POLITIET
KRIPOS

Cyberkriminalitet 2025

Politiets årlige rapport om cyberrettet
og cyberstøttet kriminalitet

Cyberkriminalitet 2025, Kripos
Politiets årlige rapport om cyberrettet og cyberstøttet kriminalitet

Grafisk formgivning: Økokrim
Opplag og trykk: 350x, Aksell
ISSN: 2704-2537

Foto: Shutterstock

Forord

I det digitale rom er alle verdens hjørner våre nærområder. Språklige, kulturelle og teknologiske barrierer til fjerntliggende områder senkes stadig. Særlig er utviklingen innen kunstig intelligens og utbyggingen av digital infrastruktur medvirkende til å utvide de kriminelles rekkevidde og oppmerksomhet.

Norge er et av verdens mest digitaliserte samfunn, besitter store verdier og eksporterer kritiske ressurser til nytte for verdenssamfunnet. Norge har i tillegg engasjert seg i flere konflikter verden over. Samlet utgjør derfor nordmenn, norske verdier og norske virksomheter attraktive mål for cyberkriminelle. Likevel viser oversikter over den globale fordelingen av cyberrettet kriminalitet at Norge i dag foreløpig ikke er et prioritert mål blant cyberkriminelle aktører, men dette kan raskt endre seg. Uavhengig av dette opplever norske enkeltpersoner og virksomheter å bli utsatt for cyberkriminalitet hver eneste dag, og for de som rammes kan konsekvensene være omfattende. Innen cyberstøttet kriminalitet er særlig norske barn utsatt. Dette forsterkes av at de har meget høy grad av digital tilstedeværelse.

Rask teknologisk utvikling og en stadig voksende sårbarhetsflate utgjør to sider av samme sak. Dette innebærer at fordeler som følger av digitaliseringen også medfører nye og mer sammensatte sårbarheter – både som følge av teknologiske, forretningsmessige og samfunnsmessige avhengigheter. Sammen med den eksplosive veksten i tilgjengelig informasjon, gir disse utviklingstrekkene næring til et mangfoldig og bevegelig cyberkriminelt aktørlandskap. I kombinasjon med at sårbarhetsflaten vokser, representerer kunstig intelligens en ny og mindre forstått sårbarhetsflate. Dette fører til stor usikkerhet knyttet til mulighetene for kriminell utnyttelse. På samme tid driver økonomiske interesser virksomheter til å implementere KI-teknologien i sitt digitale nervesystem. Bekymringer knyttet til disse utviklingstrekkene forsterkes av at det introduseres nye sårbarheter raskere enn vi klarer å avdekke og reparere de eksisterende.

Den kriminelle utnyttelsen av digitaliseringen har vært fremtredende i lengre tid, men Kripos forventer et taktskifte i tiden fremover. Hastigheten og alvorligheten i kriminaliteten øker. Vi ser både rask utnyttelse av nye sårbarheter, deling av nye verktøy og metoder, økt tilbud av kriminelle tjenester, samt kriminelle som går lengre i sin virkemiddelbruk for å nå sine mål. Innen cyberstøttet kriminalitet blir våre yngste rammet av seksuallovbrudd, noe som kan ha livslange konsekvenser for de fornærmede barna. Bedragerier rammer både enkeltpersoner og virksomheter, og er et hurtigvoksende problem som tilfører store økonomiske verdier til organiserte kriminelle i utlandet. Tradisjonelle organiserte kriminelle nettverk benytter også teknologiske verktøy for å kommunisere, flytte penger og skjule identiteten sin. Derfor er det viktig at politiet ser cyberkriminalitet som en integrert del av annen alvorlig og organisert kriminalitet, uavhengig av domene. For å møte trusselen nå og i det videre, må samfunnet betraktes som en helhet, og vi må bygge digital robusthet mot cyberkriminalitet gjennom åpenhet og forebyggende tiltak.

Rapporten beskriver cyberkriminalitetsbildet slik Kripos ser og forstår det og gir beslutningsstøtte til beslutningstakere på forskjellige nivåer. Kripos ønsker med denne rapporten å bidra med kunnskap og innsikt om cyberkriminalitet for å ruste samfunnet, virksomheter og enkeltpersoner mot lovbrudd.

Kristin Kvigne
Sjef Kripos

Innhold

Sammendrag 6
Rapportens formål 8
Leseveiledning 9
Cyberkriminalitetens kjennetegn 11
Aktørgalleriet 13
Muliggjørere og tilretteleggere i det cyberkriminelle økosystemet 21
Cyberrettet kriminalitet 29
Cyberrettede kriminalitetstyper 30
Nåsituasjon - det cyberrettede trussellandskapet 2024 30
Normalbildet innenfor cyberrettet kriminalitet 33
Handlingsmønstre 35
Operasjonell teknologi (OT) 55
Mulige konsekvenser 59
Cyberstøttede seksuallovbrudd 71
Nåsituasjon – cyberstøttede seksuallovbrudd i 2024 72
Kriminalitetstyper 74
Handlingsmønstre 79
Aktører 82
Konsekvenser 89
Ventet utvikling 2025 95
Trusselen mot enkeltpersoner 95
Trusselen mot virksomheter 96
Trusselen mot samfunnet 97
Vedlegg 100
Sannsynlighetsord 100
Begreper 100
Figuroversikt 109

Sammendrag

Cyberkriminalitet 2025 gir en gjennomgang av trussellandskapet for cyberkriminalitet i 2024 og forventet utvikling i 2025. Rapporten fremhever at cyberkriminalitet er et globalt fenomen med rask overføring av trender og metoder på tvers av landegrenser. Kripos introduserer i årets rapport en nyansering av fjorårets todeling mellom cyberrettet og cyberstøttet kriminalitet ved å plassere kriminaliteten på en glideskala, som viser at det ikke er tette skott mellom kategoriene.

Deretter presenteres det cyberkriminelle aktørgalleriet, hvor Kripos beskriver profittmotiverte kriminelle og aktivister, i tillegg til uklassifiserte cyberkriminelle og gråsoneaktører. Behovet for økt bevissthet rundt hele det cyberkriminelle spekteret, hvor kriminalitetskryssende handlinger med ulike motiv er i vekst, forsterkes av den spente sikkerhetspolitiske situasjonen og behovet for et styrket samarbeid og videreutvikling av totalforsvaret. Cybertrusselen kan vokse svært raskt – det er nok at en person eller gruppering bestemmer seg for å utføre et angrep, før effektene merkes umiddelbart. I årene fremover blir det derfor avgjørende å etablere en felles forståelse for det samlede trusselbildet i cyberdomenet.

Kripos introduserer videre begrepene muliggjørere og tilretteleggere for cyberkriminalitet. Todelingen er relevant da muliggjørere er teknologiske verktøy og digital infrastruktur, mens tilretteleggere er personer som i kraft av sin tilgang og kompetanse medvirker til kriminalitet eller sørger for at kriminaliteten tilsløres. Organiserte kriminelle nettverk har også i økende grad tatt i bruk både det mørke nettet og det åpne nettet som sosiale medier, noe som har bidratt til å forenkle spredningen av kriminelle tjenester og metoder.

Innen cyberrettet kriminalitet har Kripos oppdatert begrepskartet fra i fjor, for å vise at kriminaliteten ikke bare retter seg mot datasystemer, men også kan komplimenteres av kriminalitet utført i datasystemer, som datatyveri og etterfølgende utpressing. Et datainnbrudd er ofte et startpunkt for videre kriminelle handlinger i datasystemene. Videre beskrives trussellandskapet for 2024, hvor det har vært moderate endringer og en økning i løsepengevirus mot norske virksomheter.

Kripos beskriver deretter hvordan økt digitalisering og teknologiske avhengigheter har åpnet for nye sårbarheter som utnyttes av kriminelle. Spesielt legger cyberkriminelles utnyttelse av verdikjeder og tredjepartsrelasjoner til rette for å ramme mange fornærmede samtidig.

Innen løsepengevirus beskrives utvikling og endring i handlingsmønstre, der aktørene innen løsepengevirus som handelsvare (LSH) gjerne

samarbeider om flere skadevarer samtidig. I tillegg beskriver Kripos løsepengevirusvarianter som har rammet norske verdier i 2024.

Deretter omtales bruk av kunstig intelligens til kriminelle formål, gjennom beskrivelser av dypforfalskninger og bruk av KI-agenter. Dypforfalskninger kan brukes til ulike kriminelle formål, eksempelvis ved å forlede i sanntid.

Kapittelet om cyberrettet kriminalitet avsluttes med et dypdykk i integrasjonen av operasjonell teknologi (OT) med internettbaserte systemer, samt mulige konsekvenser som følge av cyberangrep. I denne sammenheng belyses hvordan cyberdomenet kan benyttes i statlige aktørers sammensatte virkemiddelbruk.

Rapportens andre hoveddel handler om cyberstøttede seksuallovbrudd og beskriver at cyberstøttede seksuallovbrudd spenner fra kriminalitet som er helt avhengig av datasystemer til fysiske lovbrudd som suppleres av datasystemer.

I kapittelet beskrives først trussellandskapet for 2024, der særlig muliggjørerne kunstig intelligens og krypterte meldingsplattformer har hatt innvirkning. Videre presenteres ulike kriminalitetstyper, med vekt på typene hvor Kripos har observert en endring. Et eksempel er at syntetiske overgrepsbilder er mer realistiske enn før og omfanget øker, samtidig som generering av materialet rammer faktiske personer.

Seksuell utpressing beskrives som en vedvarende trussel, men spesielt utpressing med profittmotiv hadde stort omfang i 2024. De fornærmede er norske gutter og menn, mens aktørene er fra land som Filippinene, Nigeria og Elfenbenskysten. Kripos anslår at gjerningspersonenes grad av organisering er mindre enn tidligere antatt, hvor man trodde at utpressing skjedde fra store callsenter-lignende virksomheter. Det er også observert mer kyniske utpressingsteknikker.

Kripos presenterer videre hvordan trusselaktører tilnærmer seg barn på internett med en svært mangfoldig verktøykasse, hvilke straffbare forhold som begås og hvilke konsekvenser det medfører for de fornærmede barna.

I siste del av rapporten presenteres ventet utvikling for 2025. Kripos forventer at organiserte kriminelle nettverk vil få et større handlingsrom fremover som følge av økt bruk av digitale muliggjørere. Kripos anslår at kriminelle vil fortsette å utnytte avstanden mellom rask teknologisk utvikling og samfunnets tregere evne til å utvikle effektive mottiltak. Videre forventes det at KI vil medføre at kulturelle og språklige barrierer senkes, som vil føre til at norske enkeltpersoner og virksomheter blir mer utsatt for cyberkriminalitet enn tidligere. Kripos anslår også at de samfunnsøkonomiske kostnadene av cyberstøttede seksuallovbrudd er store, som følge av de langvarige konsekvensene kriminaliteten har for de mange fornærmede.

Kripos understreker til slutt at cyberkriminalitet kan ramme alle nivåer i samfunnet og vi er alle potensielle mål for de kriminelle. Den raskt voksende mengden bedragerier og seksuallovbrudd mot enkeltpersoner utgjør derfor samlet en trussel mot den alminnelige tryggheten i samfunnet.

Rapportens formål

Dette er tredje utgivelse i rekken av Kripos' årlige etterretningsrapporter om cyberkriminalitet. Rapportseriens formål er å øke kunnskapsgrunnlaget for både den cyberrettede og cyberstøttede kriminaliteten, og beskriver cyberkriminalitetens kjennetegn, utviklingstrekk og ventede utvikling. Samfunnets beredskaps- og sikkerhetstenkning er fortsatt i positiv utvikling når det gjelder forståelse av alvoret som truslene fra det digitale rom innebærer. Et kontinuerlig opplysningsarbeid omkring truslene er likevel nødvendig.

Årets utgave bygger i større grad enn tidligere på sine to forgjengere[1] og bør derfor ses i sammenheng med disse. Datagrunnlaget for rapporten er i hovedsak fra 2024 og omfatter politiets straffesaks- og etterretningsregister, informasjon fra private og offentlige samarbeidspartnere, internasjonalt politisamarbeid, samt informasjon fra åpne kilder.

Felles nasjonalt begrepsapparat på cyberkriminalitet er fortsatt under utvikling. Kripos har derfor utarbeidet en begrepsliste som er vedlagt rapporten for å fremme felles forståelse og bruk av terminologi på cyberkriminalitetsfeltet. For å støtte samfunnet med å forebygge og bekjempe cyberkriminalitet fortsetter Kripos å introdusere nye og videreutviklede rammeverk for strategisk etterretningsanalyse.

Rapporten drøfter ikke hvilke tiltak som kan iverksettes på bakgrunn av de belyste utfordringene og truslene.

1 Kripos. (2024). *Cyberkriminalitet 2024*. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf og Kripos. (2023). *Cyberkriminalitet 2023*. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf

Leseveiledning

Kapitlene om cyberrettet og cyberstøttet kriminalitet og tilhørende underkapitler er skrevet for å kunne leses individuelt. Noen kapitler i årets rapport har en høyere teknisk vanskelighetsgrad enn andre. Dette skyldes at rapporten har flere målgrupper med forskjellige bakgrunner, teknisk innsikt og interesseområder. Det er derfor benyttet fargekoder – grønn, gul og rød – for å indikere kapitlenes tekniske nivå.

Lesere kan fritt velge ut tematikk i rapporten basert på behov og interesse. Nedenfor er et forslag til navigering, basert på noen generelle målgrupper:

Samfunnsborgere: Sammendrag (side 6) og ventet utvikling 2025 (side 94) gir en oversikt over relevante trusler. Foreldre og andre i kontakt med barn kan videre ha nytte av cyberstøttede seksuallovbrudd (side 71).

Virksomheter: Muliggjørere og tilretteleggere (side 21) og cyberrettet kriminalitet (side 29) gir innsikt i operative utfordringer og tiltak.

Teknisk ekspertise: Handlingsmønstre (side 35) og operasjonell teknologi (OT) (side 55) gir avanserte analyser og detaljer.

- **Lett** – krever få forhåndskunnskaper og skal være mulig for alle lesere å følge.
- **Medium** – er tilrettelagt for lesere med noe forkunnskap til tematikken, men innholdet kan likevel være av interesse for lesere uten forkunnskaper.
- **Vanskelig** – er mer teknisk krevende og detaljert enn de to andre nivåene og fordrer at leseren har en viss innsikt i tematikken og noe mer teknisk forståelse.

Foto: Shutterstock

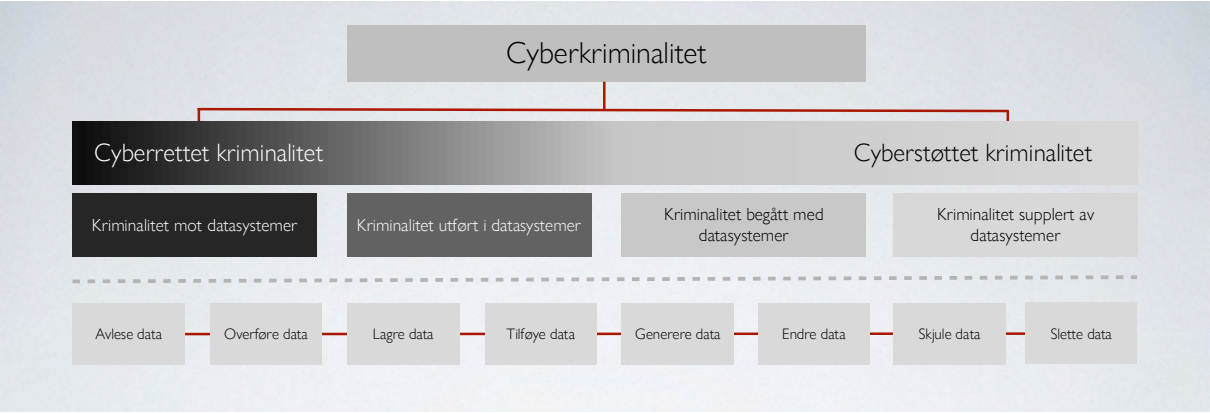
Cyberkriminalitetens kjennetegn

Cyberkriminalitet strekker seg over landegrenser og jurisdiksjoner, og utgjør ofte en del av kriminalitet som utøves i det fysiske domenet. Mye av cyberkriminaliteten utføres av organiserte kriminelle, enten fordi tradisjonell organisert kriminalitet får et digitalt fotavtrykk, eller som følge av at cyberkriminelle må delegere oppgaver og anvende spesialistkompetanse for å kunne utføre tekniske og sammensatte kriminelle handlinger. Kripos har tidligere delt cyberkriminalitet inn i to søyler: (1) cyberrettet kriminalitet og (2) cyberstøttet kriminalitet. Todelingen som utgjør det cyberkriminelle spekteret gjelder fortsatt, men i årets rapport viser Kripos at inndelingen befinner seg på en glideskala, fra *kriminalitet mot datasystemer* i den ene enden, til k*riminalitet supplert av datasystemer* i den andre enden.[2]

Den glidende overgangen illustrert av figur 1, viser at cyberrettet og cyberstøttet kriminalitet ikke utgjør absolutte kategorier, men at kriminaliteten kan helle mer i den ene retningen enn den andre. Derimot kan cyberkriminaliteten ofte omtales mer presist gjennom atskilte kategorier som indikerer teknologiens funksjon og relevans i kriminalitetsutøvelsen. Basert på dette er begrepskartet utvidet til å inkludere fire distinkte underkategorier av cyberkriminalitet. Som nevnt i fjorårets rapport, fantes ikke k*riminalitet mot datasystemer* og *kriminalitet utført i datasystemer* før det digitale rom oppstod. I kriminalitet utført i datasystemer går også skillet mellom det Kripos omtaler som cyberrettet og cyberstøttet kriminalitet. *Kriminalitet begått med datasystemer* og *kriminalitet supplert av datasystemer* er tradisjonell kriminalitet som foregår utenfor, men også begås i det digitale rom.

Kriminalitet mot datasystemer skiller seg fra annen cyberkriminalitet ved at den *retter seg direkte mot et datasystem*, fremfor mennesker som bruker datasystemer eller informasjon

2 Inndelingen er inspirert av Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies.* Forensic Sciences, 2(2), s. 379–398. https://doi.org/10.3390/forensicsci2020028



Figur 1: Illustrerer at cyberkriminalitet strekker seg fra kriminalitet mot datasystemer til kriminalitet i det fysiske rom som er supplert av datasystemer. Dette utgjør det cyberkriminelle spekteret. Cyberkriminalitetens byggeklosser som er vist nederst i modellen utgjør de grunnleggende aktivitetene som er felles for all cyberkriminalitet og gjelder på tvers av glideskalaen. Modellen er utviklet av Kripos.

som er lagret på datasystemer. Eksempler inkluderer blant annet datainnbrudd og digitalt skadeverk. Et datainnbrudd er ofte et startpunkt for videre kriminelle handlinger i datasystemene. Kriminalitet utført i datasystemer er kriminalitet som, i likhet med kriminalitet mot datasystemer, er unikt for det digitale rom, men som *retter seg mot menneskene* som tar i bruk datasystemer eller *informasjon* som er lagret på datasystemer. Eksempler er generering av syntetisk overgrepsmateriale, nettfisking[3] og kryptosvindel. Dette er kriminalitet som ikke angriper datasystemer direkte, men som ikke kan begås utenfor det digitale rom. Kriminalitet begått med datasystemer er kriminalitet som *begås i det digitale rom*, men som like gjerne kan begås utenfor. Eksempler på dette kan være kjærlighetsbedragerier, salg av narkotika, seksuell utpressing og hatefulle ytringer i sosiale medier. Sist er kriminalitet supplert av datasystemer som er tradisjonell kriminalitet som *begås i det fysiske domenet*, men som benytter datasystemer som et supplement. Eksempler er at organiserte kriminelle kommuniserer seg imellom på kryp-

3 Refererer til metoder for å urettmessig tilegne seg andres persondata eller påloggingsdetaljer gjennom sosial manipulasjon, for eksempel gjennom e-post. Eng: *Phishing*

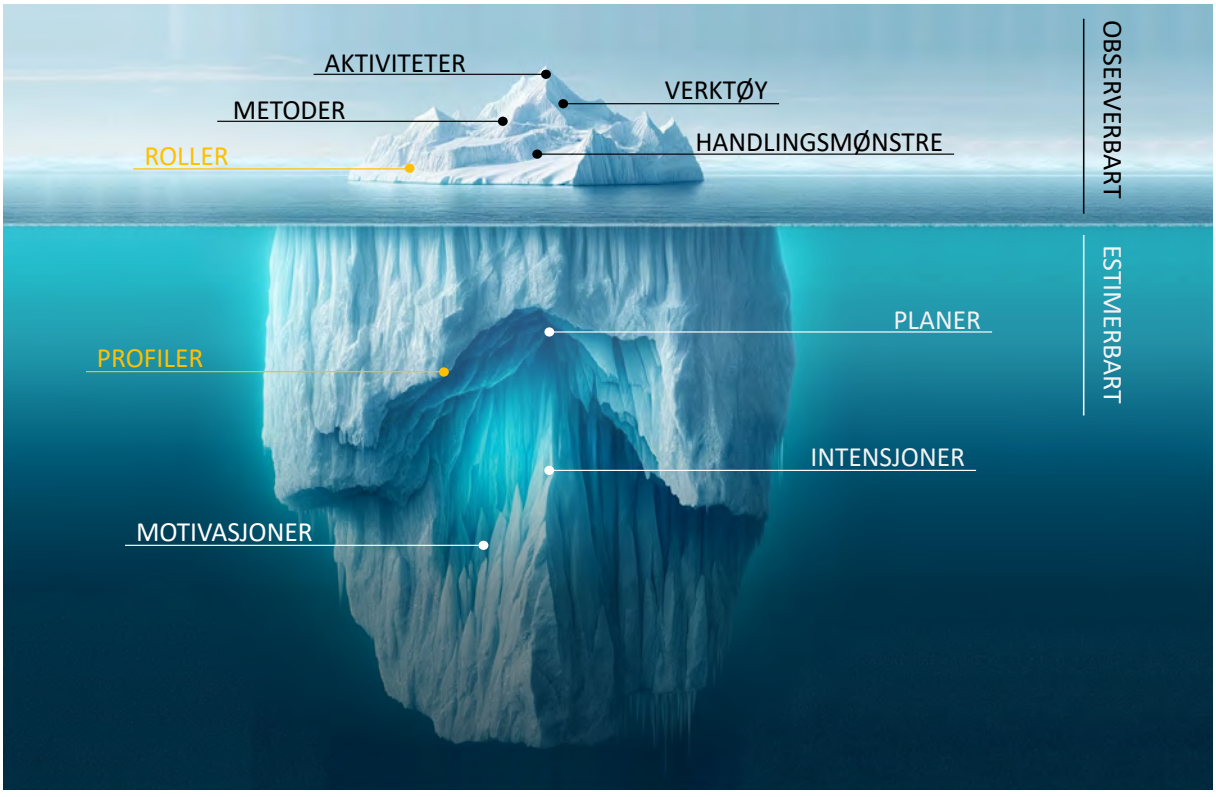
terte telefoner eller meldingsplattformer, eller at voksne avtaler fysiske møter med barn i sosiale medier for å begå seksuelle overgrep.

Aktørgalleriet

I dette kapittelet vil Kripos beskrive overordnede trekk ved det cyberkriminelle aktørgalleriet, altså de ulike aktørene i aktørlandskapet. Beskrivelsene gjelder på tvers av kriminalitetsområdene.

Aktører som faller innunder Kripos' mandat befinner seg ofte innenfor sfæren av *organisert kriminalitet*. Selv om organisert kriminalitet tradisjonelt har blitt assosiert med narkotika- og gjengkriminalitet, opererer også mange cyberkriminelle nettverk som organiserte kriminelle nettverk.

I fjorårets rapport introduserte Kripos aktørinndelingene roller og profiler, i årets rapport er navngivningen av disse to byttet om ettersom



Figur 2: Viser aktørers sammensetning (teksten er lagt oppå et KI-generert bilde). Modellen er utviklet av Kripos.

det samsvarer bedre med samfunnsforståelsen av begrepene. Kripos har definert følgende fem profiler[4]: (1) *profittmotiverte kriminelle*, (2) *seksuallovbrytere*, (3) *aktivister*, (4) *statlige aktører*, og (5) *terrorister*. I dette kapittelet beskriver Kripos profittmotiverte kriminelle og aktivister, i tillegg til gråsoneaktører og aktører som foreløpig ikke er klassifisert. Seksuallovbrytere blir beskrevet i kapittelet om cyberstøttede seksuallovbrudd (side 82).

Gjennom å identifisere aktørens *profil* kan politiet, hendelseshåndterere og sikkerhetsledere danne seg et inntrykk av aktørens kapabiliteter og intensjoner. Ettersom profilene er basert på hva aktørene ønsker å oppnå fremfor handlinger eller metoder, kan inndelingen også bidra til å gjenkjenne aktører og kriminalitetstyper på tvers av det digitale og fysiske domenet.

Kriminelles *roller*[5] kan forstås som tjenesten eller funksjonen en kriminell tilfører det cyberkriminelle økosystemet. Eksempler inkluderer tilbydere av løsepengevirus som handelsvare (LSH), hvitvaskere, tilgangsmeglere, selgere av direkteoverførte bestillingsovergrep (DOBO) eller menneskesmuglere. Enkeltaktører kan inneha flere roller på samme tid, hvilket også betyr at profilene ikke er avgjørende for hvilken kriminalitet aktørene utfører. En aktivist kan eksempelvis bruke taktikker forbundet med profittmotivert kriminalitet for å ramme en fornærmet i tråd med egen ideologisk overbevisning.

Nåværende profilkategorisering fører til at aktører kan overlappe flere profiler. Dette ble omtalt som gråsoner i fjorårets rapport, og vil bli beskrevet fra side 18.

Profittmotiverte cyberkriminelle

Som beskrevet i fjorårets rapport, utgjør profittmotiverte cyberkriminelle en av de største bestanddelene i det cyberkriminelle aktørgalleriet. Profittmotiverte cyberkriminelle finnes både innenfor sfæren av cyberrettet kriminalitet, som for eksempel løsepengevirusaktører (les mer om dette fra side 44), men også innenfor cyberstøttet kriminalitet, som for eksempel aktører som driver med seksuell utpressing (les mer om dette fra side 82).

En stor andel av de profittmotiverte cyberkriminelle aktørene opererer i kriminalitet som handelsvare (KSH)-markedet. Det er observert at de samarbeider på tvers av grupperinger og landegrenser, har ulike roller og er gjensidig avhengige av hverandre for å kunne utføre kriminelle handlinger. Samtidig fører salg av

4 Omtalt som «roller» i rapport: Kripos. (2024). *Cyberkriminalitet 2024*. s. 24. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

5 Omtalt som «profiler» i rapport: Kripos. (2024). *Cyberkriminalitet 2024*. s. 24-27. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

kriminelle varer og tjenester til at det er lett å forbedre egne verktøy ved behov, eller skaffe til veie nødvendig kompetanse eller programvare for å endre handlingsmønster helt.

I løpet av de siste årene har Kripos observert nye handlingsmønstre og konstellasjoner innenfor profittmotivert cyberkriminalitet. Det er eksempelvis observert at enkelte løsepengevirusaktører ikke krypterer datasystemer til fordel for datatyveri (les mer om dette fra side 30). Kripos observerer at profittmotiverte cyberkriminelle sjelden er låst til ett spesifikt handlingsmønster eller en spesifikk handlemåte, og at de kan benytte mange metoder for å presse en fornærmet til å betale løsepenger.

Kripos har tidligere vurdert at profittmotiverte cyberkriminelle er svært tilpasningsdyktige og endringsvillige, og at teknologiske fremskritt, de fornærmede, samt mottiltak er faktorer som fører til endring eller utvikling. Denne vurderingen er styrket fra i fjor.

Aktivister - politisk motiverte cyberkriminelle

Politisk motiverte cyberkriminelle er aktivister som begår kriminalitet motivert av politisk oppfatning eller overbevisning. Tradisjonelt har denne profilen ofte vært knyttet til hacktivister og forbundet med cyberrettet kriminalitet, spesielt ulike former for tjenestenektangrep. Trusselen fra hacktivister ble i løpet av 2023 nedjustert da oppmerksomhet og politisk påvirkning som følge av tjenestenektangrep hadde hatt liten innvirkning på samfunnskritiske funksjoner i Norge.

I 2024 er det observert flere endringer i handlemåten til hacktivister. Flere hacktivistgrupperinger har benyttet seg av egenutviklede og lekkede kildekoder for å begå politisk motiverte løsepengevirusangrep internasjonalt. Dette er foreløpig ikke observert i norsk sammenheng. I tillegg til dette har hacktivister og profittmotiverte cyberkriminelle direkte og indirekte påvirket cyber-fysiske systemer (se kapittel om operasjonell teknologi fra side 55) for å understøtte sine mål.

Videre er det observert at hacktivister påvirkes av internasjonale hendelser, eksempelvis ved eskalering i ulike regionale konflikter, som krigen i Ukraina. Dette fører gjerne til økt polarisering i samfunnet og har i 2024 ført til en økning i hacktivist-allianser på begge sider. Eksempelvis skal *The Holy League* være en ny ansamling av flere hacktivistgrupperinger, inkludert pro-russiske hacktivister. Selv om de ulike grupperingene i den nye ansamlingen har forskjellige handlemåter og ambisjoner, har The Holy League formet en allianse basert på felles anskuelse med anti-vestlige, anti-israelske og pro-russiske holdninger.

Utviklingen i 2024 belyser at hacktivister ikke er bundet til én handlemåte, og at cyberkriminelle går stadig lenger i sin virkemiddelbruk for å oppnå sine ønskede mål. Samarbeid mellom ulike grupperinger, som i The Holy League, kan utvide kapabiliteter og styrke muligheten for gjennomføring av cyberkriminalitet av økt

kompleksitet og skadepotensial. Samtidig illustrerer endringene i 2024 at det eksisterer en mer dynamisk gruppe kriminelle som kan bytte mellom ulike handlemåter ved hjelp av KSH, ettersom både muliggjørere og tilretteleggere (fra side 21) er tilgjengelige for dem som kan betale.

Kripos har i 2024 observert en økning i aktører som tar del i det cyberkriminelle aktørlandskapet gjennom borgervernlignende aktiviteter. Spesielt fremtredende har aktører som ønsker å henge ut eller ta personer som ønsker seksualisert kontakt med barn vært, både gjennom bruk av vold og eksponering i sosiale medier – omtalt som «pedo-hunting». Borgerverngrupperinger vokser gjerne frem som konsekvens av mistillit til politiet og rettsvesenet og deres underliggende motivasjon kan derfor tolkes som en politisk overbevisning. Personer som utsettes for vold eller eksponering fordi de har en seksuell interesse for barn forventes å ha lav anmeldelsestilbøyelighet, noe som gjør at mørketallene også blir høye. Gruppenes aktiviteter fører til forskyvinger i det cyberkriminelle aktørlandskapet, gjennom å forstyrre andre cyberkriminelles handlinger. I noen grad er deres ønskede sluttilstand lik som for samfunnet for øvrig; de ønsker at barn skal være trygge i den digitale og fysiske verden. Samtidig fører aktiviteten til alvorlige voldslovbrudd, spesielt i den fysiske verden. Svært unge aktører tar del i disse voldslovbruddene, også barn under strafferettslig lavalder, selv om også voksne er representert. På tross av at volden skjer i den fysiske verden, skjer planleggingen, organiseringen og den innledende kontakten mellom aktørene og de som utsettes for vold på ulike digitale plattformer der fysiske møter avtales. Videre skjer delingen av konfrontasjonene på flere sosiale medier og andre digitale arenaer, både nasjonalt og internasjonalt.

Delvurderinger

Hacktivister påvirkes av politikk og geopolitiske forhold og kan direkte og indirekte bidra til å eskalere konflikter gjennom sin aktivitet. Selv om endringene innenfor hacktivisme ikke er observert i norsk sammenheng i 2024, vurderes det som sannsynlig at de observerte endringene også vil få konsekvenser for norske interesser det neste året. Det er mulig at bruk av lekkede og lett tilgjengelige hyllevare-løsepengevirus kan føre til at flere hacktivister utvider sin kriminelle verktøykasse til å inkludere denne angrepsformen og dermed utgjøre en større trussel mot norske virksomheter.

Uklassifiserte cyberkriminelle og gråsoneaktører

Ikke alle kriminelle aktører har en bestemt motivasjon, bakgrunn eller ideologi. Noen drives eksempelvis av hevn, nysgjerrighet, en søken etter spenning, berømmelse eller anerkjennelse, eller det foreligger omstendigheter knyttet til avhengighet. Det gjenstår derfor en rekke krimi-

Foto: Shutterstock

nelle som ikke like enkelt lar seg definere. Denne aktørkategorien omtaler Kripos som uklassifiserte cyberkriminelle.

I likhet med de fem aktørprofilene er ikke kompetansenivået til uklassifiserte cyberkriminelle en faktor som avgjør profiltilhørighet. Disse aktørene kan ha høy teknisk kompetanse, og i noen tilfeller ha unik innsikt i og tilgang til IKT-systemer i kraft av en tilknytning til den fornærmede, for eksempel gjennom et ansettelsesforhold. Andre kan ha svært lav teknisk kompetanse, men likevel utføre kriminalitet som kan plasseres på det cyberkriminelle spekteret.

Innen cyberstøttede seksuallovbrudd ser Kripos at mange barn og unge gjør seg til aktører i det cyberkriminelle aktørlandskapet uten at motivasjonen er seksuell tilfredstillelse eller profitt. Det dreier seg ofte om barn som ukritisk, og uten å ha et seksuelt motiv bak handlingen, deler overgrepsmateriale, som «virale videoer»[6] i sosiale medier, eller de filmer eller tar bilder av jevnaldrende der de enten er nakne eller i seksualiserte situasjoner. Motivasjonen kan i mange tilfeller være ukjent, men mobbing, hevn, forsøk på å være morsom, få oppmerksomhet eller sjokkere er tidligere registrert.

Et annet eksempel på en uklassifisert cyberkriminell er en ingeniør tidligere ansatt i et vannhåndteringsfirma i Australia som utførte en hevnaksjon mot sin tidligere arbeidsgiver. Den tidligere ansatte manipulerte fysiske prosesser gjennom radiosignaler, noe som førte til at ca. 800 000 liter kloakk rant ut i nærområdet og angivelig forårsaket lokal miljøforurensning og tap av marint liv.

Som beskrevet i kapittelet om aktørgalleriet (fra side 13), kan noen aktører havne i flere profiler, såkalte gråsoneaktører. Disse kan ha flerdelte motivasjoner og begå kriminalitetskryssende handlinger.

Et eksempel er selgere av direkteoverførte bestillingsovergrep (DOBO), som begår seksuallovbrudd – disse aktørene er som regel seksuelt motiverte cyberkriminelle (profilen seksuallovbryter), men i dette tilfellet er de motivert av profitt (profilen profittmotivert kriminell). Et annet eksempel er hacktivistgrupperinger som i tillegg til å være politisk motiverte, også kan være motivert av profitt. Andre kan benytte hacktivist-hatten som et skalkeskjul.

I et sammenvevd cyberkriminelt økosystem oppstår det ulike konstellasjoner, samarbeidsmodeller og avhengigheter som kan gjøre det vanskelig å avgjøre hva som er den bakenforliggende motivasjonen til aktørene. Forsterkende årsaksforhold inkluderer:

6 Virale videoer kan i denne sammenhengen både være videoer som viser seksuelle overgrep mot barn, men også videoer som viser grov vold og drap, ulykker eller andre ekstreme eller sjokkerende fenomener

1. åpent tilgjengelige verktøy og skadevarer uten begrensninger på hvem som kan ta dem i bruk;
2. deling av metoder på kriminelle nettfora;
3. offentliggjøring av sårbarheter og utnyttelsen av disse;
4. anonymiseringsteknologier; og
5. hyppig opprettelse og nedleggelse av cyberkriminelle grupperinger.

I den innledende fasen av et cyberangrep er det av disse årsakene ofte vanskelig å identifisere hvem som begår kriminaliteten eller hvorfor kriminaliteten blir begått. Siden resultatet er færre identitetsmarkører, gir det generelt gode forutsetninger for villedning og fornektbarhet i det digitale rom.

Forhold i den fysiske verden kan også ha innvirkning på dynamikker mellom aktører med ulik profiltilhørighet. Geopolitiske spenningsforhold kan tåkelegge allerede uklare skillelinjer mellom statlige aktører og aktivister[7], mellom aktivister og profittmotiverte cyberkriminelle[8] og mellom profittmotiverte

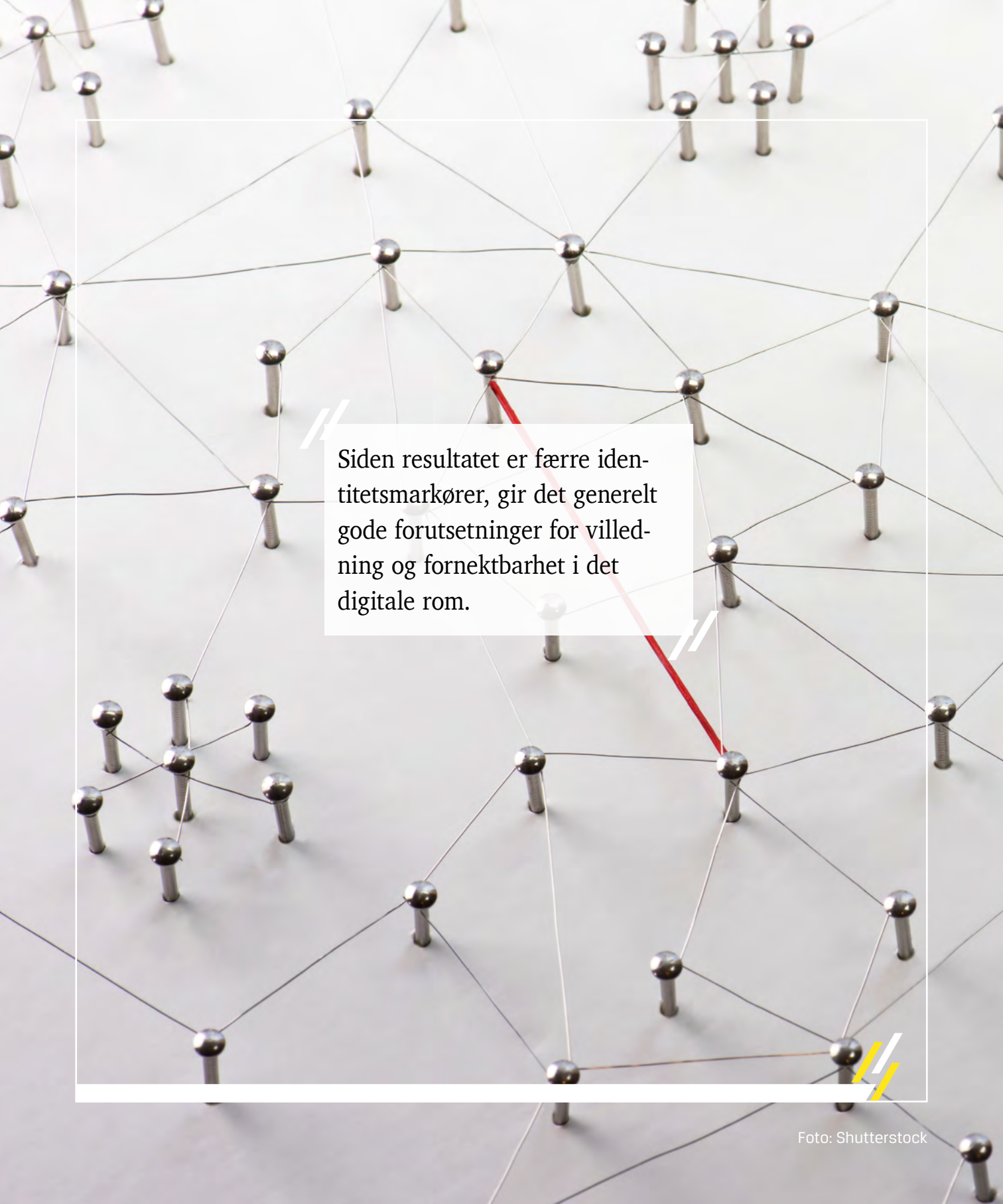
Spekteret av statlig ansvar

1. **Statlig forbudt:** Staten bidrar til å stoppe angrepet fra tredjepart.
2. **Statlig forbudt, men utilstrekkelig:** Staten er samarbeidsvillig, men ute av stand til å stoppe angrepet fra tredjepart.
3. **Statlig ignorert:** Staten er klar over angrepet fra tredjepart, men er uvillig til å foreta offisielle tiltak.
4. **Statlig oppmuntret:** Tredjepart kontrollerer og gjennomfører angrepet, men staten oppmuntrer dem som en del av sin politikk.
5. **Statlig formet:** Tredjepart kontrollerer og gjennomfører angrepet, men staten gir en viss støtte.
6. **Statlig koordinert:** Staten koordinerer tredjepartsangripere, for eksempel ved å «foreslå» operasjonelle detaljer.
7. **Statlig ordnet:** Staten instruerer tredjepart til å gjennomføre angrepet på deres vegne.
8. **Statlig avhopper:** Ukontrollerte elementer ved statens cyberstyrke gjennomfører angrepet.
9. **Statlig utført:** Staten gjennomfører angrepet ved hjelp av cyberstyrker under dens direkte kontroll.
10. **Statlig integrert:** Staten angriper ved hjelp av en integrert tredjepart og statlige cyberstyrker.

Figur 3: KI-støttet oversettelse av *The Spectrum of State Responsibility*, Atlantic Council.

7 Noen ganger omtalt som (eng:) *State-sponsored Hacktivism* eller *Hybrid-hacktivism*

8 Noen ganger omtalt som (eng:) *Hacktivists-for-hire*



Siden resultatet er færre identitetsmarkører, gir det generelt gode forutsetninger for villedning og fornektbarhet i det digitale rom.

Foto: Shutterstock

cyberkriminelle og statlige aktører[9]. Et eksempel på dette er løsepengevirusgrupperinger som velger ut sine mål både for å oppnå profitt og for å oppfylle geopolitiske interesser.

I lys av dette har norske og utenlandske myndigheter rapportert om ulik grad av samarbeid og krysspollinering mellom kriminelle aktører og mellom kriminelle aktører og statlige aktører. Krysspollinering innebærer at verktøy, metoder og skadevarer blir overført fra en aktør til en annen, men uten at det nødvendigvis er et samarbeid. Kripos vil i denne sammenheng trekke frem Atlantic Councils rammeverk (*spekteret av statlig ansvar*, Figur 3[10]) som lister opp ti nivåer av statlig ansvar for cyberangrep begått av kriminelle. Listen strekker seg fra statlig bidrag til å stoppe en kriminell handling (nivå 1) til at staten utfører cyberangrepet selv (nivå 9) eller gjennom en integrert tredjepart (nivå 10). Rammeverket danner et nyttig bakteppe som beriker det cyberkriminelle situasjonsbildet og kan brukes til å tolke oppdukkende cyberrettet kriminalitet spesielt. Bevissthet rundt hele dette spekteret er viktig sett i lys av dagens spente sikkerhetspolitiske situasjon der man opplever økt bruk av staters samlede verktøykasse, også omtalt som sammensatt virkemiddelbruk.

Muliggjørere og tilretteleggere i det cyberkriminelle økosystemet

For å begå cyberkriminalitet er kriminelle aktører avhengige av å anvende tilgjengelig teknologi, såkalte muliggjørere. Med muliggjørere menes her teknologiske verktøy og digital infrastruktur som gjør det mulig – eller enklere – å begå kriminelle handlinger, men som gjerne ikke er ulovlige i seg selv. Cyberkriminelle som begår både cyberrettet og cyberstøttet kriminalitet benytter tjenester, tekniske verktøy og digital infrastruktur som selges eller leies ut til kriminelle formål. Samtidig nyttiggjør de seg av gratis tilgjengelige muliggjørere som også benyttes til legitime formål. Kriminalitet som handelsvare utføres både på det mørke og åpne nettet.

I tillegg er de cyberkriminelle i større eller mindre grad avhengig av det Kripos omtaler som tilretteleggere: personer som i kraft av sin

9 Gjennom eksempelvis løsepengevirus som et røykteppe. (Eng:) *Ransomware-as-a-Smokescreen*

10 Atlantic Council. (2011). *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*. https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF

tilgang og kompetanse medvirker til kriminalitet eller sørger for at kriminaliteten tilsløres.[11] Spesialiserte tjenester som leies ut eller selges til kriminelle formål, altså KSH, er et eksempel på slike tilretteleggere. En person kan være en tilrettelegger for en annen aktør samtidig som den selv begår kriminalitet.

Et eksempel for å illustrere forskjellen mellom en muliggjører og en tilrettelegger er en aktør som benytter seg av en markedsplass på det mørke nettet (muliggjører) for å kjøpe narkotika av en selger (tilrettelegger) som selger varen for en organisert kriminell gruppering i den fysiske verden. Et annet eksempel er en aktør som benytter seg av en ende-til-ende-kryptert meldingsplattform (muliggjører) for å kjøpe direkteoverførte bestillingsovergrep av en selger (tilrettelegger) på Filippinene.

Kripos har over tid erfart at kjøp eller leie av muliggjørere og tilretteleggere er et økende behov også innenfor cyberstøttet kriminalitet. Dette gjelder eksempelvis organiserte kriminelle som opererer i den fysiske verden, men som har et økende behov for kjøp eller leie av muliggjørere og tilretteleggere i det digitale rom for opprettholdelse og drift av sin kriminelle operasjon i den fysiske verden.

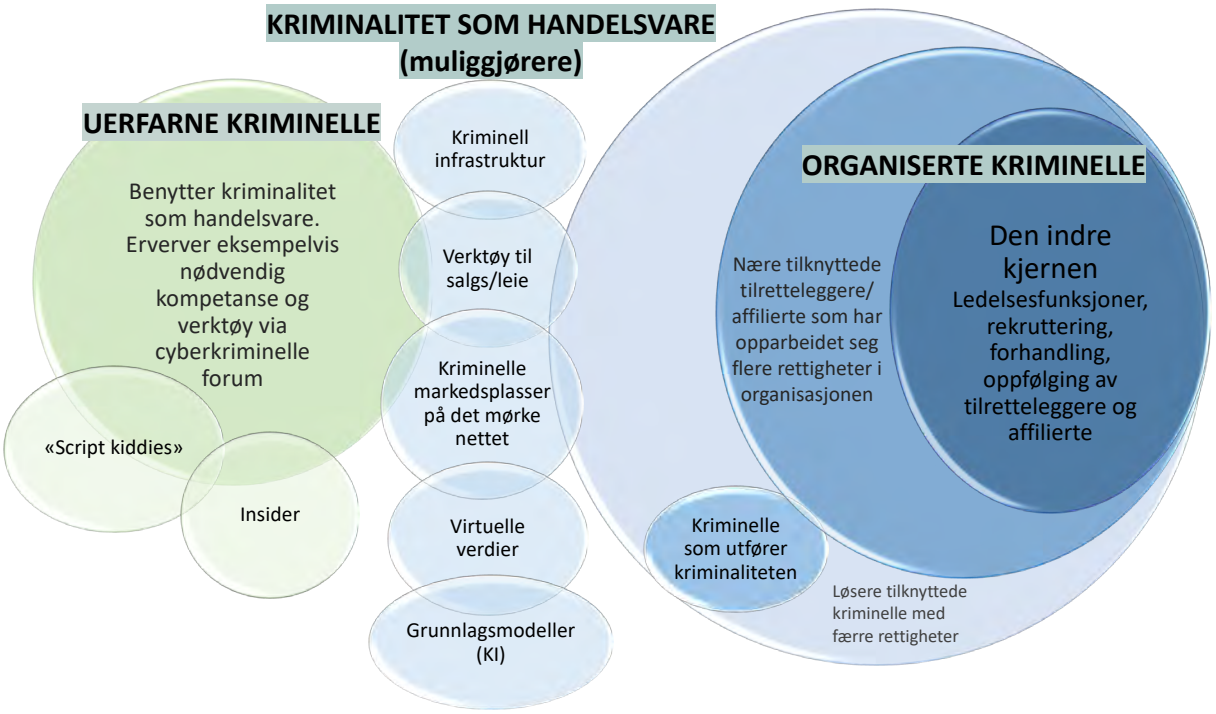
> Økt etterspørsel etter kjøp og leie av muliggjørere og tilretteleggere peker i retning av kriminelles økte avhengighet av det digitale rom for å utøve sin kriminelle virksomhet...

Muliggjørere for cyberkriminalitet

Cyberkriminelle og tradisjonelle organiserte kriminelle benytter muliggjørere for å skjule hvem de er, hva de kommuniserer og deler seg imellom og hvor pengestrømmene flyter.

Kriminelle benytter anonymiseringsteknologier sammen med andre sikkerhetstiltak for å skjule sin identitet og redusere risiko for å bli tatt, men også for skadereduksjon dersom de blir tatt. Evnen til å operere fordekt er ansett som en avgjørende driver for mye av cyberkriminaliteten. Tekniske og taktiske tiltak for å opprettholde

11 Økokrim. (2024). *Trusselvurdering 2024 – Den kriminelle økonomien*. s. 20. https://img8.custom-publish.com/getfile.php/5363097.2528.ajtsilqbikkmsk/2024_Trusselvurdering_%C3%98kokrim_nett.pdf?return=www.okokrim.no



Figur 4: Viser hvordan uerfarne og organiserte kriminelle nyttiggjør seg KSH, ved kjøp/leie av muliggjørere i utførelsen av kriminalitet. Modellen er utviklet av Kripos.

anonymitet inkluderer blant annet sikkerhetsfokuserte operativsystemer, VPN og proxy,[12] Tor[13], hostingtjenester[14], fiktive kontoer på tjenester uten krav til identifisering, samt kryptovaluta for økonomiske transaksjoner.

Samtidig har det i de senere år etablert seg en trend der kriminelle søker mot land som har særlig beskyttelse mot straffeforfølgelse fra

12 Les mer her: Kripos. (2024). *Cyberkriminalitet 2024*. s. 42. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

13 Eng: *The Onion Router* (Tor) er en gratis og fritt tilgjengelig anonymiseringstjeneste som blant annet brukes for å skjule kommunikasjon på internett

14 Viser til for eksempel (eng:) *Bullet Proof Hosting*

utlandet. Et eksempel er Tyrkia, hvor Kripos observerer at kriminelle investerer store summer i bytte mot statsborgerskap. Dette bidrar til at personen kan begå cyberkriminalitet med lav risiko for utlevering til Norden.

Kripos har i løpet av 2024 blant annet observert at organiserte kriminelle nettverk med knytninger til svenske aktører er i ferd med å etablere seg på markedsplasser for narkotikasalg på det mørke nettet. Dette illustrerer tradisjonelle organiserte kriminelles bruk av digitale muliggjørere.

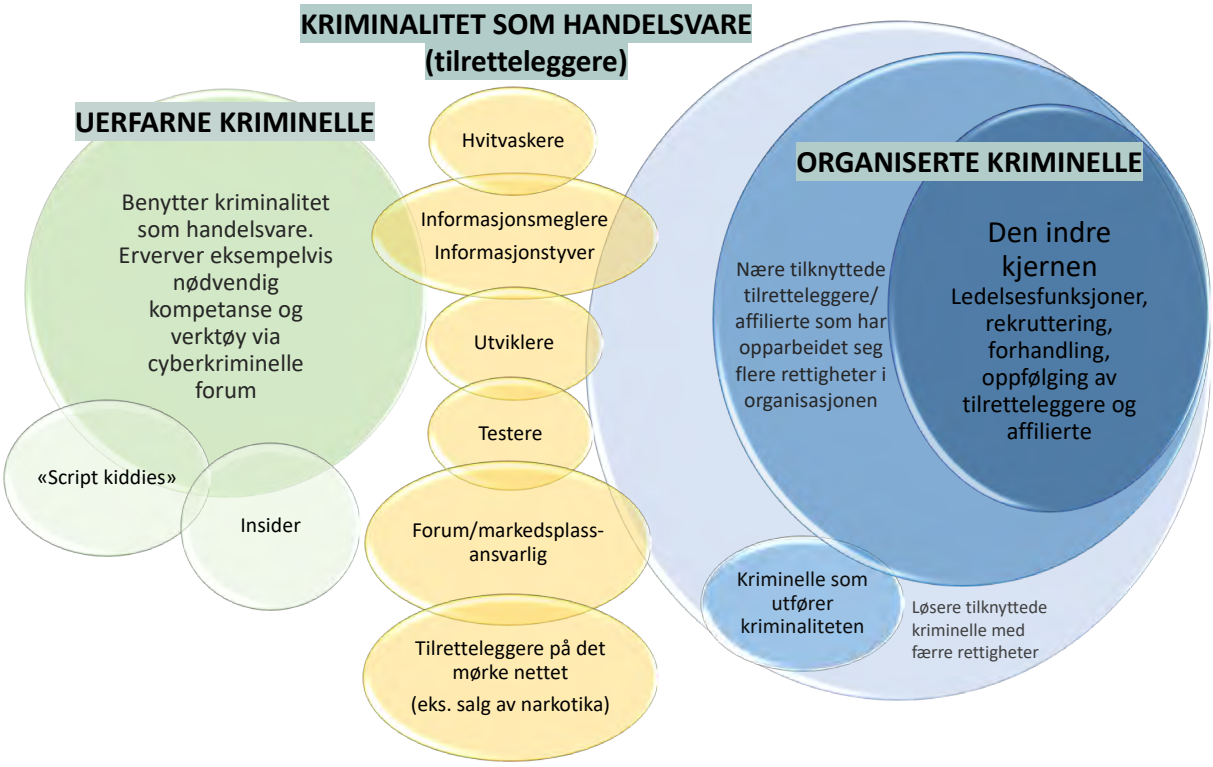
For å selge narkotika på det mørke nettet benytter organiserte kriminelle seg av en rekke muliggjørere. Denne måten å operere på gir kriminelle en følelse av økt operasjonell sikkerhet. I tillegg fører det til kostnadskutt for deler av operasjonen. Alt fra annonsering til kommunikasjon og betaling skjer på internett. På den måten vil det ikke være behov for fysiske tilretteleggere i like stor grad. Kjøper og selger må ikke kjenne til hverandre for å utføre handler, og det er ikke behov for å møtes fysisk. Utviklingen har i løpet av 2024 medført lavere priser og høyere kvalitet på narkotikaen som selges via det mørke nettet.

Samtidig har Kripos i senere år sett at denne typen kriminalitet også bruker det åpne nettet og sosiale medier i stadig økende grad. Her blir det åpent reklamert for kriminaliteten på tjenester som Telegram, Snapchat, Signal, Instagram og TeleGuard. Hele det kommersielle aspektet av kriminaliteten er godt organisert.

Når organiserte kriminelle nettverk som tidligere har solgt narkotika i den fysiske verden flytter deler av sin operasjon til både det åpne og mørke nettet, vil det føre til et større handlingsrom for de kriminelle.

Et annet eksempel som illustrerer organiserte kriminelles bruk av digitale muliggjørere er bruk av såkalte kryptokort i hvitvasking av utbyttet fra narkotikavirksomheten. Disse kortene ligner vanlige debetkort, men tillater kryptovaluta som betalingsmiddel i vanlige kortautomater i ordinære butikker, samt ved uttak av kontanter fra minibanker. Bruken av kryptokort muliggjør en omgåelse av tradisjonelle finansielle systemer som er underlagt regulatoriske rapporteringskrav og gir dermed en viss anonymitet i transaksjonene. Et annet eksempel er at Vipps i 2024 har utvidet sitt virkeområde for direktebetaling til Sverige, Finland og Danmark. Mulighetsrommet for aktører som for eksempel ønsker å kjøpe egenprodusert seksualisert materiale av barn fra andre nordiske land er derfor blitt betraktelig større. Kripos har likevel ennå ikke observert tilfeller der barn i Norge har solgt egenprodusert seksualisert materiale til nordiske borgere.

Økt etterspørsel etter kjøp og leie av muliggjørere og tilretteleggere peker i retning av kriminelles økte avhengighet av det digitale rom for å utøve sin kriminelle virksomhet, altså helt til høyre i det cyberkriminelle spekteret (figur 1, side 12).



Figur 5: Viser hvordan uerfarne og organiserte kriminelle nyttiggjør seg av KSH, ved kjøp/leie av tilretteleggere i utførelsen av kriminalitet. Modellen er utviklet av Kripos.

Tilretteleggere for cyberkriminalitet

I tillegg til muliggjørere er kriminelle i større grad avhengige av spesialister som kan utføre spesifikke oppgaver i cyberdomenet. Økt etterspørsel har gjort det lukrativt å tilby både varer og tjenester på det kriminelle markedet. Dette har ført til at den enkelte ikke lenger har behov for å tilegne seg disse egenskapene, og kjøp eller leie av spesialiserte tjenester har over tid ført til økt profesjonalisering i alle ledd i cyberkriminaliteten.

I årets rapport defineres disse spesialistene som tilretteleggere og besitter gjerne spesialistkompetanse innenfor ett felt. For cyberrettede kriminelle kan dette være skadevarebyggere, informasjonstyver eller penetrasjonstestere. For kriminelle som utfører cyberstøttet kriminalitet, innebærer dette et behov for bruk av hvitvaskere,

økonomiansvarlige og personer som drifter forum for salg av overgrepsmateriale, men også de som tilrettelegger for salg av fysiske varer som narkotika på internett.

Kripos har observert at rekrutteringsprosessen av tilretteleggere innenfor enkelte cyberrettede grupperinger følger en form for tidslinje. Det er i noen tilfeller observert at tilrettelegere først rekrutteres fra legitime jobbsøkerplattformer. Videre i rekrutteringsprosessen benyttes ulike muliggjørere, hvor kontakten med aktuelle kandidater foregår på krypterte meldingsplattformer. Der blir kandidaten spurt om arbeidserfaring og testet i hvilken kunnskap vedkommende innehar. Om kandidaten er aktuell, tas vedkommende med videre på en sikker chat-plattform. Der blir det diskutert andel av utbytte eller lønn. Derfra tildeles arbeidsoppgaver basert på kompetanse.

Videre har Kripos observert at enkelte cyberkriminelle grupperinger ofte rekrutterer fra eksisterende cyberkriminelle nettverk, gjerne basert på bekjentskap og renommé, og at ulike grupperinger konkurrerer med hverandre om de cyberkriminelle med mest erfaring og ettertraktet kompetanse.

Kripos anser muliggjørere og tilretteleggere som sentrale komponenter for opprettholdelse og drift av organisert og annen alvorlig kriminalitet på internett. De skaper et mulighetsrom for kriminelle på internett ved at de tilrettelegger, og driver kriminaliteten fremover.

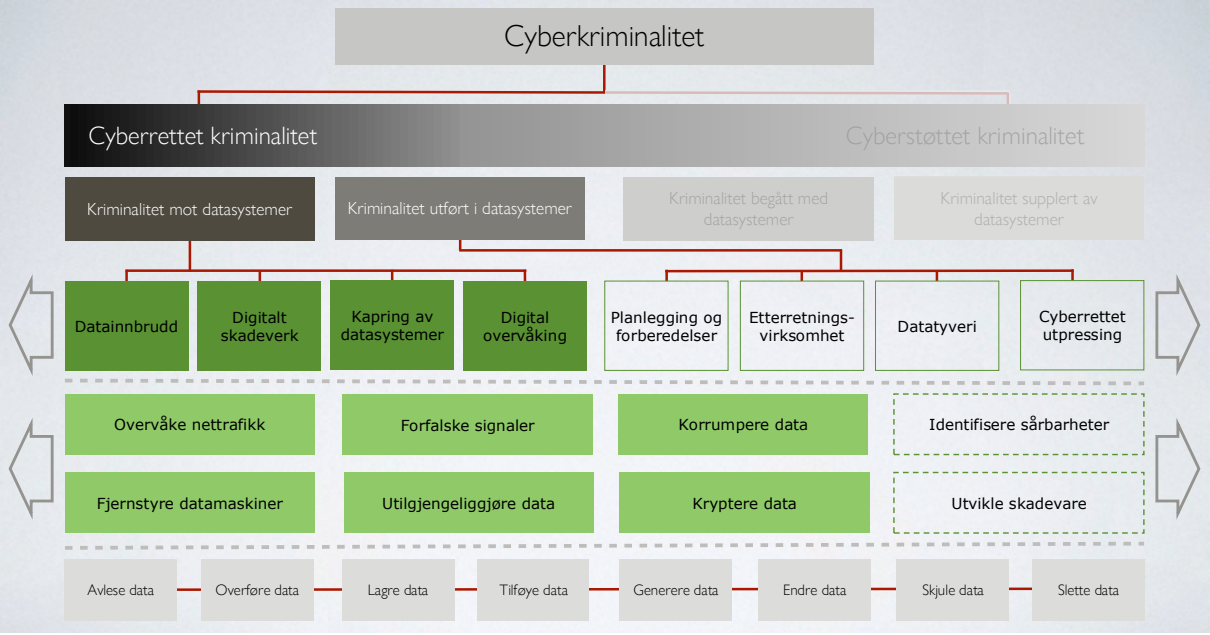
Kripos har tidligere identifisert elleve grunnleggende drivere for cyberkriminalitet.[15] De fem driverne «planlegging og målrettethet», «kommunikasjon», «koordinering», «påvirkning» og «deling av informasjon og data» omtales som operasjonelle drivere og er forholdsvis like uavhengig av kriminalitetstype. Organiserte kriminelle nettverk trenger muliggjørere og tilretteleggere for å imøtekomme behov som de operasjonelle driverne skaper. Dette understreker teknologiens relevans i bekjempelse av organisert og annen alvorlig kriminalitet.

15 Kripos. (2023). *Cyberkriminalitet 2023.* s. 14. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf


Edit
Cocaine | Silk Road
http://anxz6zefk72ulzz
Silk Road
anonymous marketplace
sort by
seller feedback
Drugs(436)
Stimulants(52)
Cocaine(11)
Prescription(16)
Meth(1)
Mephedrone(1)
Cannabis(134)
Ecstasy(15)
Dissociatives(6)
Psychedelics(71)
Opioids(25)
title
8 ball (3.5g) cocaine
1 gram cocaine litm
3.5 gram cocaine li
Cocaine 0.5g SAM
Pretty Good Coca
Cocaine to you.
Cocaine Shippe
Cocaine - 1 gra
Cocaine - 1 gr
Cocaine - 1 g

Foto: Shutterstock

Cyberrettet kriminalitet



Figur 6: Oppdatert begrepskart for cyberrettet kriminalitet. Endringer inkluderer tilføying av kapring av datasystemer og digital overvåking under *kriminalitet mot datasystemer*, i tillegg til planlegging og forberedelser og etterretningsvirksomhet under *kriminalitet utført i datasystemer*. Eksempler på cyberrettede handlinger (avlange bokser i midten) er også nye av året. Modellen er utviklet av Kripos.

Cyberrettede kriminalitetstyper

Kripos har oppdatert kriminalitetsoversikten innen cyberrettet kriminalitet fra i fjor. Begrepskartet i figur 6 viser fire kriminelle handlinger som *retter seg mot datasystemer*: datainnbrudd, digitalt skadeverk, kapring av datasystemer[16] og digital overvåking (mørkegrønne bokser). I tillegg er det en rekke handlinger som ikke rammer datasystemer direkte, men som innen cyberrettet kriminalitet, blir *utført* i datasystemer. Eksempler kan ses i modellen som bokser uten figurfyll med grønn kantlinje, og inkluderer planlegging og forberedelser av alvorlige cyberangrep,[17] etterretningsvirksomhet mot datasystemer,[18] datatyveri og cyberrettet utpressing[19]. Disse handlingene understøttes av andre kriminelle og mulig kriminelle[20] handlinger plassert i midten av modellen, eksempelvis å forfalske elektroniske signaler[21]. Alle handlinger utføres basert på en rekke grunnleggende aktiviteter (lysegrå bokser nederst) som danner byggeklossene for all cyberkriminalitet – både cyberrettet og cyberstøttet.

Nåsituasjon - det cyberrettede trussellandskapet 2024

Det overordnede situasjonsbildet innenfor cyberrettet kriminalitet viser en noe moderat endring, og politiets data – til tross for mørketall og noe lav anmeldelsesrate – indikerer en

16 Her viser vi til at en utenforstående tar kontroll over en datamaskin, enhet eller programvare i den hensikt å utnytte teknologien til kriminelle formål. Eksempler er aktører som tar styringen over OT-systemer for å påvirke fysiske prosesser, eller slave-enheter som inngår i botnet

17 For eksempel å identifisere sårbarheter og utvikle skadevare som er utviklet for å begå digitalt skadeverk mot kritisk infrastruktur

18 For eksempel innhenting av informasjon for å kartlegge nettverk

19 For eksempel løsepengevirus eller distribuert tjenestenektangrep med løsepengekrav

20 Ikke alle handlinger som understøtter kriminalitetstypene er straffbare i seg selv, men disse vil kunne være straffbare dersom visse forutsetninger er oppfylt, for eksempel dersom de må regnes som en nødvendig del av den straffbare handlingen. I mange tilfeller vil disse handlingene uansett være uønskede fra et samfunnsmessig perspektiv, da de utgjør en nødvendig forutsetning for den straffbare handlingen, og de ofte bidrar til en kriminell økonomi

21 Eng: *Spoofing*. Går ut på å utgi seg for å være en annen ved å forfalske avsenderinformasjon. Dette forbindes ofte med forfalskede e-post domener, IP-adresser eller telefonnummer, men kan også innebære forfalskede GPS-signaler fra skip, fly, kjøretøy, satellitter eller smarttelefoner

> Cyberkriminelle har over tid erfart at lovlig og ulovlig tilegnet informasjon om de fornærmedes systemer og brukere er sentralt for å utøve cyberrettet kriminalitet.

økning innen all cyberrettet kriminalitet i 2024. Dette med unntak av tjenestenektangrep, som i stort preges av meget lav anmeldelsesrate og store mørketall.

Kripos observerte en liten økning i antall løsepengevirusangrep mot norske virksomheter i 2024. Basert på dette er kombinasjonen av datainnbrudd, datatyveri, kryptering og utpressing fortsatt den primære handlemåten for løsepengevirusaktører. Dette til tross for at det i år, som i fjor, registreres at enkelte løsepengevirusaktører velger datainnbrudd og datatyveri etterfulgt av utpressing, men uten kryptering. Dette er også observert internasjonalt. Opplysninger fra åpne kilder og politiets egne data indikerer at utviklingen kan være en konsekvens av at flere virksomheter har tilpasset seg trusselsituasjonen og har etablert bedre rutiner for sikkerhetskopiering. For noen virksomheter vil kryptering være en midlertidig driftskonsekvens, mens tyveri av data utgjør ofte en langvarig utfordring. For andre vil det være motsatt.

Kripos observerer at mengden data som stjeles er større enn før. Det er også observert at enkelte løsepengevirusaktører annonserer på det åpne nettet at de har stjålne data til salgs. Publisering av stjålet data på det åpne nettet kan føre til økt risiko for den fornærmede ved at den stjålne informasjonen spres bredere. Dermed kan presset mot den fornærmede øke ved at flere får tilgang til sensitiv informasjon.

Datatyveri utgjorde en vesentlig trussel mot norske virksomheter også i 2024. Cyberkriminelle har over tid erfart at lovlig og ulovlig tilegnet informasjon om de fornærmedes systemer og brukere er sentralt for å utøve cyberrettet kriminalitet. Cyberkriminelle nyttiggjør seg derfor i stor grad av informasjon i utøvelsen av cyberrettet kriminalitet, eksempelvis ved sosial manipulering og tilgang til IT-systemer, eller i utpressingsøyemed. Det samme gjelder kjøp og salg av tilgangsopplysninger. I tillegg til dette har Kripos sett en tydelig utvikling der bruk av offentlig kjente og ukjente sårbarheter har vært en sentral angrepsvektor.

I mai 2024 ble det USA-baserte selskapet Ticketmaster utsatt for datatyveri grunnet et datainnbrudd i skytjenesten til en underleverandør. Gjerningspersonen fikk tilgang til skytjenesten ved bruk av stjålne påloggingsdetaljer fra en bruker som ikke hadde aktivert to-faktorautentisering. De stjålne påloggingsdetaljene lå åpent til salgs på kriminelle nettforum, der noen kan dateres fire år tilbake i tid. I etterkant av datainnbruddet ble Ticketmaster utpresset med den stjålne dataen ved tre anledninger, og av to ulike trusselaktører. Kriminaliteten mot Ticketmaster eksemplifiserer hvordan informasjonens allsidige bruksområde utvider de cyberkriminelles handlingsrom og øker sannsynligheten for å oppnå de kriminelle målene. Samtidig illustrerer hendelsen hvordan de cyberkriminelle stadig går lengre i sin virkemiddelbruk.

Enkelte private og offentlige virksomheter rapporterte i 2024 om en økning innenfor tjenestenektangrep. Eksempelvis rapporterte

Nordea i andre halvdel av 2024 at tjenestenektangrepene økte i intensitet, og at et av angrepene mot dem i oktober 2024 varte i over 25 dager og var mye kraftigere og i en helt annen form enn tidligere observert.[22] Telenor meldte at de i snitt registrerte rundt 140 tjenestenektangrep i måneden i 2024. Til sammenligning hadde politiet per september 2024 mottatt informasjon om 16 hendelser som involverte tjenestenektangrep. Det er svært få som anmelder slike forhold til politiet, og derfor er det vanskelig for politiet å gi eksakte tall for tjenestenektangrep i Norge.

Delvurderinger
Store datamengder som ligger til salgs på markedsplasser er en betydelig trussel da det skaper mulighetsrom for videre kriminalitet og mer utpressing. Det er også mulig at vi kan se flere mindre profesjonelle aktører forsøke å nyttiggjøre seg av stjålet informasjon til utpressingsformål, spesielt dersom informasjon deles på det åpne nettet og spesielt i sosiale medier.

Normalbildet innenfor cyberrettet kriminalitet

Normalbildet innenfor cyberrettet kriminalitet er, slik politiet ser det, som oftest angrep utført av profittmotiverte kriminelle. De små og mellomstore bedriftene i Norge rammes oftest da de er enklere mål, i motsetning til større virksomheter som gjerne har ressurser og kapasiteter til å forebygge og håndtere cyberangrep. Samtidig forekommer målrettede angrep, men disse er ofte rettet mot sentrale tredjeparter for å skaffe seg tilgang til flere virksomheter samtidig (se kapittel om tredjepartsangrep fra side 40). Normalsituasjonen fortsetter derfor å være at små og mellomstore norske virksomheter som ikke har tilstrekkelig med ressurser, kompetanse eller ikke prioriterer beskyttelse av egne verdier, er særlig sårbare for cyberangrep.[23]

Det er i 2024 observert flere cyberangrep hvor trusselaktørene velger å rette sin innsats mot andre deler av verdikjeden for å få tilgang til virksomheters IT-systemer, (se kapittel om verdikjedeangrep fra side 36). Ettersom mange offentlige og private virksomheter er en del av komplekse verdikjeder, hvor det er praktisk umulig å holde oversikt over alle sårbarhetene,

22 E24. (2024, 19. oktober). *Nordea utsatt for kraftige DDoS-angrep: – Enorm økning*. https://e24.no/boers-og-finans/i/MnEQar/nordea-utsatt-for-kraftige-ddos-angrep-enorm-oekning

23 Kripos. (2024). *Cyberkriminalitet 2024*. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

Foto: Shutterstock

vil denne type angrep være en vedvarende risiko for norske virksomheter.

Samspillet mellom eldre og etablerte OT-systemer[24], og nyere, raskt skiftende IT-systemer byr på en rekke nye sikkerhetsutfordringer som forventes å øke i årene som kommer. Eksempelvis vil løsepengevirus rettet mot virksomhetssystemer kunne føre til indirekte påvirkning på fysiske prosesser. Det er i løpet av 2024 observert flere tilfeller av dette i utlandet.

Handlingsmønstre

Cyberkriminelles utnyttelse av verdikjeder og tredjepartsrelasjoner

I fjorårets rapport ble begrepet *leverandørkjedeangrep* brukt for å omtale to relaterte, men ulike teknikker: *verdikjedeangrep* og *tredjepartsangrep*.

Et verdikjedeangrep skjer før produktet eller produktoppdateringen tas i bruk, altså underveis i produktutviklingsprosessen, og skjer gjerne ved at en uautorisert aktør setter inn eller endrer eksisterende kode eller en fysisk komponent i produktet. Denne endringen kan utnyttes på et senere tidspunkt.

Til forskjell innebærer et tredjepartsangrep at aktøren utnytter en sårbarhet hos en tredjepart for å få tilgang til en eller flere andre virksomheter. Et tredjepartsangrep kan kombineres med et forutgående verdikjedeangrep, men de to teknikkene er på ingen måte forpliktet til hverandre. Forenklet kan man si at verdikjedeangrep retter seg mot én bestemt teknologi, mens tredjepartsangrep retter seg mot virksomhetens helhetlige sårbarhetsflate. Til sammen omtaler Kripos disse teknikkene som *kjedeangrep*, da begge teknikkene kan føre til en kjede av nye fornærmede. Dette skillet er nødvendig for å mer nøyaktig vurdere trusselen som følge av de respektive teknikkene, samt implementere effektive og relevante mottiltak.

24 Operasjonell teknologi (OT) er teknologien som understøtter produksjon, leveranse og vedlikehold av fysiske varer og tjenester. Les mer om OT fra side 55

Verdikjedeangrep

Cyberrettede verdikjedeangrep[25] skjer når noen uten tillatelse tilfører egenskaper eller endrer deler[26] av produktet for å utnytte dette senere. Slike endringer kan skje i alle ledd i verdikjeden, enten via programvare, maskinvare eller systemdokumentasjon. Likevel er det ikke *hva* som blir angrepet som avgjør om det er et verdikjedeangrep, men *når* i livsløpet angrepet inntreffer. Et verdikjedeangrep kan benyttes for å begå mange ulike kriminelle handlinger og er derfor ikke bundet til en bestemt kriminalitetstype eller aktørprofil.

> En **verdikjede** beskriver hvor produktet (vare eller tjeneste) tilføres verdi gjennom de ulike leddene i kjeden. Verdikjeden kan strekke seg over flere virksomheter som tilbyr eller etterspør varer og tjenester som inngår i produktet. Begrepet inkluderer hele livsløpet til et sluttprodukt og omfatter rekken av ressurser, prosesser og aktiviteter for produksjon av et produkt.[27]

Innen cyberrettet kriminalitet utføres verdikjedeangrep som regel av aktører som forsøker å tilegne seg uautorisert tilgang til et datasystem via programvare. Programvare utvikles av forskjellige virksomheter og enkeltpersoner. Dette fører til at kriminelle kan utføre verdikjedeangrep via programvare hos førstepart[28], på nettsamfunn for deling av åpen kildekode[29] eller hos tredjepart[30] (Figur 7).

Med teknologiutviklingen blir også programvare stadig større og mer kompleks.

25 Enten eksisterende kode, fysiske komponenter eller systemrelatert dokumentasjon. Uønsket kode kan være bakdører eller annen skadevare som implementeres i programvaren. Fysiske komponenter refererer til innebygde feil, skjulte funksjoner eller uautoriserte deler som inkorporeres i maskinvaren. Systemrelatert informasjon kan være feilkonfigurasjoner eller endring av designspesifikasjoner og manualer som skaper eller utnytter sårbarheter i et system

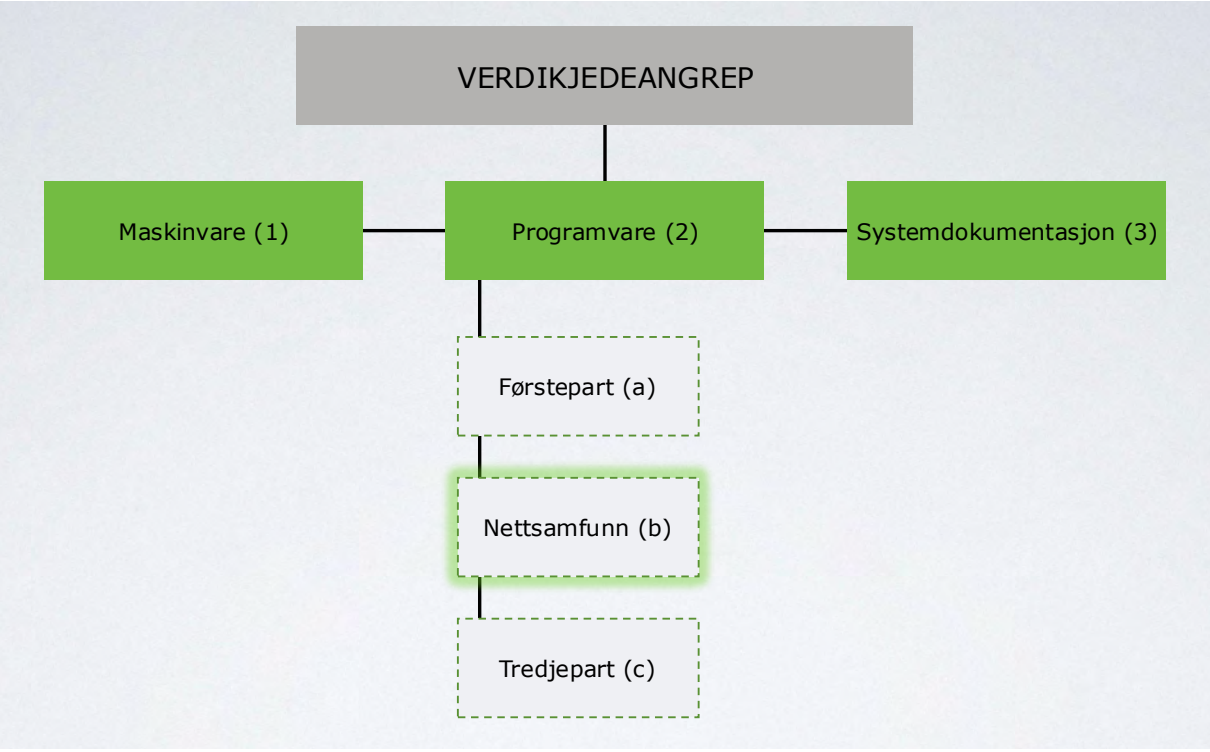
26 Av andre noen ganger omtalt som bakdørangrep eller (eng:) *Shim Attack*

27 Beskrivelsen er sammenstilt basert på: Rolstadås, Asbjørn. (2024, 28. juni). *verdikjede*. Store Norske Leksikon. https://snl.no/verdikjede

28 Viser til e*n virksomhet som utvikler programvare til eget bruk. Eng: In-house Software Development eller First Party Software*

29 Viser til vertsplattformer for deling av kildekode. Eng: *Source-code-hosting Facility* eller «*Forge*»

30 Viser til leverandører som (eng:) *Independent Software Vendor (ISV)/Software Publisher* eller *Original Equipment Manufacturer (OEM)*



Figur 7: Skisserer opp tre ulike typer cyberrettede verdikjedeangrep – via maskinvare (1), programvare (2) og systemdokumentasjon (3). Under verdikjedeangrep via programvare er det listet opp tre steder der en aktør kan forstyrre verdikjeden for programvare – førstepart (a), nettsamfunn (b) eller tredjepart (c). De sistnevnte tre kategoriene har stiplet linje for å indikere at det ikke er gjensidig utelukkende kategorier, da både første- og tredjeparts programvare kan bygge på åpen kildekode. *Nettsamfunn* (2b) er uthevet for å illustrere hvilken del av modellen som er omtalt i teksten nedenfor. Modellen er utviklet av Kripos.

På grunnlag av dette har det vokst frem et behov for samarbeid og deling av kildekode mellom programvareutviklere. Et resultat av dette er at sluttprodukter er satt sammen av flere programvarekomponenter[31] som er skrevet av andre enn programvareutvikleren. Til sammen utgjør dette et stadig voksende og mer uoversiktlig økosystem av utviklere og programvarekomponenter som bygger på hverandre og skaper nye avhengigheter mellom seg.

Verdikjeder for programvare utgjør en massiv sårbarhetsflate med mange involverte parter. Store digitale tjenester som blir utviklet i dag kan – gjennom verdikjeder for programvare med åpen kildekode – være berørt av flere hundre tusen programvarekomponenter og involverer millioner av bidragsytere. Alle disse bidragsyterne representerer en mulig inngang for kriminelle aktører. I perioden 2021-2024 har bruken av åpen kildekode fra nettsamfunn økt med omtrent 200 prosent, og vekstraten er stigende. I samme periode har antall identifiserte ondsinnede programvarekomponenter økt med omtrent 7000 prosent, også med en stigende vekstrate.[32]

Verdikjedeangrep via programvare har i løpet av de siste fem-seks årene gått fra å være en lite utbredt nisjeteknikk til å være blant de raskest voksende teknikkene innen cyberrettet kriminalitet globalt. Aktørene bak verdikjedeangrep har i enkelte tilfeller vist standhaftighet ved å bruke to år på å komme seg i posisjon til å implementere en bakdør, i tillegg til å ha opparbeidet seg høy teknisk kompetanse over lengre tid. Likevel krever ikke alle typer[33] verdikjedeangrep standhaftighet eller særlig teknisk kompetanse, men disse representerer gjerne et mindre skadepotensial.

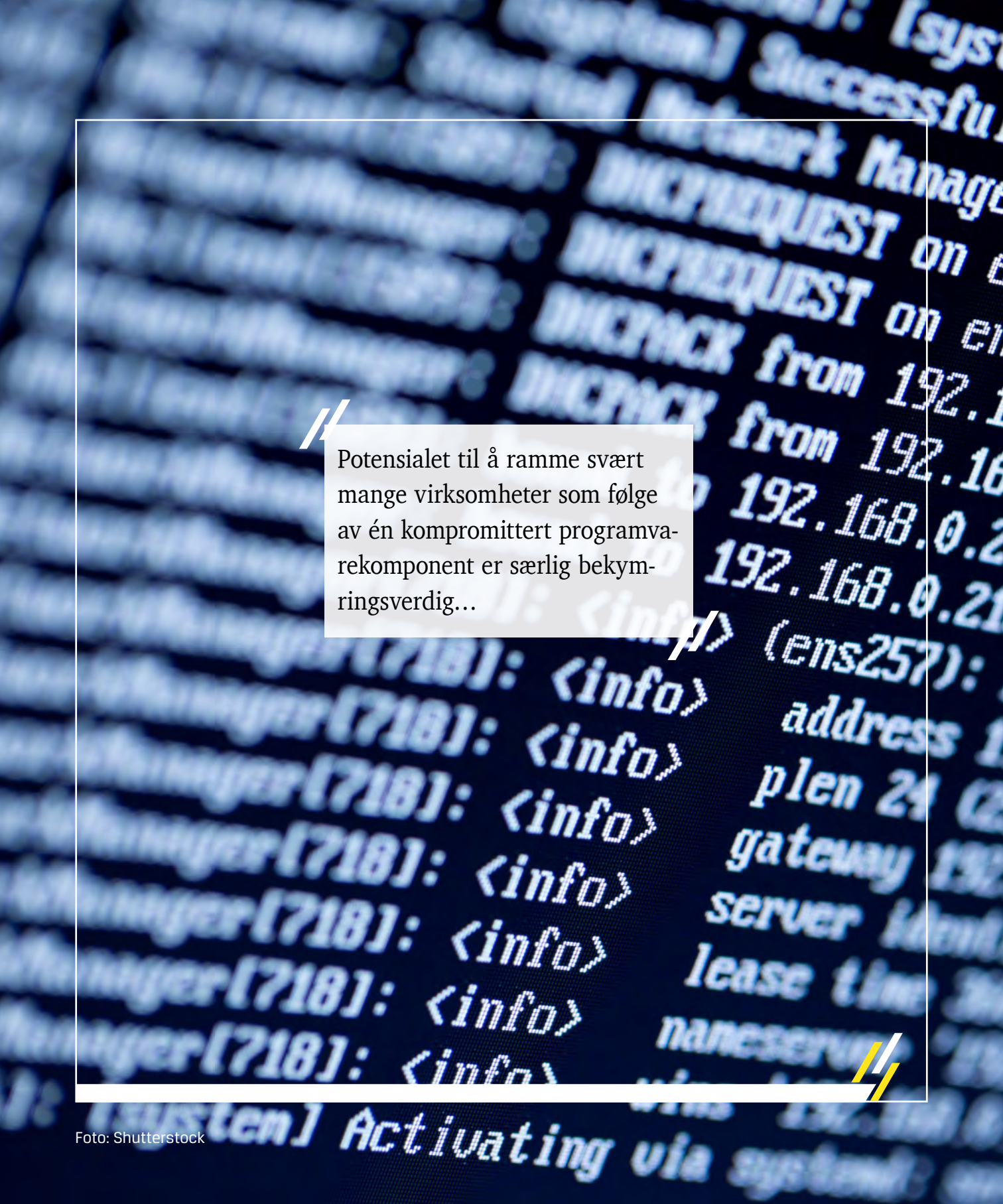
Potensialet til å ramme svært mange virksomheter som følge av én kompromittert programvarekomponent er særlig bekymringsverdig, i tillegg til den økende andelen KI-modeller med åpen kildekode som representerer et sett med nye utfordringer forbundet med verdikjedeangrep. Blant de mest kjente eksemplene på et 2c-verdikjedeangrep (beskrevet i figur 7) var da russisk etterretning installerte en bakdør i SolarWinds Orion-programvaren i 2019-2020. Hovedårsaken til at hendelsen har fått mye oppmerksomhet i ettertid, er et stort omfang berørte virksomheter globalt som følge av at SolarWinds' kunder også ble kompromittert.

---

31 Viser til utdata av en byggeprosess for programvare, også omtalt som (eng:) *Package*

32 Sonatype. (2024). *State of the Software Supply Chain*, *a Decade of Data*. s. 9 og 26. https://www.sonatype.com/hubfs/SSCR-2024/SSCR_2024-FINAL-10-10-24.pdf

33 For eksempel (eng:) *Repo Confusion Attacks* eller dataforgifting av KI-modeller med åpen kildekode ved bruk av verktøy som *EasyEdit*



> Potensialet til å ramme svært mange virksomheter som følge av én kompromittert programvarekomponent er særlig bekymringsverdig…

Foto: Shutterstock

Eksemplet belyser det store skadepotensialet som oppstår i kombinasjonen verdikjedeangrep og tredjepartsangrep.

En hendelse som ikke har fått like mye oppmerksomhet i massemediene er bakdøren som ble lagt inn i programvarekomponenten XZ Utils[34] med åpen kildekode, i mars 2024. Bakdøren ble tilfeldigvis oppdaget like før storskala utrulling. Om dette 2b-verdikjedeangrepet (beskrevet i figur 7) hadde blitt fullbyrdet, kunne det utgjort det mest signifikante verdikjedeangrepet (og muligens datainnbruddet) noen gang.

Tredjepartsangrep

Cyberrettede tredjepartsangrep[35] utføres når en kriminell aktør går via en tredjepart for å ramme en eller flere virksomheter (endemål). Tredjepartsangrep er ikke bundet til ett bestemt handlingsmønster eller én teknikk, ettersom de samme type sårbarheter ofte går igjen hos ulike virksomheter. Det kan være like mange måter å initiere et tredjepartsangrep på, som for cyberrettede angrep generelt. Noen utbredte teknikker inkluderer nettfiskingsangrep som får ansatte til å klikke på ondsinnede lenker eller laste ned infiserte filer, misbruk av lekkede eller stjålne brukernavn og passord, utnyttelse av offentlige kjente og

I denne sammenhengen viser **tredjepart** til en virksomhet som er utenforstående i forholdet til en prinsipal virksomhet.[36] En tredjepart kan være en tjenesteleverandør, for eksempel en skytjeneste- eller internettleverandør, som leverer integrerte tjenester til virksomheter. Tjenesteleverandører kan også levere eksterne tjenester, for eksempel banktjenester eller juridisk rådgivning. Det kan også være en underleverandør, eksempelvis produsenter av maskinvarekomponenter eller leverandør av råmateriale, som er oppstrøms i forsyningskjeden. Andre tredjeparter inkluderer samarbeidspartnere innen eksempelvis logistikk. I noen tilfeller kan også andre kunder utgjøre en tredjepart som følge av gjensidige avhengigheter via for eksempel et felles datasenter.

34 Viser til *XZ Utils* som har avhengigheter til blant annet (eng:) *Secure Shell (SSH) Protocol* og *Linux Distros*

35 Av andre noen ganger omtalt som forsyningskjedeangrep, leverandørkjedeangrep, (eng:) I*sland Hopping Attack* eller *Leapfrogging*

36 Med prinsipal virksomhet mener vi den parten i et forretningsforhold som initierer et oppdrag. Prinsipal kan også forstås som en førstepart i relasjon til en tredjepart

ukjente sårbarheter i tredjeparts programvare eller utførelse av verdikjedeangrep.

Dagens tjenestemarked består av lange og komplekse forsyningskjeder som gjerne involverer flere ledd for å levere et ferdig produkt til sluttkunden. Mengden digitale tjenester som en moderne virksomhet tar i bruk, fører dermed til en tiltagende vekst i antall inngangsporter til alle de involverte virksomhetene. Dette gjør det krevende å holde oversikt, en utfordring som ofte er disproporsjonal med virksomhetenes størrelse og ressurser til å redusere risiko.

Tredjepartsangrep fordrer naturligvis flere steg i angrepsprosessen enn et cyberangrep som har til hensikt kun å ramme én virksomhet. Likevel kan det være flere årsaker til hvorfor en aktør velger å gå den ekstra omveien via en tredjepart. I likhet med verdikjedeangrep kan kompromittering lengre opp i forsyningskjeden gi tilgang til flere mulige fornærmede virksomheter lengre ned i forsyningskjeden, altså flere mulige endemål. Andre forhold som kan oppmuntre til et tredjepartsangrep er tilfeller der en større virksomhet har gode sikkerhetsrutiner og effektive sikkerhetsløsninger som vanskeliggjør tilgang. I slike tilfeller kan den kriminelle aktøren identifisere sårbarheter hos en tilknyttet virksomhet, og på den måten benytte tredjeparten som et springbrett for å nå det vanskeligere tilgjengelige endemålet.

Etter hvert som flere virksomheter gjør seg avhengig av en tredjepart, øker samtidig tredjepartens verdi i kriminelles øyne. Profittmotiverte cyberkriminelle kan basert på en slik sentralisering av verdier, øke lønnsomheten ved å investere mer tid og ressurser i å kompromittere én sentral tredjepart. Alternativet er å bruke potensielt mindre tid på å kompromittere kun én hovedvirksomhet. I tilfeller der tredjepartens tjenester er integrert med kundens egne systemer – eksempelvis skytjenester og internettleverandører som nevnt innledningsvis – vil kriminelles tilgang raskt vokse seg større ved å gå via tredjeparten.

Små og mellomstore bedrifter (SMB) har som regel ikke de samme forutsetningene til å håndtere sikkerhet på samme nivå som store selskaper som leverer profesjonelle sikkerhetsløsninger. Når SMB velger å benytte leverandører som tilbyr blant annet økt sikkerhet – eksempelvis tjenester som gir fjerntilgang via skyløsninger[37]
– kan det oppstå et sikkerhetsdilemma: De kan ta del i en større, sentral løsning som er mer interessant for kriminelle, men fører til bedre sikkerhet generelt. Eller så kan de velge bort profesjonelle tjenester og dermed være et

37 Eksempelvis (eng:) *Managed Service Providers* (MSPs)

mindre attraktivt mål for kriminelle, men samtidig inneha et lavere sikkerhetsnivå.

Kripos har sett flere eksempler på tredjepartsangrep i løpet av 2024, blant annet et tilfelle der en kjent sårbarhet i en mye brukt sikkerhetsløsning, ble benyttet til å kompromittere en norsk totalleverandør av IT-tjenester. Dette tredjepartsangrepet ble med andre ord muliggjort på grunn av to tredjeparter – den kjente sårbarheten hos *programvareleverandøren*, og *totalleverandøren* som benyttet programvaren som en del av sitt tjenestetilbud. Cyberangrepet mot totalleverandøren førte til at flere norske kunder ble rammet av løsepengevirus.

Delvurderinger

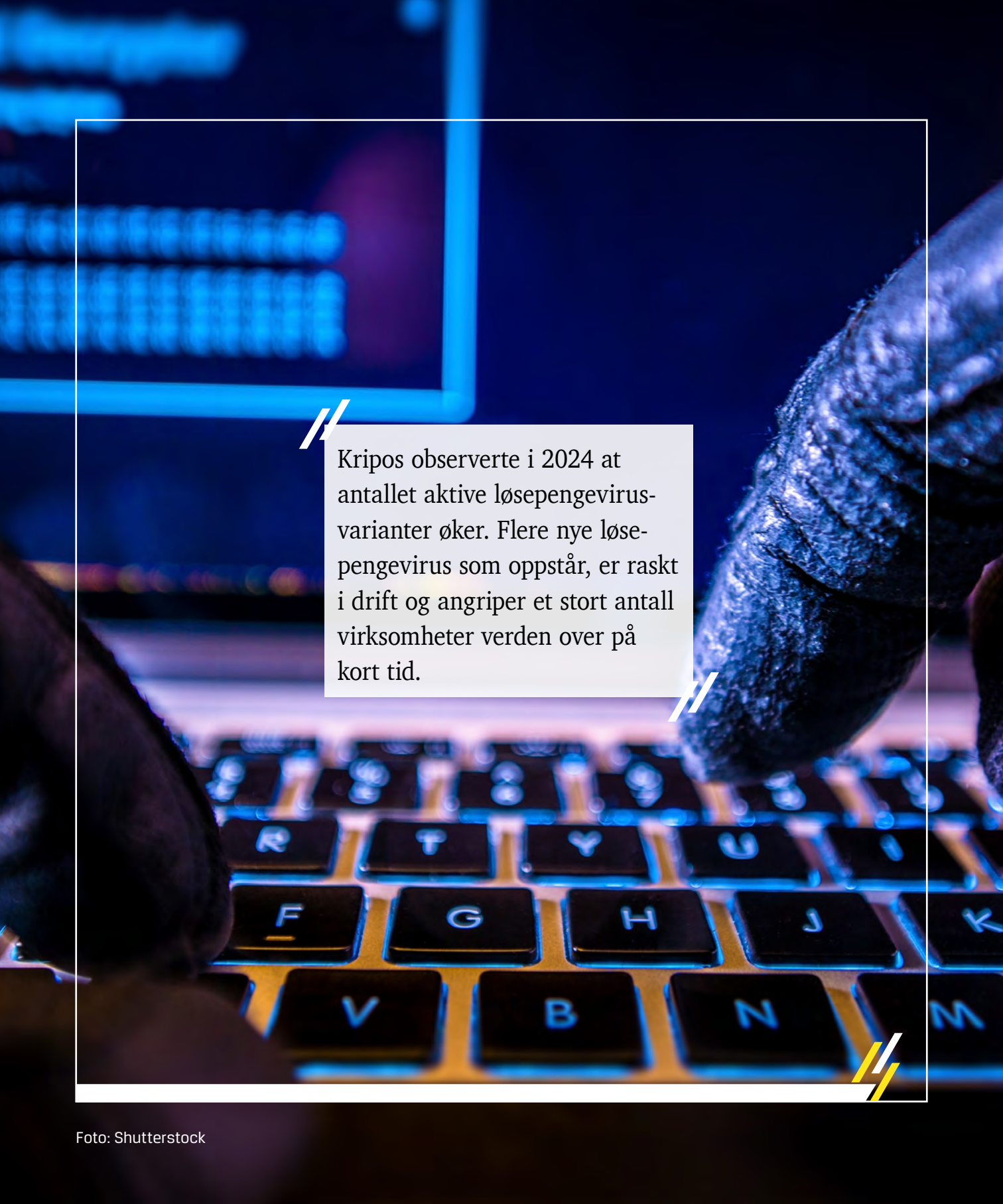
Etter hvert som utvikling innen kunstig intelligens gjør det mulig å automatisere stadig større deler av angrepsprosessen er det *sannsynlig* at kjedeangrep blir mer aktuelle for cyberkriminelle. Videre, med utgangspunkt i dagens kapasitetsbegrensninger blant de kriminelle, er det *mulig* at kombinasjonen KI-agenter og kjedeangrep på sikt vil føre til en vesentlig mengdeendring i antall cyberangrep.

Basert på behovet for store ressurser, tid og målrettethet, er det *sannsynlig* at sofistikerte verdikjedeangrep utføres av statlige aktører eller statlig støttede aktører. Det er likevel *sannsynlig* at profittmotiverte kriminelle vil fortsette å utforske mulighetsrommet som følge av verdikjedeangrep, eksempelvis ved å utplassere skadevare til bruk i utpressing.

Basert på en stadig økende mengde programvare, og avhengigheter mellom disse, er det *sannsynlig* at det blir vanskeligere å avdekke verdikjedeangrep via programvare med åpen kildekode, gitt at prosessen med å oppdage skadelig kildekode ikke blir automatisert.

Det er *sannsynlig* at det i dag dedikeres betydelige ressurser til å posisjonere enkeltaktører eller falske profiler i miljøer for åpen kildekode, som på et senere tidspunkt kan utplassere skadelig kildekode i sentrale programvarekomponenter brukt av norske virksomheter.

Det er *sannsynlig* at det krever større ressurser for å lykkes med et storskala verdikjedeangrep enn det kreves for å finne og utnytte en sårbarhet i en tredjepartstjeneste.



> Kripos observerte i 2024 at antallet aktive løsepengevirus-varianter øker. Flere nye løse-pengevirus som oppstår, er raskt i drift og angriper et stort antall virksomheter verden over på kort tid.

Foto: Shutterstock

Utvikling og endring i handlingsmønstre hos løsepengevirusaktører

Kripos observerer at aktører innenfor LSH-markedet samarbeider om flere skadevarer på samme tid. Aktørene påvirkes av menneskelige relasjoner, erfaringer og internasjonale hendelser, men de er i hovedsak profittmotiverte.

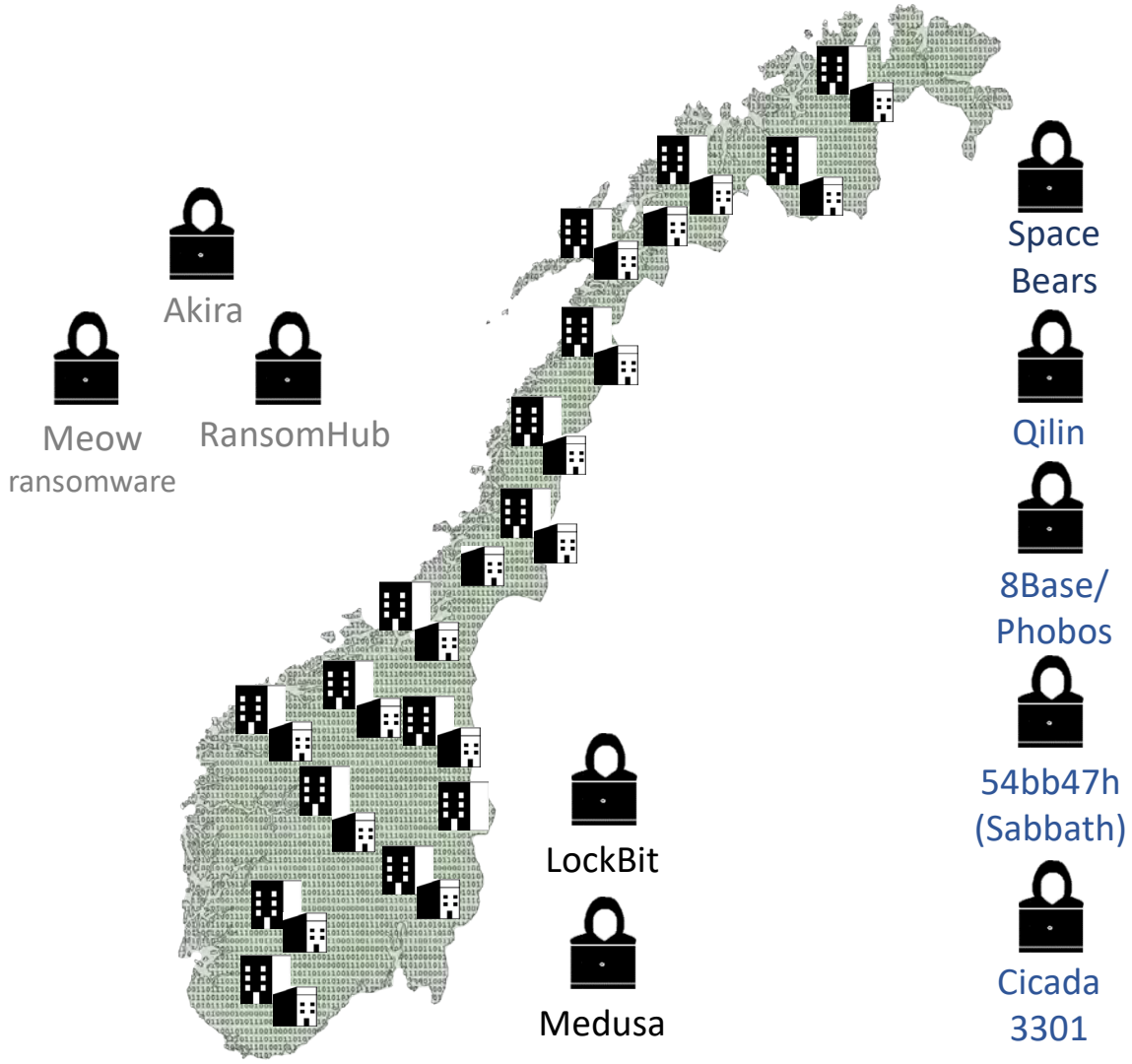
På samme tid observeres det at løsepengevirusvarianter oppstår, legges ned eller tas ned og gjenoppstår under andre navn. Kripos observerte i 2024 at antallet aktive løsepengevirusvarianter øker. Flere nye løsepengevirus som oppstår, er raskt i drift og angriper et stort antall virksomheter verden over på kort tid. Gjennom internasjonalt politisamarbeid fremkommer det at minimum 50 ulike løsepengevirusvarianter hadde blitt brukt til å begå løsepengevirusangrep fra 1. januar 2024 til og med september 2024. Til sammen utgjorde disse 2515 kjente angrep på internasjonal basis. De reelle tallene på antall aktive og nye løsepengevirus er høyere, ettersom det innenfor løsepengevirus er underrapportering av hendelser til politiet og andre myndighetsorganer som fører til mørketall.

De ulike aktive løsepengevirusvariantene i 2024 kan etterlate et inntrykk av at det er mange aktører innenfor løsepengevirusmarkedet. Kripos har derimot observert at løsepengevirusgrupperinger er sammensatte og i bevegelse. Enkeltaktører samarbeider som nevnt med flere ulike løsepengevirus samtidig, og i flere tilfeller er det få kriminelle som utfører angrepet. Kripos har også observert at flere enkeltaktører er seg bevisst hvilken skadevare de velger til hvilken tid og til hvilket angrep.

I tillegg har Kripos observert at løsepengevirusaktører er tilpasningsdyktige. De nedlegger gjerne egen operasjon for en kortere tid av ulike årsaker. Eksempler på årsaker kan være at den gamle kildekoden er lekket, utdatert, eller at deler av infrastrukturen er kompromittert og i fare for å bli tatt ned av politimyndigheter. Den nye løsepengevirusvarianten kan da gjerne bygge på den gamle kildekoden. Samtidig kan den også bygge på en lekket kildekode til et mer profilert og anerkjent løsepengevirus, men da er det i flere tilfeller observert at handlingsmønstre og deler av infrastruktur er den samme.

I fjorårets rapport beskrev Kripos nettopp denne trenden, hvor cyberkriminelle setter sammen nye løsepengevirus ved å bruke fragmenter av lekkede eller stjålne kildekoder.

I løpet av 2023 og 2024 har også flere profilerte og svært profitable LSH-grupperingers infrastruktur blitt tatt ned som følge av internasjonale politiaksjoner. Eksempelvis ble løsepengevirusgrupperingen *LockBits* infrastruktur tatt



Figur 8: Oversiktskart over løsepengevirusvarianter som har rammet norske verdier i 2024. Bygningene viser ikke de faktiske plasseringen til de fornærmede. Modellen er utviklet av Kripos.

ned i mars 2024, og i løpet av en to måneders periode skal to tredjedeler av de affilierte[38] ha forlatt grupperingen. Internasjonalt politi sin innsats mot LSH-grupperinger de siste årene har ført til at løsepengeviruslandskapet har blitt mer fragmentert, blant annet at flere affilierte har forflyttet seg vekk fra profilerte løsepengevirus med et kjent myndighetsfokus. Ifølge Europol skal det både være observert at affilierte forflytter seg til mindre profilerte løsepengevirus, samtidig er en hypotese at affilierte også oppretter egne skadevarer.

Per oktober 2024 var det for politiet kjent at 33 små og store virksomheter innenfor mange ulike sektorer i Norge var rammet av løsepengevirus. Dette er en økning fra 2023, hvor det for politiet var kjent at 26 virksomheter i Norge var rammet. Samtidig er politiet kjent med at flere virksomheter ikke anmelder når de blir utsatt for løsepengevirus, og det er derfor mørketall.

Som kan ses av figur 8 er det totalt 10 ulike løsepengevirusvarianter som står bak. Av disse, skal fem varianter angivelig være nye navn på eldre løsepengevirusvarianter.[39] Disse er alle gruppert sammen i modellen og markert i blått. Dette baserer seg på at det er funnet likheter i blant annet handlingsmønster, infrastruktur eller kildekode. Tre av løsepengevirusvariantene bygger angivelig på lekket kildekode.[40,41] Disse er plassert sammen og markert i grått. Kripos observerer i flere tilfeller at affilierte som eksempelvis er gode på forhandling eller som utfører de faktiske angrepene, nødvendigvis ikke innehar like god teknisk kompetanse selv. Dersom affilierte ikke innehar teknisk kompetanse til selv å utvikle skadevare, må de i større grad benytte lekkede kildekoder til å lage egen skadevare.

Lekkede kildekoder i de senere år har skapt et mulighetsrom for mindre kapable aktører. Videre utvikling peker mot nedleggelse og rask opprettelse av nye løsepengevirusvarianter, nye konstellasjoner for samarbeid grunnet mottiltak fra politi og andre offentlige myndigheter, samt at KSH tilgjengeliggjør kjøp av lekket kildekode som hyllevare. Derfor vil også overlapp med kildekode være en naturlig konsekvens.

På bakgrunn av utviklingen som er observert de senere år, har Kripos erfart at det er viktig å forstå de bakenforliggende mekanis-

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

39 *Cicada 3301*, *54bb47h (Sabbath)*, *8Base/Phobos*, *Qilin* og *Space Bears*

40 *Akira*, *Meow Ransomware* og *RansomHub*

41 *LockBit* og *Medusa* (i sort, figur 8) er kjente løsepengevirusgrupperinger som opererer med flere ulike versjoner av egen skadevare

mene som driver LSH fremover, samt dynamikken, samspillet og samarbeidet mellom ulike løsepengevirusaktører. Samtidig er internasjonalt samarbeid og mottiltak for å identifisere menneskene bak essensielt. Likevel vil det fortsatt være viktig med god kunnskap og innsikt i de ulike løsepengevirusvariantene.

Analyse og videre arbeid med aktører krever forståelse av løsepengeviruslandskapet i sin helhet, hvor både miljø, knytninger på tvers av grupperinger og opparbeidet kompetanse, eller eventuelt mangel på kompetanse som sådan, er en viktig del av bildet.

Delvurderinger

Økt myndighetsfokus har effekt på kriminelle nettverk og gruppedynamikker, og det er *mulig* at flere kriminelle vil forflytte seg fra større til mindre grupperinger for å unngå å havne i myndighets søkelys. Vi vil *sannsynlig* fortsette å se flere grupperinger som opererer innenfor løsepengevirus de neste årene, enten som mindre løselig organiserte kriminelle grupper eller som organiserte kriminelle nettverk.

Kunnskaps- og kompetanseoverføring innad i kriminelle miljøer har bidratt til at flere små grupper tilpasser seg raskt. Videre er det *sannsynlig* at vi vil se flere profittmotiverte kriminelle som benytter mange ulike metoder for å presse fornærmede til å betale løsepenger.

Endringer i handlingsmønstre basert på kunstig intelligens

Kripos har så langt identifisert tre prinsipielt ulike måter å utnytte kunstig intelligens (KI[42]) til kriminelle formål:

1. generere ulovlig innhold;
2. understøtte kriminelle handlinger og aktiviteter; eller
3. selvstendig utføre kriminelle handlinger og aktiviteter på vegne av mennesker.

I tillegg til disse tre ulike måtene å utnytte KI til kriminelle formål, muliggjør KI også nye former for cyberkriminalitet som eksempelvis å angripe KI-systemer eller å indirekte[43] misbruke teknologien. Foreløpig er storparten av observert cyberkriminalitet støttet av KI innenfor en av de to første kategoriene.

I løpet av 2024 har kunstig intelligens fungert som en katalysator for en rekke cyberrettede og cyberstøttede kriminelle handlinger. Eksempler inkluderer syntetisk innhold[44] brukt til å generere overgrepsmateriale (kategori 1), ulike former for bedragerier, forlede nettbrukere til å klikke på skadelige lenker og til å nøre opp under desinformasjonskampanjer. Innen *kriminalitet mot datasystemer* genereres tekst til blant annet passordgjetting og kildekode til blant annet skadevareutvikling (de foregående eksemplene faller innunder kategori 2).

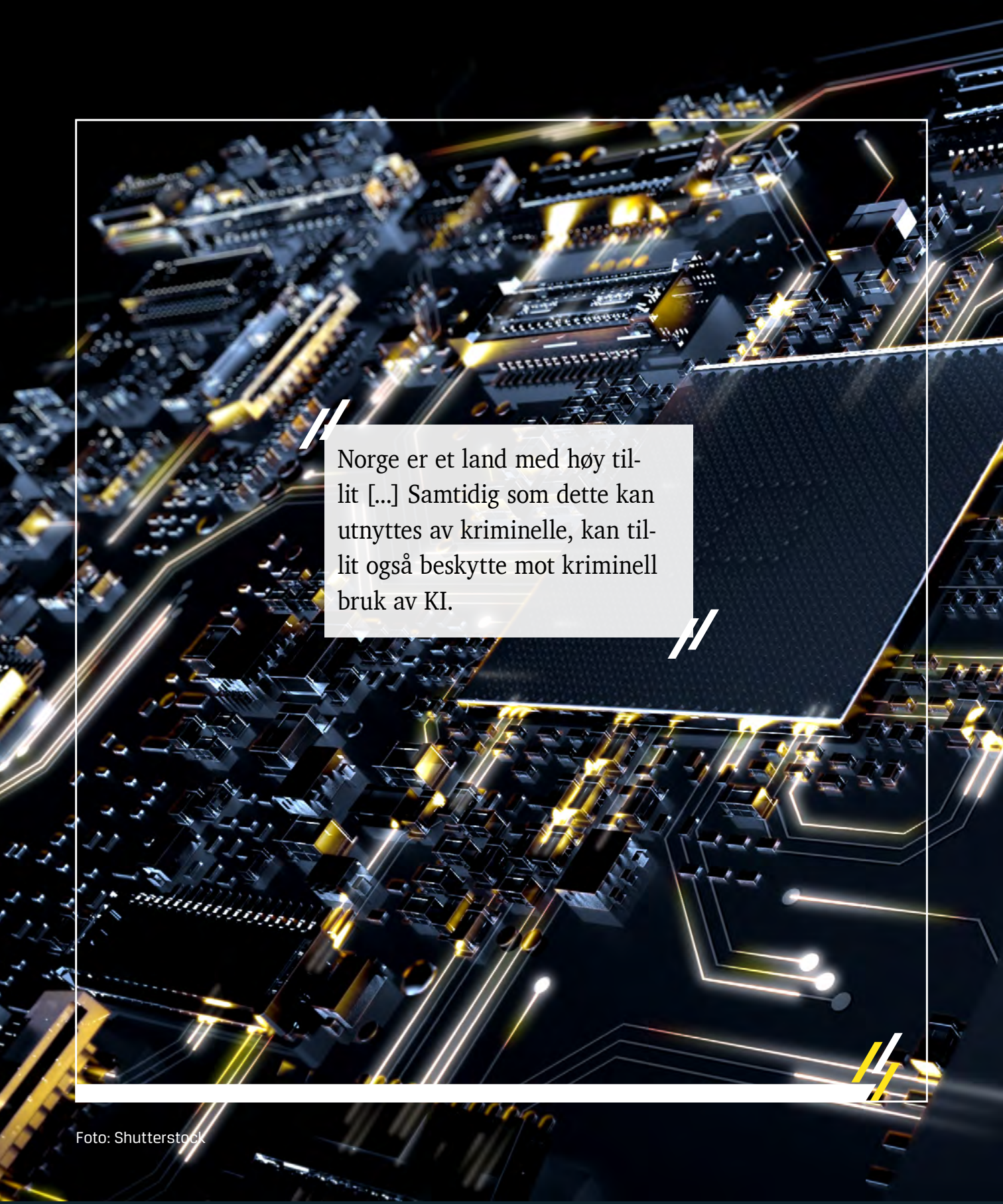
Den nevnte bruken av KI til kriminelle formål inngår i det nye normalbildet hvor KI utgjør en forsterkende faktor som øker kriminelles kapabiliteter og kan understøtte alle typer cyberkriminalitet.[45] Samtidig viser kjente tilfeller av kriminell utnyttelse, at KI er bedre egnet til å understøtte visse kriminelle handlinger og aktiviteter basert på teknologiens nåværende muligheter og begrensninger, i tillegg til aktørenes ekspertise, utstyr, tid og finansielle

42 I denne rapporten benyttes KI overordnet og noen ganger i tilfeller der det ville vært mer presist å bruke betegnelser som maskinlæring, dyp læring eller generativ kunstig intelligens

43 Med indirekte misbruk menes handlinger der teknologien ikke er direkte involvert, men hvor selve eksistensen av den blir utnyttet til å svindle eller lure. Eksempler inkluderer investeringsbedragerier som gir falske lovnader om gevinst basert på urealistiske egenskaper ved teknologien; å lure nettbrukere til å laste ned et KI-program eller -applikasjon som inneholder skadelig kode; eller å fremsette falske påstander om at teknologien har blitt brukt uten at det har skjedd

44 Viser i denne sammenheng til bilde, video, lyd eller tekst

45 Varslet i: Kripos. (2023). *Generativ kunstig intelligens* og *cyberkriminalitet*. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/etterretningsrapport-generativ-kunstig-intelligens-kripos.pdf



> Norge er et land med høy tillit [...] Samtidig som dette kan utnyttes av kriminelle, kan tillit også beskytte mot kriminell bruk av KI.

Foto: Shutterstock

ressurser. Innen cyberrettet kriminalitet gjelder dette spesielt rekognoseringsaktiviteter – som blir mer effektive gjennom automatisering og optimalisering – samt bruk av syntetisk medieinnhold av både ekte og oppdiktede personer som brukes i sosial manipulasjon (kategori 2).

Dypforfalskninger i møterommet

Kvaliteten på KI-generert innhold utvikler seg raskt, og grunnlagsmodeller[46] genererer nå bilder og lyd som mennesker alene ikke kan skille fra ekte innhold. Kripos forventer at dette etter hvert også vil gjelde syntetisk video av ekte mennesker, som kan genereres i sanntid uten forsinkelser. Samtidig utvikles nye metoder som, i kombinasjon med tid og andre ikke-tekniske metoder, vil bidra til å bekrefte at innhold er syntetisk. Det endelige utfallet av utviklingen innen troverdig syntetisk innhold og verktøy som avdekker slikt innhold er foreløpig uklart.

I fjorårets rapport vurderte Kripos at KI vil utfordre tilliten i samfunnet ved å problematisere hva som er ekte og hva som er syntetisk generert innhold. Norge er et land med høy tillit, både sosial tillit og tillit til institusjoner. Samtidig som dette kan utnyttes av kriminelle, kan tillit også beskytte mot kriminell bruk av KI. Eksempelvis utgjør tillit en grunnleggende forutsetning for landets evne til å håndtere kriser og befolkningens deltagelse i demokratiet.

I løpet av 2024 dukket det stadig opp nye tilfeller med dypforfalskninger[47] av kjendiser og statsledere som sier eller gjør noe de aldri har sagt eller gjort. Som regel er dette opptak av forhåndsgenerert innhold som spres i sosiale medier, og det har foreløpig vært forholdsvis enkelt å avskrive disse tilfellene som dypforfalskninger. Blant annet fordi det som regel ikke foreligger tidspress, og aktuelt innhold blir gjenstand for nærmere undersøkelse.

Til tross for økt bevissthet i samfunnet rundt kriminelles misbruk av teknologien, eksempelvis sosial manipulasjon og nettfisking i tillegg til kriminelles bruk av KI, kan selv den mest årvåkne bli lurt av stadig mer utspekulerte og kreative kriminelle metoder. Kripos er derfor på kort sikt mindre bekymret for samfunnets evne til å avgjøre om innhold er ekte eller syntetisk, og mer bekymret for at enkeltpersoner ikke er kritisk til autentisiteten til avsenderen i sanntidskommunikasjon.

Denne bekymringen springer ut fra dypforfalskninger som genereres i sanntid og

46 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, herunder også store språkmodeller. Kjente eksempler inkluderer OpenAI: *ChatGPT*, Google: *Gemini* og *Anthropic: Claude.* Eng: *Foundation Models*

47 Eng: *Deepfakes*

bidrar med en sosial tilstedeværelse gjennom interaksjon med andre mennesker og dypforfalskninger. Et eksempel på dette er å digitalt klone en persons utseende og stemme som legges over en direkteoverført video.[48] På den måten fremstår det som om personen sier og gjør det som blir sagt og gjort i videoen. Det er nå mulig å skape troverdige dypforfalskninger som dette med teknologi som er tilgjengelig for allmenheten.

Et annet eksempel på dynamiske[49] dypforfalskninger er såkalte KI-avatarer[50] som, i tillegg til audiovisuelle likheter til personer de representerer, er trent eller finjustert basert på personlig historikk og personlighetstrekk. Dette gjør at en KI-avatar kan selvstendig interagere med andre og utvise holdninger og personlighet som reflekterer personen den er trent til å etterligne. Kripos har foreløpig ikke observert KI-avatarer som umulig kan skilles fra ekte mennesker. Likevel indikerer en økende mengde kommersielle tjenestetilbydere at interessen er stor og at teknologien fortsatt er i rask utvikling.

Når slike dynamiske dypforfalskninger interagerer med mennesker i sanntid, kan dette oppleves mer troverdig enn forhåndsinnspilte dypforfalskninger av offentlige personer. På den ene siden er flertallet i nettsamfunnet nå klar over at KI kan brukes til å generere dypforfalskninger, og bevisste nettbrukere har generelt blitt mer skeptiske til innhold som deles i sosiale medier. På den andre siden er det som regel mindre tid og færre tilgjengelige ressurser til å undersøke hvorvidt direkteoverført medieinnhold er ekte. Samtidig er kjennskapen til direkteoverførte dypforfalskninger av privatpersoner antageligvis lavere, noe som antydes ved at lav teknisk kvalitet på slike dypforfalskninger har blitt misforstått som dårlig nettverksforbindelse.

Et eksempel der direkteoverført dypforfalskning har blitt brukt til kriminelle formål i 2024 var da ansatte i et multinasjonalt selskap ble lurt til å overføre 200 millioner Hongkongdollar (i overkant av 280 millioner norske kroner) til svindlere. En avgjørende fase i svindelen var en videokonferanse der alle andre enn den ansatte var syntetiske fremstillinger av ekte mennesker, deriblant selskapets økonomidirektør (CFO) som beordret den ansatte til å utføre flere «hemmelige transaksjoner». Etterforskningen som ble ledet av politiet i Hong Kong viste at svindlerne hadde brukt offentlig

48 Også omtalt som (eng:) *Face Swap, Digital Face Replacement* eller *Reface*, sammen med stemmekloning

49 Altså medietyper som er i endring (video og lyd), til forskjell fra statiske dypforfalskninger som ikke endrer seg (bilder)

50 Også omtalt som digitale tvillinger eller virtuelle mennesker

tilgjengelig lyd- og videoopptak til å digitalt klone ansattes stemme og ansikt.

KI-agenter under oppmarsj

Dette delkapittelet bygger videre på forrige rapport,[51] der Kripos varslet om utviklingen innen KI-agenter. I løpet av 2024 har denne utviklingen for alvor begynt å ta form ved at flere kommersielle tilbydere tilfører agentiske egenskaper[52] til grunnlagsmodeller, samtidig som det stadig dukker opp nye KI-agenter med åpen kildekode.

Kripos har tidligere vurdert at den store mengdeendringen i cyberrettet kriminalitet vil først skje etter at KI-systemer selvstendig utfører kriminelle handlinger og aktiviteter på vegne av mennesker (*kategori 3* nevnt innledningsvis på side 48). Utviklingen innen agentiske systemer fører teknologien nærmere denne endringen, og allerede nå er det mulig å helautomatisere datatekniske oppgaver som tidligere har fordret menneskelig involvering. Dette er direkte overførbart til kriminelle handlinger som begås med datamaskiner.

> ...den store mengdeendringen i cyberrettet kriminalitet vil først skje etter at KI-systemer selvstendig utfører kriminelle handlinger og aktiviteter på vegne av mennesker.

De mest kapable KI-agentene som utvikles i dag er utviklet basert på programvaredesign[53] som legges utenpå eksisterende grunnlagsmodeller. Til forskjell fra disse grunnlagsmodellene alene, kan KI-agenter blant annet ta kontroll over datamaskiner, bruke digitale verktøy, planlegge fremgangsmåter, forfølge en ønsket sluttilstand og samarbeide med andre KI-agenter eller mennesker. Disse funksjonene utvider bruksområdet til grunnlagsmodeller, ettersom modellen ikke lenger begrenses til kontekstvin-

51 Kripos. (2024). *Cyberkriminalitet 2024*. s. 63. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

52 Med agentiske egenskaper menes (nor/eng:) mål (*Objectives*), handlinger (*Actions*), minne (*Memory*) og refleksjon (*Rethink*)

53 Til forskjell fra selve grunnlagsmodellen som gjerne er konstruert basert på neurale nettverk. Dette plasserer samtidig dataingeniørfaget sentralt i den videre utviklingen av teknologien

duet[54] hvor brukeren legger inn instruksjoner og grunnlagsmodellen genererer svar.

I tillegg til å utvide den digitale rekkevidden til grunnlagsmodeller, fører agentiske egenskaper også til økte prestasjoner. Til sammenligning med mennesker, genererer ikke nødvendigvis grunnlagsmodeller det beste svaret på første forsøk. Det viser seg at når en grunnlagsmodell får flere forsøk på å løse en oppgave og evaluerer egne svar, fører dette grunnlagsmodellen nærmere sitt absolutte potensial. Disse reflekterende egenskapene innebærer ikke endringer i selve grunnlagsmodellen, men fører likevel til økte kapabiliteter. Dette innebærer at enkelte eldre modeller som er avskrevet med utgangspunkt i funksjons- og kvalitetsmessige begrensninger, nå bør revurderes med hensyn til kriminell nytteverdi.

Delvurderinger

Kriminell utnyttelse av teknologien er ikke underlagt reguleringer eller standarder og kan dermed raskt tas i bruk, med høy toleranse for feil og ufullkommenheter. Basert på dette er det *sannsynlig* at kriminelle aktører vil fortsette å være mer tjent med teknologiske nyvinninger som KI-agenter i et begrenset tidsrom, før det utvikles effektive mottiltak.

Kripos har tidligere vurdert at KI-generert innhold *meget sannsynlig* vil utfordre tilliten i samfunnet. Dette gjelder både tilliten til digitalt innhold som deles av enkeltpersoner, massemedier og institusjoner, i tillegg til digital kommunikasjon mellom mennesker. Denne vurderingen står seg, samtidig er det *sannsynlig* at dypforfalskninger som benyttes i sanntidskommunikasjon vil utfordre den sosiale tilliten på et dypere plan enn forhåndsgenerert innhold.

Det er videre *sannsynlig* at samfunn som Norge, som er preget av kort maktavstand og høy individualisme, er bedre rustet til å håndtere utfordringer forbundet med tillit til informasjonens troverdighet.

54 Kontekstvindu viser til brukergrensesnittet («chatten») der grunnlagsmodellen mottar en instruks fra en bruker (inndata) og genererer svar (utdata). Kontekstvindu brukes også som et mål på hvor mye informasjon en modell kan ta hensyn til per instruks, og kan dermed ha et kort eller langt kontekstvindu

Foto: Shutterstock

Operasjonell teknologi (OT)

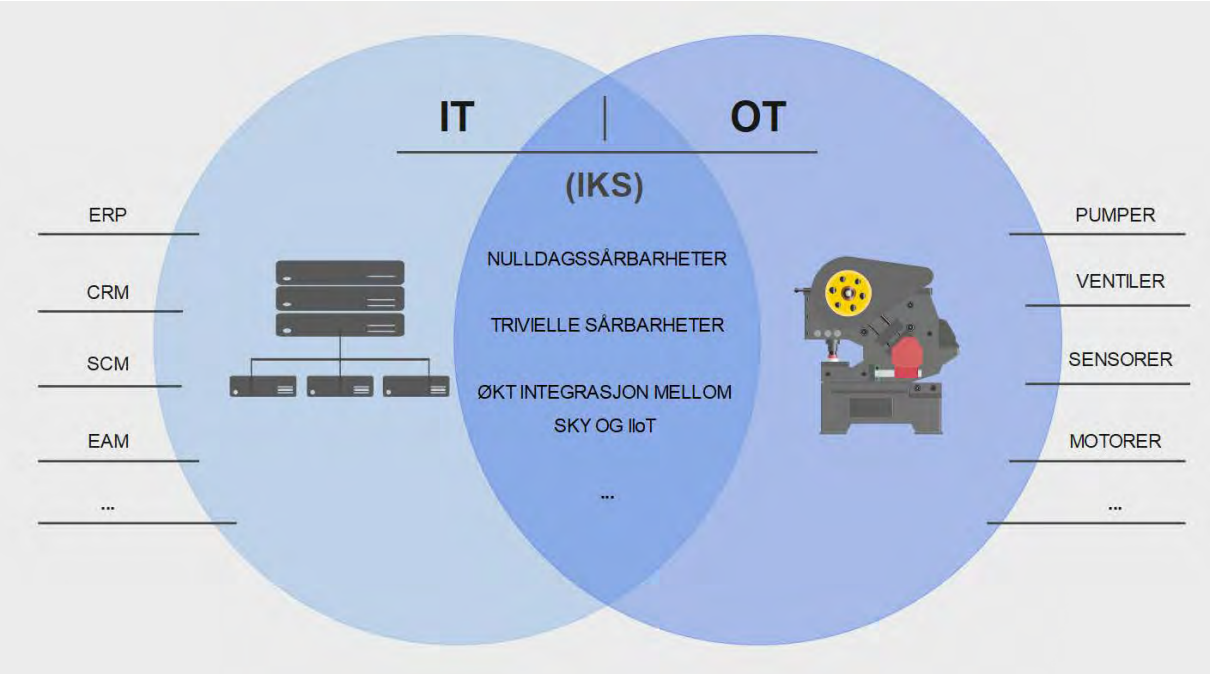
En stor andel av teknologien som benyttes i industrielle miljøer i dag ble utviklet før cybersikkerhet var en bekymring. Disse systemene er lagd for å vare lenge, og etter hvert som annet utstyr har blitt tilpasset og integrert med denne eldre teknologien, har utdaterte enkeltdeler blitt vanskelige og kostbare å skifte ut. Samtidig er moderne industriselskaper avhengig av data som sier noe om tilstanden til de løpende prosessene for å effektivisere drift, optimalisere profitt og trygge fysiske prosesser. Dette behovet for løpende informasjon om operasjonell drift fører til at den eldre teknologien, som ikke har innebygde sikkerhetsfunksjoner, nå kobles til internett og kan nås av aktører som ønsker å påvirke de fysiske prosessene eller ramme virksomheter med løsepengevirus. Dette fører til store økonomiske, teknologiske og sikkerhetsmessige utfordringer som angår store deler av samfunnet, inkludert kritisk infrastruktur og kritiske samfunnsfunksjoner.

Storparten av fysiske varer og tjenester som tas for gitt i hverdagen er avhengige av datamaskiner og nettverksteknologi. Virksomhetene innen blant annet energiproduksjon, vann og avløp, logistikk og helsetjeneste har over tid brukt såkalt operasjonell teknologi (OT). OT er teknologien som understøtter produksjon, leveranse og vedlikehold av fysiske varer og tjenester,[55] og utgjør en sentral del av den cyber-fysiske koblingen som ble introdusert i fjorårets rapport.[56] OT-systemer har lenge vært isolert fra internettilkoblede virksomhetssystemer[57], men basert

55 Eksempler inkluderer fysiske enheter som pumper, ventiler og sensorer, i tillegg til spesialtilpassede protokoller og IT-systemer som er utviklet for å understøtte fysiske prosesser

56 Kripos. (2024). *Cyberkriminalitet 2024*. s. 69-73. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

57 Virksomhetssystemer viser til IT-systemer som understøtter administrative og forretningsmessige funksjoner i en virksomhet. IT-systemer er å finne i både virksomhetssystemer og OT-systemer, men virksomhetssystemer involverer ikke oppgaver som er direkte knyttet til operasjonell drift. Se figur 9 (side 56) med støttetekst for ytterligere eksemplifisering



Figur 9: Illustrerer at det finnes flere digitale sårbarheter i overlappen mellom IT og OT som gjelder for begge teknologiområdene. IT-området som ikke overlapper med OT-området utgjør det som omtales som virksomhets-systemer. Dette er altså IT-systemer som ikke er direkte tilknyttet OT. Overlapp mellom områdene utgjør det som omtales som industrielle kontrollsystemer (IKS). OT-området som ikke overlapper med IT-området er operasjonell teknologi som i utgangspunktet ikke er avhengig av IT for å utføre sin funksjon. Digitaliseringen reduserer OT-området som ikke overlapper med IT-området. Modellen er utviklet av Kripos.

på et ønske om å effektivt styre, overvåke og analysere fysiske prosesser, har de to teknologiområdene blitt stadig mer sammenflettet og integrert. I tillegg til å gi økonomiske fordeler og økt operasjonell trygghet[58], bidrar digitaliseringen av fysiske prosesser også til nye avhengigheter og sårbarhetsflater som kan utnyttes av cyberkriminelle.

Teknologiske avhengigheter og en voksende sårbarhetsflate

OT-avhengige virksomheter må ta hensyn til IT-sikkerhet på lik linje med IT-sentrerte virksomheter.[59] De må sørge for en trygg og pålitelig drift med tilhørende ingeniørtekniske utfordringer, i tillegg til å ta hensyn til sårbarhetene som oppstår i den cyber-fysiske koblingen. Disse virksomhetene har med dette enda en dimensjon som må beregnes inn i den totale sårbarhetsflaten, sammenlignet med IT-sentrerte virksomheter. Dette åpner opp for nye muligheter for uønsket påvirkning.

OT-systemer er mer sårbare enn virksomhetssystemer. Sentrale årsaker til dette er lange produktlivssykluser og spesialtilpasset utstyr som er utviklet med hensyn til trygghet fremfor sikkerhet. OT-avhengige virksomheter har ofte strenge krav til tilgjengelighet og oppetid[60], med særlig vekt på pålitelighet, robusthet og redundans. Dette fører til gjensidige avhengigheter mellom nye og eldre OT-systemer som er produsert av forskjellige leverandører, i ulike tidsaldre og med varierende sikkerhetsstandarder. Disse avhengighetene kan være vanskelig å redusere på grunn av blant annet kostnader og tid forbundet med utskifting. Samlet bidrar dette til sterkere avhengigheter og mer kompleksitet i OT-miljøet.

I praksis øker gjerne antall avhengigheter med nytt utstyr som blir introdusert i opera-

58 Trygghet (eng: *Safety*) handler om å forhindre negative konsekvenser av naturlige og menneskeskapte ulykker eller andre uønskede tilstander. Dette til forskjell fra sikkerhet (eng: Security) som handler om å forhindre tilsiktede uønskede handlinger

59 I denne sammenhengen blir virksomheter som ikke er avhengig av OT, men som har en digital sårbarhetsflate, omtalt som IT-sentrerte virksomheter. Begrepet kan like greit byttes ut med bare «virksomheter», men spesifiseringen er gjort for å tydeliggjøre et teknologisk skille som baserer seg på primærfunksjonen til virksomheten

60 Det er ofte ikke mulig å erstatte enkeltutstyr uten å samtidig stanse driften. I noen tilfeller må også større segmenter i OT-miljøet erstattes som følge av utskifting av en enhet eller enkeltkomponenter. For noen virksomheter, eksempelvis vannbehandling, kjemikalieproduksjon eller sykehus, er nedetid uakseptabelt og kan få fatale følger

sjonsmiljøet, noe som fører til i et teknologisk lappeteppe der programvarebaserte sikkerhetsfunksjoner bygges rundt utstyr som er vanskelig å bytte ut. Samtidig fører flere linjer med programkode til en økende angrepsflate i industrielle miljøer. Aktive sårbarheter i OT-systemer kan dermed sies å utgjøre et mengdeproblem, og toleransen for tilstedeværelsen av sårbarheter er derfor ofte høyere for OT-systemer enn for virksomhetssystemer.

Trusselen mot OT-avhengige virksomheter

Risikoen for uønsket påvirkning fra uvedkommende skyldes hovedsakelig at eldre OT-systemer som ble utviklet for å være trygge, robuste og pålitelige – men ikke nødvendigvis med hensyn til sikkerhet[61] – nå kobles sammen med moderne IT-systemer som kan nås via internett. Cyberangrep som påvirker fysiske prosesser i særlig OT-avhengige bransjer[62] har hatt en gjennomsnittlig årlig vekstrate på 90 prosent siden 2019, basert på offentlige kjente tilfeller globalt.[63] Flesteparten av disse tilfellene skyldtes løsepengevirusangrep. I 2022 ble det registrert omtrent like mange løsepengevirusangrep med fysiske konsekvenser[64] som de foregående elleve årene. I 2023 utgjorde løsepengevirus over halvparten av cyberangrepene mot OT-avhengige virksomheter som førte til fysiske konsekvenser.[65]

Det er få kjente tilfeller der trusselaktører har forårsaket skade eller ødeleggelse gjennom manipulasjon av fysiske prosesser. Til forskjell utgjør løsepengevirus mot OT-avhengige

61 Enkelte OT-systemer som er i bruk i dag begynner å nærme seg 100 år og fungerer like godt som den dagen de ble installert. Samtidig blir flere moderne OT-systemer utviklet for å være sikre og motstandsdyktige mot uønsket påvirkning. Dette prinsippet omtales som (eng:) *Secure By Design*

62 Bransjer som er inkludert i statistikken er byggautomasjon, transport, produksjon, tungindustri og kritisk infrastruktur

63 Waterfall. (2024). *2024 Threat report.* s. 1. https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-ot-cyberattacks-with-physical-consequences/

64 Viser til hendelser som førte til driftsstans eller operasjonelle forstyrrelser for OT-avhengige virksomheter

65 Statistikken baserer seg på offentlig kjente hendelser der cyberangrep mot ovennevnte industrisektorer fra hele verden har medført fysiske konsekvenser. Waterfall. (2024). *2024 Threat report.* s. 3; 25-33. https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/2024-threat-report-ot-cyberattacks-with-physical-consequences/

> Til forskjell utgjør løsepengevirus mot OT-avhengige virksomheter en økende og forventet trussel.

virksomheter en økende og forventet trussel. Foreløpig observerte løsepengevirusvarianter fører ikke nødvendigvis til nedstengning av operasjonelle prosesser i seg selv, men løsepengevirus kan skape betydelige forstyrrelser som kan resultere i produksjonstap og nedetid, ofte med ringvirkninger for forsyningskjeder og samfunnet forøvrig.

Det er ikke nødvendigvis slik at alle internettilkoblede OT-systemer kan utnyttes av en trusselaktør. I et tilfelle der en trusselaktør har skaffet fullstendig kontroll over OT-systemene, kan det likevel være umulig å oppnå fysisk skade, kun ved hjelp elektroniske signaler. Samtidig kan en irrelevant sårbarhet i én komponent, utstyr eller nettverk være kritisk i en annen. Dette som følge av teknologiens funksjon og plassering i OT-miljøet. Heldigvis for risikoeiere er ikke alle sårbarheter utnyttbare, og ikke alle utnyttbare sårbarheter er relevante i et gitt OT-miljø. Likevel utgjør uautorisert tilgang til og påvirkning på OT-systemer en potensiell trussel som kan forårsake fysiske konsekvenser. Det er med utgangspunkt i dette skadepotensialet at Kripos har delt inn trusselen mot OT-avhengige virksomheter i to overordnede kategorier: *trusselen mot administrative prosesser* og *trusselen mot operasjonelle prosesser* (se også fra side 68).[66]

Delvurderinger

Basert på blant annet teknisk vanskelighetsgrad og ulike intensjoner ved å utføre cyber-fysiske angrep, er det *lite sannsynlig* at cyberrettede angrep mot fysiske prosesser vil føre til fysisk ødeleggelse eller skade på utstyr, mennesker eller miljø i Norge i løpet av 2025. Videre er det *lite sannsynlig* at hacktivister eller uklassifiserte cyberkriminelle vil utgjøre et mengdeproblem for hva gjelder cyberrettede angrep mot norske OT-avhengige virksomheter i 2025.

66 Dette er en endring fra tidligere inndeling av trusselen som ble gjort i rapport: Kripos. (2024). *Cyberkriminalitet 2024*. s. 71. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

Disse virksomhetene har med dette enda en dimensjon som må beregnes inn i den totale sårbarhetsflaten…

Foto: Shutterstock

Mulige konsekvenser

Samfunnet vårt er gjennomdigitalisert. Digitaliseringen fører til åpenbare fordeler som kostnadsbesparelser, økt produktivitet og tilgjengelighet, mer synlighet og bredere nedslagsfelt for formidlingen, samt økt innsikt gjennom analyse av stordata. En følge av denne digitaliseringen er at det skapes stadig nye avhengigheter gjennom en voksende digital sårbarhetsflate. Dette utnyttes av kriminelle aktører.

De komplekse avhengighetsforholdene gjør det særlig vanskelig å forutse konsekvensene av at datasystemer og informasjon blir utilgjengelig, endres eller blir kjent for uvedkommende. Avhengigheter oppstår på et teknologisk, forretningsmessig og samfunnsrelatert nivå, og disse kan være kjente eller ukjente for risikoeier. Eksempler på situasjoner hvor ukjente avhengigheter *kan* oppstå inkluderer henholdsvis: programvarekomponenter som bygger på hverandre (verdikjeder), flere virksomheter som benytter samme logistikkleverandør (tredjepartsrelasjoner) eller enkeltpersoner og virksomheter som er avhengig av kritiske samfunnsfunksjoner som kraft- og vannforsyning (operasjonell teknologi). På grunn av kompleksiteten i hvordan samfunnet henger sammen, fra et teknologisk til samfunnsmessig nivå, vil det i noen tilfeller være praktisk umulig å forutse alle betydelige konsekvenser av et cyberrettet angrep.

> Dette fører til at svært mange [...] er i posisjon til å forårsake alvorlige konsekvenser for norske interesser basert på handlinger ofte begått fra utlandet.

Kombinasjonen av avhengigheter og flerbruksverdien av informasjon på avveie er sentral i å utvide utfallsrommet som følge av cyberrettet kriminalitet. Konsekvensene av cyberangrep kan derfor være både direkte og indirekte, tilsiktet eller ikke, og kan føre til ringvirkninger som sprer seg utover den umiddelbart berørte parten. Disse konsekvensene kan manifestere seg i både det digitale og fysiske domenet, med skadepotensial for utstyr og systemer, mennesker, virksomheter, miljø og samfunn. Dette fører til at svært mange, uavhengig av profiltilhørighet, geografisk plassering eller bakgrunn, er i posisjon til å forårsake alvorlige konsekvenser for norske interesser basert på handlinger ofte begått fra utlandet.

Noen eksempler på cyberangrep med uforutsette konsekvenser i 2024 er de mange løsepengevirusangrepene mot utenlandske helseforetak.[67] I tillegg til datalekkasjer med sensitive personopplysninger som noen ganger ble etterfulgt av utpressingsforsøk, har løse-

67 Eksempelvis *Lurie Children's Hospital of Chicago*, helsesystemet Ascension, amerikanske *Change Healthcare*, britiske *Synnovis* og rumenske *Hipocrate Information System* (HIS)

pengevirusangrepene ført til problemer med utlevering av resepter, forhindret kommunikasjon mellom leger og pasienter, samt utsettelse eller kansellering av planlagte operasjoner, i tillegg til blodmangel i London.

Konsekvensene av cyberrettede angrep mot OT-avhengige virksomheter

Konsekvensene av cyberrettede angrep mot OT-avhengige virksomheter strekker seg fra driftsforstyrrelser som følge av *indirekte påvirkning* på fysiske prosesser,[68] til bortfall av kritiske samfunnsfunksjoner og fysisk skade på utstyr, miljø og menneskeliv[69]. Noe som fundamentalt skiller OT-avhengige virksomheter fra IT-sentrerte virksomheter er de mulige fysiske konsekvensene som følge av *direkte påvirkning* på fysiske prosesser. Avhengig av hva slags fysiske prosesser[70] som er involvert, hvilken samfunnsfunksjon[71] de tjener og hvilke verdier som trues, vil også de mulige konsekvensene variere. Dersom enkelte av disse OT-avhengige samfunnsfunksjonene slutter å fungere, er det i noen tilfeller ingen planlagte alternativer.

Kripos har tidligere beskrevet den ledende målutvelgelsen blant profittmotiverte cyberkriminelle som *opportunistisk.* Begrepet er byttet ut med ***tilgangsdrevet*** for å gi rom for at disse aktørene kan utvise forskjellig grad av bevissthet og preferanser knyttet til målutvelgelse. Målutvelgelse kan for eksempel utgjøre en kombinasjon av absolutte seleksjonskriterier og sektorvise preferanser, sammen med opportunistiske muligheter som følge av nye tilganger til fornærmedes systemer.

Nylige hendelser med mulige fysiske konsekvenser som er attribuert til profittmotiverte cyberkriminelle inkluderer løsepengevirusangrepene mot det amerikanske oljeserviceselskapet Halliburton og produsenten av mikrokontrollere Microchip Technology Incorporated, som begge ble rammet i august 2024. Som følge av løse-

68 Via virksomhetssystemer
69 Via OT-systemer
70 Fysiske prosesser har ulike karaktertrekk og sårbarheter som utgjør forskjellig skadepotensial. Eksempler inkluderer kjemiske, biologiske, mekaniske og elektriske prosesser
71 Samfunnsfunksjon refererer her til nyttefunksjonen som OT-systemene tjener i samfunnet. Det kan eksempelvis være å sørge for at bydeler har tilgang på vann, strøm og mat, eller at pumpene på et sykehus responderer som tiltenkt og sørger for at kirurgen har tilgang på væske når hun trenger det

pengevirusangrepet ble produksjon og drift i Halliburton forstyrret, men angrepet medførte også til en nedgang i publikums tillit til selskapet og aksjefall.

Cyberangrep med fysiske konsekvenser kan enten være *målrettet* mot operasjonelle prosesser eller de kan resultere fra ringvirkninger som følge av *tilgangsdrevne* cyberangrep rettet mot virksomhetssystemer. I noen tilfeller er de kriminelle ikke klar over at den fornærmede er en OT-avhengig virksomhet, og i andre tilfeller kan digital uønsket tilstedeværelse i et OT-miljø være nok til at trygghetsorienterte ansatte stenger ned fysiske prosesser som et skadereduserende tiltak. Et eksempel på slike trygghetsorienterte prosedyrer er togstansen 20. desember 2024, da ansatte i Bane NOR besluttet å stanse alle tog som følge av en feil på radiosystemet. Selv om det ikke er tegn til aktivitet fra uvedkommende, viser hendelsen hvordan tekniske feil kan føre til fysiske konsekvenser. Med en slik tilnærming kan kriminelle påføre store kostnader uten nødvendigvis å besitte kunnskap eller evne til å direkte påvirke de fysiske prosessene.

Det er derfor ikke nødvendigvis en positiv korrelasjon mellom cyberkriminelle aktørers intensjon og antall cyberangrep med fysiske konsekvenser. Samtidig kan den samme taktikken, teknikken og prosedyren føre til ulike konsekvenser i forskjellige situasjoner. Denne usikkerheten knyttet til sluttresultatet av uønsket påvirkning utfordrer hvordan vi analyserer og forstår trusselen. Ved å rette oppmerksomheten mot *mulige konsekvenser* som følge av påvirkning fra uvedkommende, åpnes samtidig muligheten for at den samme cyberkriminelle handlingen kan resultere i svært ulike konsekvenser. En slik konsekvenstilnærming til trusselen mot OT-avhengige virksomheter vil med fordel kunne trekke oppmerksomheten vekk fra et utstyrs-, teknologi- eller domenefokus, og støtte sikkerhetsspesialister til å se helhetlig på sikkerhet i industrielle miljøer og samfunnet helhetlig.

Når sensitive data blir allemannseie – en kumulativ trussel

Når informasjon kommer på avveie, kan det utgjøre en trussel mot enkeltpersoner, virksomheter og nasjonale sikkerhetsinteresser. Ansamlinger av store datamengder er utbredt i det digitale rom. Dataens innhold varierer fra sensitive personopplysninger[72] og forretningshemme-

72 Oppfatninger om hva som utgjør personopplysninger kan variere. Mest vanlig er kanskje å tenke på demografiske kjennetegn, helseopplysninger eller kontaktinformasjon som navn, adresse, telefonnummer eller digitale brukerkontoer. Andre typer personopplysninger inkluderer lyd og bildemateriell, IP-adresser, seksuelle preferanser og atferdsdata som blant annet daglige rutiner, kjøpshistorikk og fysiske forflytninger

ligheter[73], til tekniske beskrivelser og sikkerhetsgraderte dokumenter. På samme måte har også informasjonen ulik verdi for de kriminelle.

Det finnes mange eksempler på lekkasjer av store mengder sensitiv informasjon som er offentliggjort eller kompromittert, og enkeltpersoner og virksomheter kan fortsette å bli berørt mer enn ti år etter at informasjonen har kommet på avveie. I forbindelse med Russlands invasjon av Ukraina i 2022 og eskaleringen mellom Israel og omkringliggende aktører siden 2023, har det de siste årene vært flere eksempler der sikkerhetsgradert informasjon har blitt lekket eller nedgradert for offentlig distribusjon. Basert på den store mengden tilgjengelig informasjon er det ikke mulig å forutsi hvordan sammenstillingen av informasjon fra ulike kilder kan føre til ny innsikt og åpne opp nye muligheter for kriminelle nå og i det videre.

Samtidig som skadepotensialet til enkelte informasjonspakker kan være betydelig, fører den stadig økende mengden informasjon til nye trusler og uidentifiserte konsekvenser. I løpet av 2024 har det vært flere tilfeller der ti- og hundretalls millioner av personopplysninger har blitt (1) kompromittert eller (2) vært eksponert for offentligheten. Et eksempel på kompromittert informasjon (1) er datainnbruddet mot to hovedleverandører av helseforsikring i Frankrike. Hendelsen førte til at navn, adresser, fødselsdato, personnummer og forsikringsdetaljer til over 33 millioner innbyggere ble kompromittert. I tillegg er politiet klar over at cyberkriminelle aktører sitter på store mengder informasjon om virksomhetene de har kompromittert, uavhengig av om informasjonen har blitt brukt i utpressing eller offentliggjort av andre årsaker.[74]

Et eksempel på data som utilsiktet har blitt eksponert for offentligheten (2) i 2024 er da en feil på en søkemotor med åpen kildekode førte til at 223 millioner poster med fullt navn, fødselsdato, kjønn og skattenummer på brasilianske innbyggere var offentlig tilgjengelig over en uviss periode. I 2022 opplevde Norkart at persondata for opp til 3,3 millioner nordmenn var eksponert for offentligheten og kan ha vært stjålet. Andre tilfeller med kompromitterte eller lekkede data stammer fra blant annet feilkonfigurasjoner, tjenesteleverandører og verdikjeder for programvare – alle med et utvidet skadepotensial.

Det er ikke bare lekkasjer og datatyveri som utgjør den kumulative trusselen som følge av store datamengder på avveie. Det gjelder også informasjon man frivillig gir fra seg gjennom

73 Eksempelvis kundelister, pris- og markedsstrategi, prosedyrer, design og mønstre, oppskrifter/formler eller sammenstilling av informasjon som ikke er allment kjent eller tilgjengelig

74 Typisk informasjonen cyberkriminelle kan besitte etter et vellykket datainnbrudd er oversikter over brukernavn og passord (data fra eks. *Active Directory*)

> Samtidig som skadepotensialet til enkelte informasjonspakker kan være betydelig, fører den stadig økende mengden informasjon til nye trusler og uidentifiserte konsekvenser.

Foto: Shutterstock

sosiale medier, stillingsutlysninger og forbrukerapplikasjoner som musikk-, mat- og transporttjenester. Et eksempel fra oktober 2024 er da franske livvakter uvitende publiserte joggeturer på treningsapplikasjonen Strava. Basert på dette klarte den franske avisen *Le Monde* å avsløre livvaktenes navn og adresse, i tillegg til den franske presidenten Emmanuel Macrons forflytninger.

I tillegg til forbrukertjenester og tredjepartsrelasjoner der man frivillig gir fra seg skjermingsverdig informasjon, blir også informasjon lagret i forskjellige registre[75]. Hvilke informasjoner som blir lagret eller hvordan informasjonen oppbevares kan i liten grad påvirkes av den enkelte. Noen av registrene er offentlig tilgjengelig eller kan utleveres etter innsynsbegjæringer. Samtidig som åpenhet i samfunnet er viktig for å ivareta demokratiske verdier og tillit, kan åpenhet også gjøre oss sårbare for aktører som utnytter denne tilliten til egne formål.

Kripos observerer at mengden data som stjeles er større enn den har vært tidligere. Samtidig er den samlede verdien av tilgjengelig informasjon i irreversibel vekst og informasjon som på et tidspunkt blir offentliggjort digitalt, forsvinner i noen tilfeller aldri. Dette er en følge av blant annet nettbaserte arkiver[76], søkemotorer og lekkasjesider[77] på det åpne og mørke nettet. Dette gjør det vanskelig å avgjøre om kompromittert informasjon som har blitt fjernet, faktisk er utilgjengelig for utenforstående.

Teknologisk utvikling innebærer nye og stadig forbedrede kapabiliteter som ikke nødvendigvis blir tatt hensyn til på tidspunktet informasjonen blir offentliggjort eller kompromittert. Særlig utviklingen innen kunstig intelligens og maskinlæring gjør det mulig å identifisere relevant informasjon, nye mønstre og nye sammenhenger i store datasett. Dette er gjerne sammenhenger som ikke er mulig for mennesker å fange opp.

---

75 For eksempel registre som lagrer helseopplysninger, skatteopplysninger, virksomhetsopplysninger eller strafferettslige opplysninger

76 Viser til en type webarkivering der en søkerobot (eng: Crawler) kontinuerlig og systematisk navigerer nettsider og lagrer informasjonen den kommer over. Det er mange aktører med varierende motiv som bedriver webarkivering. Noen eksempler på tjenester som gir tilgang til historisk innhold inkluderer: *Wayback Machine (Internet Archive), Archive.today, FreezePage* og *ReplayWeb*

77 Viser til nettsider der kriminelle publiserer stjålet informasjon, som regel er dette et steg i å fullbyrde trusler i et utpressingscenario

Delvurderinger

Det er *meget sannsynlig* at store datamengder vil få ny verdi for kriminelle som følge av den videre utviklingen innen kunstig intelligens. Eksempelvis er Kripos kjent med at cyberkriminelle i dag har store mengder sensitiv informasjon fra fornærmede som de så langt ikke har vært i stand til å bearbeide eller utnytte til kriminelle formål. Basert på dette er det *sannsynlig* at allerede kompromittert informasjon vil benyttes i cyberrettet utpressing i 2025 og videre.

Det er stor usikkerhet forbundet med hvordan kriminelle kan bruke kunstig intelligens for å nyttiggjøre seg av informasjon som enkeltpersoner, virksomheter og myndighetene deler offentlig. Det er samtidig *meget sannsynlig* at vi i dag ikke kan forutsi konsekvensene av informasjon som vi frivillig gir fra oss.

Fragmentert ansvar og økende avhengigheter – utfordringer for en helhetlig konsekvensvurdering

Norske virksomheter[78] er oppfordret til å gjøre seg *mindre* avhengige av andre virksomheter, samtidig som de teknologiske og forretningsmessige avhengighetene vokser som følge av den pågående digitaliseringen. Dette avhengighetsfenomenet gjør at ansvaret og risikovurderingen i stor grad blir overlatt til den enkelte virksomhet.

En helhetlig tilnærming som fokuserer på konsekvensene av cyberkriminelle handlinger forutsetter at de skjermingsverdige verdiene[79] identifiseres i stor detalj. Denne vekslingen mellom «helhet» og «detaljer» fordrer samtidig et samspill mellom teknologer og sikkerhets- og beredskapsspesialister, og mellom virksomheter og myndigheter.

Kripos er ikke kjent med en helhetlig kartlegging av IKT-systemer som direkte eller indirekte understøtter de til enhver tid identifiserte grunnleggende nasjonale funksjoner (GNF) eller kritiske samfunnsfunksjoner. Selve identifiseringen og kartleggingen av GNF og kritiske samfunnsfunksjoner er sektorinndelt på departementsnivå. Dernest gjennomfører identifiserte virksomheter

78 Viser til virksomheter som ansees som grunnleggende nasjonale funksjoner (GNF) eller utgjør samfunnskritiske funksjoner, eller har en vesentlig og avgjørende betydning for disse virksomhetene. Jf. virksomhetsikkerhetsforskriften § 13 1. ledd bokstav d

79 Herunder objekter og infrastruktur

en skadevurdering[80] av hendelser for å vurdere hvilke konsekvenser dette kan føre til for GNF. En slik ansvarsfragmentert skadevurdering kan utfordre myndigheters evne til å se samspillseffekter av avhengigheter og sårbarheter, ettersom skadefølgene vurderes isolert og av virksomheter med begrenset innsikt i samfunnets samlede avhengighetsforhold. Problemstillingen blir ytterligere aktualisert som følge av nåtidens spente sikkerhetspolitiske situasjon.[81]

Fra teknologiske avhengigheter til samfunnsmessige konsekvenser

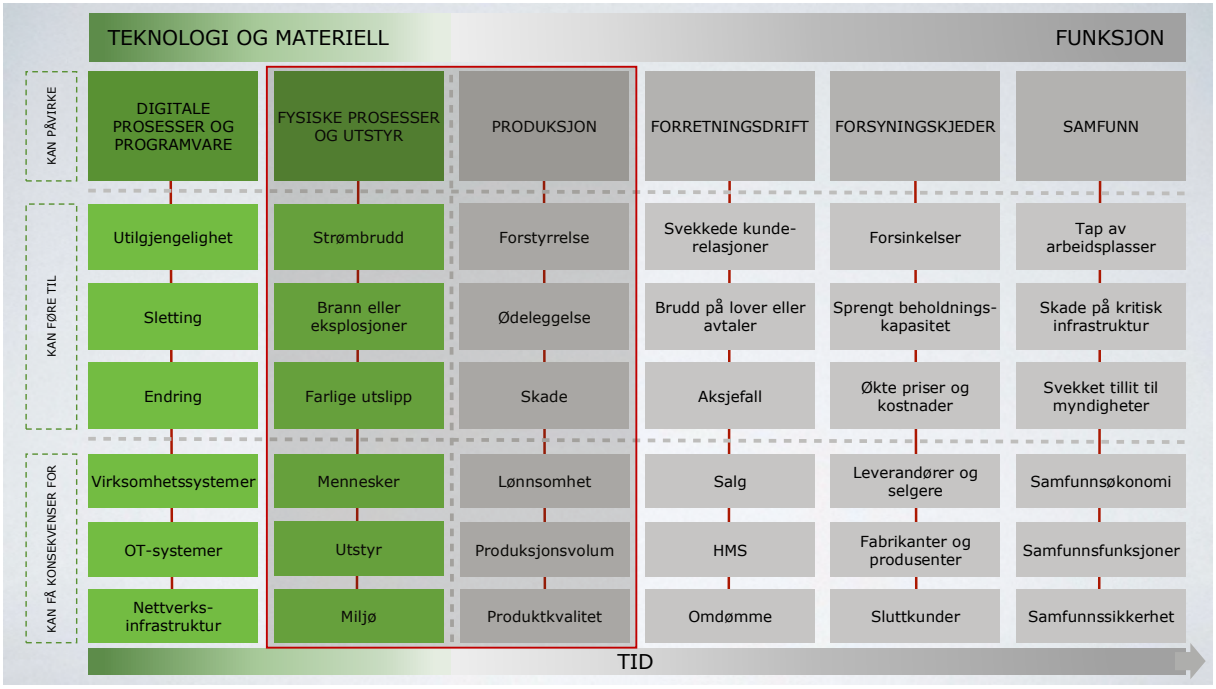
For å belyse kompleksiteten i å forutse skadeomfanget av et cyberangrep – i tillegg til sammenhenger mellom teknologi, forretningsdrift og samfunnsfunksjoner – har Kripos gjort en tematisk inndeling av forskjellige verdier som kan påvirkes og eksempler på konsekvenser innenfor disse. Utfallsrommet strekker seg fra umiddelbare administrative og fysiske konsekvenser, til langsiktige forretningsmessige og samfunnsrelaterte konsekvenser.

Konsekvensmatrisen (figur 10) viser sammenhenger mellom «detaljer» og «helhet» (nevnt på side 67) gjennom konseptuelt ulike måter å kategorisere verdier og konsekvenser. Til venstre i figuren er konsekvensene sentrert rundt teknologi og materiell (grønne bokser), som følge av påvirkning på *digitale* og *fysiske prosesser*. Disse kategoriene er nært relatert til trusselinndelingen mot administrative og operasjonelle prosesser (side 59). Basert på disse to påvirkningsmulighetene kan konsekvensene utspille seg over flere områder som *produksjon, forretningsdrift, forsyningskjeder* og *samfunn* (grå bokser).

Mørklagt område innrammet med heltrukken rød strek utgjør verdier og konsekvenser som er særlig forbundet med OT-avhengige virksomheter. Øverste gruppe (*kan påvirke*) viser tematiske avgrensninger basert på aktiviteter og avhengigheter som er involvert i å levere et produkt. Midterste gruppe (*kan føre til*) tilbyr

80 NSM adresserer utfordringen med prinsippet om systematisk risikostyring i sin håndbok om skadevurdering: «Med utgangspunkt i at virksomheten ikke nødvendigvis har forutsetninger for å vurdere de direkte konsekvensene for GNF, kan de fokusere på hva det betyr det for virksomhetens funksjon om det enkelte objekt eller infrastruktur faller helt eller delvis ut». NSM. (2020, 26. august). *Håndbok i skadevurdering*. https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/fremgangsmate-for-skadevurdering/skadevurdere-objekter-og-infrastrukturer-3/

81 Regjeringen. (2025, 10. januar). Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen— Forberedt på kriser og krig*. https://www.regjeringen.no/no/dokumenter/meld.-st.-9-20242025/id3082364/?ch=1



Figur 10: Konsekvensmatrisen illustrerer ulike måter å kategorisere verdier, fra teknologi og materiell til venstre, til funksjoner til høyre. Modellen er logisk innrettet vertikalt, samtidig er det forsøkt å opprettholde en horisontal sammenheng for å belyse ulike avhengigheter. Modellen er utviklet av Kripos.

noen eksempler på konsekvenser av cyberangrep innenfor hver tematisk avgrensning. Nederste gruppe (*kan få konsekvenser for*) viser noen berørte verdier innenfor de utvalgte områdene. Konsekvensmatrisen belyser teknologiens funksjon i samfunnet og derigjennom hvordan cyber kan inngå i staters sammensatte virkemiddelbruk.

Sett i lys av et cyberangrep, kan modellen forstås som en tidslinje der konsekvensene til venstre i modellen som regel vil inntreffe før konsekvenser plassert lengre til høyre i modellen. Listen er ikke uttømmende og det vil være overlapp mellom konsekvensene på ulike nivåer.

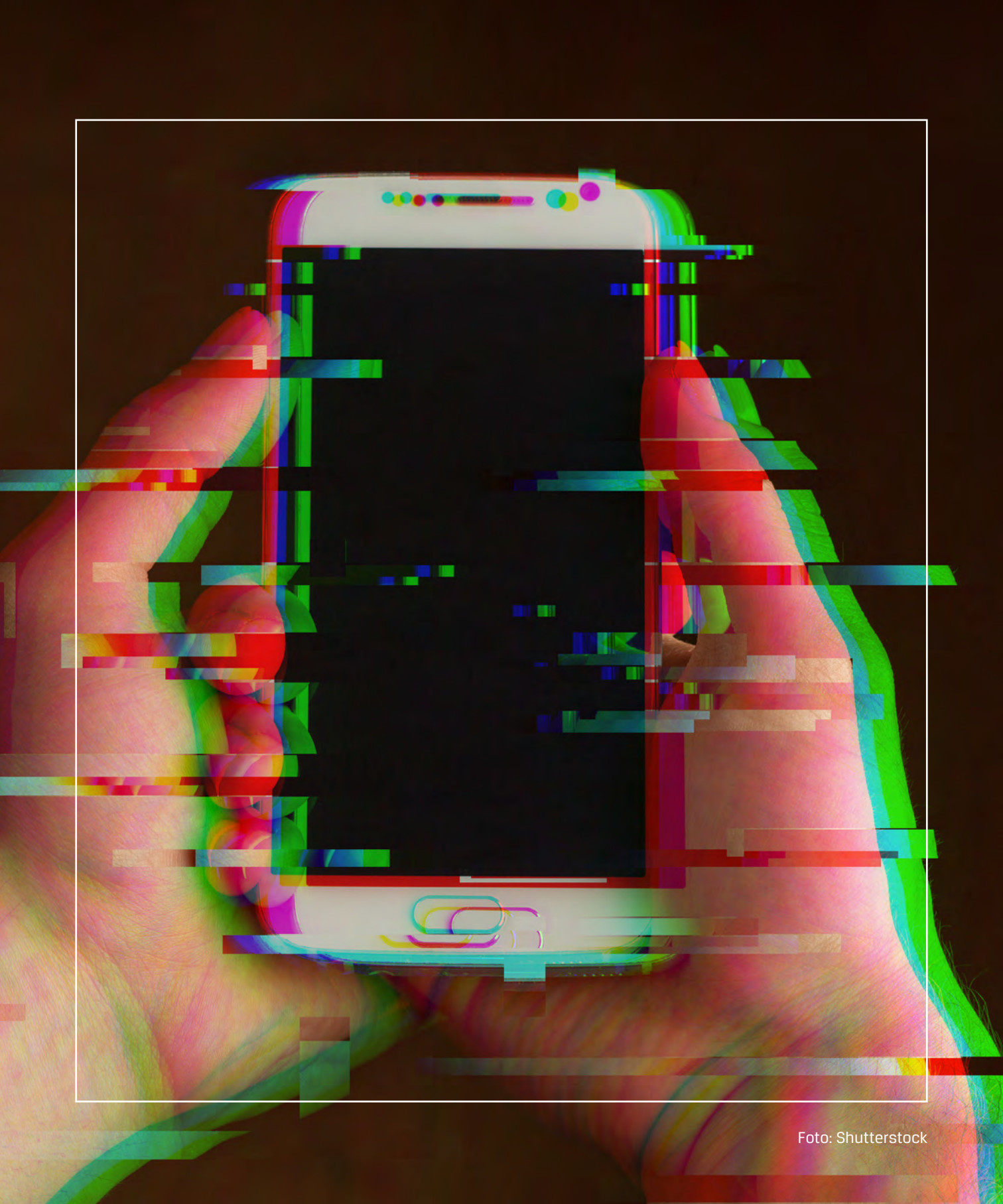
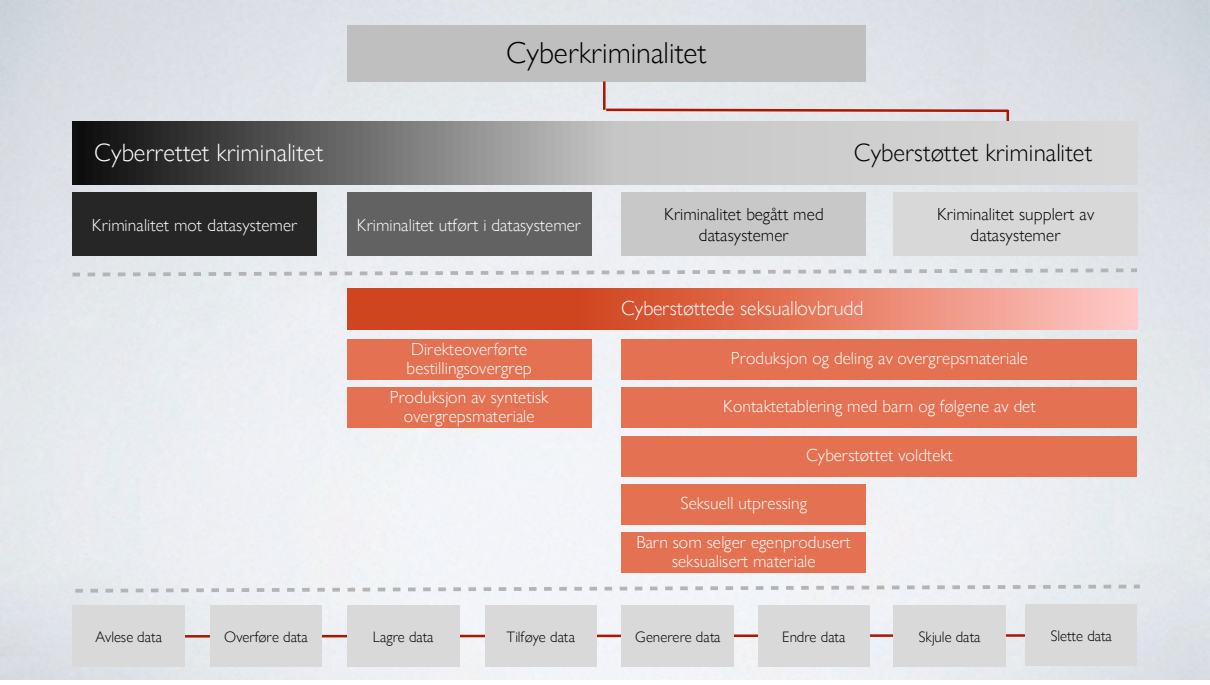


Foto: Shutterstock

Cyberstøttede seksuallovbrudd

Som nevnt i kapittelet om cyberkriminalitetens kjennetegn (side 11) er cyberstøttet kriminalitet hovedsakelig forbundet med tradisjonell kriminalitet som foregår i den fysiske verden, men som nå forsterkes av eller begås i det digitale rom. Cyberstøttet kriminalitet kan i tillegg inn-



Figur 11: Viser kriminalitetstypene innen cyberstøttede seksuallovbrudd som omtales i årets rapport. Kriminalitetstypene er plassert på glideskalaen mellom cyberstøttet og cyberrettet, og figuren illustrerer hvordan cyberstøttede seksuallovbrudd i ulik grad er avhengig av datasystemer for å begås. Modellen er utviklet av Kripos.

befatte *kriminalitet utført i datasystemer* som ikke fantes før det digitale rom oppstod og som dermed kun begås i cyberdomenet.

Cyberstøttet kriminalitet inkluderer i denne rapporten seksuallovbrudd, økonomisk kriminalitet og organisert kriminalitet. Årets rapport presenterer hovedsakelig cyberstøttede seksuallovbrudd, med vekt på endring og utvikling som er observert i 2024.

Cyberstøttede seksuallovbrudd spenner fra deling av overgrepsmateriale til cyberstøttede voldtekter. Figur 11 viser kriminalitetstypene innenfor cyberstøttede seksuallovbrudd som omtales i årets rapport, satt i sammenheng med inndelingen som ble introdusert på side 12.

Figur 11 illustrerer hvordan noen former for cyberstøttede seksuallovbrudd, som produksjon av syntetisk overgrepsmateriale, er helt avhengig av datasystemer og på den måten også en ny form for kriminalitet, mens eksempler som produksjon og deling av overgrepsmateriale både kan være kriminalitet begått i datasystemer og kriminalitet supplert av datasystemer. De nederste boksene, de grunnleggende aktivitetene innen cyberkriminalitet, er det som skiller cyberstøttede seksuallovbrudd fra seksuallovbrudd ellers, nettopp fordi én eller flere av disse aktivitetene skjer som ledd i kriminaliteten.

Nåsituasjon – cyberstøttede seksuallovbrudd i 2024

I likhet med tidligere år, begikk norske gjerningspersoner i 2024 en rekke kriminelle handlinger med seksuelt motiv. Kripos vil i dette delkapittelet beskrive året som har gått i lys av vurderingene fra fjorårets Cyberkriminalitet-rapport.[82]

Kripos vurderte at omfanget av seksuallovbrudd begått på ende-til-ende-krypterte meldingsplattformer ville øke i 2024 og at flere former for cyberstøttede seksuallovbrudd ville forekomme på slike plattformer. Ettersom blant annet Facebook Messenger har gått over til ende-til-ende-kryptering, kan vurderingen sies å ha inntruffet. I tillegg har politiet registrert flere tilfeller enn tidligere der barn har blitt utsatt for ulike seksuallovbrudd, blant annet voldtekt, på ulike ende-til-ende-krypterte meldingsplattformer. I gjennomføringen av direkteoverførte bestillingsovergrep har Kripos også observert at flere aktører går bort fra ukrypterte plattformer og heller benytter ende-til-ende-krypterte meldingsplattformer.

I fjor vurderte Kripos at det i løpet av 2024 ville bli generert syntetisk overgrepsmateriale i form av bilder av barn i alle aldre og at det ville være umulig å skille mellom ekte og syntetisk materiale med det blotte øyet. Kripos har i 2024 observert at gjerningspersoner produserer et

82 Kripos. (2024). *Cyberkriminalitet 2024.* https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf

rikt spekter av syntetisk overgrepsmateriale, fra fotorealistiske bilder av barn i alle aldre, til obskure fantasibilder av kjendisbarn. Likevel er andelen syntetisk materiale som rapporteres til organisasjoner som Internet Watch Foundation (IWF) og National Center for Missing and Exploited Children (NCMEC) fortsatt lav. Som for annet overgrepsmateriale deles det syntetiske overgrepsmaterialet primært mellom aktører som har seksuell interesse for barn, men Kripos er kjent med at noe syntetisk overgrepsmateriale selges, også på bestilling.

Kripos vurderte i 2024 at verktøy basert på KI ville bli benyttet av gjerningspersoner til å komme i kontakt med barn på internett. Kripos er ikke kjent med at slike verktøy brukes for å komme i kontakt med norske barn, men forekomsten av dette i Norge kan heller ikke utelukkes. KI-agenter kan brukes til å opprette dialog med et stort antall barn, for raskere å komme i kontakt med barn som kan forledes til seksuell utnyttelse. Et annet eksempel er at aktører kan bruke KI til å generere bilder, tekst og annen informasjon for at en sosial medie-profil skal fremstå realistisk og norsk. En av årsakene til at Kripos ikke kan utelukke bruk av slike verktøy i Norge er at det i de fleste tilfeller ikke blir undersøkt om bilder, videoer eller tekst som barn mottar er ekte eller syntetisk generert.

Cyberstøttede seksuallovbrudd begås fortsatt både av barn og voksne, og mange gjerningspersoner er fortsatt under kriminell lavalder. Mange svært unge norske barn har høy grad av digital tilstedeværelse, og cyberstøttede seksuallovbrudd rammer derfor barn ned i barneskolealder. Barn i alle aldre er i tillegg avbildet i overgrepsmateriale som deles av norske gjerningspersoner.

Cyberstøttede seksuallovbrudd preges fremdeles av store mørketall. Det er velkjent at mange fornærmede aldri forteller hva de har blitt utsatt for, ikke forstår at de er utsatt for lovbrudd eller først forteller om det når de er voksne. Handlingsrommet for aktørene kan være stort, når en enkelt aktør kan begå overgrep mot svært mange fornærmede over lang tid uten at noen sier ifra eller det blir avdekket av politiet.

I tillegg gjør utstrakt bruk av anonymiseringsteknologi som VPN[83] det utfordrende å skille mellom kriminelle handlinger som begås av norske gjerningspersoner og hvilke handlinger

83 Virtuelt privat nettverk

som begås i utlandet. Likevel observerer Kripos at antall tips fra tjenestetilbydere[84] fortsatt er høyt.[85,86]

Innen spesielt kriminalitetstypen seksuell utpressing med profittmotiv[87] har gjerningspersonene utviklet gjennomføringen av kriminaliteten til det grovere i løpet av 2024. Dette ble vurdert som en forventet utvikling i fjorårets rapport. Når det gjelder andre kriminalitetstyper innen cyberstøttede seksuallovbrudd observeres det fremdeles at gjerningspersonene har et stort spekter av handlingsmønstre, der noen er grovere enn andre. Eksempler på grovere handlingsmønstre er bruk av alvorlige trusler i gjennomføringen av cyberstøttede voldtekter og mer utspekulerte utpressingsteknikker, for eksempel gjennom utpressing over lang tid og kartlegging av fornærmedes liv i form av når fornærmede får lønn for å kunne tilpasse utpressingskravene til det. I tillegg kontakter noen utpressere fornærmede gjentatte ganger på kort tid.

Kriminalitetstyper

Det er en rekke ulike kriminalitetstyper som faller innunder cyberstøttede seksuallovbrudd. Årets rapport vil ikke inkludere alle, men rette oppmerksomhet mot de kriminalitetstypene som har preget 2024 ved at det er observert en endring, utvikling eller eskalering, og som i tillegg utgjør en trussel mot individ og samfunn.

For det første er seksuell utpressing med profittmotiv en kriminalitetstype der Kripos har observert en utvikling det siste året, både i omfang og hvordan kriminaliteten gjennomføres. Seksuell utpressing kan begås på flere måter av

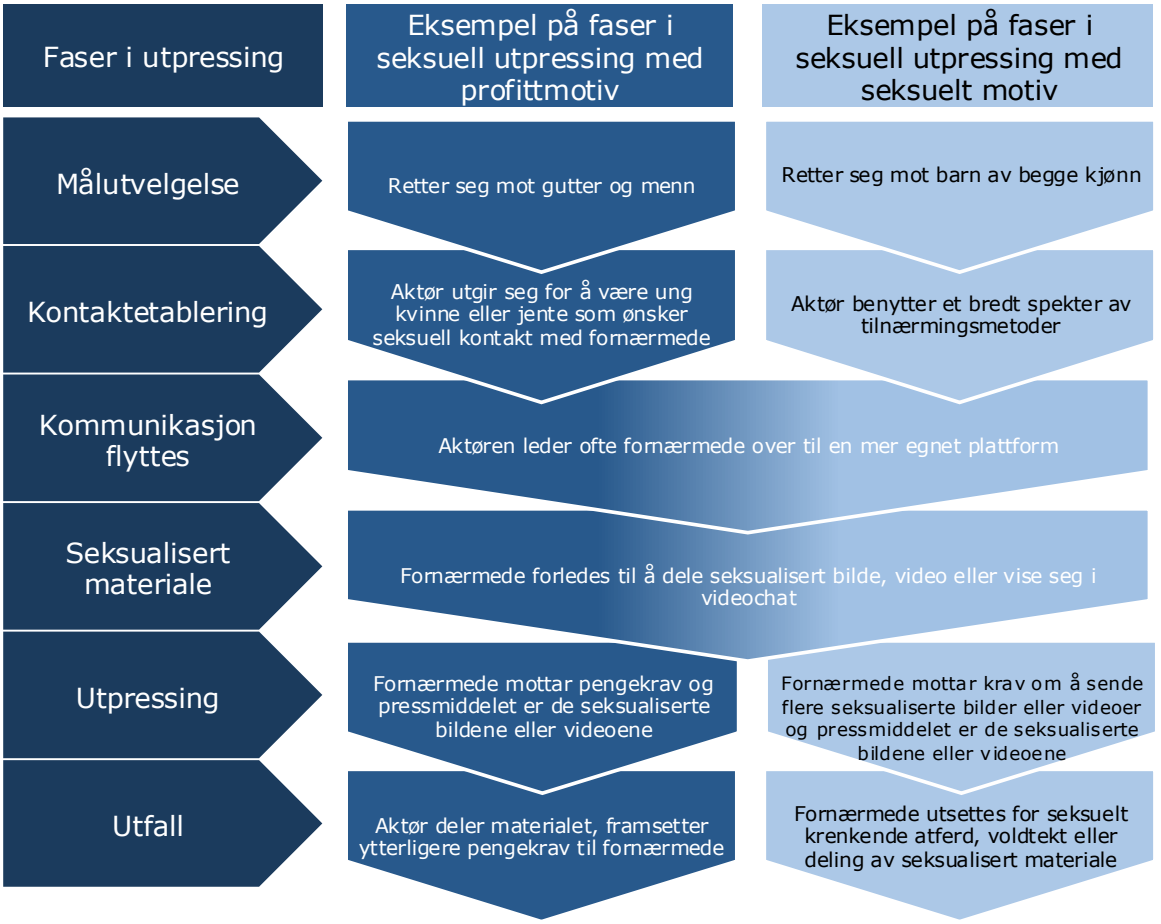
84 Med tjenestetilbydere menes her tilbydere av ulike digitale tjenester, som sosiale medier, lagringstjenester og kommunikasjonstjenester. Eksempler på tilbydere som sender tips via NCMEC er Google (eks. Gmail, Google Images), Meta (eks. Facebook, Instagram og WhatsApp), Microsoft (eks. Bing-søk, Outlook), TikTok og Snapchat

85 Mottatt Kripos fra National Center for Missing and Exploited Children (NCMEC): 2022: 9920, 2023: 13612, 2024: 12663

86 Se mer i: Kripos. (2024). *Informasjon fra tjenestetilbydere: Seksuell utnyttelse av barn på digitale plattformer*. https://www.politiet.no/globalassets/tall-og-fakta/voldtekt-og-seksuallovbrudd/2024-10-25_a_informasjon-fra-tjenestetilbydere-seksuell-utnyttelse-av-barn-pa-digitale-plattformer.pdf

87 I tidligere rapport (Kripos. (2024). *Cyberkriminalitet 2024*. https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf) og ofte omtalt som seksuell utpressing med økonomisk motiv

Foto: Shutterstock



Figur 12: Viser eksempler på faser i seksuell utpressing. Figuren uthever likheter og forskjeller mellom seksuell utpressing med profittmotiv og med seksuelt motiv. Modellen er utviklet av Kripos.

aktører med ulikt motiv og både barn og voksne rammes. For å illustrere fasene i seksuell utpressing med profittmotiv og med seksuelt motiv, som er de vanligste formene for seksuell utpressing, samt synliggjøre likheter og forskjeller, har Kripos i årets rapport utarbeidet figur 12. I tillegg til de to motivene for utpressing som er illustrert i figuren til venstre er et annet kjent motiv relasjonell utpressing. Dette innebærer at fornærmede presses til å forbli i en kjæresterelasjon mot sin vilje, som regel motivert av hevn eller et kontrollbehov hos utpresser. Forekomsten av denne formen for seksuell utpressing er registrert i langt mindre grad enn de to andre formene. I tillegg viser politiets data at seksuell utpressing med seksuelt motiv rapporteres sjeldnere enn seksuell utpressing med profittmotiv.

Kripos ser at målutvelgelsen, kontaktetableringen og utfallet av utpressingen varierer mellom profittmotivert og seksuelt motivert utpressing, men at store deler av den øvrige utførelsen er lik. Av denne årsak kan det i noen tilfeller være uklart hva aktøren ønsker å oppnå før selve utpressingen finner sted.

Det siste året har Kripos analysert nesten 2000 tilfeller av utpressing som har rammet norske gutter og menn. Gjennom analysen har Kripos avdekket mønstre og innsikt som ikke tidligere har vært kjent. Datagrunnlaget stammer fra 1. januar 2023 frem til 31. oktober 2024 og inkluderer både tilfeller som er rapportert eller anmeldt til politiet og tilfeller som er avdekket i undersøkelser av transaksjoner gjort til kjente utpressere. Det er likevel antakeligvis store mørketall, da analysen av transaksjonene avdekket at få av disse tilfellene tidligere var rapportert til politiet.

> Dersom lønnsomheten går ned som følge av at utpressere bruker syntetiske nakenbilder, vil det kunne føre til at utpressere tar i bruk andre virkemidler for å oppnå samme profitt [...]

Seksuell utpressing med profittmotiv rammer fortsatt primært gutter og menn i stort omfang i Norge. Over 90 prosent av de fornærmede blir forledet til å dele seksualiserte bilder og videoer av seg selv til utpresseren, mens det i de resterende tilfellene er syntetisk generert materiale eller materiale aktøren har tilegnet seg på andre måter. Behovet for at den fornærmede deler seksualisert materiale kan derfor sies å ha blitt mindre aktuelt i løpet av 2024, til tross for at det fremdeles brukes ekte nakenbilder i de fleste tilfeller.

I de tilfellene det brukes syntetiske nakenbilder trenger ikke aktøren å forlede fornærmede

til å dele nakenbilder av seg selv før utpressingen. Samtidig kan det faktum at aktøren ikke har ekte bilder av den fornærmede i noen tilfeller føre til at fornærmedes betalingsvilje blir lavere, noe som gjør aktørens pressmiddel svakere. Likevel er det fortsatt slik at det i de fleste forholdene som gjelder seksuell utpressing med profittmotiv brukes ekte bilder eller video av fornærmede som pressmiddel. Også ved utpressing med ekte bilder eller video, kan forekomsten av syntetiske nakenbilder føre til lavere betalingsvilje hos den fornærmede, for eksempel fordi den fornærmede kan hevde at de ekte bildene er syntetiske dersom de blir offentliggjort. Dersom lønnsomheten går ned som følge av at utpressere bruker syntetiske nakenbilder, vil det kunne føre til at utpressere tar i bruk andre virkemidler for å oppnå samme profitt, eksempelvis ved å skalere opp og automatisere kontaktetableringsprosesser for å nå flere fornærmede raskere.

Et av de mest alvorlige straffbare forholdene innen cyberstøttede seksuallovbrudd er cyberstøttede voldtekter.[88] Disse kan begås på flere måter, også med utpressing. Kripos har også i 2024 observert at gjerningspersoner bruker utpressing og trusler til å få fornærmede til å utføre grove seksuelle handlinger på seg selv, som derfor ender som voldtekt. For eksempel voldtok en mann ei elleve år gammel jente ved at han fikk henne til å sende ham bilder av at hun penetrerte seg selv med en gjenstand. Samtidig kan cyberstøttede voldtekter også begås med andre virkemidler, som å forlede barnet ved å utgi seg for å være jevnaldrende eller selv utføre handlinger som svarer til det gjerningspersonen ønsker at barnet skal utføre.

De siste årene har politiet registrert økt rapportering om barn som selger egenprodusert seksualisert materiale til voksne på internett, en kriminalitetstype som kan strekke seg over mange ulike straffbare forhold – fra cyberstøttede voldtekter til å skaffe seg seksualisert materiale av barn. I løpet av 2024 er det registrert tre former for eskalering innen denne kriminalitetstypen. I noen tilfeller sender selgerne mer og mer materiale, enten fordi kjøperne er pågående, eller fordi de selv ønsker å tjene mer penger. I andre tilfeller skjer eskaleringen i form av seksuell utpressing, ved at kjøper truer selger dersom selger ikke ønsker å sende mer materiale. En tredje type eskalering skjer når kjøper avtaler å møte selger fysisk, for å kjøpe seksuelle tjenester. Dette skjer som regel etter initiativ fra kjøper. I de fleste tilfellene trekker

88 Den som får et barn under 14 år til å utføre handlinger som svarer til seksuell omgang med seg selv straffes etter Straffeloven. (2005). *Lov om straff* (LOV-2005-05-20-28). § 299 bokstav b om voldtekt av barn under 14 år

likevel selger seg, av ulike grunner, og gjennomfører ikke møtet.

Materialet barna produserer og selger er en form for overgrepsmateriale. Samtidig observerer Kripos at norske aktører tilegner seg og deler overgrepsmateriale på svært mange digitale arenaer, og at delingen består av materiale av svært ulik karakter. Fora og nettsider på det mørke og det åpne nettet, samt ulike chatteplattformer og forskjellige fildelingstjenester brukes til å anskaffe, omsette og dele materiale videre. Overgrepsmaterialet består av både bilder og videoer, viser barn av begge kjønn og i alle aldere, og viser mange ulike former for seksualisering – fra lettkledde poseringsbilder til grove voldtekter.

Syntetisk overgrepsmateriale gjorde sitt inntog i 2023 og har i 2024 fått høy kvalitet og økt i omfang. Mengden av slikt materiale har blitt stor og prisen på overgrepsmateriale på det mørke nettet har sunket, noe som kan ha årsakssammenheng.

Handlingsmønstre

Kunstig intelligens brukes ikke bare til å produsere syntetisk overgrepsmateriale, men kan også være en del av handlingsmønsteret innen andre former for cyberstøttede seksuallovbrudd. Kripos er kjent med at aktører bruker chatboter som chatter som barn, slik at gjerningspersoner kan kommunisere med det som fremstår som barn. Det er likevel uvisst hvilke motiv gjerningspersonene har ved å bruke slike chatboter, da de både kan brukes til egen tilfredstillelse og til å trene opp egne kommunikasjonsevner. Uavhengig av gjerningspersonenes formål vil slike fiktive chatter med det som fremstår som barn være straffbare i Norge dersom de er seksualiserte.

> Å lage, ha og/eller dele syntetisk overgrepsmateriale eller syntetisk materiale som seksualiserer barn er straffbart i Norge, på samme måte som andre fremstillinger som seksualiserer barn, som tegninger, tekst og gjenstander som dukker.[89]

I tillegg til den nye kriminaliteten som har gjort seg gjeldende etter at cyberdomenet oppstod, har som nevnt også tradisjonell kriminalitet blitt enklere å gjennomføre ved bruk av datasystemer. Kontaktetablering mellom barn og aktører er en sentral del av mange cyber-

89 Straffeloven. (2005). *Lov om straff* (LOV-2005-05-20-28). § 311. Fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn

støttede seksuallovbrudd.[90] Som tidligere år benytter aktørene fortsatt flere ulike virkemidler for å etablere kontakt og oppnå sin ønskede sluttilstand. I figur 13 til høyre eksemplifiseres handlingsmønsteret for å etablere kontakt med barn på digitale plattformer, satt i sammenheng med det aktørene søker å oppnå (kriminalitetstype). Figuren viser også hvilke mulige konsekvenser forskning og politiets egen informasjon har identifisert hos de fornærmede barna for disse kriminalitetstypene.[91]

I første fase av kontaktetableringen tilnærmer aktøren seg barnet, enten ved å tilkjennegi seg som voksen, eller ved å opptre fordekt og utgi seg for å være yngre enn sin faktiske alder, eventuelt også som jente.[92] Eksempelvis har mange spillplattformer funksjonalitet for stemmekommunikasjon, ettersom skriftlig kommunikasjon i kombinasjon med gaming er tungvint, og programvare som endrer stemmen blir derfor en sentral muliggjører for å oppnå troverdighet.

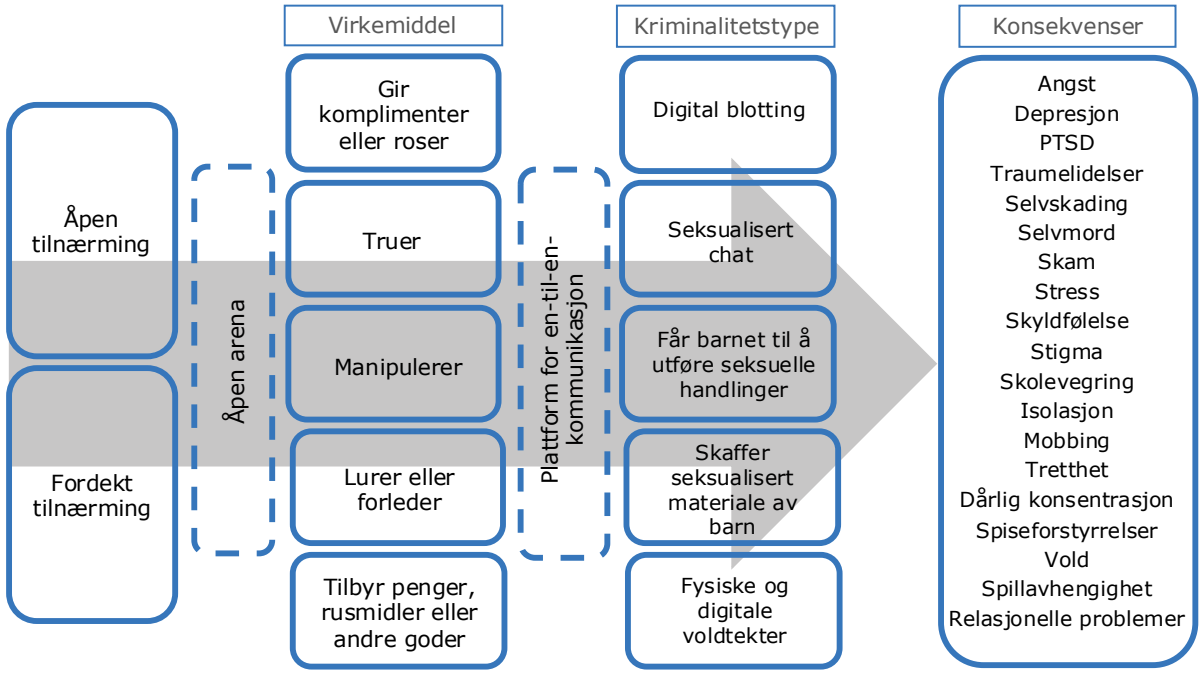
Kontaktetableringen foregår ofte på en åpen arena, eksempelvis i et kommentarfelt på TikTok, eller som følge av at aktøren har kjennskap til barnet i den fysiske verden. Også spillplattformer som Roblox og Fortnite, samt plattformen Discord som brukes til kommunikasjon mellom gamere i spill, er arenaer hvor både barn og seksuallovbrytere ferdes og som aktivt benyttes til kontaktetablering med barn. Flere aktører anser Discord-servere som omhandler spill for å være gunstige steder å komme i kontakt med barn, særlig gutter, og i likhet med spillenes målgrupper er også Discord-servere knyttet til ulike spill mer aktuelle for ulike aldersgrupper av barn. Likevel er Snapchat den dominerende plattformen for kontaktetablering med barn, også blant de yngste barna. Snapchat benyttes ofte ikke bare til selve kontaktetableringen, men også til gjennomføringen av det straffbare forholdet.

Aktøren benytter ulike virkemidler for å etablere videre kontakt, og flytter gjerne

90 Se mer i: Kripos. (2024). *Trusselaktørers kontaktetablering med barn på internett.* https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/2024-11-27_a_trusselaktorers-kontaktetablering-med-barn-pa-internett.pdf

91 Hellevik, P., Kruse, A. E., Dullum, J. V., Frøyland, L. R., Skar, A. S., Andersen, L. C., Helseth, H., Frafjord, O. S. G., Haugen, L. A., & Øverlien, C. (2023). *Digitale seksuelle overgrep mot barn og unge – gjerningspersoner og fornærmede.* NKVTS. https://www.nkvts.no//content/uploads/2024/01/NKVTS-Rapport-3-2023-Digitale-seksuelle-overgrep-mot-barn-og-unge.pdf

92 De aller fleste aktører som tilnærmer seg barn på internett er menn



Figur 13: Viser typisk fremgangsmåte som benyttes av aktører som ønsker å etablere kontakt med barn for å utsette dem for seksuell utnyttelse. Figuren fremhever også mulige konsekvenser for barn som utsettes for slike handlinger. Konsekvensene er blant annet hentet fra Hellevik, P., Kruse, A. E., Dullum, J. V., Frøyland, L. R., Skar, A. S., Andersen, L. C., Helseth, H., Frafjord, O. S. G., Haugen, L. A., & Øverlien, C. (2023). *Digitale seksuelle overgrep mot barn og unge – gjerningspersoner og fornærmede*. NKVTS. https://www.nkvts.no//content/uploads/2024/01/NKVTS-Rapport-3-2023-Digitale-seksuelle-overgrep-mot-barn-og-unge.pdf. Modellen er utviklet av Kripos.

dialogen over på en mer egnet plattform for en-til-en-kommunikasjon og utveksling av bilder og videoer, eksempelvis Snapchat eller ende-til-ende-krypterte meldingsplattformer. Her begår aktøren seksuallovbrudd mot barnet, og lovbruddet kan ta ulike former. Kontaktetablering gjennom digitale arenaer kan også føre til ulike former for seksuelle overgrep ved at barnet og gjerningspersonen møtes fysisk. Som vist i figur 13 er konsekvensene av seksuallovbrudd mange. For mer om konsekvenser, se side 89. Samlet sett øker cyberstøtten potensialet for flere typer seksuallovbrudd og større forekomst av overgrep mot barn.

Aktører

Cyberstøttede seksuallovbrudd i stort begås av svært ulike aktører i alle aldere og fra alle samfunnslag. Det er imidlertid betraktelig flere menn enn kvinner som begår slike lovbrudd. I dette delkapittelet vil Kripos beskrive gjerningspersonene som begår seksuell utpressing med profittmotiv og gjerningspersonene som kjøper egenprodusert seksualisert materiale av barn. Begge disse kriminalitetstypene har elementer av økonomiske drivere, men aktørgruppenes motivasjon er ulik.

Seksuell utpressing mot norske fornærmede begås fra hele verden

Kripos har observert at aktører som driver med seksuell utpressing med profittmotiv mot norske fornærmede befinner seg i ulike land og i flere verdensdeler. Blant annet forekommer det hyppig utpressing fra land som Filippinene, Nigeria og Elfenbenskysten. Norske aktører utsetter også norske fornærmede for seksuell utpressing med profittmotiv, selv om disse er i mindretall.

Tidligere har det vært en rådende oppfatning at seksuell utpressing med profittmotiv utføres av store, organiserte kriminelle nettverk i utlandet. I analysen Kripos har utført av seksuell utpressing med profittmotiv tegnes et bilde av en aktørgruppe der færre samarbeider med hverandre enn hva som tidligere har vært antatt. Likevel fremstår det som at aktører tilknyttet Filippinene er mer organisert enn aktører i Nigeria og Elfenbenkysten. Kripos er også kjent med at bruksanvisninger for å begå seksuell utpressing selges eller distribueres i sosiale medier, som gjør at mange kan bruke fremgangsmåten for å oppnå profitt.

Aktørene fra de tre tidligere nevnte landene har ulik fremgangsmåte og benytter forskjellige plattformer. Ved å kjenne til modus er det mulig å sannsynliggjøre hvilket land utpresser opererer fra, uten videre undersøkelser.

Utpresserne fra Nigeria rammer flest norske barn sammenlignet med aktørene fra de to andre landene. De etablerer fortrinnsvis kontakt på Snapchat og Instagram, plattformer hvor

> Aktørene fra Nigeria, Elfenbenskysten og Filippinene har ulik fremgangsmåte og benytter forskjellige plattformer. Ved å kjenne til modus er det mulig å sannsynliggjøre hvilket land utpresser opererer fra, uten videre undersøkelser.

Foto: Shutterstock

barn har høy grad av tilstedeværelse. Nigerianske aktører bruker primært engelsk språk[93] i sin kommunikasjon med de fornærmede.

Aktører fra Elfenbenskysten benytter i hovedsak Facebook som plattform for kontaktetablering og utpressing. De benytter ofte navn i profilen som fremstår som norske, oppgir å være fra små steder i Norge og har ofte felles venner med fornærmede. Elfenbenkysten har fransk som sitt offisielle språk, og benytter i større grad oversettelsesverktøy i sin kommunikasjon med fornærmede, som ofte foregår på norsk.

Aktører fra Filippinene benytter i størst grad dating-applikasjoner som Tinder og Happn for å etablere kontakt med de fornærmede, og rammer følgelig i mindre grad barn. Engelsk er ett av to offisielle språk på Filippinene og kommunikasjonen foregår på engelsk. Aktører fra Filippinene er utholdende og Kripos har sett eksempler på fornærmede som har blitt utpresset i månedsvis.

Norske menn kjøper seksualisert materiale av norske barn

Aktørene som kjøpte egenprodusert seksualisert materiale av norske barn var norske menn bosatt over hele landet. Aktørene er i alderen 16 til 68 år, men de fleste er menn i midten av tretiårene. De fleste hadde ikke egne barn. Mange av aktørene er tidligere mistenkt, siktet eller domfelt for seksuallovbrudd mot barn.

Blant aktørene som har kjøpt egenprodusert seksualisert materiale av norske barn er det også enkelte med svært alvorlig straffehistorikk innen vold og seksuallovbrudd. At aktører med et potensial til å utføre svært grov voldskriminalitet begår denne formen for kriminalitet bekymrer Kripos, da eskalering eksempelvis kan føre til at de fornærmede barna møter aktørene fysisk. Aktører med tilbøyelighet til å utføre grove volds- og seksuallovbrudd kan være en betydelig fare for de fornærmede barna som eventuelt møter disse fysisk.

De utsatte barna

Kripos har tidligere kategorisert utsatte barn og unge i fem kategorier.[94] Kategoriene er:

1. barn som fremstilles i overgrepsmateriale på internett;
2. barn som forledes inn i seksuell kontakt over internett;
3. barn som utsettes for direkteoverførte bestillingsovergrep;
4. barn og unge som fotograferes/filmes av jevnaldrende i en seksualisert situasjon; og

93 Engelsk er det offisielle språket i Nigeria

94 Kripos. (2019). *Seksuell utnyttelse av barn og unge over internett.* https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/seksuell-utnyttelse-av-barn-over-internett.pdf

5. barn og unge som frivillig produserer seksualiserte bilder eller filmer av seg selv.

I denne rapporten beskrives kategori 1 og 2 nærmere med nyere informasjon.

I undersøkelsen UngVold 2023 ble det avdekket at 36 prosent av jentene og 10 prosent av guttene i videregående skole hadde blitt utsatt for minst én digital seksuell krenkelse i løpet av livet.[95] Eksempler på handlinger inkludert i definisjonen av digital seksuell krenkelse var å bli presset eller truet til å sende seksualiserte bilder eller film (som flest var utsatt for)[96], til et fysisk seksuelt overgrep fra en man ble kjent med på internett (lavest forekomst)[97]. Undersøkelsen viste også at utsattheten var størst på ungdomstrinnet og at de fleste var utsatt for krenkelsen fra en jevnaldrende de kjente fra før.[98] Antallet som oppgir at de selv har vært utsatt for disse straffbare forholdene er betraktelig større enn hva informasjon i politiets registre viser, noe som er en klar indikasjon på at mørketallene er store, selv om selvrapporteringsstudier også har noen svakheter.

Barna som fremstilles i overgrepsmateriale på internett

Det er gjort flere undersøkelser av barn som er avbildet og filmet i overgrepsmateriale. De siste årene har en stor del av nytt overgrepsmateriale vært egenprodusert materiale, der barn har filmet eller avbildet seg selv. IWF har avdekket at 64 prosent av materialet de fjernet i 2023 var egenprodusert, og andelen er spesielt høy der den avbildede er jente (94 prosent).[99] Selv om slikt materiale kan fremstå å være produsert av barnet selv uten ytre påvirkning, er barn avbildet i slikt materiale i mange tilfeller utsatt for voldtekt, seksuell utpressing eller andre cyberstøttede seksuallovbrudd. Barna som er avbildet i egenprodusert materiale er helt ned i 4-5 årsalder, men

95 Frøyland, L. R., Lid, S., Schwencke, E. O., & Stefansen, K. (2023). *Vold og overgrep mot barn og unge. Omfang og utviklingstrekk 2007-2023*. s. 71. https://oda.oslomet.no/oda-xmlui/handle/11250/3083676

96 30 prosent av jenter, 5 prosent av gutter

97 4 prosent av jenter, 1 prosent av gutter

98 Frøyland, L. R., Lid, S., Schwencke, E. O., & Stefansen, K. (2023). V*old og overgrep mot barn og unge. Omfang og utviklingstrekk 2007-2023*. s. 73-74. https://oda.oslomet.no/oda-xmlui/handle/11250/3083676

99 Internet Watch Foundation. (2023). *Annual report 2023: Trends and data*. https://www.iwf.org.uk/annual-report-2023/trends-and-data/self-generated-child-sex-abuse/

det er i mindre grad ytre påvirkning som har ført til at de yngste barna har avbildet seg selv. Likevel kan disse bildene og videoene ende opp som overgrepsmateriale som deles mellom aktører med seksuell interesse for barn.

Også produksjon av syntetisk overgrepsmateriale kan føre til at ekte barn blir fremstilt i overgrepsmateriale, selv om de ikke har vært utsatt for overgrep. I teorien kan alle barn som er avbildet eller filmet bli en del av syntetisk overgrepsmateriale, fordi aktører kan benytte vanlige bilder eller videoer i produksjonen av syntetisk overgrepsmateriale. Også voksne kan bli utsatt, da teknologien muliggjør aldersreduksjon i bilder.

Barna som forledes til seksualisert kontakt på internett

Norske barn har høy grad av digital tilstedeværelse, både i skolen og på fritiden. I medietilsynets Barn og medier-undersøkelse 2024 ble det avdekket at tilnærmet alle barn fra 13-årsalderen bruker sosiale medier[100], og at halvparten av 9-åringene gjør det.[101] Undersøkelsen avdekket også at 86 prosent av 9–18-åringer spiller spill på mobil, PC og TV, hvor Fortnite og Roblox er de mest populære spillene, begge plattformer der politiet har informasjon om at aktører kontakter barn.[102] Mens barns tilstedeværelse på sosiale medier øker med alder, synker andelen som bruker spillplattformer når barna blir eldre. Siden både spillplattformer og sosiale medier brukes av trusselaktører for å kontakte barn, er det sentralt at ikke all oppmerksomhet rettes mot utfordringene i sosiale medier, men at det også vies oppmerksomhet til spill der barn har tilstedeværelse, særlig på grunn av risikofaktorer som en-til-en-kommunikasjon og muligheter for videosamtaler.

Medietilsynets Barn og medier-undersøkelse 2024[103] viser at flere jenter enn gutter har fått uønskede seksuelle kommentarer på nettet, 23 prosent av jentene mot 14 prosent av guttene.

---

100 I undersøkelsen definert som: Snapchat, Instagram, TikTok, X (tidligere Twitter), Discord, Facebook, Whatsapp, Viber, Yubo, Messenger, Yolo, Reddit og BeReal

101 Medietilsynet. (2024). *Barn og medier 2024. Barn og unges medievaner og tilgang til teknologi.* https://www.medietilsynet.no/fakta/rapporter/barn-og-medier/barn-medievaner-2024/

102 Medietilsynet. (2024). *Barn og medier 2024. Barn og unges spillvaner*. https://www.medietilsynet.no/fakta/rapporter/barn-og-medier/2024/barn-og-unges-spillvaner/

103 Medietilsynet. (2024). *Barn og medier 2024. Skadelig innhold, seksuelle kommentarer og nakenbilder på nett.* https://www.medietilsynet.no/fakta/rapporter/barn-og-medier/skadelig-innhold-nakenbilder-pa-nett/

> I teorien kan alle barn som er avbildet eller filmet bli en del av syntetisk overgrepsmateriale, fordi aktører kan benytte vanlige bilder eller videoer i produksjonen av syntetisk overgrepsmateriale

Foto: Shutterstock

Litt over halvparten har fått kommentarene fra fremmede på nettet. I tillegg har jenter i større grad enn gutter mottatt nakenbilder, oftest av en fremmed på nettet, og flere jenter enn gutter har blitt spurt om å dele nakenbilder av seg selv, også oftest av en fremmed på nettet. 9 prosent av 13-18-åringer har sendt nakenbilde av seg selv det siste året, noe som er en nedgang sammenlignet med i 2022 (15 prosent) og 2020 (12 prosent). Andelen som svarer at de har delt nakenbilde av seg selv i aldersgruppen 13-14 år er 3 prosent. Om lag 13 prosent av de som har sendt nakenbilde, har sendt det til en fremmed på nettet.[104]

Også fra politiets egen informasjon observerer Kripos at flere jenter enn gutter blir kontaktet av aktører som ønsker å begå ulike former for seksuallovbrudd. Snapchat er den dominerende plattformen for slik kontakt mellom norske barn og voksne trusselaktører. Barn og medier-undersøkelsen viste at så mye som 26 prosent av 9-11-åringer og 84 prosent av 12-14-åringer bruker Snapchat, til tross for at plattformen har 13 års aldersgrense. Barnas tilstedeværelse på plattformen øker risikoen for at mange av dem kan bli utsatt for kontaktetablering fra aktører som ønsker å begå seksuallovbrudd.

For noen barn som ble forledet til seksualisert kontakt på internett hadde politiet informasjon om at de var i en særlig sårbar situasjon. Noen av barna hadde tidligere vært utsatt for vold eller seksuelle overgrep og andre hadde fysisk eller psykisk uhelse. Noen hadde en vanskelig familiesituasjon, eksempelvis foresatte med rusproblematikk. Andre igjen hadde tiltak fra barnevernet eller bodde på institusjon. Undersøkelsen UngVold 2023 viste at andelen barn som i løpet av livet hadde blitt utsatt for digitale seksuelle krenkelser var større hos barn som opplevde oppvekstproblemer[105], sammenlignet med barn som ikke opplevde oppvekst-

104 Medietilsynet. (2024). *Barn og medier 2024. Skadelig innhold, seksuelle kommentarer og nakenbilder på nett*. https://www.medietilsynet.no/fakta/rapporter/barn-og-medier/skadelig-innhold-nakenbilder-pa-nett/

105 Oppvekstproblemer i hjemmet er definert som alkoholproblemer, bruk av andre rusmidler, psykiske problemer og fengsling (i Frøyland, L. R., Lid, S., Schwencke, E. O., & Stefansen, K. (2023). *Vold og overgrep mot barn og unge. Omfang og utviklingstrekk 2007-2023*. https://oda.oslomet.no/oda-xmlui/handle/11250/3083676)

problemer.[106, 107] Det er kjent at barn i en sårbar situasjon har høyere risiko for å bli utsatt for seksuell utnyttelse på internett. Mange barn i en sårbar situasjon har i tillegg færre tillitspersoner som kan ivareta dem i etterkant av at de har blitt utsatt for noe straffbart.

Omtrent en sjettedel av de som utsettes for seksuell utpressing med profittmotiv i Norge er barn, noen helt ned i 10-årsalderen, selv om de fleste er i tenårene. Av de voksne som er utsatt er de fleste i alderen 18-30 år, selv om også eldre fornærmede er utsatt, helt opp i 85-årsalder. Denne kriminaliteten rammer nesten utelukkende gutter og menn, selv om også noen få kvinner rammes.

Konsekvenser

Med konsekvenser menes i dette delkapittelet de individuelle og samlede følgene av at barn blir utsatt for ulike seksuelle overgrep i det digitale rom. Konsekvensene kan både være psykiske, fysiske, relasjonelle og økonomiske.

Belastningen av å bli utsatt for digitale seksuelle overgrep kan være svært stor for de fornærmede barna og kan føre med seg en rekke konsekvenser. Forskning viser at barn som får seksualiserte bilder av seg spredt, opplever mange ulike negative konsekvenser, blant annet angst og depresjon, selvmordstanker og selvskading.[108] Ofte er disse konsekvensene knyttet til tanker om hvem som har sett bildene og hva de vil tenke om den avbildede etter å ha sett bildene. Et konkret eksempel finnes i Borgarting lagmannsretts avgjørelse der to fornærmede for deling av seksualiserte bilder av barn «(...) forklarte seg i retten om de betydelige psykiske påkjenninger dette har medført for dem, som hvordan dette har negativt påvirket deres skolegang og sosiale liv.»[109]

I et annet tilfelle ble en voldtekt av ei mindreårig jente filmet og Frostating lagmannsrett

106 Frøyland, L. R., Lid, S., Schwencke, E. O., & Stefansen, K. (2023). *Vold og overgrep mot barn og unge. Omfang og utviklingstrekk 2007-2023.* https://oda.oslomet.no/oda-xmlui/handle/11250/3083676

107 Blant barn med 2-4 oppvekstproblemer hadde 45 prosent opplevd minst ett tilfelle av digital seksuell krenkelse i løpet av livet, mens for barn uten oppvekstproblemer var andelen 19 prosent

108 Hellevik, P., Kruse, A. E., Dullum, J. V., Frøyland, L. R., Skar, A. S., Andersen, L. C., Helseth, H., Frafjord, O. S. G., Haugen, & L. A., Øverlien, C. (2023). *Digitale seksuelle overgrep mot barn og unge – gjerningspersoner og fornærmede.* NKVTS. https://www.nkvts.no//content/uploads/2024/01/NKVTS-Rapport-3-2023-Digitale-seksuelle-overgrep-mot-barn-og-unge.pdf

109 LB-2023-166528

uttaler at «For fornærmede innebærer dette [delingen av det seksualiserte materialet] – i tillegg til overgrepsopplevelsen – en enorm personlig belastning. Hun har da også svært store utfordringer hva gjelder psykisk helse og fungering på skolen og i hverdagslivet ellers.»[110] Dette viser at de fornærmede som blir utsatt for cyberstøttede seksuallovbrudd ikke bare utsettes for en belastning når hendelsen skjer, men at belastningen kan vedvare over tid og på den måten føre til konsekvenser for skolegang og arbeidsdeltakelse også i senere i livet.

KI-modeller (grunnlagsmodeller) benyttes til å re-aktualisere gammelt overgrepsmateriale ved at slike modeller brukes til å forbedre kvaliteten på eksisterende materiale, fylle inn med bilder fra andre vinkler eller gjenskape materiale aktørene hadde tapt. Dagens grunnlagsmodeller kan også lage film av eksisterende overgrepsbilder, slik at overgrep som aldri ble filmet, men avbildet, nå tilnærmet kan eksistere som syntetiske overgrepsvideoer. Gjennom denne prosessen blir fornærmede, som var barn for 20–30 år siden, igjen avbildet og materialet delt og dermed utsatt for nye krenkelser. Belastningen for de avbildede kan være stor, dersom de blir klar over at en slik fornying av materialet finner sted. Samlet kan dette føre til at en potensielt stor gruppe voksne mennesker, som egentlig har gått videre i livet etter overgrep i barndommen, igjen blir utsatt for belastning som kan påvirke ikke bare enkeltpersonen, men også deres familie.

En annen bekymringsfull konsekvens av syntetisk overgrepsmateriale er at det kan bli vanskelig å skille mellom syntetisk generert overgrepsmateriale og ekte overgrepsmateriale, noe som kan føre til at bevisverdien av den enkelte overgrepsvideoen eller -bildet synker. Hva gjelder gjerningspersoner som har befatning med overgrepsmateriale er ikke dette et problem for myndighetene i Norge, da alt seksualisert materiale av barn er straffbart uavhengig av produksjonsmetode. Men som bevis for at overgrep har funnet sted, vil det syntetiske materialet utfordre politiet, påtalemyndigheten og rettsvesenet i tiden fremover.

Videre vil, som nevnt, alle bilder av barn – uavhengig av om barna har vært utsatt for overgrep – kunne brukes til å produsere syntetisk overgrepsmateriale. Å bli avbildet i slikt materiale og videre deling av det, kan føre til en belastning for den avbildede og dens familie. På denne måten utvides potensielle fornærmede betraktelig, gjennom at helt ordinære familiebilder delt i sosiale medier, misbrukes og deles. Kripos har observert at kjendisbarn, som er avbildet og filmet i omfattende grad fra ung alder, har blitt utsatt for et slikt misbruk gjennom produksjon av syntetisk overgrepsmateriale med disse enkeltpersonene.

110 LF-2024-104999-2

Seksuell utpressing med profittmotiv fører også til en stor belastning for den som rammes, og Kripos observerer at de fornærmede i mange tilfeller får selvmordstanker, sliter med psykisk uhelse, opplever samlivsbrudd og kommer i økonomiske vanskeligheter som følge av utpressingen. Til forskjell fra andre cyberstøttede seksuallovbrudd har utpressingen i tillegg en helt konkret økonomisk konsekvens for de fornærmede. I datagrunnlaget Kripos har analysert er det avdekket at omtrent halvparten av de voksne som er utsatt for seksuell utpressing med profittmotiv betaler kravet fra aktøren, mens omtrent 20 prosent av de utsatte barna betaler. At færre barn enn voksne betaler kan forklares på flere måter. Spesielt de yngste barna har ikke tilgang til digitale betalingsmidler, ei heller faktisk betalingsevne. Av de barna som betaler ser Kripos at de i snitt betaler 2 800 kr til utpresserne, mens de voksne som betaler i snitt betaler 10 000 kr til utpresserne. Mange av de utsatte betaler i flere omganger, noe som klart indikerer at utpresseren ikke avslutter utpressingen ved første betaling. Betaling blir heller et tegn på at det er et potensial for å presse ut de fornærmede ytterligere. Samlet har de norske fornærmede i datagrunnlaget Kripos har analysert, i perioden 1. januar 2023 til 31. oktober 2024, betalt omtrent 7,6 millioner kroner til utpressere rundt i verden.

> Samlet har de norske fornærmede i datagrunnlaget Kripos har analysert [...] betalt omtrent 7,6 millioner kroner til utpressere rundt i verden.

Til tross for at seksuell utpressing med profittmotiv fører til konkrete økonomiske tap for den enkelte, er det ikke like tydelig hvilken samfunnsøkonomisk konsekvens både seksuell utpressing og alle andre cyberstøttede seksuallovbrudd har for samfunnet. Kripos er ikke kjent med at det er foretatt en samfunnsøkonomisk beregning av disse kostnadene. Tatt i betraktning det store omfanget av disse lovbruddene, som finner sted hver eneste dag, og hvor store konsekvenser det har for den enkelte, er den samlede trusselen svært stor, både på individnivå og samfunnsnivå.

Delvurderinger

Det er *meget sannsynlig* at det vil være en økning i omfanget av syntetiske overgrepsbilder i 2025. Det er også *meget sannsynlig* at eldre overgrepsmateriale som er delt tidligere vil bli delt på nytt, både med høyere kvalitet og i nye varianter. Det er *sannsynlig* at syntetiske overgrepsvideoer av realistisk kvalitet vil forekomme i 2025.

Det er *sannsynlig* at forekomsten av cyberstøttede seksuallovbrudd på ende-til-ende-krypterte meldingsplattformer vil fortsette å øke i 2025, både fordi flere gjerningspersoner tar et aktivt valg om å bruke slike plattformer og fordi flere plattformer går over til ende-til-ende-kryptering.

Det er *meget sannsynlig* at seksuell utpressing med profittmotiv vil være et omfattende problem også i 2025. Dersom betalingsviljen til de utsatte reduseres er det *sannsynlig* at aktørene vil tilpasse sin virksomhet. Et tenkt scenario kan da være at aktørene skalerer opp og automatiserer kontaktetableringsprosesser med potensielle fornærmede for å nå ut til flere, raskere.

Det er *sannsynlig* at gjerningspersoners geografiske nedslagsfelt øker når språklige barrierer brytes ned ved hjelp av KI. Som følge av dette er det *sannsynlig* at flere gjerningspersoner enn tidligere utsetter norske barn for cyberstøttede seksuallovbrudd i 2025.

Foto: Shutterstock

Foto: Shutterstock

Ventet utvikling 2025

Cyberkriminalitet kan ramme alle nivåer i samfunnet og vi er alle potensielle mål for de kriminelle. Blant de mange digitale og menneskelige slagsidene kan det være utfordrende å avgjøre hvilken trussel som utgjør størst risiko og som fortjener økt fokus og innsats. Disse utfordringene må møtes på flere nivåer og Kripos anerkjenner utfordringen som enkeltpersoner, virksomheter og offentlige myndigheter står overfor. De viktigste vurderingene i denne rapporten er derfor fordelt på disse tre nivåene.

Trusselen mot enkeltpersoner

Nordmenn blir stadig oftere utsatt for cyberkriminalitet i form av bedragerier, seksuell utpressing eller digitale overgrep mot barn. I tillegg blir enkeltpersoner indirekte skadelidende som følge av cyberkriminalitet begått mot virksomheter og felles verdier. På samme tid senkes kulturelle og språklige barrierer med teknologisk utvikling, noe som fører til at cyberkriminalitet mot enkeltpersoner ofte er mer skalerbar enn cyberkriminalitet som retter seg mot digital teknologi og infrastruktur. Den raskt voksende mengden cyberkriminalitet mot enkeltpersoner utgjør en trussel mot den alminnelige tryggheten i samfunnet.

Vurderinger

Det er *sannsynlig* at dypforfalskninger som benyttes i sanntidskommunikasjon vil bli brukt til å begå bedragerier og i utpressingsøyemed mot norske enkeltpersoner og virksomheter i 2025. Det er *mulig* at cyberkriminelle vil ta i bruk KI-avatarer til samme formål i løpet av 2025.

Det er *sannsynlig* at ekte overgrepsmateriale av mange aktører vil foretrekkes fremfor syntetisk overgrepsmateriale. Det er derfor *mulig* at økningen av syntetisk overgrepsmateriale vil føre til en økning i direkteoverførte overgrep i 2025 fordi aktører ønsker å verifisere ektheten i overgrep som deles.

Det er *mulig* at den geografiske utvidelsen av Vipps vil føre til at norske barn selger egenprodusert seksualisert materiale til nordiske aktører og at norske aktører vil kjøpe egenprodusert seksualisert materiale av nordiske barn i 2025.

Trusselen mot virksomheter

Norske virksomheter står overfor en stadig mer sammensatt og krevende trussel i det digitale rom. Virksomheter utsettes for alt fra løsepengevirus og bedragerier til tap av sensitiv data som også kan føre til juridiske og forretningsmessige implikasjoner. Kravet til egensikring er høyt, og ofte er utfordringene de samme for små, mellomstore og store virksomheter. Selv om det ikke er praktisk mulig å sikre virksomheter fullstendig, er grunnleggende forebygging, bevissthet og god sikkerhetshygiene ofte effektivt i å forhindre kriminell utnyttelse.

Vurderinger

Det er *sannsynlig* at cyberkriminelle vil ta i bruk KI-agenter i løpet av 2025, men som følge av en fremdeles umoden teknologi er det likevel *lite sannsynlig* at KI-agenter vil utgjøre en betydelig mengdeendring innen cyberrettet kriminalitet i samme periode. I tillegg til å effektivisere de kriminelles prosesser, er det *mulig* at KI-agenter vil benyttes som en del av selve kriminalitetsutøvelsen i løpet av 2025.

Det er *sannsynlig* at påvirkning fra uvedkommende på fysiske prosesser vil føre til produksjonsstans og store økonomiske kostnader for norske OT-avhengige virksomheter i løpet av 2025. Videre er det er det *sannsynlig* at vellykkede cyberangrep mot OT-avhengige virksomheter vil føre til følgekonsekvenser i forsyningskjeden, og derigjennom *mulig* forstyrre fysiske prosesser tilknyttet grunnleggende nasjonale funksjoner eller kritisk infrastruktur.

Det er *meget sannsynlig* at den største andelen cyberangrep mot OT-avhengige virksomheter retter seg mot virksomhetssystemer. Det er *sannsynlig* at løsepengevirus vil utgjøre den største andelen cyberrettede angrep mot OT-avhengige virksomheter i Norge, med indirekte konsekvenser for operasjonell drift. Det er videre *meget sannsynlig* at flesteparten av løsepengevirusangrep mot OT-avhengige virksomheter vil stamme fra et ønske om profitt.

Trusselen mot samfunnet

Cyberkriminalitet representerer en alvorlig trussel mot samfunnets sikkerhet, funksjonalitet og våre felles verdier. Økt digitalisering hos alle innbyggere og teknologiske avhengigheter bidrar til å effektivisere samfunnet og tilgjengeliggjøre tjenester, samtidig som det åpner opp for nye sårbarheter. I ytterste konsekvens kan kriminell utnyttelse av disse sårbarhetene true kritiske samfunnsfunksjoner, enkeltpersoners trygghet i det digitale rom og demokratiske verdier som åpenhet, tillit og frie valg.

Vurderinger

Det er i løpet av 2024 observert at organiserte kriminelle nettverk flytter deler av sin operasjon til både det åpne og mørke nettet. Det er *meget sannsynlig* at dette fører til en større avhengighet av tilretteleggere og digitale muliggjørere, som igjen peker i retning av kriminelles økte avhengighet av det digitale rom.

Dersom organiserte kriminelle i større grad benytter internettet som markedsplass for narkotikasalg vil det *sannsynlig* føre til at narkotikaprisene på internett reduseres. Kripos vurderer det som *meget sannsynlig* at dette vil føre til et større handlingsrom for organiserte kriminelle nettverk som i stort har solgt narkotika i det fysiske rom. Det er *meget sannsynlig* at kriminelle vil fortsette å utnytte avstanden mellom rask teknologisk utvikling og samfunnets tregere evne til å utvikle effektive mottiltak. Videre er det *sannsynlig* at utnyttelsen av denne avstanden hardest vil ramme de eldste og yngste i samfunnet, i tillegg til små og mellomstore virksomheter som ikke prioriterer tilstrekkelige ressurser til å innføre grunnleggende sikkerhetstiltak.

Det er *meget sannsynlig* at kulturelle og språklige barrierer som tidligere har utgjort en del av det digitale forsvaret til norske enkeltpersoner og virksomheter, nå er i ferd med å jevnes ut som følge av kunstig intelligens. Videre er det *sannsynlig* at norske virksomheter og enkeltpersoner vil bli utsatt for cyberkriminalitet fra aktører som tidligere har rettet ressursene sine mot virksomheter i andre land.

På bakgrunn av stadig flere avhengigheter i, og samfunnets utstrakte bruk av, programvarekomponenter med åpen kildekode, er det *meget sannsynlig* at

verdikjedeangrep (via programvare med åpen kildekode) vil representere et større skadepotensial enn tredjepartsangrep isolert sett. Det er likevel *sannsynlig* at flesteparten av kjedeangrep med konsekvenser for det norske samfunnet vil oppstå som følge av et tredjepartsangrep. Videre er det *mulig* at flertallet av alle cyberrettede utpressingsforsøk i 2025 vil oppstå som følge av en kompromittert tredjepart.

Det er *sannsynlig* at cyberstøttede seksuallovbrudd fører til betydelig skade i form av selvskading, spiseforstyrrelser og psykiske lidelser samt årlige tap av liv i Norge som følge av selvmord. Det er videre *meget sannsynlig* at de samlede psykologiske og fysiologiske konsekvensene av cyberstøttede seksuallovbrudd innebærer et betydelig økonomisk tap for samfunnet gjennom manglende deltakelse i utdanning og yrkesliv, ressurser fra helsevesenet og andre statlige virksomheter, som politiet og rettsvesenet.

Det er *sannsynlig* at foresatte har blitt mer oppmerksomme på trusselen barns bruk av sosiale medier medfører, men det er samtidig *sannsynlig* at samme bevissthet ikke gjelder spillplattformer. Disse er, i likhet med de sosiale medieplattformene, også en arena for kontaktetablering og seksuell utnyttelse av barn, og kan sies å utgjøre en økende risiko ettersom flere barn er på spillplattformer og færre er på sosiale medier sammenlignet med tidligere.

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 over).

Begreper

Den raske utviklingen innen digital teknologi skyldes i stor grad bredt internasjonalt samarbeid og det brukes derfor store verdensspråk for å kommunisere på tvers av landegrenser. Som følge av denne utviklingen oppstår det ting eller fenomener som ikke finnes fra før og som trenger nye ord. Ofte blir disse nye ordene importert fra engelsk.

Kripos har nasjonalt fagansvar for å definere og utvikle begrepsapparatet innen cyberkriminalitet. I dette arbeidet forsøker vi så langt mulig å fornorske språket, enten ved å endre skrivemåten av fremmedord eller ved å innføre norske avløserord. Dette forsøker vi å balansere uten å bryte for mye med begrepsbruken ellers i samfunnet. Samtidig må vi også definere en rekke begreper som brukes om teknologi, kriminalitet, sikkerhet og samfunnsfunksjoner, men som kan ha ulik betydning i andre sammenhenger. Derfor følger det et oppdatert begrepsapparat med hver rapport.

Teknologi

Cyber (også kyber) benyttes om all teknologi som anvender digital informasjon, i tillegg til den fysiske infrastrukturen som benyttes for å bearbeide, lagre eller sende informasjon ved hjelp av elektroniske signaler. Dette inkluderer, men er ikke begrenset til datamaskiner, radioutstyr og internett. **Cyberdomenet** står i motsetningsforhold til det fysiske domenet. Eng: *Cyberspace*

Det digitale rom refererer til en global helhet av sammenkoblede datasystemer og informasjonsressurser, og brukes som en metafor på linje med begrepet «det offentlige rom». I rapporter utgitt av Kripos er det digitale rom helheten av datasystemer, nettverk, enheter og programvare hvor cyberkriminalitet begås.

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. Eng: *Darknet*.

Nulldagssårbarhet er en sårbarhet i programvare som noen får kunnskap om, før produsenten/leverandøren eller brukerne av programvaren.[111] Eng: *Zero-day* eller *0-day*. Begrepet er relatert til n-dagssårbarhet som refererer til n antall dager siden sårbarheten i programvaren ble offentlig kjent.

Feilretting er prosessen med å korrigere sikkerhetshull, reparere feil eller øke systemets beskyttelse mot cyberangrep. **Sikkerhetsoppdatering** innebærer å anvende en feilretting til en programvare eller et system for å fjerne en kjent sårbarhet. Eng: *Patching*.

«I det fri» viser til en virkelig trussel (ikke bare en teoretisk) som blir observert i det digitale rom 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-tjeneste består av nettverk med flere servere som fungerer som mellomledd (noder) mellom internettbrukere og internett. Når internettbrukeren benytter en proxy-tjeneste 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-tjeneste** tar det samme oppsettet et skritt videre ved å også kryptere datatrafikken mellom brukeren og nodene i VPN-tjenesten. 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-kryptert meldingsplattform er en kommunikasjonskanal, eksempelvis *Signal* eller *WhatsApp*, som benytter seg av ende-til-ende-kryptering. Det vil si at det kun er deltakerne i en en-til-en-samtale eller i en lukket gruppe som sender meldinger til hverandre, som har tilgang til meldingene. Meldingene og

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

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.

Virksomhetssystem er programvareløsning som understøtter administrative og forretningsmessige funksjoner i en virksomhet. Oppgaven som virksomhetssystemene utfører inkluderer blant annet datahåndtering relatert til ansatte, økonomi, administrasjon tilknyttet produksjon, salg og innkjøp. IT-systemer er å finne i både virksomhetssystemer og OT-systemer, men i rammene av virksomhetssystemer berører de ikke oppgaver direkte tilknyttet operasjonell drift. Virksomhetssystemer blir i denne rapporten derfor benyttet som motstykke til OT-systemer. Eksempler inkluderer ressursplanleggingssystemer (ERP), kundehåndteringssystemer (CRM) og dataanalyse (BI).

KI-system er en samlebetegnelse for ulik program- og maskinvare som utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål.[112]

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**, herunder også store språkmodeller. Kjente eksempler inkluderer OpenAI: *ChatGPT*, Google: *Gemini* og Anthropic: *Claude*. Eng: *Foundation Model.*

KI-agenter kan beskrives som automatiske roboter som selvstendig eller i samarbeid med andre KI-agenter eller mennesker, kan utføre datatekniske oppgaver autonomt eller under menneskelig veiledning. Dette inkluderer bruk av digitale verktøy og kontroll over datasystemer. KI-agenter kjennetegnes ved interaktivitet, fleksibilitet, reaktivitet og proaktivitet for å finne optimale løsninger på problemer. De mest kapable KI-agentene som utvikles i dag er utviklet basert på programvaredesign som legges utenpå eksisterende grunnlagsmodeller. Eng: *AI Agents* eller *Intelligent Agents (IA).* Andre KI-systemer kan også utvise **agentiske egenskaper** uten nødvendigvis å bli omtalt som KI-agenter. Disse egenskapene inkluderer (nor/eng:) mål (*Objectives*), handlinger (*Actions*), minne (*Memory*) og refleksjon (*Rethink*).

Operasjonell teknologi (OT) er teknologien (systemer, enheter og kommunikasjonsinfrastruktur) som understøtter produksjon, leveranse og vedlikehold av fysiske varer og tjenester – ofte forbundet med industriproduksjon eller andre omfattende prosessmiljøer. OT inkluderer også maskin- og programvare som benyttes

112 Regjeringen. (2020). *Nasjonal strategi for kunstig intelligens*. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-kunstig-intelligens/id2685594/

til å styre andre systemer eller enheter som monitorerer eller endrer fysiske prosesser. Se industrielle kontrollsystemer (IKS). OT benyttes for å omtale et teknologiområde (tilsvarende bruk som IT), mens «OT-systemer» beskriver en samling av fysiske og digitale deler (samt underliggende systemer) som er høyst integrert for å oppnå et overordnet mål.[113] Begrepet benyttes i motsetning til «virksomhetssystemer». Eng: *Operational Technology* (OT)

Industrielle kontrollsystemer (IKS) er en underkategori av OT-systemer som omfatter ulike typer utstyr, nettverk og systemer som blir brukt til å operere og automatisere industrielle prosesser. Dette kan inkludere blant annet feltutstyr, kontrollsystemer og applikasjoner. Eng: *Industrial Control Systems* (ICS).

-miljø viser til et avgrenset geografisk (og logisk) område der flere prosesser, enheter og systemer virker sammen for å nå en ønsketilstand eller et sluttprodukt. Miljø brukes uavhengig av teknologisk domene. I forbindelse med OT henviser miljø til fysiske prosesser og digitale støttesystemer som virker sammen for å produsere fysiske varer og tjenester. Eksempler inkluderer OT-miljø, industrielt miljø, prosessmiljø, operasjonsmiljø, virksomhetsmiljø og IT-miljø.

Komponenter er en samlebetegnelse for de individuelle delene som utgjør teknologien. Komponenter er med andre ord byggeklossene som utgjør sammensatte sluttprodukter, inkludert instrumenter, maskinvare og programvare. Eksempler på komponenter inkluderer brytere, kretskort elle databasemoduler.

Kriminologi

Cyberkriminalitet viser til hele det cyberkriminelle spekteret som strekker seg fra cyberrettet til cyberstøttet kriminalitet. Dette innebærer enhver kriminalitet som suppleres av eller begås med informasjons- og kommunikasjonsteknologi, inkludert datasystemer, nettverk, enheter og programvare. Se begrepskart (figur 1) for en utvidet definisjon.

Kriminalitetstyper bygger på straffebud i straffeloven, men kan også være fenomen som ikke er en egen paragraf i straffeloven, eksempelvis seksuell utpressing. Det er per i dag ikke en omforent forståelse i politiet for hva som ligger i kriminalitetsfelt, -område og -type, og bruken kan derfor være forskjellig i andre sammenhenger.

Det cyberkriminelle økosystemet består av: (1) aktørene som begår kriminaliteten, altså aktørlandskapet, (2) miljøet der kriminaliteten finner sted, altså det digitale rom, og (3) uten-

113 Saurabh, K. (2009). *Systems engineering modeling and design*. I A. Bajaj, & S. Wrycza (red.), Systems Analysis and Design for Advanced Modeling Methods: Best Practices. (1 utg. s. 96-100). Information Science Reference

forliggende faktorer som påvirker aktørlandskapet, for eksempel politiske, psykologiske, tekniske, juridiske og økonomiske forhold. En naturlig del av dette økosystemet innebærer at aktører kommuniserer, deler, selger, samhandler, samarbeider, opererer, konkurrerer og kolliderer med hverandre. Samtidig eksisterer ikke det cyberkriminelle økosystemet isolert, og flere av aktørene livnærer seg på fornærmede enkeltpersoner, virksomheter og samfunnsfunksjoner.

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 samarbeider for å oppnå et felles mål gjennom å begå cyberkriminalitet.

Aksjon, eller politiaksjon, er et polisiært begrep som her brukes for å omtale politiets pågripelser og ransakinger, eller situasjoner der politiet på andre måter griper inn for å stanse kriminell virksomhet.

Aktører

Aktør brukes som en generell betegnelse på 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 der det ikke er mulig eller ønskelig å indikere aktørens profiltilhørighet, og innebefatter statlige aktører og terrorister, i tillegg til enkelte cyberkriminelle og cyberkriminelle grupperinger. Videre brukes trusselaktør i tilfeller der aktøren utgjør en konkret trussel mot en enkeltperson, virksomhet eller et datasystem.

Kriminell og cyberkriminell brukes begge om enkeltpersoner som utøver kriminalitet. Kriminell er domenenøytralt, mens cyberkriminell viser til en person som begår kriminalitet i det digitale rom. Kriminalitet supplert av datasystemer (se begrepskart for cyberkriminalitet) er dermed en kategori kriminelle som ikke omtales som cyberkriminell i denne rapporten. **Gjerningsperson** brukes også med samme mening for språklig variasjon, spesielt innen seksuallovbrudd.

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 er domeneuavhengig og ikke entydig med noe kriminelt.

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

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

Kapasiteter henviser til kriminelles kvan-

tifiserbare egenskaper og verdier, svært ofte volum. Eksempler inkluderer fysisk og mental utholdenhet, antall enkeltpersoner i en gruppe, i tillegg til digitale verdier. **Kapabiliteter** legger til grunn at både nødvendige kapasiteter og evnen til å utnytte dem er til stede.

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. **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.

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 og som benytter seg av løsepengevirus som handelsvare. Eng: *Affiliates*.

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

Innsider henviser til en person som utnytter en legitim tilgang til eller informasjon om virksomhetens verdier for kriminelle formål, på vegne av seg selv eller andre.[114] En ansatt som lures til å åpne en lenke eller fil med skadelig innhold er etter denne definisjonen ikke en innsider.

Kriminalitetsutøvelse

Cyberangrep benyttes som et paraplybegrep for å omtale ulike typer cyberrettet kriminalitet, både inntrufne og tenkte scenarier, når man ikke kan eller ønsker å beskrive detaljene omkring den uønskede handlingen. Eksempler på cyberangrep kan være datainnbrudd og datatyveri, i tillegg til militære implikasjoner

114 KraftCERT. (2024). *Trusselvurdering 2024.* s. 9, https://www.kraftcert.no/filer/KraftCERT-Trusselvurdering2024.pdf#page=9.09

som destruktive cyberoperasjoner, her omtalt som digitalt skadeverk. Cyberangrep[115] er straffbare etter norsk straffelov.

Hendelse, noen ganger også sikkerhetshendelse, brukes i denne rapporten for å omtale en begivenhet som kan ha betydning for sikkerheten til en enkeltperson, virksomhet eller samfunnet som sådan. En hendelse residerer fra en kriminell aktørs villede handlinger og involverer minst to parter, en aktør og en fornærmet eller et datasystem, og kan inkludere både cyberrettet og cyberstøttet kriminalitet. Hendelser kan også brukes for å omtale aktiviteter som understøtter kriminelle mål og kan oppstå i ulike deler av angrepskjeden. En hendelse kan oppstå uavhengig av om påvirkning fra uvedkommende har lykkes eller ikke. Eksempler på hendelser kan inkludere skanning av åpne porter i et nettverk, kartlegge sårbarheter i en programvare eller forsøk på å rekruttere innsidere.

Handlemåte 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 kan operasjonsmønster eller *Modus Operandi* benyttes istedenfor handlemåter. En handlemåte bygger på en sammenstilling av **handlinger**, altså en konkret og villet prosess som består av flere steg med **aktiviteter**. Datainnbrudd eller kontaktetablering med barn er eksempler på handlinger. Avlese, overføre, lagre, tilføye, generere, endre, skjule og slette data er aktivitetene som begås i det digitale rom.

Kriminalitet som handelsvare (KSH) er kjøp og salg av kriminelle tjenester, programvare og verktøy. KSH bidrar til å gjøre kriminaliteten profitabel, finansiere ny kriminalitet og gjøre kriminalitet enklere tilgjengelig – også for aktører som ikke kunne utøvd slik kriminalitet på egen hånd. Eng: *Crime-as-a-Service* (CaaS). **Løsepengevirus som handelsvare (LSH)** er en underkategori av KSH og innebærer salg eller utleie av et eksisterende løsepengevirus. Eng: *Ransomware-as-a-Service* (Raas). Et alternativ til LSH er at aktører utvikler og bruker løsepengevirus uten å selge eller leie det ut til andre aktører – et såkalt proprietært løsepengevirus.

Angrepskjeden refererer til et rammeverk utviklet av Lockheed Martin for å identifisere og forhindre datainnbrudd og uønsket aktivitet i et nettverk. Rammeverket identifiserer hvilke

115 I EU sin rådsforordning om restriktive tiltak mot cyberangrep, som gjelder som norsk forskrift er «cyberangrep» definert som handlinger som omfatter ett eller flere av følgende elementer: a. tilgang til informasjonssystemer, b. forstyrrelser av informasjonssystemer, c. forstyrrelser av data eller d. dataavlytting,når det ikke er gitt behørig tillatelse til slike handlinger […]» Forskrift om restriktive tiltak mot cyberkriminalitet. (2021). Lovdata. https://lovdata.no/forskrift/2021-05-11-1459

steg en trusselaktør må utføre for å lykkes med å kompromittere et datasystem. Eng: *Cyber Kill Chain™*.

Cyberrettet utpressing er i denne rapporten benyttet som en samlebetegnelse for ulike modi operandi 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 gjentatte tjenestenektangrep.

Digitalt skadeverk benyttes i denne rapporten om cyberrettede kriminelle handlinger og aktiviteter som medfører skade på IKT. Eksempler på dette kan være tjenestenektangrep utført av hacktivister eller skadeverk på kritisk infrastruktur.

Kjedeangrep representerer en mulighet for kriminelle som ønsker å ramme mange fornærmede som følge av sårbarheter i en felles eller sammenkoblet maskinvare eller programvare. Det finnes flere typer kjedeangrep, men i rammen av denne rapporten utgjør kjedeangrep summen av verdikjedeangrep og tredjepartsangrep.

Tjenestenektangrep har som formål å nekte, forstyrre eller forringe tilgangen til en server, tjeneste eller et nettverk. Eng: *Denial-of-Service* (DoS) *Attack*. I tilfeller der et botnet blir benyttet til å oversvømme et datasystem med nettrafikk, omtales dette som distribuert tjenestenektangrep. Eng: *Distributed-Denial-of-Service* (DDoS) *Attack*.

Sosial manipulasjon er en manipulasjonsteknikk som utnytter menneskelige variasjoner i atferd og ytelse for å få tilgang til beskyttet informasjon, verdigjenstander eller andre ressurser. Faktorer som tidspress, stress, uhell, tankeløshet og manglende opplæring er ofte bakenforliggende årsaker til at en aktør lykkes med sosial manipulasjon, snarere enn den utsattes tilbøyelighet til å utføre kriminelle handlinger. Eng: *Social Engineering.*

Dypforfalskninger (også dypfalsk) er syntetisk medieinnhold (bilde, video eller lyd) som gjenskaper eller digitalt endrer steder, objekter eller levende vesener, og som blir presentert som ekte innhold. Dypforfalskning kan for eksempel bli brukt til å fremstille en politisk figur som sier noe vedkommende aldri har sagt, filmatisere en ekte person som blir kidnappet, men med stemme og utseende til en annen person, eller vise et leveområde som gjennomgår klimaforandringer som ikke har skjedd. Dypfalsk genereres ved hjelp av kunstig intelligens, herunder maskinlæring og dyp læring. Eng: *Deepfake*

Overgrepsmateriale eller **seksualisert materiale av barn** er fremstillinger av seksuelle overgrep mot barn eller fremstillinger som seksualiserer barn under atten år.[116]

116 Straffeloven. (2005). Lov om straff (LOV-2005-05-20-28), § 311

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.

Verdier

Forsyningskjede og verdikjede viser til ulike sider ved ledd i produksjonsprosessen. **Forsyningskjede** er en kjede av virksomheter som direkte eller indirekte er involvert i å oppfylle et kundebehov. En forsyningskjede spenner over flere virksomheter og omfatter flyten av varer, informasjon og betalingsmidler mellom disse Eng: Supply Chain. **Verdikjede** beskriver hvor produktet (varen eller tjenesten) tilføres verdi gjennom de ulike leddene i kjeden. Verdikjeden kan strekke seg over flere virksomheter som tilbyr eller etterspør varer og tjenester som inngår i produktet. Begrepet inkluderer hele livsløpet til et sluttprodukt og omfatter rekken av ressurser, prosesser og aktiviteter for produksjon av et produkt. Eng: *Value Chain*.[117]

Tredjepart viser til en utenforstående i forholdet til en prinsipal virksomhet som er den parten i et forretningsforhold som initierer et oppdrag. En tredjepart kan være en tjenesteleverandør som tilbyr for eksempel banktjenester, skytjenester eller internetinternettjenester. Det kan også være en underleverandør, eksempelvis produsenter av maskinvarekomponenter eller leverandør av råmateriale, som er oppstrøms i forsyningskjeden. I noen tilfeller kan også andre kunder utgjøre en tredjepart som følge av gjensidige avhengigheter via for eksempel et felles datasenter.

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.

Grunnleggende nasjonal funksjon (GNF) er definert som 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.[118]

---

117 Definisjoner er sammenstilt fra nettside: Rolstadås, Asbjørn. (2024, 28. juni). *verdikjede*. Store Norske Leksikon. https://snl.no/verdikjede og Rolstadås, Asbjørn. (2023, 15. september). *forsyningskjede (produksjonsteknikk)*. Store Norske Leksikon. https://snl.no/forsyningskjede_-_produksjonsteknikk

118 Sikkerhetsloven. (2018). Lov om nasjonal sikkerhet. (LOV-2018-06-01-24) https://lovdata.no/lov/2018-06-01-24 § 1-5 nr. 2

OT-avhengige og IT-sentrerte virksomheter er organiserte enheter som leverer tjenester eller utfører aktiviteter for å oppnå bestemte formål. Dette inkluderer offentlige og private enheter hvor formålet kan være økonomisk gevinst eller å levere samfunnsnyttige tjenester. OT-avhengige virksomheter er avhengig av OT-systemer for å kunne levere sine varer og tjenester, mens IT-sentrerte virksomheter representerer alle virksomheter som har en digital sårbarhetsflate, men som ikke benytter operasjonell teknologi for å understøtte sine primærverdier. Avhengig av kontekst blir virksomheter også omtalt som risikoeier, ressurseier eller anleggseier.

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.[119]

Figuroversikt

- Figur 1 – Begrepskart cyberkriminalitet. Side 12
- Figur 2 – Isfjellet. Side 13
- Figur 3 – Spekteret av statlig ansvar. Side 19
- Figur 4 – Muliggjørere i cyberkriminelle nettverk. Side 23
- Figur 5 – Tilretteleggere i cyberkriminelle nettverk. Side 25
- Figur 6 – Begrepskart cyberrettet kriminalitet. Side 29
- Figur 7 – Verdikjedeangrep. Side 37
- Figur 8 – Oversiktskart over utvalgte løsepengevirusvarianter. Side 45
- Figur 9 – Sammensmeltingen mellom IT og OT. Side 56
- Figur 10 – Konsekvensmatrise. Side 69
- Figur 11 – Begrepskart cyberstøttede seksuallovbrudd. Side 71
- Figur 12 – Faser i seksuell utpressing. Side 76
- Figur 13 – Fremgangsmåte for kontaktetablering med barn. Side 81

119 Straffeloven. (2005). Lov om straff (LOV-2005-05-20-28)." § 20 1. ledd bokstav a

Politiet skal beskytte person, eiendom og fellesgoder, verne om all lovlig virksomhet og verne mot alt som truer den alminnelige tryggheten i samfunnet. Politiet skal også forebygge kriminalitet, avdekke og stanse kriminell virksomhet og forfølge straffbare forhold.

Kripos er politiets nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet. Kripos er også nasjonalt kontakt- og koordineringspunkt for internasjonalt politisamarbeid og ansvarlig for politiets nasjonale etterretningsproduksjon.

Nasjonalt cyberkrimsenter (NC3) ved Kripos bekjemper cyberrettet- og cyberstøttet kriminalitet med særlig fokus på seksuelle overgrep mot barn. NC3 har særskilt kompetanse innen initialetterforskning av cyberkriminalitet. Avdelingen skal forebygge, avverge og bekjempe teknologidrevet kriminalitet, med særlig fokus på cyberrettet kriminalitet og internettrelaterte overgrep.

Politiet ønsker i utgangspunktet at alle straffbare forhold anmeldestil til lokalt politi. Er du usikker på om forholdet er straffbart eller har du informasjon du ønsker å dele med oss?

Ta gjerne kontakt gjennom NC3 sine tipsmottak.

Tips oss om cyberstøttede seksuallovbrudd

Tips oss om cyberrettet kriminalitet

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

Foto fremsiden: Laget med KI