, mens endringen primært omfatter generell kvalitetsforbedring og ressursoptimalisering. Utfallet er en økning i cyberkriminelles kapabiliteter, og et potensial til å ramme fornærmede i stor skala og høyt tempo, med stor grad av spesialtilpasning.

49 KI bygger på statistiske utregninger og programmatiske resultater gjennom å identifisere mønstre i data. Til tross for likheter mellom sluttproduktet av menneskelig og maskingenerert innhold, er prosessen for å komme frem til sluttproduktet svært ulikt. For at et KI-system skal forstå på samme måte som mennesker, forutsetter dette en grunnleggende endring i hvordan teknologien fungerer

sendring. Dette er imidlertid en av mange forestilte fremtidsscenarioer ettersom teknologien har stort potensial. Til tross for en mengde spekulasjoner om mulige utfall, er det viktig å vurdere trusselen basert på teknologien slik den er i dag.

Et av de mest fremtredende eksemplene på anvendelsen av KI er generativ kunstig intelligens (GKI). GKI, en undergruppe av KI-systemer, er trent på omfattende datasett fra ulike kilder og kan generere variert innhold fra grunnlagsmodeller 🗝 basert på forespørsler fra brukeren. Siden introduksjonen av ChatGPT i november 2022 har interessen for slike grunnlagsmodeller økt betydelig, parallelt med en utvikling mot stadig mer multimodale[50] funksjoner. Denne utviklingen muliggjør stadig mer komplekse interaksjoner med grunnlagsmodeller og bidrar til en betydelig reduksjon i kompetansekrav, kostnader og tidsbruk for å begå enkelte cyberkriminelle handlinger.

Kommersielle versus uregulerte grunnlagsmodeller

Kripos har tidligere vurdert at uregulerte grunnlagsmodeller[51] utgjør en større trussel enn regulerte, kommersielle grunnlagsmodeller[52]. Selv om kommersielle modeller for øyeblikket er de mest avanserte, har de innebygde sensureringsmekanismer for å hindre misbruk og uønsket atferd. Selv om det finnes metoder for å omgå disse sensurinnretningene, forblir kildekoden og treningsgrunnlaget utilgjengelig for offentligheten. Risikoen øker imidlertid betydelig dersom kildekoden til slike modeller skulle bli lekket eller gjort offentlig tilgjengelig. Dette ville tillate fjerning av sensureringsmekanismer, samt tilpas-

50 Refererer til KI-systemer som kan ta imot, bearbeide, og generere informasjon på tvers av flere forskjellige medietyper (eks: tekst, kildekode, bilde, lyd, eller video). Dette innebærer at grunnlagsmodeller kan integrere og koordinere data fra flere forskjellige kilder

51 Brukes i denne sammenheng om grunnlagsmodeller med åpen kildekode som kan lastes ned og brukes uten krav til internettilkobling eller behov for registrering av brukerkontoer hos en leverandør

52 Ofte omtalt som proprietære grunnlagsmodeller der bruken er gratis eller tilgjengelig gjennom betalingsløsninger, men kildekoden og treningsgrunnlaget er en bedriftshemmelighet

ning[53] av modellene for kriminelle formål. I dag kreves det imidlertid betydelig maskinkraft og spesialisert kompetanse for å implementere, tilpasse, validere og vedlikeholde grunnlagsmodeller med tilsvarende størrelse og kapabilitet som de mest avanserte modellene, selv når kildekoden er åpent tilgjengelig.

Som med andre digitale verktøy som automatiserer og forbedrer operasjoner i cybersikkerhetsbransjen, har grunnlagsmodeller også en mørk slagside som utnyttes av cyberkriminelle. Det finnes flere eksempler på modeller spesifikt utviklet og markedsført for kriminell bruk. Disse inkluderer mindre, spesialiserte modeller[54] for konkrete oppgaver som passordgjetting, koding eller tale og tekstgenerering til phishing-kampanjer. Slike spissede modeller krever stadig færre ressurser for utvikling og bruk, og kan operere uavhengig av tredjepartsleverandører.

KI-agenter

I likhet med uregulerte grunnlagsmodeller, representerer også kunstig intelligente agenter (KI-agenter 🗝) en betydelig trussel dersom de misbrukes til cyberkriminelles formål. Disse agentene er avanserte problemløsere som tilpasser seg og reagerer på komplekse, skiftende miljøer eller datamengder. KI-agenter skiller seg fra grunnlagsmodeller ved deres evne til å kontinuerlig trekke slutninger og utlede nye gjøremål for å oppnå definerte mål. KI-agenter løser flere oppgaver simultant, tilpasser seg basert på tilbakemeldinger fra omgivelsene, og endrer handlingsforløp for å nærme seg en ønsket sluttilstand.

Eksempler på slike KI-systemer i dag spenner fra selvkjørende biler til digitale agenter i bærbare enheter og på nett. Noen av gjøremålene som utføres av KI-agenter er kontroll over datamaskiner, nettlesere, applikasjoner, og lesing og skriving av filer[55]. De kan også dele ut oppgaver til andre grunnlagsmodeller

53 Ofte omtalt som finjustering. Dette innebærer at forhåndstrente modeller blir trent videre på små datasett spisset mot et bestemt formål. Eng: Fine-tuning eller Re-training

54 Eng: Narrow AI eller Weak AI

55 Filer kan i denne sammenheng være digital informasjon som programvare, tekstfiler, bilder, musikk eller annet innhold som kan lagres på en lagringsenhet

Politiet kan også stå overfor syntetiske bilder som er så realistiske at de vanskelig kan skilles fra ekte overgrepsmateriale, som kan medføre forsøk på å identifisere barn som ikke finnes.

Foto: Laget med KI

eller hente informasjon fra menneskelige kilder.

Innen cybersikkerhet demonstrerer KI-agenter en betydelig kapasitet gjennom proaktiv oppdagelse av trusler og dynamiske sikkerhetstiltak, noe som potensielt øker effektiviteten av mottiltak betydelig. Kompleksiteten knyttet til å forutse sluttresultatet øker når KI-agenter som er programmert til å forhindre trusler interagerer med agenter med ondsinnede intensjoner. Dette kan skje helt uten menneskelig inngripen eller overvåking. Et slikt scenario kan overføres til etterforskning i politiet som ønsker å ta i bruk KI til å straffeforfølge cyberkriminelle, samtidig som cyberkriminelle ønsker å ta i bruk KI for å unngå straffeforfølgelse. Kripos har foreløpig ikke observert KI-agenter som utfører handlinger til å understøtte cyberkriminalitet.

Kriminelle anvendelsesområder

Grunnlagsmodeller kan generere innhold som i seg selv er ulovlig, som oppfordringer til vold eller syntetiske seksualiserte fremstillinger av barn. De kan også brukes til å understøtte ulike cyberkriminelle aktiviteter som å generere tekst eller tale til bruk i sosial manipulasjon eller å generere skadevarekode. Som følge av at grunnlagsmodellene utgjør en ny sårbarhetsflate kan cyberkriminelle også angripe teknologien. Dette kan føre til nye metoder for digital utpressing, data-tyveri og skadeverk.[56]

Deepfakes er et potent verktøy som brukes til å spre desinformasjon, forlede, generere seksualisert innhold og presse fornærmede til å gjøre handlinger de ellers ikke ville gjort. Gitt muligheten til å produsere troverdig innhold, sammen med utfordringer knyttet til effektiv deteksjon av syntetiske tekst- og mediefiler, utnytter cyberkriminelle avstanden mellom rask teknologisk utvikling og samfunnets tregere tilpasningsevne. Eksempler inkluderer kloning av stemmer for bruk i direktørsvindel og utpressing, eller troverdige videoer av myndighetspersoner som formidler falske budskap.

56 Utnyttelse av disse sårbarhetene utgjør store potensielle belønninger med relativt lave risikoer. En bekymring er at personlig identifiserbar informasjon eller annen sensitiv informasjon som grunnlagsmodeller er trent på, kan komme på avveie

GKI bidrar til å redusere ressurs- og kompetansegapet mellom aktører med ulike roller ved å gjøre avanserte og tidkrevende operasjoner tilgjengelige med færre ressurser. Et slikt eksempel, gjennom foreløpig ulovfestede handlinger, er spredning av desinformasjon fra trollfabrikker 🗝.

Samfunnet, som er avhengig av tillit til informasjonens autentisitet og opphav, står overfor økte utfordringer i å skille mellom ekte og falskt innhold. Ved bruk av GKI kan kriminelle handlinger og aktiviteter som tidligere har krevd betydelige menneskelige og økonomiske ressurser, og derfor ofte har vært forbundet med terrororganisasjoner og statlige aktører, utrettes av én enkelt aktør med begrensede ressurser. Kapabiliteten til grupper og organisasjoner med store ressurser oppskaleres tilsvarende. Dette representerer et potensial til å øke størrelse, kompleksitet, spredning og varighet av desinformasjonskampanjer. Uten effektive mottiltak kan GKI bidra til å svekke tilliten til informasjon ytterligere.[57]

Generativ kunstig intelligens i seksuallovbrudd

I 2023 så norsk politi flere tilfeller av at bilder av voksne personer ble brukt til å lage falske nakenbilder ved bruk av KI. Politiet mottok også de første rapportene om syntetisk overgrepsmateriale 🗝 generert av norske gjerningspersoner.

Gjerningspersoner som ønsket å generere overgrepsmateriale ved bruk av KI-modeller diskuterte fremgangsmåter og ga hverandre tilbakemeldinger på ulike fora på det mørke nettet.

Modeller som er trent på voksenpornografisk materiale og modeller som er trent på ikke-seksualiserte bilder og video av barn kan kombineres for å produsere syntetisk overgrepsmateriale av prepubertale barn, slik at det ikke er nødvendig for gjerningspersonene å trene modellene på ekte overgrepsmateriale. Samtidig vil gjerningspersoner trene egne modeller på eksisterende overgrepsmateriale. Dette kan føre til at barna i det syntetiske materialet som produseres er svært like ekte barn, både barn som har vært utsatt for overgrep og barn som aldri har vært det. Politiet

57 Rapport: Kripos, Generativ kunstig intelligens og cyberkriminalitet, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/etterretningsrapport-generativ-kunstig-intelligens-kripos.pdf

kan også stå overfor syntetiske bilder som er så realistiske at de vanskelig kan skilles fra ekte overgrepsmateriale, som kan medføre forsøk på å identifisere barn som ikke finnes. GKI kan brukes til å maskere ekte overgrepsmateriale slik at deteksjonsmekanismer vil klassifisere materialet som syntetisk. Dette kan innebære at politiet ikke vil gjøre forsøk på å identifisere de avbildede barna fordi materialet fremstår syntetisk.

KI muliggjør at gjerningspersoner lettere kan finne arenaer hvor barn oppholder seg på internett, samt tilegne seg kunnskap om hvordan aktuelle spill- og kommunikasjonsplattformer fungerer. Videre finnes det grunnlagsmodeller som bruker dyp læring for å analysere og forstå skriftspråk[58], og som på den måten kan hjelpe brukeren med tilpasning av språk, ord og uttrykk for å effektivt tilnærme seg barn på internett.

KI kan brukes til å oppdage og avverge at cyberkriminelle med seksuell interesse for barn tilnærmer seg disse på internett. Politiet jobber tett med cybersikkerhetsfirmaet AIBA, som har utviklet et KI-verktøy som blant annet har til hensikt å detektere og avverge cybergrooming[59], før dialogen rekker å utvikle seg til noe straffbart.

Vurderinger

Grunnlagsmodeller gjør kriminelle handlinger som planlegging, rekognosering og målutvelgelse lettere å utføre og mer effektive. Disse forholdene, sammen med en økt psykologisk distanse til fornærmede gjennom mer autonome prosesser, vil *meget sannsynlig* føre til en økning i antall cyberkriminelle og deres kapabiliteter.

Det er *sannsynlig* at kapabilitetsgapet mellom cyberkriminelle og statlige aktører reduseres som følge av utviklingen innen kunstig intelligens.

Det er *meget sannsynlig* at cyberkriminelles bruk av KI-agenter på sikt vil utgjøre en større trussel enn cyberkriminelles bruk av grunnlagsmodeller isolert sett. Det er imidlertid *lite sannsynlig* at cyberkriminelles bruk av KI-agenter vil utgjøre en betydelig trussel i løpet av 2024.

---

58 Et eksempel på en slik type grunnlagsmodell er Eng: Large Language Models (LLM)

59 Låneord fra engelsk. Definert som en prosess der en voksen person tar kontakt med barn (og ofte utgir seg for å være med en annen/yngre person) der målet er å begå seksuelle overgrep

> Et vellykket cyberangrep mot IKS vil kunne medføre umiddelbar konsekvens for operasjonell teknologi, omgivelsene og menneskeliv

Foto: Laget med KI

Grunnlagsmodeller, fremgangsmåter og eventuelle datasett som benyttes for å spisse KI-systemer til kriminelle formål vil *meget sannsynlig* deles og selges på det åpne og mørke nettet. Det er *meget sannsynlig* at flere og mer kapable grunnlagsmodeller som er utviklet og spisset til kriminell bruk kan kjøres på én enkelt datamaskin.

Det er *meget sannsynlig* at GKI vil brukes til å automatisere opprettelse og vedlikehold av massive mengder digitale profiler for fiktive personer og virksomheter. GKI kan over måneder og år utføre troverdig aktivitet gjennom disse profilene, og slik bygge plausible identiteter som kan benyttes til ulike typer påvirkning og kriminalitet. Det er *sannsynlig* at slike identiteter vil bli en handelsvare.

Store datasett bestående av sensitiv og annen verdifull informasjon vil *meget sannsynlig* bli mer ettertraktede mål for datatyveri. Slike datasett kan brukes til trening av modeller eller som inndata for å trekke ut sammenhenger som er vanskelig tilgjengelig for ufaglærte. Eksempelvis vil det være nyttig for cyberkriminelle å bruke GKI til å hente ut og sammenstille relevant informasjon fra store databaser som offentlige helseregistre, valgregistre, folkeregistre, oversikter over rettssaker og domfellelser, eller registre over kritisk infrastruktur.

Det er *meget sannsynlig* at det i løpet av 2024 vil genereres syntetisk overgrepsmateriale i form av bilder, av barn i alle aldre. Det vil være umulig for mennesker å skille mellom ekte og syntetisk overgrepsmateriale.

Det er *sannsynlig* at KI-verktøy vil benyttes av gjerningspersoner til å komme i kontakt med barn på internett, både ved å tilegne seg kunnskap om arenaer barn bruker, og ved tilpasning av språk og sjargong.

Det er *lite sannsynlig* at nye typer innhold med kriminell nytteverdi vil bli generert av GKI.

Den cyber-fysiske koblingen

Cyber-fysiske systemer

Tradisjonelt har informasjonsteknologi (IT) blitt sett på som et avskåret domene som byr på særegne utfordringer, muligheter og avhengigheter. Etter hvert som teknologien har utviklet seg har menneskelige behov drevet utviklingen i retning av økt integrering av datamaskin- og nettverksteknologi med fysiske prosesser. Fenomenet omtales som den cyber-fysiske koblingen og inkluderer en rekke teknologier som vi tar for gitt i hverdagen, eksempelvis assistert bilkjøring, det moderne strømnettet og hurtig varetransport. Utviklingen medfører en rekke fordeler som mer automatiserte

prosesser, enklere arbeidsflyt og økt trygghet i produksjon, men også nye avhengigheter og sårbarhetsflater som kan utnyttes av cyberkriminelle.

Moderne industri er avhengig av den cyber-fysiske koblingen i ulik grad. Fabrikkproduksjon, energiforsyning, maritim næring eller mat- og drikkeproduksjon er eksempler på dette. Ofte er disse virksomhetene definert som grunnleggende nasjonale funksjoner eller utgjør et ledd i forsyningskjeder 🗝 som understøtter nasjonale sikkerhetsinteresser. Den generelle utviklingen de siste 25 årene viser en økt avhengighet av IT for å produsere, levere og vedlikeholde fysiske varer og tjenester.

Det er ikke bare operasjonell sektor og nasjonal infrastruktur som er avhengige av den cyber-fysiske koblingen. Det produseres stadig flere fysiske enheter som er designet for å kobles til internett og kommunisere med omverdenen. Dette konseptet omtales ofte som tingenes internett[60] som gjenkjennes i en rekke forbruksvarer som husholdningsapparater, underholdningsenheter, og helseovervåkning, i tillegg til energiadministrasjon og klimakontroll.

I dag er flere milliarder slike enheter tilkoblet internett, en utvikling som har vært i stabil vekst de senere årene, og de utgjør en stadig større del av våre daglige liv. I tillegg til å gjøre hverdagen enklere, tryggere og mer effektiv, representerer tingenes internett også en stadig økende sårbarhetsflate. En sentral bekymring er at disse enhetene som regel ikke er designet med sikkerhet som prioritet. Dette gjør det krevende å holde oversikt over mulige sårbarheter, samtidig som det er utfordrende å feilrette 🗝 sårbarhetene som enhetene medbringer. Økt teknologisk avhengighet, lange og komplekse leverandørkjeder, mangfoldig utvalg og produktutvikling drevet av markedsetterspørsel fremfor helhetlige sikkerhetskrav, er viktige årsaker som utgjør trusselen fra kriminelles misbruk av teknologien. Forskere har i forskningsprosjekter tatt over kontrollen av kjørende biler og utnyttet svakheter i medisinsk utstyr[61], noe som illustrerer teknologiens skadepotensial., Det er derfor viktig å ta med seg at mulighetene for misbruk er på linje med mulighetene for legitim bruk.

60 Eng: Internet of Things (IoT)

61 For eksempel pacemakere, defibrillatorer og insulinpumper

Trusselen mot industrien

Over lengre tid har operasjonell teknologi (OT 🗝) blitt utsatt for ulike former for forstyrrelser fra trusselaktører. Eksempler på dette er driftsforstyrrelser som følge av løsepengevirusangrep[62] eller direkte manipulasjon av fysiske prosesser gjennom spesialtilpasset skadevare[63]. På et overordnet nivå kan trusselen mot industrien deles inn i to hovedkategorier: trusselen mot **fysiske prosesser** gjennom cyberrettet skadeverk på OT, og trusselen mot **digitale prosesser** gjennom cyberrettet skadeverk på IT.

I konteksten av cyberrettet kriminalitet, er direkte påvirkning på fysiske prosesser ofte et resultat av spesialutviklet skadevare som rammer driften gjennom de dypeste lagene[64] i OT-miljøet 🗝. De mest sentrale systemene i OT-miljøet er industrielle kontrollsystemer (IKS 🗝), som gir trusselaktører muligheten til å påvirke maskinvare og datakommunikasjon som er involvert i fysiske prosesser. Et vellykket cyberangrep mot IKS vil kunne medføre umiddelbar konsekvens for operasjonell teknologi, omgivelsene og menneskeliv. Historien har vist at det krever både spisskompetanse, tid og betydelige ressurser for å utvikle IKS-spesifikk skadevare, en kapabilitet som så langt har vært forbeholdt statlige aktører. Det er foreløpig et fåtall unike IKS-spesifikke skadevarer som er observert «i det fri» 🗝.

Påvirkning på digitale prosesser innebærer at en trusselaktør får tilgang til IT-systemene til virksomheten, uten nødvendigvis å kunne påvirke fysiske prosesser direkte. Slike angrep vil likevel ofte ha en indirekte påvirkning på OT-miljøet gjennom å utilgjengeliggjøre informasjon og forhindre kommunikasjon mellom systemer og mellom systemer og mennesker[65]. Dette påvirker virksomhetens evne til å opprettholde produksjon og vil i de fleste tilfeller få konsekvenser for flere ledd i forsyningskjeden. Skade-

62 Eksempel: Løsepengevirus mot Norsk Hydro (2019) og Colonial Pipeline (2021)

63 Eksempel: Stuxnet (2010) og Industroyer2 (2022)

64 Det er vanlig å dele OT-miljø inn i flere lag som strekker seg fra fysiske enheter og maskineri på laveste nivå, gjennom kontrollsystemer og overvåkingsfunksjoner, til planlegging og bedriftsledelse på de øverste nivåene

65 Fører til tap av overvåkningsmuligheter og kontroll over OT-systemer. Eng: Loss of View og Loss of Control

vare og annen uautorisert tilgang som har til hensikt å ramme virksomhetens IT-systemer kan i noen tilfeller også føre til påvirkning på fysisk prosesser. Enten ved at bedriften selv stenger ned produksjon som et skadebegrensende tiltak, eller ved at skadevaren inneholder egenskaper som gjør den i stand til å bevege seg mellom sikkerhetssoner i et nettverk og på den måten påvirke IKS direkte. Påvirkning på fysiske prosesser kan være uforutsette egenskaper ved løsepengevirus som gjerne har begrenset påvirkningsmulighet på IKS. Som følge av opportunistiske angrepsmodi kan løsepengevirus allikevel få utilsiktede konsekvenser for den fysiske driften. Imidlertid er den mest vanlige konsekvensen av påvirkning på digitale prosesser knyttet til bedriftens evne til å produsere og levere varer og tjenester, som regel med konsekvenser for forsyningskjeden og samfunnet for øvrig.

Ingen OT-miljø er identiske. Forskjellen ligger primært i hvordan systemene er satt sammen og tilpasset lokale behov. Høye kompetansekrav innen både IT og OT, samt behovet for grundig planlegging og rekognosering, er nødvendig for å oppnå direkte påvirkning på fysiske prosesser. Cyberkriminelles utfordringer forbundet med å skaffe tilgang til skjermet IKS, sammen med kompetansekrav for å utnytte detaljert kunnskap om spesifikke OT-systemer, bidrar til å vanskeliggjøre påvirkning på fysiske prosesser. Løsepengevirus utgjør dermed flertallet av cyberangrep mot industrien, og flere kjente eksempler viser at løsepengevirus kan få alvorlige konsekvenser for virksomheten.[66] Selv om fysiske prosesser ikke blir rammet direkte, kan et vellykket løsepengevirusangrep føre til produksjonsstopp og store kostnader for gjenopprettelse av driften. Et nyere eksempel er løsepengeviruset som rammet Tomra i juli 2023.

Vurderinger

Det er *sannsynlig* at påvirkning på digitale prosesser, gjennom løsepengevirus, vil ramme norske OT-avhengige virksomheter i løpet av det kommende året. Det er *meget sannsynlig* at norsk næringsliv vil bli indirekte berørt som følge av cyberangrep på industrivirksomheter i andre land i løpet av 2024.

Det er *sannsynlig* at OT-avhengige

66 Eksempel: DP World Australia (2023), Colonial Pipeline (2021), JBS foods (2021), Maersk (2017)

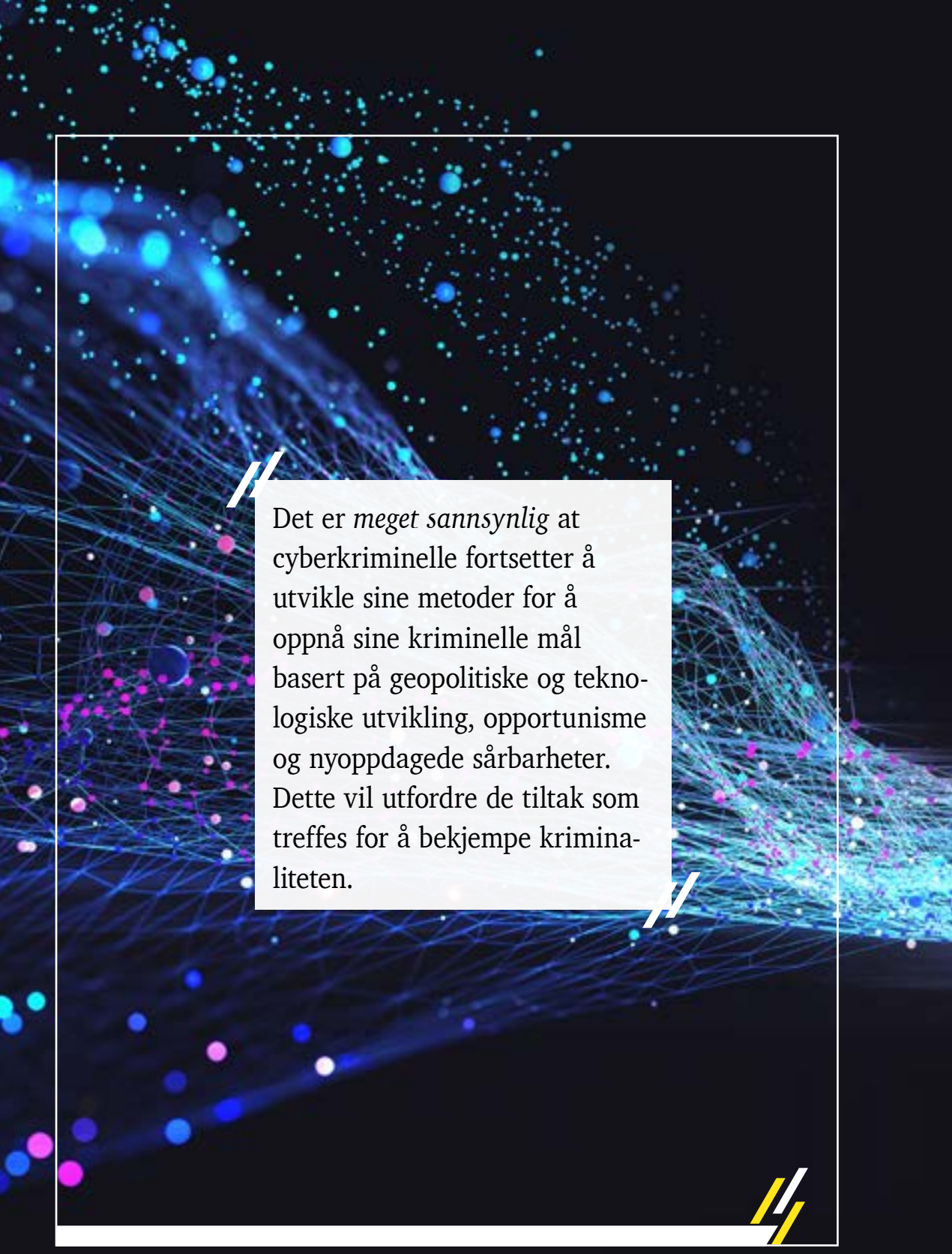
virksomheter er spesielt utsatt for påvirkning på digitale prosesser som følge av at betalingsvillighet øker med lange leverandørkjeder og avhengighet av automasjon. Det er *meget sannsynlig* at cyberkriminelle aktører vil fortsette å utvikle nye utpressingsmetoder for å øke betalingsvilligheten blant OT-avhengige virksomheter.

Det er *mulig* at påvirkning på digitale prosesser i OT-avhengige virksomheter vil få uintenderte konsekvenser for fysiske prosesser.

Det er *meget sannsynlig* at ressurs- og kompetansekrav for å utvikle IKS-spesifikk skadevare reduseres som følge av utviklingen innen kunstig intelligens, sammen med allerede kjente IKS-spesifikke skadevarer der kildekoden er offentlig tilgjengelig. Grunnet særegenhet og lokale tilpasninger i OT-systemer vil det fremdeles være krevende å utplassere og utføre IKS-spesifikk skadevare.

Med økt digitalisering og reduserte ressurs- og kompetansekrav for å utvikle IKS-spesifikk skadevare er det *mulig* at profittmotiverte kriminelle vil benytte IKS-spesifikk skadevare for å øke presset mot- og betalingsvilligheten blant industrivirksomheter, i løpet av de neste tre årene. Det er *sannsynlig* at et bevisst forhold til terskelen for iverksettelse av offensive mottiltak fra myndighetene, reduserer cyberkriminelles villighet til å ramme OT-systemer i samfunnskritiske virksomheter.

Det er ikke åpenbart hvordan profittmotiverte kriminelle kan dra økonomisk fordel av fysisk påvirkning, ettersom denne typen angrep vanligvis resulterer i nedstengning av systemene og etterlater lite rom for en forhandlingssituasjon. Det er allikevel *mulig* at profittmotiverte kriminelle kan true med å offentliggjøre eller selge kritiske sårbarheter til andre aktører og på denne måten presse virksomheter til å betale løsepengekrav.



Det er *meget sannsynlig* at cyberkriminelle fortsetter å utvikle sine metoder for å oppnå sine kriminelle mål basert på geopolitiske og teknologiske utvikling, opportunisme og nyoppdagede sårbarheter. Dette vil utfordre de tiltak som treffes for å bekjempe kriminaliteten.

Foto: Shutterstock

Ventet utvikling 2024

Det er *sannsynlig* at vi vil se en mengdeøkning av cyberkriminalitet innen alle kriminalitetstyper i 2024. Det er *meget sannsynlig* at cyberkriminelle fortsetter å utvikle nye metoder for å oppnå sine kriminelle mål basert på geopolitisk og teknologisk utvikling, opportunisme og nyoppdagede sårbarheter. Dette vil utfordre de tiltak som treffes for å bekjempe kriminaliteten. Det er behov for et generelt kunnskapsløft og disiplinert sikkerhetskultur for hva gjelder cybersikkerhet på alle nivåer i det norske samfunnet. Mer og kvalitetsmessig bedre samarbeid og informasjonsdeling mellom risikoeiere og sikkerhetsmiljøene er en forutsetning for å danne seg en helhetlig forståelse av trusselen. Det er *sannsynlig* at bedret samarbeid vil redusere skadevirkningene fra cyberkriminalitet.

Cyberkriminaliteten treffer nivåene i samfunnet på ulike måter. Fra bedrageri eller deling av seksualisert materiale av mindreårige på individnivå, nye metoder for å presse virksomheter til å betale løsepengekrav på organisasjonsnivå, til behov for internasjonal lovgivning og regulering av ny teknologi som vil påvirke samfunnet som helhet. Kripos vil særlig trekke frem de elleve driverne[67] for cyberkriminalitet som gjør seg relevante for vurderingene på samtlige nivåer.

Trusselen mot samfunnet

Cyberkriminalitet utgjør en kompleks trussel, den rammer på tvers av samfunnssektorer og utfordrer derfor det norske sektorprinsippet. Dette må sees i sammenheng med totalforsvaret og samfunnsberedskapen.

KI vil *meget sannsynlig* utfordre tillit i samfunnet ved å problematisere hva som er ekte og hva som er syntetisk generert innhold. En økende grad av mistillit kan utnyttes av alle cyberkriminelle aktører og understøtte alle kriminelle formål der menneskelig oppfatning utgjør en sentral komponent.

67 Rapport: Kripos, Cyberkriminalitet 2023, side 14, https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Samtidig er det *sannsynlig* at utviklingen innen KI vil utfordre åpenhet i samfunnet. Informasjonens verdi øker med teknologiske kapabiliteter til å nyttiggjøre seg store datamengder. Eksempelvis er det *sannsynlig* at tilgjengelige offentlige registre på internett vil utgjøre nye sårbarheter som ikke var påtenkt på tidspunktet de ble tilgjengeliggjort.

Det er *sannsynlig* at utviklingen med lavere mediedekning og oppmerksomhet i befolkningen fremtvinger andre og mer aggressive handlemåter blant hacktivister for å oppnå ønsket effekt.

Den totale sårbarhetsflaten øker med den pågående digitaliseringen i samfunnet. Det vil bli vanskelig å holde oversikt over alle sårbarheter for alle endepunkt i alle virksomheter.

Digital sikkerhet blir i stadig større grad et kollektivt ansvar. Den økende tekniske avhengigheten mellom virksomheter fører til et større skadepotensial når én enkelt virksomhet blir utsatt for datainnbrudd. Det er *sannsynlig* at flertallet av norske virksomheter som blir rammet av datainnbrudd i 2024 blir rammet på bakgrunn av en kompromittert virksomhet i leverandørkjeden eller via en tjeneste fra tredjepartsleverandør.

Sårbarheter som ikke lar seg sikkerhetsoppdatere, kreative og opportunistiske cyberkriminelle og skadevarer som selges som handelsvare, gjør at OT-avhengige virksomheter som er knyttet opp mot grunnleggende nasjonale funksjoner og kritisk infrastruktur er særlig utsatt for cyberangrep.

Trusselen mot virksomheter

KI vil *meget sannsynlig* introdusere nye og per i dag ukjente sårbarheter som følge av at virksomheter tar i bruk teknologien, sammen med en økt kvalitet og effektivitet på cyberkriminaliteten.

Skytjenester fører til sentralisering av verdier og dermed til mer ettertraktede mål blant profittmotiverte kriminelle og statlige aktører. Dette vil *sannsynlig* medføre at cyberkriminelle legger ned større innsats i å bryte seg inn i skytjenestene. Det er *meget sannsynlig* at vi vil oppleve datainnbrudd mot- og datatyveri fra slike skytjenester. Det er *mulig* at slike datainnbrudd vil øke antall opportunistiske mål for cyberkriminelle.

Cyberkriminelle grupperinger vil fortsette profesjonaliseringen, noe som vil føre til effektivisering og bedre kapabiliteter innen cyberkriminaliteten. Profittmotiverte aktører vil *mulig* bli mer attraktive for andre trusselaktører som følge av profesjonaliseringen, og på den måten forsterke verdien av kriminalitet som handelsvare.

Det er *sannsynlig* at løsepengevirus-

grupperinger vil utvikle nye metoder for å presse fornærmede. Eksempelvis kan cyberkriminelle true med å selge stjålne forretningshemmeligheter til statlige virksomheter for å øke betalingsvillighet blant fornærmede.

Trusselen mot enkeltpersoner

Det er *sannsynlig* at KI vil føre til at stadig flere enkeltpersoner blir utilsiktet skadelidende som følge av automatisering og spesialtilpasning av cyberkriminaliteten. Det er *sannsynlig* at dette vil være spesielt gjeldende innenfor bedrageri og desinformasjonskampanjer.

Det er *sannsynlig* at forsøk på å utnytte enkeltpersoners fjerntilgang til sensitive virksomhetssystemer vil øke som følge av den trådløse hverdagen.

Det er *sannsynlig* at stadig mer avanserte og lett tilgjengelige anonymiseringstjenester vil gjøre det enklere for cyberkriminelle å operere fordekt.

Cyberstøttede seksuallovbrudd er en vedvarende høy trussel. Det er *sannsynlig* at gjennomsnittsalderen til gjerningspersoner og fornærmede vil være lavere i 2024 enn foregående år. Det er *meget sannsynlig* at seksuallovbrudd på ende-til-ende-krypterte meldingsplattformer vil øke i omfang og *sannsynlig* at bruksområdet for slike plattformer vil utvides. Det er *sannsynlig* at gjerningspersoner som bruker seksuallovbrudd som virkemiddel vil fortsette å utvikle modus i en grovere retning i form av for eksempel mer offensive overtalelsesteknikker og ved bruk av KI.

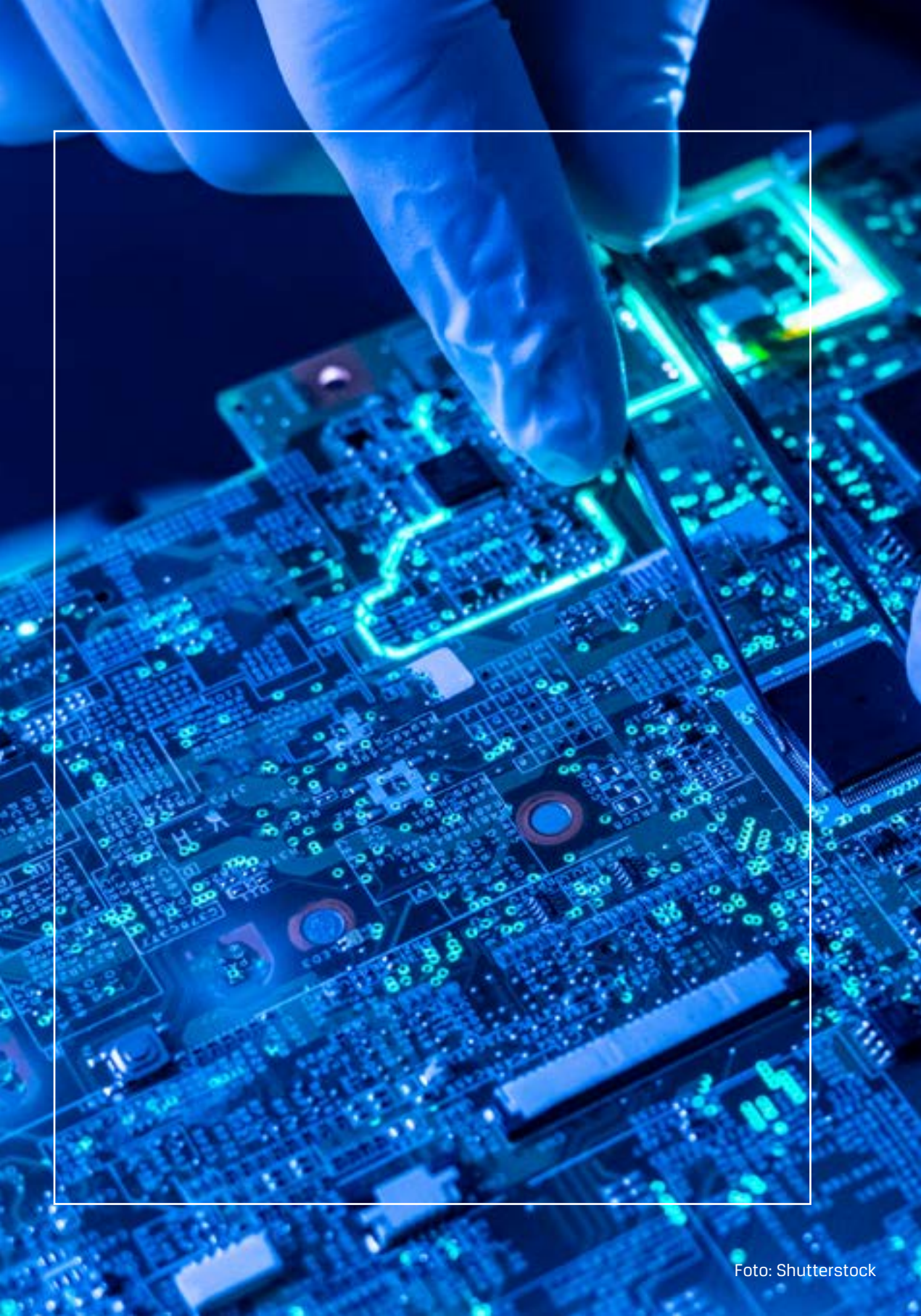


Foto: Shutterstock

Vedlegg

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%

Sannsynlighetsord

Vurderinger vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte, er det benyttet sannsynlighetsord (se tabell):

Begreper

Begrepsliste

🗝 **Det digitale rom** refererer oftest til en global helhet av sammenkoblede datasystemer og informasjonsressurser, og brukes som en metafor på linje med begrepet «det offentlige rom». I denne rapporten betegner det digitale rom helheten av datasystemer, nettverk, enheter og programvare hvor cyberkriminalitet begås.

🗝 **Datasystem** er én eller flere datamaskiner, programvarer eller annet datautstyr som kommuniserer i et digitalt økosystem.

🗝 **Internett** er et globalt nettverk av mindre digitale nettverk, systemer og enheter som er koblet sammen gjennom en felles kommunikasjonsprotokoll. Cyberkriminalitet finner sted i ulike deler av internett. Den delen av internett folk flest benytter kalles også det åpne nettet.

🗝 **Det dype nettet** er summen av alt på internett som ikke er indeksert og direkte søkbart ved bruk av standard søkemotorer. Det meste består av lovlig innhold, som adgangskontrollerte databaser og innhold bak betalingsmurer. 🗝 **Det mørke nettet** er en liten del av internett som består av nettverk som ofte bruker egne kommunikasjonsprotokoller. For å navigere i disse nettverkene kreves spesialisert programvare.

🗝 **Kriminalitetsfelt** benyttes i denne sammenheng om et overordnet saksfelt

som kan inkludere flere kriminalitetsområder innenfor samme domene. 🗝 **Kriminalitetsområde** er i denne sammenheng brukt til å gruppere beslektede kriminalitetstyper. Cyberrettet og cyberstøttet kriminalitet utgjør kriminalitetsområdene innenfor cyberkriminalitet. 🗝 **Kriminalitetstype** bygger på lovbruddsgruppene som danner registreringspraksisen i politiets strafferegister. I denne rapporten er begrepet utvidet til å inkludere cyberrelaterte kriminalitetstyper som datakriminalitet og digitalt skadeverk. Andre eksempler på kriminalitetstyper er seksuallovbrudd og økonomisk kriminalitet.

🗝 **Kapasiteter** henviser til kriminelles fysiske, mentale og digitale kvantifiserbare verdier, svært ofte volum, mens 🗝 **kapabiliteter** legger til grunn at både nødvendige kapasiteter og evnen til å utnytte dem er til stede.

🗝 **Handlemåter** benyttes om en bestemt fremgangsmåte som cyberkriminelle vanligvis følger for å oppnå sine mål. Det er altså rekkefølgen og metoden som anvendes for å utføre kriminelle handlinger. I andre sammenhenger blir kan operasjonsmønster eller Modus Operandi benyttet istedenfor handlemåter. En handlemåte bygger på en sammenstilling av 🗝 **cyberkriminelle handlinger**, eksempelvis datainnbrudd eller kontaktetablering med barn, og 🗝 **aktiviteter**, eksempelvis endre, slette eller tilføye data.

🗝 **Hendelser** benyttes i denne rapporten som en samlebetegnelse på cyberkriminalitet, enten cyberrettet eller cyberstøttet, og annen aktivitet som kan understøtte militære formål. Hendelser er ikke nødvendigvis omtalt i norsk straffelov, eksempelvis ved påvirkningsoperasjoner[68].

🗝 **Cyberangrep** benyttes i denne rapporten som en samlebetegnelse på cyberrettet kriminalitet som kan innebefatte datainnbrudd og/eller datatyveri og/eller digitalt skadeverk. Cyberangrep brukes om hendelser som enda ikke har inntruffet eller som ikke lar seg beskrive mer konkret. I tillegg til å falle innunder norsk straffelov, har cyberangrep også en militær slagside som eksempelvis sabotasje, her omtalt som digitalt skadeverk.

🗝 **Gråsoner** oppstår der ulike områder møtes. Grenselinjen mellom de ulike områdene kan være uklar av en rekke årsaker, og omtales da ofte som en gråsone.

68 Regjeringen har lagt frem et lovforslag om å kriminalisere skadelige påvirkningsoperasjoner i Norge. Pressemelding: Regjeringen, https://www.regjeringen.no/no/aktuelt/regjeringen-vil-kriminalisere-skadelige-pavirkningsoperasjoner-i-norge/id3021665/.

Gråsoner kan oppstå overalt. I rammen av denne rapporten henvises det til gråsonen mellom statlige og cyberkriminelle aktører, der like verktøy, metoder og aktiviteter kan gjøre det vanskelig å skille mellom aktørene. Dette utfordrer jurisdiksjon og politiets mandat.

🗝 **Trollfabrikker** er organisasjoner eller grupper som koordinerer og bruker internett for å påvirke offentlig mening og diskurs, ofte gjennom falske kontoer eller desinformasjon.

🗝 **Sosial manipulasjon** er en manipulasjonsteknikk som utnytter menneskelige feil for å få tilgang til privat informasjon, verdigjenstander eller annen tilgang. Eng: Social Engineering.

🗝 **Phishing** er et låneorrd fra engelsk som noen ganger er omtalt som nettfisking på norsk. Phishing refererer til metoder for å urettmessig tilegne seg andres persondata eller påloggingsdetaljer gjennom sosial manipulasjon, for eksempel gjennom e-post.

🗝 **Cyberrettet utpressing** er i denne rapporten benyttet som en samlebetegnelse for ulike modi innen cyberrettet kriminalitet, der profittmotiverte kriminelle begår handlinger for å presse fornærmede til å betale et løsepengekrav. Dette kan være, men er ikke begrenset til, løsepengevirusangrep. Andre eksempler kan være trusler om offentliggjøring av sensitiv informasjon eller syntetisk generert innhold.

🗝 **Cyberrettet skadeverk** benyttes i denne rapporten om cyberrettede kriminelle handlinger og aktiviteter som medfører skade på IKT, uten at det foreligger et åpenbart økonomisk motiv. Eksempler på dette kan være tjenestenektangrep utført av hacktivister eller sabotasje av kritisk infrastruktur.

🗝 **Tjenestenektangrep** har som formål å nekte, forstyrre eller forringe tilgangen til en server, tjeneste eller et nettverk. Eng: Denial-of-Service (DoS) Attack.

🗝 **Angrepskjeden** refererer til et rammeverk utviklet av Lockheed Martin for å identifisere og forhindre datainnbrudd og ondsinnet aktivitet i et nettverk. Rammeverket identifiserer hvilke steg en trusselaktør må utføre for å lykkes med å kompromittere et datasystem. Eng: Cyber Kill Chain.

🗝 **Forstyrrelser** benyttes i denne rapporten om summen av alle mottiltak fra sikkerhetsindustrien (lovlydige enkeltindivider, forskningsmiljøer eller offentlige og private virksomheter) som bidrar til å begrense cyberkriminelles handlingsrom. Forstyrrelser kan også oppstå som følge av forhold utenfor direkte påvirkning fra sikkerhetsindustrien. Eksempler på dette er interne rivaliseringer mellom cyberkriminelle grupperinger, geopolitiske forhold eller fysisk skade på IKT-utstyr. Denne typen forstyrrelser er ikke gjort rede for i denne rapporten.

🗝 **Aksjon** er et polisiært begrep som i denne rapporten brukes for å omtale politiets pågripelser og ransakinger, eller situasjoner der politiet på andre måter griper inn for å stanse en kriminell virksomhet.

🗝 **Cyberkriminelt økosystem** utgjør trussellandskapet der profittmotiverte kriminelle, seksuallovbrytere, aktivister, statlige aktører og terrorister opererer, samarbeider, samhandler, kommuniserer, deler, selger, kjøper, konkurrerer og kolliderer med hverandre.

🗝 **Cyberkriminelt nettverk** er en samling av enkeltindivider og/eller grupper som samarbeider, er gjensidig avhengige eller utveksler varer eller tjenester for å begå cyberkriminalitet.

🗝 **Cyberkriminell gruppe** er en samling av enkeltindivider som samhandler for å oppnå et felles mål/begå cyberkriminalitet.

🗝 **Kriminell og cyberkriminell** brukes begge som betegnelse på personer som utøver kriminalitet. Kriminell er domenenøytralt, mens cyberkriminell henviser til personer som begår kriminalitet i det digitale rom. 🗝 **Gjerningsperson** brukes også med samme mening for språklig variasjon, spesielt innen seksuallovbrudd.

🗝 **Motiv** benyttes for å beskrive hva en aktør ønsker å oppnå med kriminaliteten. Dette kan være et ønske om økonomisk gevinst, seksuell tilfredsstillelse, sosial endring, tilgang til sensitiv informasjon eller å påføre fysisk skade. En aktør omtales som motivert gjennom å forfølge et motiv. Eksempelvis en profittmotivert aktør. 🗝 **Motivasjon** refererer til den grunnleggende drivkraften bak aktørers handlinger. Motivasjon er ikke bare orientert rundt hva en aktør ønsker å oppnå (mål), men også den bakenforliggende årsaken til at aktøren ønsker å oppnå et gitt mål.

🗝 **Intensjon** benyttes i denne sammenheng om en overordnet og langtrekkende tilstand som en aktør retter sin vilje mot. Intensjon er ikke bare summen av flere konkrete planer og mål, men også et bilde på en ønsket sluttilstand.

🗝 **Gevinst** brukes som en samlebetegnelse for kriminell vinning og inntekt.

🗝 **Aktør** brukes som en generell betegnelse på både enkeltindivider og grupper. I tilfellet med grupper kan aktørbegrepet eksempelvis brukes om en konkret gruppering som begår løsepengevirusangrep. I slike tilfeller brukes «løsepengevirusaktører». 🗝 **Trusselaktør** brukes som en variasjon av aktørbegrepet og innebefatter statlig aktør, enkelte cyberkriminelle og cyberkriminelle grupperinger der konteksten er at disse utgjør en trussel.

🗝 **Statlig aktør** betegner nasjonalstater som utgjør en trussel eller som begår cyberkriminalitet.

🗝 **Hacktivist** er en aktør (enkeltperson eller gruppe) som begår kriminelle

handlinger i det digitale rom for å fremme et religiøst, politisk eller annet ideologisk budskap. Betegnelsen må ikke forveksles med «aktivist» som både er domeneuavhengig og som ikke indikerer at personen gjør noe kriminelt.

🗝 **Innsider** forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap.[69]

🗝 **Pengemuldyr** er enkeltpersoner som motvillig, velvillig eller gjennom overbevisning, stiller bankkonto til disposisjon som en mellomstasjon i en pengetransaksjon, eller som kjøper gavekort og sender disse til bakmenn. Eng: *Mule*.

🗝 **Stråperson** refererer til en person som opptrer som en front for noen andre i den hensikt å skjule den reelle kontrollen over en transaksjon eller eiendel. Stråperson gir personer et handlingsrom for å begå kriminalitet, ved at de blir «usynlige» for offentlige myndigheter

🗝 **Kjernegruppe** er en betegnelse på den innerste sirkelen av cyberkriminelle i et LSH-system. Varianten «LSH-gruppering» brukes også om kjernegruppen avhengig av kontekst.

🗝 **Affiliert** er en person som har en forretningsmessig tilknytning til en LSH-kjernegruppe og som benytter seg av løsepengevirus som handelsvare. Eng: *Affiliates*.

🗝 **Tilgangsmegler** brukes som en betegnelse for cyberkriminelle som stjeler og/eller selger stjålet informasjon og ulovlig aksess til datasystemer. Tilgangsmeglere er et eksempel på en profil som ofte forbindes med rollen «profittmotiverte kriminelle». Eng: *Initial Access Broker (IAB).*

🗝 **Leverandørkjede** omfatter alle ledd i kjeden av leverandører og underleverandører som leverer eller produserer varer, tjenester eller andre innsatsfaktorer som inngår i en virksomhets leveranse av tjenester eller produksjon av varer fra råvarestadiet til ferdig produkt.[70] **Forsyningskjede** benyttes i denne rapporten som summen av leverandørkjede og de interne prosessene i en virksomhet som utføres for å levere en vare eller tjeneste

69 Rapport: NSM, Innsiderisiko, https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf

70 Rapport: NSM, Risiko 2023, https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

til neste ledd i leverandørkjeden.

🗝 **Tredjepartsleverandør** er en virksomhet som leverer produkter eller tjenester på vegne av andre.

🗝 **Nulldagssårbarhet** er en sårbarhet i programvare som noen får kunnskap om, før produsenten/leverandøren eller brukerne av programvaren.[71]

🗝 **Sikkerhetsoppdatering** er prosessen med å anvende oppdateringer til programvare eller systemer. 🗝 **Feilretting** er å korrigere sikkerhetshull, reparere feil, forbedre funksjonaliteten eller øke systemets beskyttelse mot cyberangrep. Eng: Patching.

🗝 «**I det fri**» refererer til en virkelig trussel (ikke bare en teoretisk) som blir observert i den digitale verden og som potensielt kan utgjøre skade på datasystemer. Begrepet brukes ofte i sammenheng med nyoppdaget skadevare eller nulldagssårbarheter utenfor et kontrollert testmiljø. Eng: *In the Wild.*

🗝 **Proxy-tjenester** består av nettverk med flere servere som fungerer som mellomledd (noder) mellom internett-brukere og internett. Når internettbrukeren benytter en proxy-løsning skjules brukerens egentlige IP-adresse bak proxy-nodens IP-adresse. Destinasjonsområdet (internett-serveren) som er målet for brukerens datatrafikk vil på denne måten ikke registrere/logge brukerens egentlige IP-adresse. 🗝 **VPN-tjenester** tar det samme oppsettet et skritt videre ved å også kryptere datatrafikken mellom brukeren og nodene i VPN-løsningen. Det er denne krypteringen som utgjør forskjellen mellom proxy-nettverk og VPN. Denne rapporten omtaler proxy-nettverk og virtuelle private nettverk (VPN) som «løsning» eller «tjeneste». «Løsning» benyttes der proxy-nettverk og VPN omtales sammen, mens «tjeneste» viser til løsninger som driftes av en kommersiell aktør.

🗝 **Ende-til-ende-krypterte meldingsplattformer** benytter seg av ende-til-ende-kryptering. Det vil si at det kun er deltakerne i en lukket gruppe som sender meldinger til hverandre som har tilgang til meldingene. Meldingene og filene krypteres før de sendes over nettverket med en nøkkel som bare deles mellom sender og mottaker. Også lyd- og videokommunikasjon kan krypteres fra ende-til-ende.

🗝 **KI system** er en samlebetegnelse for ulik program- og maskinvare som utfører handlinger, fysisk eller digitalt,

71 Rapport: NSM, Nasjonalt digitalt risikobilde 2023, s. 10, https://nsm.no/getfile.php/1313382-1697777843/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf

basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål.[72]

🗝 **Grunnlagsmodell** er et KI-system som kan tilpasses en rekke ulike oppgaver slik som språkoversettelse, bilde- og lydanalyse, i tillegg til generative egenskaper. Disse modellene utgjør grunnlaget for en rekke KI-applikasjoner som OpenAI: ChatGPT, Google: Gemini og Midjourney. Eng: *Foundation Models*.

🗝 **KI-agenter** kan beskrives som et team av automatiske roboter, kjennetegnet ved høy effektivitet, utholdenhet, og evnen til å finne optimale løsninger på problemer. Sentrale egenskaper inkluderer interaktivitet, fleksibilitet, reaktivitet og proaktivitet. Eng: AI Agents eller Intelligent Agents (IA).

🗝 **Operasjonell teknologi (OT)** er den delen av cyber-fysiske systemer som involverer fysiske prosesser, ofte tilknyttet industriproduksjon eller andre omfattende fysiske prosesser som benytter datamaskin- og nettverksteknologi. Eng: *Operational Technology (OT).*

🗝 **Industrielle kontrollsystemer (IKS)** omtales i denne rapporten som et samlebegrep for enheter, protokoller og sensorer som virker sammen i et OT-miljø. Eng: *Industrial Control Systems (ICS).* 🗝 **OT miljø** refererer til både fysiske og digitale systemer som brukes til å drifte, overvåke, kontrollere og sikre industrielle operasjoner og fysiske prosesser.

🗝 **Fornærmede** brukes om alle som har blitt utsatt for kriminalitet eller uønsket påvirkning. 🗝 **Risikoeier** brukes om virksomheter som opererer med en risiko for å bli utsatt for kriminalitet. I noen tilfeller omtales også risikoeier som 🗝 **mål** for kriminalitet.

🗝 **Barn** brukes i rapporten om personer under atten år. Jenter og gutter brukes der kjønn angis og gjelder på samme måte personer under atten år. For mindreårige gjerningspersoner angis et skille mellom barn under atten år og under femten år, ettersom barn under femten år ikke kan straffes.[73]

🗝 **Overgrepsmateriale** eller 🗝 **seksualisert materiale av barn** er fremstillinger av seksuelle overgrep mot barn eller fremstillinger som seksualiserer barn under atten

72 Hentet fra Regjeringen, Nasjonal strategi for kunstig intelligens, s. 9, https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf

73 Straffeloven § 20 1. ledd bokstav a

år.[74] 🗝 **Syntetisk overgrepsmateriale** blir brukt som samlebetegnelse for alt materiale (bilder, video, tekst m.v.) som viser seksuelle overgrep mot barn eller på annen måte seksualiserer barn, som er generert med bruk av generativ kunstig intelligens.

Cyberkriminalitetens 11 drivere

Teknologiutvikling: Den teknologiske utviklingen gjør raske fremskritt og introduserer fortløpende nye muligheter og utfordringer for cyberkriminell aktivitet.

Lovregulering: Lovverk og reguleringer skaper og avgrenser handlingsrommet for både cyberkriminelle aktører og ordensmakten. Lovgivere er alltid på etterskudd.

Økonomi og kostnader: Den digitale økonomien gjør det mulig å gjennomføre økonomiske transaksjoner uten regulering. Den digitale økonomien skaper muligheter for profitt på nye måter.

Fordekt aktivitet og anonymiseringsteknologier: Avanserte anonymiseringsteknologier gjør det enkelt å opptre uten eller med falsk identitet, noe som forenkler en aktørs evne til å opptre fordekt.

Kriminalitet som handelsvare: Kjøp og salg av kriminelle tjenester, programvare og materiell er med på å gjøre kriminaliteten profitabel, finansiere ny kriminalitet og gjøre kriminalitet enklere tilgjengelig også for aktører som ikke kunne utøvet slik kriminalitet på egen hånd.

Bruk av digital infrastruktur: Den lette tilgangen til digital infrastruktur gjennom kjøp, leie eller tyveri gjør det enkelt å understøtte kriminelle handlinger med nødvendig digital infrastruktur uten store omkostninger.

Planlegging og målrettethet: Lett tilgjengelig informasjon i det digitale rom og kraftig maskinvare med velegnet programvare gjør planlegging og tilrettelegging enkelt for både opportunistiske og målrettede aktører.

Kommunikasjon: Sammenknyttet maskinvare ved hjelp av internettets kommunikasjonsprotokoller gjør rekkevidden global og man kan fleksibelt kommunisere sikkert med tekst, tale, video og data.

Koordinering: Evnen til å enkelt kommunisere sikkert og fleksibelt forenkler koordinering mellom mange aktører.

Påvirkning: Evnen til å enkelt kommunisere sikkert og fleksibelt gjør det mulig å påvirke både mennesker og datasystemer.

Deling av informasjon og data: Evnen til å lagre store mengder data på kraftig maskinvare, kombinert med evnen til å enkelt kommunisere sikkert og fleksibelt, muliggjør effektiv deling av informasjon og data.

74 Straffeloven kap. 16, § 311

Foto: Shutterstock

POLITIET
KRIPOS

Kripos
Postadresse: Postboks 2094 Vika, 0125 Oslo
Besøksadresse: Nils Hansens vei 25, 0667 Oslo

Kontakt: 23 20 80 00 / kripos@politiet.no
Tips politiet om cyberkriminalitet: https://tips.politiet.no/web/

Foto: fremsiden: Laget med KI