



POLITIET
KRIPOS



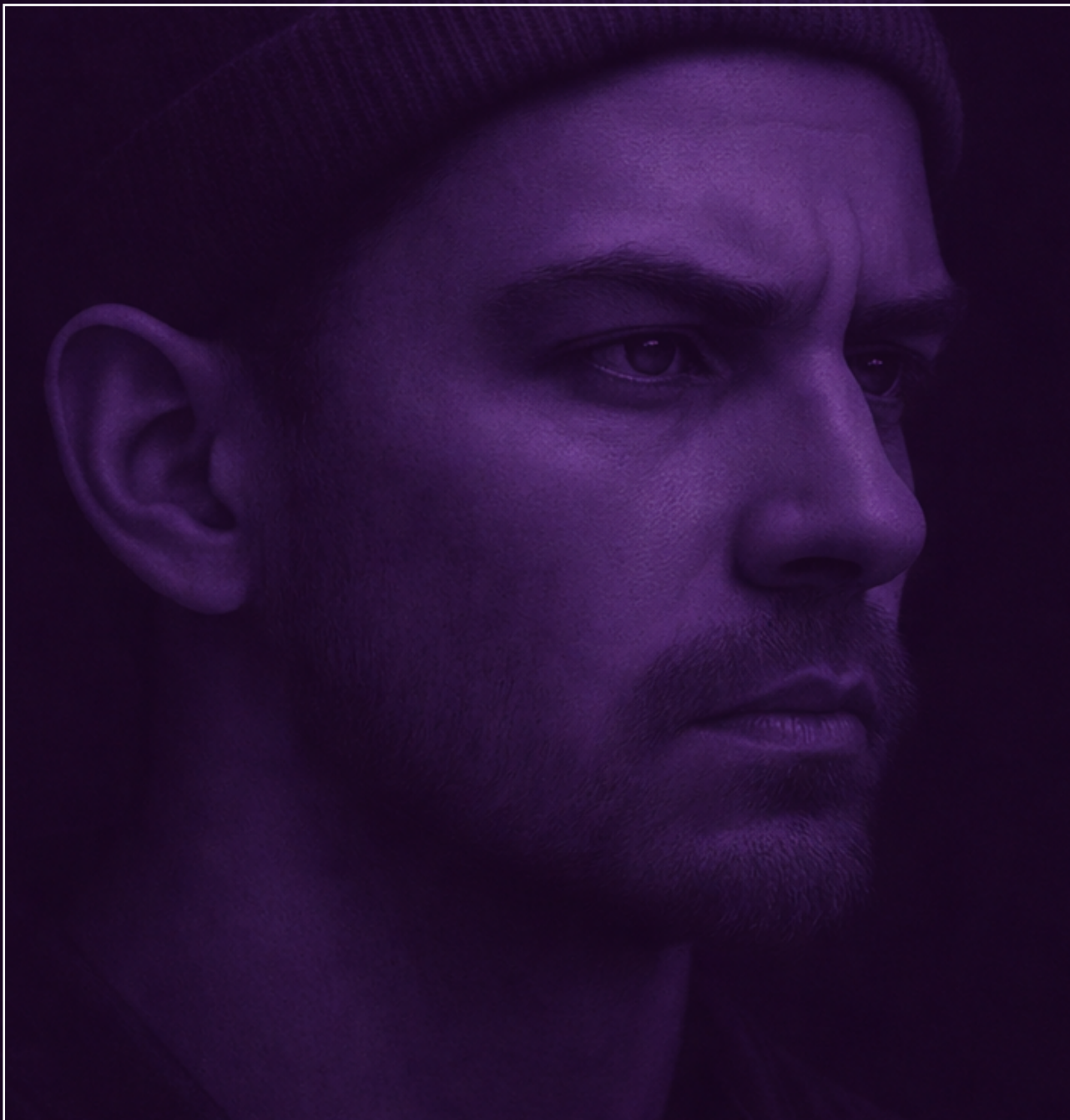
1010101110010



Cyberkriminalitet 2026

Politiets årlige rapport om cyberrettet
og cyberstøttet kriminalitet





Cyberkriminalitet 2026, Kripos

Politiets årlige rapport om cyberrettet og
cyberstøttet kriminalitet

Grafisk formgivning: Økokrim

Opplag og trykk: 350, Aksell

ISSN: 2704-2537

Foto: Kripos, KI-generert

Det digitale rom er i dag en integrert del av samfunnet vårt. Det preger hvordan vi kommuniserer, arbeider og organiserer oss, men også hvordan kriminalitet begås og utvikler seg. *Cyberkriminalitet 2026* er Kripos' bidrag til å belyse dette landskapet, og til å styrke felles forståelse av trusler, sårbarheter og utviklingstrekk som angår hele samfunnet.

Vi lever i en tid preget av økt geopolitisk spenning, teknologisk omstilling og et mer sammensatt trusselbilde. Krig i Europa, strategisk rivalisering mellom stater og økende bruk av hybride virkemidler påvirker også kriminalitetsbildet. Digitale angrep, påvirkningsoperasjoner og utnyttelse av sårbarheter i samfunnskritisk infrastruktur skjer ofte i gråsonen mellom kriminalitet og sikkerhetspolitikk. Ulike former for utnyttelse av sårbare barn og unge tar nye former og begås med forskjellige motivasjoner, med teknologien som både driver og hjelpemiddel. Dette stiller nye krav til forståelse, samhandling og beredskap.

At 2026 er utpekt som totalforsvarsåret i Norge, gir denne rapporten en særlig ramme. Totalforsvaret handler om samfunnets samlede evne til å forebygge, motstå og håndtere kriser og konflikter. I dette arbeidet er politiet og Kripo en del av et større fellesskap, der offentlige myndigheter, næringsliv og sivilsamfunn er gjensidig avhengige av hverandre. Cyberkriminalitet utfordrer nettopp disse avhengighetene, gjennom angrep på tillit, tilgjengelighet og integritet i digitale systemer.

Rapporten viser at cyberkriminalitet sjelden kan forstås som enkeltstående hendelser. Den inngår i økosystemer av aktører, tjenester og teknologier, der kommersialisering og arbeidsdeling senker terskelen for alvorlig kriminalitet. Samtidig understrekes det at kriminaliteten i stor grad følger kjente mønstre, men med nye virkemidler og økt skadepotensial. Det er i disse forskyvningene – snarere enn i det spektakulære og helt nye – at de største utfordringene ofte oppstår.

Kripo's hovedoppgave er å bidra til å forebygge og bekjempe organisert og annen alvorlig kriminalitet. I det digitale rom forutsetter dette kunnskap, etterretning og samarbeid – nasjonalt og internasjonalt. Forebygging er et gjennomgående premiss i denne rapporten, fordi tidlig forståelse og målrettet forstyrrelse av kriminelle strukturer gir størst effekt over tid.

Cyberkriminalitet 2026 er ment som et kunnskapsgrunnlag for beslutningstakere, fagmiljøer og samarbeidspartnere. Målet er ikke å gi alle svar, men å bidra til en felles situasjonsforståelse – som et nødvendig utgangspunkt for å styrke samfunnets samlede motstandskraft i en digitalisert og urolig tid.



Kristin Kvigne
Sjef Kripo

Innhold

Forord	3
Innhold	4
Sammendrag.....	5
Rapportens formål.....	7
Vårt mandat.....	9
Politiets rolle og handlingsrom	9
Cyberkriminalitet som Kripas' mandat.....	9
Om etterretning	11
Cyberdomenets særtrekk og framtidig relevans for organisert og annen alvorlig kriminalitet.....	15
Cyberkriminalitet sett fra politiets ståsted	18
Mørketall og utfordringer i politiets datagrunnlag	18
Internasjonale utviklingstrekk innen cyberkriminalitet.....	19
Nasjonale utviklingstrekk.....	46
Normalbildet for cyberkriminalitet i Norge	35
Det cyberkriminelle økosystemet	53
Aktørgalleriet	56
Prosesser og metoder innen cyberkriminalitet.....	86
Kriminelle nettverks bruk av digitale muliggjørere	95
Ventet utvikling 2026	101
Trusselen mot enkeltpersoner	101
Trusselen mot virksomheter	102
Trusselen mot samfunnet	103
Vedlegg.....	106
Sannsynlighetsord	106
Begreper	106
Figuroversikt.....	117



Sammendrag

Rapporten *Cyberkriminalitet 2026* gir et helhetlig og oppdatert situasjonsbilde av cyberkriminalitetens karakter, omfang og forventede utvikling i Norge, sett fra politiets ståsted. Rapporten bygger på Kripos' mandat innen organisert og annen alvorlig kriminalitet og tar utgangspunkt i et normalbilde som beskriver vedvarende trekk og stabile mønstre i trussellandskapet.

I rapporten omtales tilsvarende tematikk flere steder, men fra ulike perspektiv og i ulike kontekster. Hovedårsaken til det er at Kripos tilstreber å se cyberrettet og cyberstøttet kriminalitet som en del av en større helhet med fellesnevnerne og glidende overganger – ikke som separate, gjensidig utelukkende fenomener.

Et grunnleggende premiss er at digital teknologi i dag er en integrert og ofte nødvendig del av moderne kriminalitet. Rapporten skiller derfor ikke skarpt mellom cyberkriminalitet og tradisjonell kriminalitet, men beskriver kriminalitet langs et spekter basert på grad av teknologisk avhengighet. Cyberkriminalitet forstås som kriminalitet der teknologi enten er et mål eller en sentral muliggjørere. Denne tilnærmingen synliggjør hvordan digitale byggeklosser inngår i de fleste alvorlige kriminalitetsformer, og hvordan grensene mellom fysiske og digitale domener i økende grad viskes ut.

Rapporten redegjør for det *cyberkriminelle økosystemet* slik politiet ser det, og introduserer nye analytiske rammeverk for bedre å forstå aktørenes dynamikker og handlemåter. Kriminalitet forstås ikke som isolerte handlinger, men som et samspill mellom aktører, tjenester, teknologi, markeds plasser og strukturelle sårbarheter. Kommersialisering og arbeidsdeling har ført til framvekst av et marked der kriminelle tjenester tilbys i ulike former, noe som senker terskelen for deltakelse og øker både volum og tempo i kriminaliteten. Økosystem-perspektivet bidrar til å forklare hvorfor tiltak rettet mot enkeltaktører ofte har begrenset effekt dersom underliggende strukturer og muliggjørere består. Framstillingen av det cyberkriminelle økosystemet har til hensikt å synliggjøre samarbeid, avhengigheter og andre former for knytninger mellom aktører, virkemidler og moduser. Det vil også ta for seg nyanser i de forskjellige aktørgruppene og vise at eksempelvis profittmotiverte cyberkriminelle kan være så mangt.

Normalbildet for cyberkriminalitet i Norge preges fortsatt av profittmotiverte aktører, seksuallovbrytere og ideologisk motiverte aktører. Digitale bedragerier og cyberstøttede seksuallovbrudd utgjør store deler av volumet, mens cyberrettede angrep mot virksomheter

representerer et betydelig skadepotensial. Rapporten understreker at mørketallene er omfattende, blant annet som følge av under-rapportering og metodiske begrensninger i tilgjengelige datakilder.

Et sentralt utviklingstrekk er den fortsatte profesjonaliseringen av cyberkriminaliteten. Kriminelle aktører utnytter skalerbare løsninger, automatisering og tilgjengelige verktøy for å effektivisere angrep og redusere risiko. Kunstig intelligens trekkes fram som en viktig muliggjør-er, særlig innen sosial manipulasjon, automa-tisert tilpasning av angrep og produksjon av innhold.

Rapporten beskriver videre framveksten av mer komplekse samarbeidsformer og koalisjo-ner i det cyberkriminelle miljøet, spesielt innen løsepengevirus-økosystemet. Slike strukturer kan gi økt kapasitet og slagkraft, men innebærer også sårbarheter knyttet til interne konflikter og tillit. Et særlig alvorlig utviklingstrekk er fram-veksten av ekstreme, voldelige nettsamfunn som utgjør en betydelig trussel mot barn og unge gjennom radikalisering, utnyttelse, press til selvskading og grov vold.

Politiets rolle i det digitale rom framheves som både nødvendig og utfordrende. Cyber-kriminalitet kjennetegnes av anonymitet, høy

hastighet og grensekryssende aktivitet, noe som stiller store krav til etterretning, analyse og internasjonalt samarbeid. Rapporten vektlegger forebygging som det viktigste virkemiddelet, basert på tidlig identifisering av trender, forstyr-relse av kriminelle strukturer og samarbeid på tvers av sektorer. Politiet har en særskilt rolle gjennom adgang til tvangsmidler og koordi-nering med utenlandske myndigheter, men er samtidig avhengig av bidrag fra andre samfunnsaktører.

Avslutningsvis vurderer rapporten forventet utvikling i 2026. Trusselen fra cyberkriminalitet anses som vedvarende og i økende grad kom-pleks, både når det gjelder metoder, aktørbildet og konsekvenser. Små, gradvise endringer i normalbildet kan gi store utslag over tid. Samlet sett gir rapporten et kunnskapsbasert grunn-lag for strategiske vurderinger og understreker behovet for helhetlig forståelse, kontinuerlig tilpasning og målrettet forebygging i møte med et dynamisk og sammensatt cybertrusselbilde.



Rapportens formål

Kripos har i flere år advart mot ulike kriminalitetstrusler i det digitale rom. Mengden av cyberangrep har økt, og spennet av lovbrudd er stort. Trusselen er uforutsigbar, global og rammer på tvers av sektorer. Dette utfordrer koordinering, informasjonsdeling og hendelses-håndtering. I dagens spente sikkerhetspolitiske situasjon er det viktigere enn noen gang å ha et felles kunnskapsgrunnlag og et felles nasjonalt strategisk situasjonsbilde av cybertrusselen.

Kripos har derfor valgt å beskrive det *cyber-kriminelle normalbildet* i årets rapport, slik at samfunnet i felleskap kan forstå og identifisere avvik, utvikle indikatorer og navigere i det videre arbeidet med å forebygge, avverge, etterforske og skadebegrense trusselen i det digitale rom.

Cyberkriminalitet kan variere i form og utførelse, fra enkle kriminelle handlinger til avanserte og sammensatte cyberangrep. Fellesnevneren er at digital infrastruktur og programvare er nødvendig for å begå kriminaliteten.

I likhet med tidligere utgaver er årets cyberkriminalitetsrapport ment å gi bedre forståelse av kriminalitet i det digitale rom, men også av såkalte *domenekryssende kriminelle* – aktører som benytter virkemidler i både det fysiske og det digitale rom for å optimalisere og kostnads-effektivisere kriminaliteten og oppnå en kriminell målsetning.





Vårt mandat

Politiets rolle og handlingsrom

Politiets samfunnsoppdrag slik det framgår av politiloven, gjelder i det digitale som det fysiske rom. Oppdraget innebærer at politiet skal forebygge, avdekke, avverge, etterforske og iredtføre cyberkriminalitet som kan ramme norske borgere, virksomheter og verdier, som kritisk infrastruktur. Cyberkriminaliteten kjennetegnes av at den ofte skjer raskt, tilnærmet anonymt og på tvers av nasjonale og internasjonale jurisdiksjoner. Effektiv bekjempelse av cyberkriminalitet forutsetter derfor tett samarbeid mellom offentlige og private aktører både nasjonalt og internasjonalt.

Politiets hovedstrategi er å forebygge kriminalitet, som bygger på en ambisjon om å være i forkant av kriminaliteten og forhindre at den skjer. Dette innebærer en systematisk, planmessig og kunnskapsbasert tilnærming til forebygging og tett samarbeid på tvers av fagområder og sektorer.¹ Foruten etterforskning av cyberkriminalitet – som kan ha en allmenn-

preventiv effekt selv om den er iboende reaktiv – og samarbeid med andre lands politimyndigheter – som blant annet kan bidra til identifisering av nye kriminalitetstrender – består politiets forebyggende innsats mot cyberkriminalitet av en rekke ulike tiltak. De spenner fra tilstedeværelse på digitale plattformer til å ta ned digital infrastruktur som benyttes til kriminell virksomhet. I tillegg består innsatsen av å utvikle eller ta i bruk teknologi og metoder som gjør det enklere å avdekke og forstyrre kriminaliteten. Etterretningsproduksjon og kunnskapsformidling er viktige ledd i den kunnskapsbaserte tilnærmingen ved å bidra til felles situasjonsforståelse og et økt kunnskapsgrunnlag om trusselen fra cyberkriminelle aktører.

Cyberkriminalitet som Kripas' mandat

Hva som vies oppmerksomhet i *Cyberkriminalitet 2026*, må ses i lys av Kripas' mandat som er «organisert og annen alvorlig kriminalitet»².

1 Politidirektoratet (2021). *I forkant av kriminaliteten: Forebygging som politiets hovedstrategi (2021–2025)*. s. 6. <https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/pod/i-forkant-av-kriminaliteten.pdf>

2 Påtaleinstruksen. (1985). *Regler om ordningen av påtalemyndigheten* (FOR-1985-06-28-1679). Lovdata. <https://lovdata.no/forskrift/1985-06-28-1679/§37-1>

Videre er avhengighet til teknologi en sentral forutsetning for at en kriminalitetsform skal regnes som cyberkriminalitet. Det er likevel uklare skillelinjer innad i og mellom kriminalitetsformer, hvor noen åpenbart er å regne som cyberkriminalitet, mens andre ikke er det – samtidig som at disse også lener seg tungt på teknologi for å koordinere og effektivisere kriminaliteten.³

Som nevnt i fjorårets rapport, fantes ikke *kriminalitet 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.

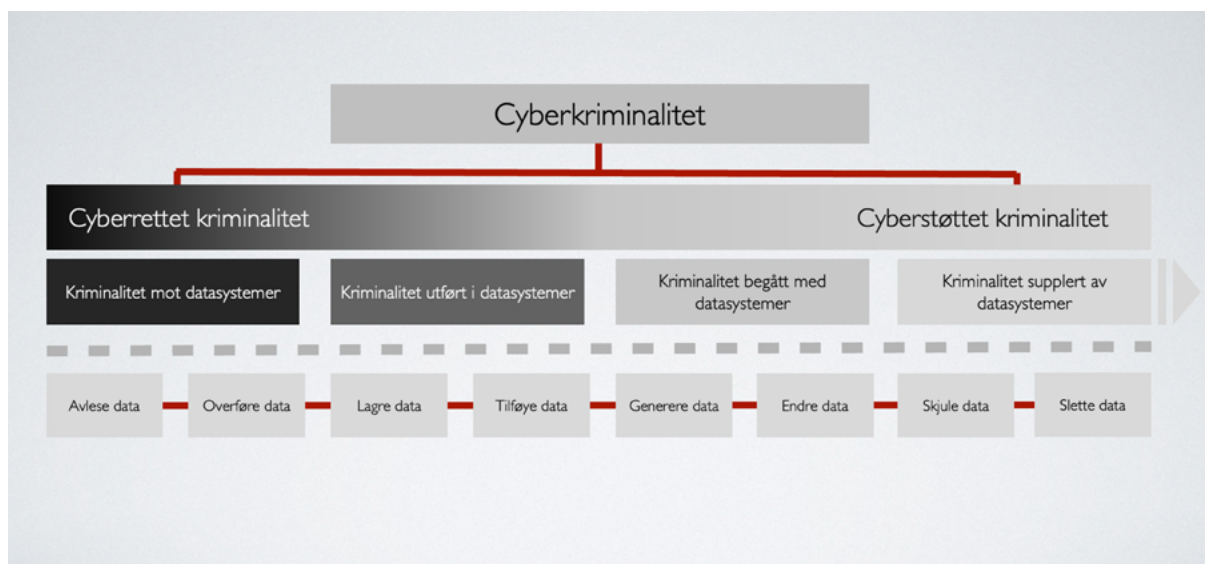
Kriminalitet mot datasystemer skiller seg fra annen cyberkriminalitet ved at den retter seg direkte mot et datasystem, framfor mennesker som bruker datasystemer eller informasjon som er lagret på datasystemer. Eksempler inkluderer blant annet datainnbrudd og digitalt skadeverk. Et datainnbrudd er ofte 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 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** – tradisjonell kriminalitet som begås i det fysiske domenet, men som benytter datasystemer som et supplement. Dette er former for kriminalitet som primært faller utenfor cyberkriminalitetsbegrepet, men som i noen tilfeller har glidende overganger til cyberstøttet kriminalitet. Eksempler er at organiserte kriminelle kommuniserer

3 Et eksempel er vold som handelsvare (VSH), (eng: *Violence-as-a-Service (VaaS)*), som i sin form og utførelse er voldskriminalitet og hvor teknologien er en viktig forutsetning, men som likevel ikke er å regne som cyberkriminalitet.



Figur 1: *Begrepskartet* 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.

seg imellom på krypterte telefoner eller meldingsplattformer, at kriminelle nettverk rekrutterer ungdom til å utføre voldsoppdrag eller at voksne avtaler fysiske møter med barn i sosiale medier for å begå seksuelle overgrep. At kriminalitetsutøvelsen i økende grad suppleres av datasystemer, medfører at viktige spor ligger hos tjenestetilbydere og på digitale plattformer og enheter. Det skaper et behov for å utvikle kompetanse og metoder i bekjempelsen av all organisert og alvorlig kriminalitet.

Om etterretning

Etterretningens primære formål er å støtte beslutningstakere og sette dem i stand til å ta velinformerte avgjørelser og iverksette tiltak. Dette gjøres ved å innhente, sammenstille, analysere og vurdere informasjon som deretter formidles til bestiller av etterretningsproduktet. Gjennom etterretningsproduksjon søker etterretningen å skape forståelse og innsikt i trusler gjennom kunnskapsproduksjon. Hensikten er å beskytte norske interesser, ivareta sikkerhet og forebygge, avdekke og motvirke framtidige trusler.

Strategisk etterretning skal gi overordnet innsikt i forhold som påvirker nasjonens interesser og sikkerhet. Det handler om å forstå de store linjene – som trender, maktforhold, trusler og muligheter som former framtiden. Det handler om å gjøre nasjonen og samfunnet i stand til å opptre proaktivt.

Et strategisk varsel omhandler mulige framtidige trusler eller hendelser som kan få betydelige konsekvenser for nasjonal sikkerhet og beredskap, og skal sette beslutningstakere i stand til å treffe tiltak før det utvikler seg til en akutt krise. Et strategisk varsel er et resultat av langsiktige observasjoner (innsamling) og mønstergjenkjenning (analyse) og gir rom for handling.

Cyberetterretning skiller seg fra andre etterretningsproduksjonsområder på flere måter fordi det fordrer tett integrasjon med andre fagdisipliner, både politifaglige, juridiske og tekniske. Selv om det *ikke* er etterretningens oppgave å identifisere sårbarheter, avdekker likevel analysen enkelte slike. Dette medfører at cyberetterretning må se på trusler (aktør), sårbarheter og verdier helhetlig og i sammenheng. Grunnet den iboende kompleksiteten er utvikling av modeller viktig som støtte til formidling av trusselens ulike sammenhenger. Kripos har derfor i år som tidligere år utviklet nye analytiske rammeverktøy og videreutviklet begrepsapparatet på cyberkriminalitet som bidrag inn i kunnskapsproduksjonen på fagfeltet.





ADDRESS	ADDRESS	SECTOR	SECTOR
78	944 66	D4	Sector A-1
95	061 74	H5	Sector A-2
25	182 38	L5	Sector A-3
	294 99	A4	Sector A-4
8	210 06	V5	Sector A-5
5	722 17	F2	Sector A-6
2	529 39	C6	Sector A-7
9	036 10	W8	Sector A-8
	870 48	R2	Sector A-9
	181 54	E8	Sector A-10
	862 39	G7	Sector A-11
	242 15	E2	Sector A-12
	242 15	E2	Sector A-12

Cyberdomenets særtrekk og framtidig relevans for organisert og annen alvorlig kriminalitet

Teknologisk utvikling er den viktigste driveren bak endringer i cyberkriminalitet. I årets rapport vektlegger Kripos derfor teknologiens betydning for gjennomføringen av flere kriminalitetstyper og beskriver det bredere cyberkriminelle økosystemet⁴ fra dette perspektivet.

Den digitale transformasjonen går i ulikt tempo på tvers av nivåer og funksjoner i samfunnet. Teknologisk nyvinning skjer raskt, mens grunnleggende menneskelig atferd og institusjonelle endringer ofte tar lengre tid. Dette gjelder også politiets egen virksomhet og evne til å ta i bruk ny teknologi i kriminalitetsbekjempelsen.

I det digitale rom utvides rekkevidden og handlefriheten for alle former for kriminalitet. Samtidig

som det digitale rom i økende grad integreres i kriminalitetsutøvelsen, har det iboende særtrekk som skiller det fra vårt fysiske oppholdsrom.

Det digitale rom gjør det mulig for geografisk og sosialt spredte aktører å selv-organisere seg for måloptimalisering i alle ledd. En konkret cybertrussel kan oppstå i løpet av kort tid.

Det digitale rom er menneskeskapt, under kontinuerlig utbygging og i konstant endring. Det har også vist seg å være grunnleggende sårbart og egnet for kriminell utnyttelse. Dette fører til særskilte utfordringer med å oppdage uønskede handlinger, identifisere hvem som står bak kriminaliteten og avdekke aktørers motivasjon og intensjon.

4 Se begrepskart på side 11.

Et strategisk viktig kjennetegn ved det digitale rom er muligheten for skalering – enten det gjelder å kompromittere mange datasystemer samtidig, generere store mengder innhold⁵, eller å nå ut til, utnytte eller manipulere store grupper mennesker. Slike handlinger ville normalt krevd betydelige ressurser og innsats, men kan raskt automatiseres ved hjelp av digitale hjelpemidler.

Cyberdomenet fungerer også som én inngangsport til mange verdier,⁶ som følge av gjensidige avhengigheter og *tillitskjeder*⁷ – i programkode, nettverk, og mellom mennesker, virksomheter og samfunnsfunksjoner. Ett kompromittert nettverk kan dermed utgjøre en strategisk viktig trussel eller sette menneskeliv i fare. I forrige utgivelse løftet Kripos to strategiske varslar: *kjedeangrep*⁸ og *angrep mot OT-systemer*⁹, med bakgrunn i henholdsvis

skaleringspotensialet og de mulig alvorlige konsekvensene for kritiske samfunnsfunksjoner og infrastruktur. Ett angrep fra én aktør kan dermed få konsekvenser for enkeltpersoner, virksomheter og samfunnet som helhet.

Vi lever i et samfunn som preges av kontinuerlig endring, tilpasning og nye trusler. Det digitale rom fasiliteter for nye, transaksjonsbaserte samarbeid mellom ulike trusselaktører og nye markedsplasser der kriminelle varer og tjenester selges som handelsvarer. Cyberkriminelles organisering, begåtte lovbrudd og handlemåter kan dermed endre seg raskt.

5 For eksempel tekst, lyd, bilde, video, programkode.

6 Kripos. (2025). *Cyberkriminalitet 2025*. ss. 35–42. <https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2025.pdf>

7 En tillitskjede er en sekvens av avhengigheter der tillit overføres trinn for trinn, fra en kjent og betrodd kilde til noe man ellers ikke kunne verifisert direkte. Kilde: SSL.com. (2021, 6. desember). *Hva er en sertifiseringsinstans (CA)?*. <https://www.ssl.com/no/faqs/what-is-a-certificate-authority/>

8 Kjedeangrep representerer en mulighet for kriminelle som ønsker å ramme mange fornærmede som følge av sårbarheter i en felles eller sammenkoblet maskinvare eller programvare.

9 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 til å styre andre systemer eller enheter som monitorerer eller endrer fysiske prosesser.



Cyberkriminalitet sett fra politiets ståsted

Mørketall og utfordringer i politiets datagrunnlag

Kripos' informasjonsgrunnlag for cyberkriminalitetsfeltet preges av ulike former for og grader av mørketall innen de forskjellige kriminalitetstypene. Dette utfordrer Kripos' evne til å forstå og beskrive normalbildet. På tross av mørketallsproblematikken har Kripos likevel innsikt i deler av cyberkriminalitetsfeltet, som deles for å bidra til den nasjonale situasjonsforståelsen.

Det er kjent for Kripos at tjenestenektangrep¹⁰ og datainnbrudd som ikke etterfølges av ytterligere ondsinnet aktivitet eller lovbrudd¹¹ preges

av mørketall. Samtidig viste *mørketallsundersøkelsen* fra 2024 at kun 24 prosent av virksomheter som opplevde datainnbrudd og datatyveri anmeldte forholdet til politiet. Kripos legger derfor til grunn at det generelt sett finnes betydelige mørketall for cyberrettet kriminalitet. På tross av mørketall har Kripos, gjennom samarbeid med Nasjonal Sikkerhetsmyndighet (NSM) og aktører i næringslivet, gradvis og over tid bygget et bedre datagrunnlag for cyberrettet kriminalitet.

Ulike former for digitale bedragerier¹² og seksuallovbrudd utgjør de klart største andelene

10 Tjenestenektangrep innebærer at informasjon, ressurser eller tjenester blir helt eller delvis utilgjengelige som følge av et målrettet angrep eller uforutsette hendelser. *Eng: Denial-of-Service (DoS)*. Kilde: Nätt, T. H. & Bartnes, M. (2025, 12. mars). *Tjenestenekt*. Store norske leksikon.

<https://snl.no/tjenestenekt>

11 Tilfeller der datainnbruddet er fullbyrdet, men uten at dette etterfølges av datatyveri eller data-skadeverk (kryptering), enten fordi angrepet ble avverget eller fordi det ble avklart at trussel-aktøren ikke utførte annen ondsinnet aktivitet i systemet.

12 Digitale bedragerier er en samlebetegnelse for en rekke ondsinnede aktiviteter utført via digitale plattformer med hensikt å manipulere, bedra eller stjele fra enkeltpersoner eller virksomheter. Det er bruken av teknologi som skiller digitale bedragerier fra andre typer bedragerier.

av all registrert cyberkriminalitet, mens den cyberrettede kriminaliteten utgjør en mindre andel av registrerte straffbare forhold. Samtidig er det også enkelte cyberstøttede kriminalitetstyper som ikke anmeldes i like stor grad.

Cyberstøttede seksuallovbrudd innbefatter en rekke straffbare handlinger som bidrar til et høyt antall registrerte straffesaker. Samtidig er det et kriminalitetsområde som på bakgrunn av en rekke faktorer også preges av underrapportering. En viktig årsak til mørketall er at seksuallovbrudd ofte anmeldes sent grunnet psykologiske faktorer som skam, skyldfølelse og frykt. I tillegg er det mange som ikke er klar over at de har vært utsatt for noe straffbart, eller forholdet behandles utenfor straffesakssporet grunnet gjerningspersonens unge alder. Det er også særlig mangel på kunnskap om kvinnelige utøvere av kriminaliteten. I tillegg forekommer en form for mørketall i politiets egne registre. Seksuallovbruddskapittelet i straffeloven er teknologinøytralt, det skilles derfor ikke på hva som har skjedd i den

fysiske verdenen og hva som har skjedd på internett. Det er også ulik praksis ved koding av straffesaker når politiet mottar eller registrerer anmeldelser. Derfor kan det være utfordrende å få en fullstendig oversikt over den informasjonen politiet allerede besitter.

Internasjonale utviklingstrekk innen cyberkriminalitet

Globalt har det vært en økning i all cyberkriminalitet. Det eneste unntaket er hactivisme, som har hatt et stabilt høyt nivå de siste årene.^{13,14,15} Hovedårsakene til denne nesten entydige trenden, er den økte tilgjengeligheten av kunstig intelligens (KI) som digitalt verktøy og den tiltagende kommersialiseringen av cyberkriminalitet. Disse to fenomenene har alene gjort alle typer cyberkriminalitet hurtigere og langt mer effektiv, samtidig som de har tilgjengeliggjort digitale verktøy for alle individer som er i det digitale rom.

-
- 13 The European Union Agency for Cybersecurity. (2025, oktober). *Enisa threat landscape 2025*. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
 - 14 Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA): Steal, deal and repeat – How cybercriminals trade and exploit you data*. <https://www.europol.europa.eu/publication-events/main-reports/steal-deal-and-repeat-how-cybercriminals-trade-and-exploit-your-data>
 - 15 United Nations Interregional Crime and Justice Research Institute. (2024, juni). *Beneath the surface: Terrorist and violent extremist use of the dark web and cybercrime-as-a-service – June 2024*. <https://unicri.org/beneath-surface-terrorist-and-violent-extremist-use-dark-web-and-cybercrime-service-june-2024>

Det er likevel nyttig å også se på noen andre *utenlandske* og *internasjonale* utviklingstrekk for å forstå og varsle om en mulig fremtidig utvikling innen cyberkriminalitet i Norge. Utenlandske utviklingstrekk er endringer som enda ikke har truffet norske enkeltpersoner eller virksomheter. Internasjonale utviklingstrekk er endringer som foregår flere steder i verden – inkludert Norge – og som ikke forholder seg til landegrenser. Disse endringene – sett i sammenheng med kapittelet om normalbildet – danner grunnlaget for hva som kan forventes å skje i 2026.

Ved å kartlegge og forstå lokale og globale forhold¹⁶ og utviklinger, samt de kriminelles samhandlingsmekanismer¹⁷, vil politiet være bedre i stand til å forutse nye trusler, bekjempe cyberkriminalitet i stort og utarbeide tiltak som har dyptgående og langvarig effekt.

Kunstig intelligens

KI har automatisert en rekke kriminelle oppgaver, som omgåelse av sikkerhetsfiltre, sammenstilling av store mengder data, skalering, forfalskning, oversettelse og tilpasning av tekst og tale, koding, pentesting og målutvelgelse. KI benyttes til å gjøre de kriminelle handlingene vanskeligere å oppdage, både gjennom å finpusse på programkode og prosesser, men også ved å innføre større variasjon i angrepene, slik at man i mindre grad kan lene seg på gjenkjennbare mønstre i forsvar mot kriminaliteten. I tillegg har den sosiale manipulasjonen i det siste blitt langt mer overbevisende både innen lyd, bilde og video. Den forbedrede kvaliteten medfører en troverdighet som gjør det enklere for aktører å forlede og utnytte mennesker, herunder barn. KI driver fram den kriminelle utviklingen, hjelper uerfarne kriminelle med lavt kompetansenivå, og bidrar til at mengden kriminalitet vokser.

16 Eksempelvis statens kontroll over borgernes bruk av internett, fattigdom, internettdekning, teknologisk grunnkompetanse, historie, kultur m.v.

17 De mekanismer som påvirker hvordan kriminelle jobber sammen.

A man and a robot are seated at a desk in a dark, futuristic environment, likely a control room or data center. The man, on the left, is wearing a dark, tactical-looking jacket and glasses, looking at a computer monitor. The robot, on the right, has a metallic, humanoid form with glowing blue eyes and is also looking at a monitor. Several other monitors are visible in the background, displaying various data and code. The scene is dimly lit, with light coming from the screens and some ambient blue and red lighting in the background. A white text box with a double-slash icon is overlaid on the upper part of the image.

KI driver fram den kriminelle utviklingen, hjelper uerfarne kriminelle med lavt kompetansenivå, og bidrar til at mengden kriminalitet vokser.

I tidligere utgaver av *Cyberkriminalitet* har Kripos omtalt KI-agenter¹⁸ og i den forbindelse vurdert at den store mengdeendringen i cyberrettet kriminalitet først vil skje etter at KI-systemer¹⁹ selvstendig utfører kriminelle handlinger og aktiviteter på vegne av mennesker. Utviklingen innen agentiske systemer²⁰ 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.

Delvurderinger

Det er *sannsynlig* at etterspørselen etter kriminelle med kompetanse innen KI øker i takt med mulighetsrommet for å bruke KI til å utføre cyberrettet kriminalitet. Samtidig som KI og kriminalitet som handelsvare (KSH)²¹ senker barrieren og tekniske kompetansekrav for å utføre cyberangrep, er det *sannsynlig* at kriminelles bruk av KI-modeller vil føre til feilsteg og avsløringer som vil hjelpe politiet å avdekke hvem de kriminelle aktørene er. Det er *sannsynlig* at kriminelle med lav teknisk kompetanse er mest utsatt for å bli avslørt basert på deres bruk av kunstig intelligens.

-
- 18 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.
- 19 KI-system er en samlebetegnelse for ulike 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. Kilde: Kommunal- og moderniseringsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens*. s. 9. Regjeringen. <https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/no/pdfs/ki-strategi.pdf>
- 20 Andre KI-systemer kan også utvise agentiske egenskaper uten nødvendigvis å bli omtalt som KI-agenter. Disse egenskapene inkluderer mål (eng: *objectives*), handlinger (eng: *actions*), minne (eng: *memory*) og refleksjon (eng: *rethink*).
- 21 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)*.

// En omfattende gråsoner er under etablering i den kommersielle delen av det cyberkriminelle økosystemet, der profesjonelle aktører selger kunnskap og verktøy uten å delta i de kriminelle handlingene.

Økt kommersialisering av cyberkriminalitet

Kommersialiseringen av cyberkriminaliteten profesjonaliseres, breddes ut og vokser – både i Norge og i verden ellers.²² Tilbudet av cyberkriminelle produkter og tjenester øker, og man ser særlig utvikling i sammenstilling av pakke-tilbud²³, leie-/abonnementstjenester, rådgivning og kundestøtte. En omfattende gråzone er under etablering i den kommersielle delen av det cyberkriminelle økosystemet, der profesjonelle aktører selger kunnskap og verktøy uten å delta i de kriminelle handlingene. Det cyberkriminelle økosystemet er i større eller mindre grad avhengig av slike tilretteleggere – personer som i kraft av sin tilgang og kompetanse medvirker til kriminalitet eller sørger for at kriminaliteten tilsløres.²⁴

Høsten 2025 ble vold som handelsvare (VSH) et kjent begrep i samtidsdebatten i Norge. Kripos ser at det internasjonalt er tydelige digitale sider ved VSH. Rekruttering, planlegging, koordinering og eventuell betaling skjer oftest digitalt. I tillegg ser vi at doxxing²⁵, trakassering, overvåkning og sabotasje kan eskalere til fysisk skade. Utviklingen følger tidligere kommersialisering av løsepengevirus og phishing som vi allerede har sett i Norge, og det er de samme digitale plattformene som benyttes.

Koalisjonsdannelser og nye samarbeidsstrukturer

I 2025 er det observert at internasjonalt etablerte cyberkriminelle nettverk har gått sammen om å danne større koalisjoner av løsepengevirus-som-handelsvare-operasjoner

22 Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA)*.

23 En pakke kan for eksempel inneholde tilgang til infeksjonsverktøy, infrastruktur for anonymitet og en trygg betalingskanal.

24 Kripos. (2025). *Cyberkriminalitet 2025*. s. 11.

25 *Doxxing/doxing* (eng.) er offentliggjøring av personlig/sensitiv informasjon om et individ eller en organisasjon.

(LSH-operasjoner)^{26, 27} Flere av løsepengevirusvariantene som nå inngår i de nydannede koalisjonene er blitt brukt i angrep på norske virksomheter i løpet av 2025.

At cyberkriminelle trusselaktører erklærer at de slår seg sammen med andre er ikke nytt, men slike samarbeid har tidligere medført endringer i grupperingers handlemønstre. I tilfeller hvor nye samarbeidsstrukturer representerer en betydelig kapasitetsendring er slike nettverk verdt å merke seg.

For en av koalisjonene som er dannet i 2025 og som nå omtaler seg som *Scattered Lapsus\$ Hunters*, rapporteres det blant annet om større bredde i trusselaktørens teknikker for å skaffe seg aksess til virksomheters systemer. Hva dette innebærer til det fulle er noe uklart, men det rapporteres om at grupperingen benytter

voice-phishing²⁸ mot ansatte i virksomheter, for derigjennom å skaffe seg aksess til systemer og data. Kripas er ikke kjent med eksempler der voice-phishing er benyttet i forbindelse med datainnbrudd mot norske virksomheter. Bruken av dette vil representere et avvik fra normalbildet i Norge.

Kriminelle i *Scattered Lapsus\$ Hunters* har i uttalelser til medier hevdet å stå bak flere cyberangrep rettet mot profilerte internasjonale foretak.

26 Løsepengevirus-som-handelsvare (LSH) er en underkategori av kriminalitet som handelsvare (KSH) og innebærer salg eller utleie av et eksisterende løsepengevirus. Eng: *Ransomware-as-a-Service (RaaS)*.

27 Eksempler er *Scattered Spider*, *LAPSUS\$* og *ShinyHunters* som har gått sammen om å danne «*Scattered Lapsus\$ Hunters*». Videre er har *DragonForce* også annonsert på sine lekkasjesider at de har gått sammen med *Qilin* og *LockBit* for å danne en koalisjon. Kilder: Culafi, A. (2025, 8. oktober). *LockBit, Qilin & DragonForce Join Forces in Ransomware «Cartel»*. Dark Reading. <https://www.darkreading.com/cyberattacks-data-breaches/extortion-gangs-join-forces-ransomware-cartel> og Picus Labs. (2025, 20. oktober). *Scattered LAPSUS\$ Hunters: 2025's Most Dangerous Cybercrime Supergroup*. Picus Security. <https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup>

28 Voice-phishing er en type phishing der cyberkriminelle bruker telefonoppringninger (og potensielt taleteknologi) for å manipulere ofre til å avsløre sensitiv informasjon.

Delvurderinger

Det kan være en rekke årsaker til at etablerte cyberkriminelle nettverk går sammen om å danne nye samarbeidsstrukturer. Det er imidlertid *sannsynlig* at økt kapasitet gjennom deling av ressurser, infrastruktur, kompetanse og erfaring bidrar til en betydelig kapasitetsendring, og det er *mulig* at dette er en ønsket effekt for nettverket.

Det er videre *sannsynlig* at sammenslåing av kjente navn innen LSH-økosystemet og deres uttalelser om dette i media også handler om merkevarebygging, og at dette bygger på en oppfatning om at profilerte cyberkriminelle nettverk i større grad opplever som en potent trussel. Det er *mulig* at dette kan øke de fornærmedes vilje til å betale løsepenger.

Det er *mulig* at nyetablerte koalisjoner, slik som Scattered Lapsus\$ Hunters, som et ledd i sin profilering, vil fokusere på å angripe store og symboltunge virksomheter. Det er *mulig* at denne utviklingen også vil berøre norske virksomheter i form av mer målrettede cyberangrep.

Samtidig er det *sannsynlig* at mer samarbeid og midlertidige allianser blant LSH-grupperinger vil føre til flere konfliktlinjer og økt rivalisering blant de kriminelle aktørene. Det er *mulig* at dette vil føre til flere tilfeller av doxxing – interne lekkasjer og kriminelle som offentliggjør informasjon om andre kriminelle.

Dersom rapporteringene om bruk av voice-phishing i forbindelse med data-innbrudd stemmer, er det *sannsynlig* at teknikken også vil bli brukt mot norske virksomheter i 2026 og videre. Det er *meget sannsynlig* at voice-phishing oppfattes som mer troverdig enn andre phishing-metoder, og det er *sannsynlig* at dette vil bidra til at cyberkriminelle i større grad lykkes med å tilegne seg påloggingsdetaljer eller sensitiv informasjon. Det er *mulig* at KI-genererte stemmer vil få samme effekt som bruk av ekte menneskestemmer, avhengig av i hvilken grad disse framstår troverdige.

The Com – ekstreme, voldelige nettsamfunn

Europol publiserte i februar 2025 en rapport²⁹ som advarte om ekstreme, voldelige nettsamfunn, også kalt kulter, hvor det framgikk at det er registrert en global økning både i omfang og utbredelse. Dette ble bekreftet av National Center for Missing and Exploited Children (NCMEC), som uttalte at de i 2022 mottok under 100 tips om fenomenet, mot 200 i 2023, 1300 i 2024 og over 1000 tips i første halvdel av 2025. Fenomenet bringer med seg en ny undergruppe uklassifiserte aktører med ulik motivasjon som utgjør en ny trussel mot barn på internett. Les mer om forekomst av fenomenet i Norge på side 46–48.

Internasjonale geopolitiske spenninger

Ettersom cyberkriminalitet er en global trussel med ulike lokale nedslagsfelt er det viktig å se utover nasjonale grenser for å danne et bilde av hva som kan treffe norske enkeltpersoner, virksomheter og det norske samfunnet. Dette delkapittelet omhandler utelukkende geopolitiske spenninger som ikke enda er observert i Norge, men som trolig direkte eller indirekte kan påvirke cyberkriminalitet i Norge.

Fysiske kriger og regionale væpnede konflikter har de senere årene tydeliggjort cyberdomenets rolle som del av moderne krigføring. Særlig i krigen mellom Russland og Ukraina foregår det rask utvikling av ny teknologi. Erfaringer og

Ekstreme, voldelige nettsamfunn eller «kulter» har vokst fram som et globalt fenomen. De ulike nettsamfunnene har sitt utspring i *The Com* – kort for *The Community* – som er det overordnede internasjonale nettverket. Aktørene har ingen klar motivasjon, men det beskrives overlapping mellom blant annet nihilisme, okkultisme, ekstremisme og seksuelle overgrep

mot barn. Noen av nettsamfunnene har koblinger til høyreekstreme miljøer som hyller terror og vold for å «ødelegge samfunnet». Miljøene sprer ekstremt voldelig innhold, utnytter sårbare barn og unge og forsøker å radikalisere dem til å begå svært alvorlige handlinger mot både seg selv og andre. Internasjonalt er flere av gruppene definert som terrororganisasjoner.

29 Europol. (2025). *The rise of online cult communities dedicated to extremely violent child abuse*. https://www.europol.europa.eu/cms/sites/default/files/documents/IN_The_rise_of_online_cult_communities_dedicated_to_extremely_violent_child_abuse.pdf



Global økonomisk ustabilitet,
handelspolitiske spenninger
og sanksjonsregimer påvirker
i økende grad det digitale
trusselbildet.

anvendte verktøy fra slike konflikter kan spres raskt og senere tas i bruk av aktører med helt andre motiver. På denne måten kan hendelser i én del av verden ha betydning for den samlede mengden av tilgjengelig kunnskap, kapasitet og trusselaktiviteter, også utenfor de fysisk-geografiske konfliktområdene.

Global økonomisk ustabilitet, handelspolitiske spenninger og sanksjonsregimer påvirker i økende grad det digitale trusselbildet. Handelskriger, som mellom USA og Kina, bidrar til høyere kostnader, forsyningsutfordringer og endringer i markedet for digitale tjenester og sikkerhetsløsninger. Dette kan gjøre det vanskeligere for virksomheter å opprettholde nødvendig cybersikkerhet og skaper samtidig nye muligheter for kriminelle som tilbyr rimeligere, men usikre, alternativer.

Parallelt pågår et globalt teknologikappløp der spesielt stormakter konkurrerer om dominans innen områder som avansert infrastruktur, kvantedatabehandling og kunstig intelligens. Konkurransen fremmer innovasjon, men bidrar også til fragmentering i digitale systemer og økt kompleksitet. Denne utviklingen skaper flere inngangspunkter som raskt kan utnyttes av både statlige³⁰ og private aktører til kriminelle formål. Samtidig kan innovasjonsprosessen innebære hyppigere eksperimentering rundt

metoder og verktøy som raskt spres på tvers av aktørtyper og landegrenser.

Samlet sett bidrar geopolitiske spenninger til et mer uforutsigbart cybertrusselbilde. Utenlandske forhold påvirker både volum, karakter og kompleksitet i cyberkriminalitet. Den følger ikke nasjonale grenser, og konsekvensene av internasjonale konflikter, økonomiske svingninger og teknologisk rivalisering kan dermed også merkes i Norge.

Delvurderinger

Det er *mulig* at teknologien som i dag utvikles til bruk i hybrid krigføring vil bli brukt til å begå kriminelle handlinger mot norske mål i 2026.

Det er *mulig* at økonomisk press og sanksjoner også kan øke insentivene til profittmotivert cyberkriminalitet, både blant enkeltpersoner, grupper og statlige aktører.

³⁰ Statlig aktør betegner nasjonalstater som utgjør en trussel eller som begår cyberkriminalitet.

Seksuell utpressing med økonomisk motiv

I andre land er det sett indikasjoner på at gjerningspersoner som begår seksuell utpressing med økonomisk motiv også deler eller selger materialet videre som overgrepsmateriale, trolig for ytterligere økonomisk vinning. Dette har vi hittil ikke registrert i Norge, men var omtalt i *Cyberkriminalitet 2023*³¹ som en mulig framtidig utvikling.

Målutvelgelse

Den cyberkriminelle målutvelgelsen er i en rivende utvikling, med flere klare og identifiserbare trender.

Stadig flere forskjellige typer virksomheter utsettes for cyberangrep. Det er en tydelig trend mot å først skaffe seg personalia, for

deretter å bruke denne for legitim tilgang inn i systemer. Videre er det i økende grad observert at de kriminelle angriper i flere kanaler samtidig.^{32, 33, 34} Dette innebærer at angriperen bruker flere angrepsvektorer mot målet, både i det fysiske og digitale domenet, for eksempel e-post, SoMe, nettsteder, telefonoppringing, fysiske adgangskort og personlig oppmøte. De kriminelle utnytter at målene navigerer mellom ulike kanaler og øker på denne måten sjansen for å lykkes med angrepet. Kripas ser også at cyberkriminelle trekker mot land med lav lovhåndhevelse for å utøve kriminaliteten der.^{35,36}

31 Kripas. (2023). *Cyberkriminalitet 2023*. s. 19. <https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf>

32 Eng: *Omnichannel Attack* eller *Multi-Channel Attack*.

33 Telenor. (2025, oktober). *Digital sikkerhet 2025: Vi må ruste oss*. s. 28. https://www.telenor.no/binaries/om/digital-sikkerhet/2025/sikkerhetsrapport_tjuefem.pdf

34 Sopra Steria. (2025). *State of cyber security 2025*, ss. 11, 13, 19. <https://www.soprasteria.no/docs/librariesprovider2/sopra-steria-no-documents/rapporter/sopra-steria-state-of-cyber-security-2025.pdf>

35 Interpol. (2025, 23. juni). *New INTERPOL report warns of sharp rise in cybercrime in Africa*. <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa>

36 Ecofin Agency. (2025, 30 september). *Cybercrime Costs Africa \$3B as Interpol Flags Legal, Cooperation Gaps*. <https://www.ecofinagency.com/news/3009-49122-cybercrime-costs-africa-3b-as-interpol-flags-legal-cooperation-gaps>



Det er en tydelig trend mot å først skaffe seg personalia, for deretter å bruke denne for legitim tilgang inn i systemer.

Det har i senere tid vært økende cyberkriminal oppmerksomhet mot OT-/IT-virksomheter.³⁷ Slike systemer kan rammes både tilsiktet og utilsiktet, og i enkelte tilfeller uten særskilte tekniske ferdigheter. Som omtalt i *Cyberkriminalitet 2025*³⁸ så fordrer imidlertid et destruktivt angrep³⁹ på OT-/IT-systemer at trusselaktøren tar i bruk avanserte teknikker. Et vellykket angrep kan gi så god avkastning at det er verdt en betydelig økt innsats. Et eksempel på et nylig vellykket angrep var angrepet rettet mot Jaguar Land Rover, som medførte over fem uker nedstenging og et tap foreløpig estimert til over 25 milliarder norske kroner.⁴⁰

Dette kan sammenfalle med en annen internasjonal trend, hvor mer avanserte kriminelle går bort fra mengdeangrep og over til en mer målrettet prosess der man bruker data, gjerne fra tidligere datatyverier, til å finne de best

egnete ofre⁴¹. Angrepet mot Collings Aerospace, som resulterte i blant annet nedstenging av automatiske innsjekk- og bagasjeleverings-systemer og store forsinkelser på flyplasser i London, Berlin og Brussel, er et godt eksempel på hvordan en tredjepartsleverandør⁴² kan være inngangsport til kritisk infrastruktur. En økt innsats fra cyberkriminelle mot OT-/IT-systemer kan være en del av det større bildet.

Denne siste trenden peker i retning av at den største mengden cyberkriminalitet utføres av nye, uerfarne og mindre kompetente aktører som støttes av KI og kommersielt tilgjengelig dataverktøy, mens den mer avanserte kriminaliteten utføres av et mindre antall individer med lengre erfaring og svært høy kompetanse.

37 The European Union Agency for Cybersecurity. (2025, oktober). *Enisa threat landscape 2025*, s. 9.

38 Kripos. (2025). *Cyberkriminalitet 2025*. ss. 55–59.

39 Se definisjon på destruktive angrep på side 43–44.

40 Jaguar Land Rover. (2025, 19. September). *Letter from Jaguar Land Rover relating to the cyber attack on the company*. <https://api.parliament.uk/committees/publications/49616>

41 Best egnede ofre vurderes å være nøkkelpersoner, tredjepartsleverandører med tilgang eller beslutningstakere i forsyningskjeden.

42 En tredjepartsleverandør er en bedrift eller organisasjon som gjennomfører logistikkjenester som importering, lagring og levering av produkter eller tjenester på vegne av andre.



Den største mengden cyberkriminalitet utføres av nye, uerfarne og mindre kompetente aktører som støttes av KI og kommersielt tilgjengelig dataverktøy, mens den mer avanserte kriminaliteten utføres av et mindre antall individer med lengre erfaring og svært høy kompetanse.



Den cyberkriminelle trusselen består av et mangfold av digitale angrepsformer og kriminelle som utnytter teknologiske sårbarheter, systemtilganger og manipulerer mennesker.

Delvurderinger

Det er *mulig* at virksomheter som rammes av cyberangrep i 2026 vil oppleve å bli angrepet i flere kanaler samtidig. Dersom virksomheter rammes av cyberangrep i flere kanaler samtidig er det *sannsynlig* at flere cyberkriminelle eller cyberkriminelle grupper står bak grunnet økt spesialisering blant cyberkriminelle.

Det er en trend at offentlige virksomheter foretrekkes som mål av cyberkriminelle. Det er *sannsynlig* at dette skyldes offentlig sektors bruk av arvede systemer⁴³, begrensede ressurser og mindre teknologisk kompetanse, samtidig som de forvalter en teknologisk kompleksitet som gjør dem digitalt sårbare.

Normalbildet for cyberkriminalitet i Norge

I dette kapittelet skisserer Kripos *normalbildet for cyberkriminalitet* sett fra politiets ståsted. Med normalbildet menes en beskrivelse av

cyberkriminaliteten med vekt på nåsituasjonen, inkludert trender som har vedvart over flere år. Beskrivelsen av normalbildet for cyberkriminalitet i Norge er ikke en nøyaktig gjengivelse av virkeligheten, men snarere en framstilling av typiske trekk ved ulike kriminalitetsformer som utgjør deler av denne virkeligheten.

Normalbildet vil fungere som en referansesamme for å kunne identifisere avvik og utvikling i kriminaliteten. Dette vil begrense risikoen for ubehagelige overraskelser og gjøre oss bedre forberedt på og rustet til å håndtere framtidens utfordringer.

Den cyberkriminelle trusselen består av et mangfold av digitale angrepsformer og kriminelle som utnytter teknologiske sårbarheter, systemtilganger og manipulerer mennesker. Cyberkriminalitet i Norge domineres fremdeles av profittmotiverte kriminelle, seksuallovbrytere og hacktivist⁴⁴. De kriminelle er tilpasningsdyktige, og trusselen de utgjør er dynamisk og preges av kontinuerlig utvikling i takt med digitaliseringen av samfunnet og framveksten av nye teknologier. Den omfatter både enkle og komplekse modi, og spenner fra automatiserte masseangrep til målrettede og sofistikerte operasjoner.

43 Arvede systemer er gamle og ofte utdaterte systemer som er sårbare for utnyttelse, fordi de ble utviklet i en annen tid under andre sikkerhetsforhold. Eng: *Legacy Systems*.

44 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.

Hacktivisme er politisk eller ideologisk motivert, ulovlig digital aktivisme som har til hensikt å oppnå sosial effekt, utfordre etablerte maktstrukturer, påvirke opinionen, svekke motstanderes troverdighet eller fremme en bestemt sak eller identitet.

Normalbildet for cyberstøttede seksuallovbrudd i Norge

Seksuallovbrudd har alltid eksistert og utgjør en vedvarende trussel mot barn og unge, men den teknologiske utviklingen har endret kriminalitetsbildet betydelig. Gjerningspersoner benytter i økende grad digitale plattformer for å etablere kontakt, gjennomføre og dokumentere overgrep, samtidig som teknologien gir nye muligheter for anonymisering og unndragelse av straffeforfølgning. Internett har ikke bare muliggjort at tradisjonelle overgrep nå også skjer digitalt, men har i tillegg skapt nye former for seksuallovbrudd som er avhengig av internett for å begås. Dette bidrar til et mer komplekst og nyansert normalbilde, og stiller skjerpede krav til politi og øvrige samfunnsaktører når det gjelder forebygging, avdekking og håndtering av seksuallovbrudd.

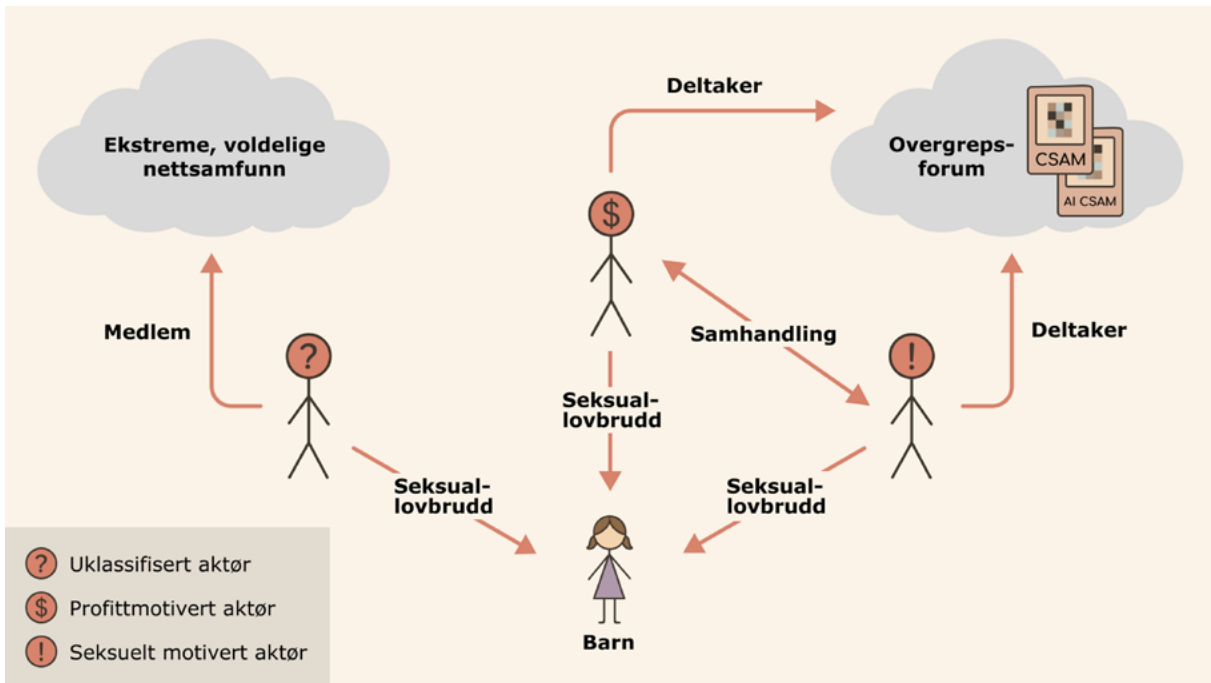
Kripos prioriterer i sitt arbeid seksuallovbrudd begått mot barn. Mange cyberstøttede seksuallovbrudd rammer barn direkte ved at de blir kontaktet av seksuallovbrytere på internett og utsatt for overgrep. Kontaktetableringen og den påfølgende seksuelle utnyttelsen skjer i all hovedsak på ordinære sosiale medier, men kontakt etableres også på chatroulette- og spillplattformer. Hvert år blir i tillegg barn seksuelt utnyttet på ende-til-ende-krypterte kommunikasjonsplattformer. Videre inngår det i normalbildet at norske aktører kjøper egenprodusert seksualisert materiale av norske barn. Kripos rapporterte i fjor om en eskalering på området, og varslet om at mange av aktørene tidligere er omhandlet med seksuallovbrudd mot barn – noen med svært alvorlig straffehistorikk innen vold og seksuallovbrudd.⁴⁵

Seksuallovbruddene som begås over internett er alt fra seksuelt krenkende atferd til voldtekt. Mange av tilfellene ender med seksualisert chat og digital blotting, samt at aktøren får barnet til å sende nakenbilder og -videoer, også mot betaling. I mange tilfeller er det ikke kjent hvor langt gjerningspersonen hadde vært villig til å gå hvis ikke kontakten av en eller annen grunn hadde blitt avbrutt. Dersom barnet gjør seksuelle handlinger med seg selv på bilde, video eller direkteoverført videochat, kan lov-

⁴⁵ Kripos. (2025). *Cyberkriminalitet 2025*. s. 84.

A close-up, low-angle shot of a person lying in bed, illuminated by the soft glow of a smartphone screen. The person's face is partially visible in profile, looking down at the device. The background is dark, suggesting a nighttime setting. The overall mood is quiet and focused on digital interaction.

Gjerningspersoner benytter i økende grad digitale plattformer for å etablere kontakt, gjennomføre og dokumentere overgrep, samtidig som teknologien gir nye muligheter for anonymisering og unndragelse av straffeforfølgning.



Figur 2: Økosystemet for cyberstøttede seksuallovbrudd. Nederst i midten av modellen er et barn, omgitt av seksuelt motiverte, økonomisk motiverte og uklassifiserte aktører (kultmedlemmer) som utsetter barnet for ulike former for seksuallovbrudd og samhandler med andre aktører – både med lik og ulik motivasjon. CSAM⁴⁶ er overgrepsmateriale av barn, og AI CSAM er syntetisk overgrepsmateriale generert ved hjelp av KI. Modellen er utviklet av Kripas.

bruddet kategoriseres som seksuell handling, seksuell omgang eller voldtekt.

Flere tilfeller resulterer i at gjerningspersonen utsetter offeret for seksuell utpressing. Utpressingen kan resultere i forskjellige lov-

brudd, og lovbruddene begås med ulike motiv. Her er en vanlig handlemåte at gjerningspersonen forleder barnet til å dele et nakenbilde av seg selv, før vedkommende bruker bildet som pressmiddel for å oppnå en ønsket slutttil-

46 Eng: *Child Sexual Abuse Material*.

stand, som å motta flere seksualiserte bilder og videoer. Også bruk av syntetisk genererte bilder er registrert. Tidligere har seksuell utpressing med økonomisk motiv vært en kriminalitetsform rettet mot voksne menn med betalingsevne. De siste fem årene har det blitt vanlig at noen av ofrene er mindreårige gutter, og det inngår nå i hva Kripos anser som normalbildet.

Norske gjerningspersoner produserer, oppbevarer, deler, kjøper og selger overgrepsmateriale. Produksjon skjer ved dokumentasjon (bilder og video) av fysiske og digitale overgrep. Deling eller handel foregår på både det åpne og det mørke nettet, på fildelingsnettverk og filutvekslingstjenester, sosiale medier og ende-til-ende-krypterte kommunikasjonsplattformer. Vanligst er bytting og deling uten vederlag, men av dem som kjøper overgrepsmateriale brukes både kryptovaluta og en rekke ulike betalings tjenester, blant annet betalingsformidlingstjenester⁴⁷. Norske aktører produserer, skaffer seg og deler i tillegg syntetisk generert overgrepsmateriale.

Direkteoverførte bestillingsovergrep (DOBO) begås av mellom hundre- og tusentalls norske gjerningspersoner hvert år. Ofrene for kriminaliteten er hovedsakelig barn i risikoland, primært jenter rammes og de er oftest bosatt på Filippi-

nene. Kontakten etableres gjerne på pornonettsider som tilbyr direkteoverført seksuelt innhold av voksne, hvor gjerningspersonene blir tilbudt å kjøpe direkteoverførte overgrep mot barn. Mange DOBO-kjøpere oppsøker nettsidene aktivt med hensikt om å kjøpe DOBO, men noen tilfeller framstår opportunistiske ved at gjerningspersonene benytter seg av tilbudet om å kjøpe DOBO når de får det, og selgerne er pågående overfor potensielle kunder. Det er vanlig at DOBO gjennomføres på ordinære, kommersielle plattformer som tilbyr videochat og filutveksling. DOBO kjøpes som regel ved bruk av alminnelige betalingsløsninger, og anses som en lite avansert kriminalitetstype. Det forekommer imidlertid at enkelte aktører betaler for DOBO med kryptovaluta.

Seksuallovbrudd som forsterkes av eller begås i det digitale rom rammer norske borgere i alle aldre, men særlig barn i alderen 13–15 år⁴⁸ er utsatt for seksuell utnyttelse. Jenter er overrepresentert i statistikken, men også gutter rammes. Eksempelvis er det flere gutter enn jenter som utsettes for seksuell utpressing med økonomisk motiv.

Sårbarhetene som muliggjør overgrepene er mange og sammensatte. Offergruppen – barna – har som følge av sin unge alder manglende

47 Betalingsformidlingstjenester er tjenester som formidler betalingen mellom to parter og fungerer som et mellomledd. Eksempler på slike tjenester er Vipps og Paypal.

48 Gjennomsnittsalder for barn utsatt for cyberstøttede seksuelle overgrep er 14 år, mens gjennomsnittsalder for seksuallovbrudd mot barn i stort er 12 år.

konsekvenstenkning og forståelse av hvilke farer som truer, særlig på internett. Digitale plattformer fungerer som en dør mellom barnerommet og resten av verden. Det er lettere å forlede barn på internett, skjule seg bak falske identiteter og lyve på alder og kjønn, for å nevne noe. Foreldre og andre voksenpersoner rundt barnet har ikke alltid tilstrekkelig kunnskap om tiltak for å beskytte barnet og forebygge overgrep, noe gjerningspersoner aktivt utnytter. Plattformer som virker innbydende for barn, som tilbyr spill, musikk, lek og samhandling med venner, legger til rette for kontakt med fremmede, og overgripere oppsøker arenaer hvor barn ferdes – på nett som i den fysiske verden.

Cyberstøttede seksuallovbrudd rammer enkeltindivider hardt. Hvert barn som utsettes blir ikke bare offer for en kriminell handling, men må potensielt også leve med omfattende og langvarige konsekvenser. Det samlede omfanget av enkeltstående skjebner utgjør et omfattende samfunnsproblem. I tillegg medfører disse lovbruddene betydelige samfunnsøkonomiske kostnader, blant annet knyttet til barns skolegang og utdanning, framtidig deltakelse i arbeidslivet, helseutfordringer og vansker med å etablere og opprettholde relasjoner.

Normalbildet for cyberrettet kriminalitet i Norge

Cyberrettet kriminalitet er en vedvarende trussel mot norske offentlige og private virksomheter og mot enkeltpersoner. Ulike kombinasjoner av datainnbrudd, datatyveri, utpressing og dataskadeverk utgjør fortsatt de primære handlemåtene for profittmotiverte kriminelle som begår cyberrettet kriminalitet. I tilfeller der kriminalitetsformen rammer enkeltpersoner begås datainnbruddet mot private epost-kontoer, brukere i sosiale medier og skylagringstjenester.

Det er en del av normalbildet at ulike løsepengevirusvarianter blir brukt i cyberangrep mot norske virksomheter. De ulike typene løsepengevirus varierer og endrer seg med tiden, som følge av at nye varianter dukker opp, mens andre forsvinner eller gjenoppstår under nye navn.⁴⁹ Framgangsmåten til kriminelle som benytter løsepengevirus har vært relativt stabil over flere år, og inkluderer datatyveri, kryptering av virksomhetens systemer eller en kombinasjon av begge deler. Dette benyttes videre som grunnlag for utpressing.

Det er vanlig at datatyveri skjer i forbindelse med datainnbrudd mot både virksomheter og enkeltpersoner. Kripos har sett eksempler på at informasjon stjålet fra virksomheter er blitt tilgjengeliggjort i ulike fora og på forskjellige

49 Disse løsepengevirusene brukes ofte av kriminelle som får tilgang til dette gjennom en LSH-forretningsmodell.

plattformer på internett. Forekomsten av dette har imidlertid vært uregelmessig. Det er vanlig at trusselaktører truer med å publisere data, men det er vel så vanlig at dette ikke blir gjennomført. Om og hvordan dataen som stjeles fra virksomheter og privatpersoner kan bli benyttet til videre kriminalitet er usikkert, men det utgjør likevel en vedvarende trussel mot både privatpersoner og virksomheter.

Tjenestenektangrep er fortsatt den mest utbredte angrepsformen som benyttes av hacktivistene. Angrepene er ofte ideologisk motivert og har til hensikt å skape uro, påvirke opinionen og svekke tilliten til norske institusjoner. Disse angrepene kjennetegnes ved stor spredning, høy frekvens og lav teknisk terskel for utøvelse. Tjenestenektangrep får sjeldent store konsekvenser for virksomheter, utover midlertidige avbrudd i tjenester og mindre forstyrrelser. Til tross for dette kan gjentatte kampanjer medføre betydelig driftsbelastning, økte beredskaps-

kostnader og omdømmetap.

Digitale bedragerier utføres på ulike måter og kriminalitetsformen kan tangere både cyberrettet og cyberstøttet kriminalitet, avhengig av hvordan den utføres. Samtidig er digitale bedragerier en kriminalitetsform som typisk rettes mot både virksomheter og privatpersoner og som derfor rammer svært bredt i det norske samfunnet. Digitale bedragerier utgjør fortsatt et mengdeproblem og de økonomiske tapene som denne kriminalitetstypen genererer er betydelige.⁵⁰

Kripos har observert at forsøk på å begå datainnbrudd mot norske virksomheter i hovedsak lykkes fordi virksomhetene har svake eller fraværende sikkerhetstiltak. I denne forbindelse er innlogging⁵¹ i virksomheters systemer eller utnyttelse av ulike sårbarheter de mest brukte metodene for å skaffe seg innledende aksess. Det er mindre vanlig at Kripos ser eksempler på at trusselaktører har skaffet seg

50 I 2024 anslo Økokrim at det kriminelle utbyttet for digitale bedragerier var på over to milliarder kroner. Kilde: Justis- og beredskapsdepartementet. (2024, 18. november). *Økt innsats i kampen mot svindel på nett*. Regjeringen. <https://www.regjeringen.no/no/aktuelt/okt-innsats-i-kampen-mot-svindelpa-nett/id3117017/>

51 De vanligste observerte teknikkene for innlogging er bruk av legitime påloggingsdetaljer som er stjålet eller på annen måte fravendt en person med systemtilgang, gjennom sosiale manipuleringsmetoder eller ved bruk av informasjonsstjeler (eng: *Infostealer*). Innlogging kan også gjøres ved bruk av passordgjetting (eng: *Brute-Force*) rettet mot brukere med svake passord og/eller manglende flerfaktoraутентisering.



* * * * *

Kripos har observert at forsøk på
å begå datainnbrudd mot norske
virksomheter i hovedsak lykkes
fordi virksomhetene har svake
eller fraværende sikkerhetstiltak.



tilgang ved hjelp av bakdører⁵² eller innsidere⁵³, selv om dette også forekommer med ujevne mellomrom.

Svake eller fraværende sikkerhetstiltak kan inkludere svake passord, manglende flerkfaktor-autentisering, uregelmessige systemoppdateringer eller sårbar infrastruktur som er eksponert mot internett. Fravær av sikkerhetskultur kan føre til at slike sårbarheter ikke avdekkes og/eller utbedres (feilrettes), som igjen stiller virksomheten sårbar for cyberangrep.

Cyberrettet kriminalitet har ulikt skadepotensial avhengig av angrepets form, hvem det rettes mot og hva slags verdier⁵⁴ som blir berørt. Sett fra et myndighetsperspektiv er cyberrettet kriminalitet begått mot kritisk infrastruktur og samfunnskritiske funksjoner en alvorlig og vedvarende trussel. Nedetid og avbrudd i kritiske tjenester, samt ondsinnet påvirkning på OT-systemer, kan gjøre utslag i den fysiske verden og skape fare for liv og helse. Cyberangrep som kun har til hensikt å ødelegge eller sabotere for virksomheters drift omtales gjerne som *destruktive cyberangrep*. Denne typen angrep utføres typisk ved bruk av skadevaretyper som permanent sletter eller ødelegger data – ofte omtalt som *wiper-skadevare*⁵⁵, og har naturligvis et

-
- 52 Bakdør brukes om en vei inn i et system som er åpnet av uvedkommende eller som følge av feil, og som ikke er kjent av systemets eier. Gjennom en slik bakdør kan noen for eksempel få tilgang til å lese, endre eller slette informasjon. Kilde: Nätt, T. H. (2024, 15. januar). *Bakdør*. Store norske leksikon. <https://snl.no/bakd%C3%B8r>
- 53 En innsider forstås som en nåværende eller tidligere ansatt, konsulent eller kontraktør som har eller har hatt legitim tilgang til virksomhetens systemer, prosedyrer, objekter og informasjon, og som misbruker denne kunnskapen og tilgangen for å utføre handlinger som påfører virksomheten skade eller tap. Kilde: NSM. (2023). *Temarapport: Innsiderisiko*. s. 9. <https://nsm.no/getfile.php/133153-1591706148/NSM/Filer/Dokumenter/Rapporter/Temarapport%20innsidere.pdf>
- 54 En virksomhets verdier kan være av materiell eller ikke-materiell art, eksempelvis konkrete fysiske gjenstander som virksomheten er avhengig av for å kunne utføre sin funksjon eller informasjon som virksomheten besitter. Kilde: NSM. (2020). *Grunnprinsipper for sikkerhetsstyring*. <https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/identifisere-og-kartlegge/identifisere-verdiene/>
- 55 Eng: *Wiper Malware*.

stort skadepotensiale. Det er imidlertid uvanlig at man ser bruk av slike skadevaretyper utenfor krigs- og konfliktsituasjoner og Kripos er ikke kjent med eksempler på at norske virksomheter er blitt rammet av destruktive cyberangrep. Cyberangrep med bruk av løsepengevirus kan ha svært ødeleggende effekter for virksomheter som rammes av dette, men er ikke det samme som destruktive cyberangrep. Mens destruktive cyberangrep normalt benyttes for sabotasje, brukes kryptering for å skaffe et pressmiddel i en økonomisk motivert utpressingssituasjon.

Cyberrettet kriminalitet som rammer enkeltpersoner får konsekvenser som for den enkelte oppleves som alvorlige. At personlig og sensitiv informasjon⁵⁶ kommer på avveie er blant de vanligste konsekvensene i tilfeller der cyberrettet kriminalitet rammer enkeltpersoner.

Covid-pandemien medførte økt integrasjon mellom privatliv og arbeidsliv som følge av at arbeidsstedet forflyttet seg utover virksomhetens tradisjonelle rammer og beskyttelsestiltak. Dette har skapt en utvidet angrepsflate der privatpersoner i større grad kan utnyttes av kriminelle aktører for å få tilgang til virksomhetssystemer.⁵⁷ Som følge av denne integrasjonen må en trussel mot enkeltpersoner også ses som en trussel mot virksomheter.

56 For enkeltpersoner kan personlig og sensitiv informasjon eksempelvis inkludere helseopplysninger, private bilder og dokumenter.

57 Kripos. (2024). *Cyberkriminalitet 2024*. s. 52. <https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2024.pdf>

Delvurderinger

Kripos legger til grunn at stjålet informasjon fortsatt vil benyttes i cyberrettet utpressing i 2026 og videre. Summen av stjålet informasjon som tilgjengeliggjøres på internett utgjør *meget sannsynlig* en kumulativ trussel. Kripos er kjent med at cyberkriminelle i dag besitter store mengder sensitiv informasjon som stammer fra datatyverier, en mengde som gradvis blir større.

De kriminelle har så langt ikke vært i stand til å bearbeide eller utnytte all data i særlig grad. Det er imidlertid *sannsynlig* at KI-systemer introduserer nye muligheter for utnyttelse av dataen til kriminelle formål. Dersom cyberkriminelle gjennom bruk av KI-systemer evner å benytte denne dataen til kriminalitet, er det *meget sannsynlig* at store datamengder vil få ny verdi for kriminelle.

Det ble i fjorårets rapport vurdert som *sannsynlig* at cyberkriminelles påvirkning på fysiske prosesser vil føre til produksjonsstans og store økonomiske kostnader for norske OT-avhengige virksomheter i 2025. Denne vurderingen inntraff i året som gikk og er stadig like aktuell. Det vurderes derfor som sannsynlig at slik påvirkning kan ramme norske OT-avhengige virksomheter i 2026. Det er stadig også *sannsynlig* at vellykkede cyberangrep mot OT-avhengige virksomheter vil føre til følgekonskvenser i forsyningskjeden, og derigjennom *mulig* forstyrre fysiske prosesser tilknyttet kritisk infrastruktur eller samfunnskritiske funksjoner.

Nasjonale utviklingstrekk

Cyberstøttede seksuallovbrudd

I 2025 har politiet registrert 3212 straffesaker som omhandler seksuallovbrudd mot barn.⁵⁸ Det er en nedgang fra 2024, hvor antall saker var 3395. 36 prosent av sakene – omtrent en tredjedel – er anmeldt mer enn et år etter at det straffbare forholdet skal ha skjedd. Kapittelet i straffeloven som omfatter de ulike formene for seksuallovbrudd er teknologinøytralt, det framgår derfor ikke av statistikken hvor stor andel av lovbruddene som er cyberstøttede. Et anslått omfang av cyberstøttede seksuallovbrudd baserer seg av den grunn på registrert modus operandi, og fordrer at denne er manuelt knyttet til den enkelte sak. Det er i underkant av 1900 seksuallovbruddssaker som er tilknyttet en digital modus operandi i 2025. Disse kan antas å være cyberstøttede.

I tillegg har Kripas i 2025 mottatt og videreformidlet 3001 tips fra NCMEC til politidistriktene, hvor samtlige tips omhandler seksuell utnyttelse av barn på internett. Dette viser at antallet anmeldte saker tilknyttet en digital modus operandi ikke gir et riktig bilde på omfanget av cyberstøttede seksuallovbrudd.

Årsaken til at ikke alle tipsene framgår av anmeldelsesstatistikken kan være at de ikke har høy prioritet i distriktets samlede saksportefølje og av den grunn får en forsinket saksbehandlingstid, at det ikke opprettes straffesak eller at de behandles utenfor straffesakssporet. Denne mulige forklaringen har direkte sammenheng med politidistriktenes ressursssituasjon.⁵⁹ Saker som typisk gis lav prioritet er saker kodet på straffelovens § 311 – fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn (311-saker). Det finnes en rekke eksempler på at etterforskning av tilsynelatende enkle 311-saker har avdekket svært alvorlige overgrep, og understreker hvilke konsekvenser manglende ressurser kan få. For mer om årsaker til mørketall som har relevans for registrerte cyberstøttede seksuallovbrudd, se side 19.

I 2025 er det registrert 1479 anmeldte 311-saker, hvorav majoriteten av dem er tilknyttet en digital modus operandi. For 2024 var tallet tilnærmet det samme med 1530 registrerte straffesaker. Når det gjelder syntetisk overgrepsmateriale har Kripas mottatt 90⁶⁰ tips i 2025 om nordmenn som har hatt befatning med syntetisk overgrepsmateriale, mot totalt

58 2780 barn var fornærmet i straffesakene. De var alle mellom 0 og 17 år på gjerningstidspunktet.

59 Politidistriktene har i mange år rapportert om at altfor få ansatte er satt til å håndtere et overveldende antall seksuallovbruddssaker. Dersom et lite distrikt behandler flere omfangsrike, komplekse saker, vil dette gå på bekostning av distriktets evne til å håndtere den øvrige saksmengden.

60 Tipsene ble sendt fra Open AI og X.AI (Grok).

15⁶¹ i 2024. Globalt er det også registrert en betydelig økning. I første kvartal av 2025 mottok NCMEC 33.100 varslinger om syntetisk materiale, sammenlignet med 67.000 i hele 2024 og 4700 i hele 2023. I 2025 er det også registrert en endring i produksjon av syntetisk overgrepsmateriale. Flere aktører som tidligere har produsert syntetiske overgrepsbilder av høy kvalitet har nå dreid sin virksomhet over til produksjon av syntetiske overgrepsvideoer. Dette har medført at kvaliteten på bildene har stagnert eller dalt, all den tid andre aktører med mindre erfaring eller kompetanse nå produserer materialet.

I 2025 har det vært en økt rapportering i Norge om saker som har indikasjoner på eller knytninger til *ekstreme, voldelige nettsamfunn*. Det første kjente tilfellet i Norge ble registrert i 2022, og forekomsten har fram til 2025 vært stabil. Sakene med norske aktører og ofre har kommet inn som tips via NCMEC og politiets øvrige kanaler, samt fra politietterforskninger i utlandet. NCMEC-varslingene har ofte blitt avdekket ved at det er begått et seksuallovbrudd mot et barn. Seksuallovbruddene kan ved første øyekast se ut som nettopp det, men viser ofte ikke det fulle og hele bildet, som avdekkes gjennom videre etterforskning.

Gjerningspersonene er ikke nødvendigvis seksuelt motiverte – i flere tilfeller er eksempelvis seksuell utpressing kun et middel for å oppnå kontroll over offeret og tvinge vedkommende til å begå andre alvorlige handlinger.

Det var per september 2025 registrert et tosifret antall straffesaker nasjonalt med indikasjoner på kultfenomenet. Det er identifisert både norske, mindreårige gjerningspersoner og norske, mindreårige fornærmede. De fornærmede som rekrutteres eller presses inn i gruppene er ofte sårbare unge og hovedsakelig jenter. Nasjonalt observeres det at plattformene som brukes til både den innledende kontakten og til videre kommunikasjon er sosiale medier, spillplattformer og ende-til-ende-krypterte meldingsplattformer. Det er også observert kontaktetablering i åpne støttegrupper for psykisk helse.

Kripas gikk i september 2025 ut med en pressemelding om kultfenomenet og publiserte informasjon på politiet.no⁶² og i Kripas' SoMe-kanaler. Fenomenet har også vært omtalt av redaktørstyrte medier.

Det har vært en stabilt høy rapportering om seksuell utpressing med økonomisk motiv i Norge i 2025. Dette samsvarer med fjorårets vurdering. Det er ikke registrert betydelige

61 Tipsene ble sendt fra Open AI. X.AI (Grok) sendte ingen tips via NCMEC i 2024.

62 Politiet. (2025). *Ekstreme nettsamfunn*. <https://www.politiet.no/rad/trygg-nettbbruk/ekstreme-nettsamfunn>

endringer i aktører, ofre, framgangsmåter eller benyttede muliggjørere⁶³, men det er registrert en marginal økning i antallet norske

gjerningspersoner og antallet mindreårige norske jenter som ofre for kriminaliteten.

Delvurderinger

Det ble i fjorårets rapport vurdert som *sannsynlig* at syntetiske overgrepsvideoer av realistisk kvalitet ville forekomme i 2025. Dette er ikke registrert av Kripos, men det er *mulig* at de allikevel eksisterer. Det er *sannsynlig* at realistiske, syntetiske overgrepsvideoer vil eksistere i 2026, og det underbygges av at aktører med kompetanse til å produsere realistiske, syntetiske overgrepsbilder har viet sin tid i 2025 til produksjon av videoer. Det er videre *sannsynlig* at norske aktørers befatning med syntetiske overgrepsbilder vil øke i 2026 ettersom det er registrert en økende tendens globalt.

Det er *meget sannsynlig* at det vil være en økning i saker som knyttes til ekstreme, voldelige nettsamfunn i 2026, og at norske barn og unge både vil være gjerningspersoner og ofre. Dette underbygges av at fenomenet har vært observert i Norge

med lav, stabil forekomst i 2022, 2023 og 2024, og at det i 2025 har økt, på lik linje med i andre land. Det er *sannsynlig* at økningen delvis skyldes økt kunnskap om og oppmerksomhet rundt fenomenet. Det er *sannsynlig* at flere norske gjerningspersoner og ofre vil utføre alvorlige handlinger i framtiden, og utsette seg selv og/eller andre for alvorlig fare.

Det er *meget sannsynlig* at seksuell utpressing med økonomisk motiv vil ha en stabilt høy forekomst også i 2026. Dette underbygges av rapporteringsfrekvensen i 2025. Det er *meget sannsynlig* at mange av de fornærmede for kriminalitetsformen vil fortsette å være mindreårige gutter, og det er også *mulig* at utviklingen som registreres i utlandet – at materialet av barnet selges videre som overgrepsmateriale – kan ramme norske gutter i 2026.

63 I fjorårets cyberkriminalitetsrapport ble muliggjørere presentert som teknologiske verktøy og digital infrastruktur. I årets rapport er begrepet også utvidet til å omfatte fysiske hjelpemidler.



// Gjerningspersonene er ikke nødvendigvis seksuelt motiverte – i flere tilfeller er eksempelvis seksuell utpressing kun et middel for å oppnå kontroll over offeret og tvinge vedkommende til å begå andre alvorlige handlinger. //



Cyberrettet kriminalitet

I 2025 har politiet registrert 349 straffesaker som omhandler *innbrudd i datasystem*. En stor andel av de fornærmede i straffesakene er privatpersoner. Dette er en økning på 104 anmeldelser fra foregående år og 98 saker fra 2023. Økningen i 2025 kan skyldes flere faktorer som et reelt høyere antall tilfeller av datainnbrudd, høyere anmeldelsestilbøyelighet blant de fornærmede, samt organisatoriske forhold, ressurser og prioritering internt i politiet. Selv om økningen fra 2024 til 2025 er betydelig sammenlignet med tall fra 2023, anses ikke økningen som et signifikant avvik fra normalbildet.

Kripos har registrert at omkring 17 ulike løsepengevirusvarianter knyttet til kjente *LSH-operasjoner*⁶⁴ er blitt brukt i cyberangrep mot norske små og mellomstore bedrifter (SMB)⁶⁵ i løpet av 2025. Kripos er ikke kjent med at store virksomheter er rammet i samme periode. Løsepengevirusvariantene er godt kjent for politiet ved at de er etablerte i det internasjonale LSH-økosystemet med ofre verden over.

I april og deretter i mai 2025 ble to norske virksomheter rammet av cyberangrep utført av samme hacktivist-gruppering. Felles for disse angrepene var at de fornærmede ble utsatt for datainnbrudd der trusselaktøren fikk adgang til å manipulere virksomhetenes OT-systemer. Disse angrepene er de første eksemplene der hacktivist har begått datainnbrudd mot norske virksomheter. At hacktivist benytter datainnbrudd som angrepsform var tidligere kun observert i internasjonal kontekst. Angrepene representerer således et avvik fra normal-situasjonen i Norge, der hacktivist vanligvis benytter tjenestenektangrep for å ramme sine mål. Selv om skadeomfanget av cyberangrep begått av hacktivist hittil har vært begrenset, viser denne utviklingen at hacktivist tilpasser metoder og verktøy for å oppnå ønsket effekt. Hacktivismefenomenet framstår dermed som både et kriminalitetsproblem og et sikkerhetspolitisk virkemiddel (se punkt 8.1.3), med gråsoner mellom ytringsfrihet, ulovlig påvirkning og grader av statlig støtte.

64 Eksempler på kjente LSH-operasjoner er Akira, Qilin, Lynx, LockBit, 8base og DragonForce.

65 Små og mellomstore bedrifter (SMB) omfatter bedrifter som sysselsetter færre enn 250 personer og har en årsomsetning som ikke overstiger 50 millioner euro og/eller en samlet årsbalanse som ikke overstiger 43 millioner euro. Kilde: *EØS-tillegget til Den europeiske unions tidende*. (2019, 4. april). EØS-tillegget til Den europeiske unions tidende, nr. 28/1133. s. 1. <https://www.regjeringen.no/contentassets/1bdef920d6cc4245b2e09a5902cb4374/vedlegg1.pdf>

Delvurderinger

Gitt utviklingen er det *sannsynlig* at antallet anmeldelser av cyberrettet kriminalitet vil fortsette å øke også i 2026. Noe av økningen vil kunne tilskrives økt anmeldelses-tilbøyelighet, men det er likevel *sannsynlig* at det vil være en faktisk økning i tilfeller av cyberrettet kriminalitet i Norge. Dette baserer seg hovedsakelig på økt kommersialisering av kriminalitet og det faktum at teknologisk utvikling i seg selv er en driver for økt cyberkriminalitet globalt.

Det er *sannsynlig* at hacktivistgrupperinger vil styrke sin operasjonelle kapasitet

gjennom digital rekruttering, erfaringsdeling og bruk av teknologiske verktøy. Økt tilgjengelighet av verktøy, samt aksept for samarbeid på tvers av grupperinger, vil *sannsynlig* bidra til forsterket kapasitet og kapabilitet⁶⁶ i målutvelgelse og gjennomslagskraft i kampanjer.

Selv om dagens hacktivistgrupper kun i begrenset grad er i stand til å gjennomføre angrep mot OT-systemer, er det *sannsynlig* at de i framtiden vil kunne oppnå fysisk skade eller ødeleggelse. Dette som følge av kompetanseoverføring, deling av skadevare og samarbeid med mer avanserte trusselaktører.

66 Kapasiteter henviser til kriminelles kvantifiserbare 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.



Teknologiutviklingen har redefinert begrepet *sosial inkludering*. Sosiale medier, forum og kommunikasjonsplattformer, samt spill og annen internettbasert underholdning har skapt nye arenaer for sosial interaksjon mellom mennesker. Personer som tidligere var avskåret fra fysiske sosiale møteplasser kan nå finne sammen med likesinnede på disse nye arenaene.

Det cyberkriminelle økosystemet

Dette kapittelet skal se nærmere på mekanismer og dynamikker i det cyberkriminelle økosystemet ved å se på tidligere rapportering og berike analysene med ny kunnskap. Kapittelet presenterer nye og videreutviklede modeller over det cyberkriminelle økosystemet, som er ment å gi støtte til framtidig analysearbeid.

Hvert år kobler rundt 280–300 millioner mennesker seg på internett for første gang – mange i land preget av høy fattigdom, lav utdanning og svak myndighetskontroll.⁶⁷ Høyhastighetsinternett kan utløse økonomisk vekst, løfte utdanning og helsesystemer, bidra til sosial inkludering og utgjøre en viktig brikke i nasjonal beredskap. Samtidig bidrar denne utviklingen også til at flere kriminelle aktører migrerer til eller flytter deler av sin kriminelle virksomhet til det digitale rom. Flere land som i senere tid har

begynt sin digitalisering og får tilgang til raskere og rimeligere internett, opplever nå sosiologiske og økonomiske utfordringer som tidligere har bidratt til framveksten av geografiske høyaktivitetsområder for cyberkriminalitet i andre land⁶⁸.

En annen stor gruppe som årlig kobler seg på internett for første gang, er barn og unge. Denne generasjonen vokser opp med sosiale medier, nettspill og kunstig intelligens som hverdagsteknologi – en uadskillelig del av deres utvidede virkelighet⁶⁹. Samtidig som barn og unge kan ha høy teknisk kompetanse fra ung alder, er barn ofte lett påvirkelige, uerfarne og har et underutviklet forhold til risiko og konsekvenstenkning. Når barn og unge får bevege seg fritt på internett og kommunisere med hvem som helst uten oppsyn eller veiledning fra voksne, øker risikoen for at de både utsettes for

67 ITU & UNESCO. (2024). *The State of Broadband: Leveraging AI for Universal Connectivity, Part One – June 2024*. Broadband Commission for sustainable development. <https://www.unesco.org/en/articles/state-broadband-2024>

68 For eksempel Russland, Ukraina, Romania, Nigeria, India, Kina og land i Sørøst-Asia.

69 Eng: *Augmented Reality (AR)*.



Når barn og unge får bevege seg fritt på internett og kommunisere med hvem som helst uten oppsyn eller veiledning fra voksne, øker risikoen for at de både utsettes for kriminalitet og rekrutteres til eller trekkes inn i kriminelle handlinger – både med og uten viten.

kriminalitet og rekrutteres til eller trekkes inn i kriminelle handlinger – både med og uten viten.

Samlet sett innebærer denne økte bruker-massen på internett en vedvarende vekst i antall cyberkriminelle aktører som utvikler nye metoder og framgangsmåter for å utnytte teknologi til å ramme norske verdier.

I det digitale rom er enkelte cyberkriminelle nettverk hierarkisk strukturert med tydelige roller og kommandolinjer, mens andre er løst organiserte og danner midlertidige, transaksjonsbaserte allianser. Et stort, fragmentert kriminalitetsbilde med mange flytende elementer, kombinert med raske endringer, gjør det utfordrende å beskrive hele økosystemet presist. I et bredere cyberkriminelt økosystem uten en fastsatt struktur eller et hierarki må en se på de faktiske samhandlingsmekanismene – altså mekanismene som påvirker hvordan kriminelle jobber sammen for å forstå utviklingen.

Figur 3 viser en modell for cyberkriminalitetens *ontologi*⁷⁰, og beskriver grunnleggende mekanismer for cyberkriminalitet. I modellens lyseblå boks «B» finner man lovbruddet, og her framkommer det hvordan en kriminell aktør

beveger seg gjennom en angrepsfase med delmål mot et endemål for å ramme en fornærmet.

For å lykkes med et angrep må aktøren gjennomføre støtteaktiviteter⁷¹ og utnytte sårbarheter hos den fornærmede. Dette framkommer i modellens lysegrønne boks «A».

Den lyserøde boksen «C» viser at aktører er avhengige av hjelpere: muliggjørere⁷², tilretteleggere⁷³ og samarbeidspartnere⁷⁴. Aktøren må også forholde seg til motstandere, herunder offentlige myndigheter, private virksomheter, forskningsmiljøer og rivaliserende kriminelle aktører.

Modellen inkluderer i tillegg grunnleggende drivere og utløsere som påvirker kriminaliteten. Disse framkommer i den lysegule boksen «D». Eksempler på utløsere kan være krig og konflikter, idrettsarrangementer, folkeavstemninger, prisutdelinger og andre begivenheter som kan frambringe cyberkriminalitet.

Modellen er altså sentrert rundt lovbruddet som begås mot enkeltpersoner, virksomheter eller infrastruktur, men kriminell virksomhet kan skje i alle de røde elementene i modellen. Det er dynamikkene mellom de røde elementene som utgjør fundamentet for det cyberkriminelle økosystemet.

70 Ontologi er det filosofiske studiet av hva som mest grunnleggende sett finnes. Kilde: Bøhn, E. D. (2025, 22. februar). *Ontologi*. Store norske leksikon. <https://snl.no/ontologi>

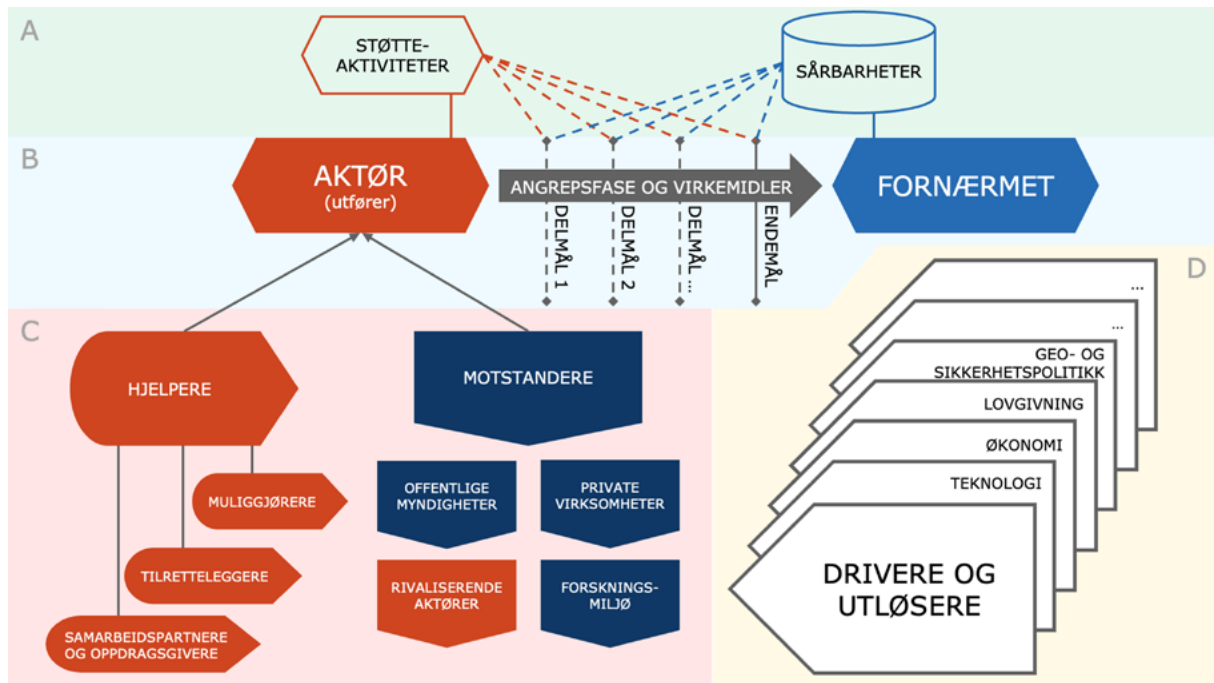
71 Ofte referert til som (eng:) *Kill Chain*.

72 For eksempel digital infrastruktur, verktøy og møteplasser.

73 For eksempel tilgangsmeklere, hvitvaskere og tilbydere av kriminelle plattformer.

74 For eksempel andre kriminelle aktører som samarbeider om et felles endemål.

Aktørgalleriet



Figur 3: *Cyberkriminalitetens ontologi*. Modellen viser at et lovbrudd (boks B) skjer gjennom en angrepsfase der en kriminell aktør har delmål mot et endemål. For å lykkes må aktøren utnytte sårbarheter og utføre støtteaktiviteter (boks A). Aktøren får ofte hjelp av muliggjørere og samarbeidspartnere, men møter også motstand fra myndigheter og andre aktører (boks C). I tillegg påvirkes kriminaliteten av drivere og utløsere som krig, konflikter eller store arrangementer (boks D). Modellen viser et dynamisk økosystem der alle elementer henger sammen. Modellen er utviklet av Kripas, inspirert av A. J. Greimas⁷⁵ og er en videreutvikling av *Elleve drivere for cyberkriminalitet*-modellen i *Cyberkriminalitet 2023*⁷⁶.

⁷⁵ Greimas, A. J. (1984). *Structural semantics: An attempt at a method*. Etera. <https://www.etera.ee/zoom/50614/view?page=267&p=separate&tool=info&view=0,0,2049,3458>.

⁷⁶ Kripas. (2023). *Cyberkriminalitet 2023*. ss. 14–32.

Aktør-begrepet har av politiet og andre blitt brukt til å beskrive både enkeltpersoner, grupper, digitale verktøy og skadevarer, og det har vært en sammenblanding av begrepene *roller* og *profiler*. Dette er forvirrende og man risikerer for eksempel feilaktig å omtale kriminelle tjenester som selges som handelsvare og enkeltpersoner eller grupper som én og samme aktør.⁷⁷ Dette utfordrer politiets og private sikkerhetsselskapers evne til å sortere i det kriminelle aktørgalleriet og derigjennom være i stand til å vurdere trusselen som ulike enkeltpersoner og grupperinger utgjør.

Modellen i Figur 4 har fått navnet *ARPA-rammeverket* og skal rydde i begrepsapparatet ved å beskrive aktørgalleriets sammensetning på fire nivåer. Modellen bygger på *Isfjell*-modellen i *Cyberkriminalitet 2025*⁷⁸, som viser sammenhengen mellom aktørers underliggende og mer varige motivasjoner og deres synlige handlinger og roller. Modellen tar høyde for cyberkriminalitetens heterogene natur⁷⁹ ved å tydeliggjøre hvilke nivåer som er dynamiske og hvilke som er mer bestandige. Modellen er derfor skygglagt for å illustrere hvilke kategorier som endrer seg raskt og hvilke som er mer varige – hvit

bakgrunn indikerer lett endring, mørkere bakgrunn større stabilitet.

Til syvende og sist handler cyberkriminalitet om *mennesker*; menneskelige interesser driver kriminaliteten. Modellen kan brukes som en sjekkliste i etterforskning for å vurdere om de ulike aktørnivåene er avdekket. En helhetlig oversikt over aktørgalleriet er relevant for å avdekke mulig sammensatt virkemiddelbruk fra statlige aktører, og kan samtidig varsle om endringer i dynamikken mellom ulike roller og profiler.

Modellen viser aktørgalleriets sammensetning på fire nivåer. Nivåene skiller mellom gjerningspersonene som står bak kriminaliteten (*aktør*), deres motivasjoner (*profil*), rollen de har i økosystemet (*rolle*), samt hvilke handlinger eller arbeidsoppgaver de utfører (*aktivitet*).

Øverste nivå (aktør) viser altså til mennesket som står bak handlingene.

På andre nivå (profil) er det fem profiler⁸⁰, samt en gruppe uklassifiserte aktører. Profilene er uendret fra fjorårets cyberkriminalitetsrapport og beskrevet ytterligere senere i dette kapitlet.

Tredje nivå (rolle) deles inn i to: *tilretteleggere* og *utøvere*. I motsetning til tilretteleggere er

77 Navnet på den kriminelle tjenesten benyttes ofte til å omtale ellers ukjente/ubenevnte/ikke navngitte enkeltpersoner eller grupper.

78 Kripos. (2025). *Cyberkriminalitet 2025*. s. 13.

79 Nye konstellasjoner oppstår og endrer seg raskt.

80 I denne rapporten er ikke terrorister beskrevet da terrorisme faller utenfor Kripos' mandat.



Til syvende og sist handler
cyberkriminalitet om mennesker;
menneskelige interesser
driver kriminaliteten.

det utøvere som begår kriminalitet mot enkeltpersoner eller virksomheter. En aktør kan både være en tilrettelegger og en utøver – avhengig av situasjonen.

På fjerde nivå (aktivitet) framkommer det en rekke bokser som beskriver forskjellige situasjoner (omtalt som «aktivitetsområder»). Hver boks viser nedbrytingen av en situasjon til observerte enkeltaktiviteter, og sier dermed noe om organiseringen av ulike roller i ulike situasjoner. Boksene trenger ikke være uttømmende for å gi analysestøtte, det er tilstrekkelig å fylle inn den kunnskapen og forståelsen man har. Analyserammeverket kan hjelpe analytikeren med å enklere forstå situasjonen og kontekstualisere trusselen. I tillegg kan det bidra til økt bevissthet når vi skal vurdere ulike kriminelle aktiviteter i det digitale rom. Analyserammeverket kan også benyttes i andre sammenhenger. Basert på observert organisering av ulike roller, har Kripos her listet opp fire eksempler på situasjoner med typiske aktiviteter.

Til høyre i modellen finner vi *muliggjørere* – teknologiske verktøy, digital infrastruktur, og fysiske hjelpemidler.

Et eksempel på bruk av modellen og dets relevans for å se aktørers sammenheng på tvers av kriminalitetsområder kan se slik ut:

- (A) Utsetter barn for seksuelt overgrep
- (R) Kultmedlem⁸¹
- (P) Uklassifisert aktør
- (A) Ola Normann

I dette tilfellet vil en antagelse om aktørens profil basert på aktørens handling (aktivitet) kunne føre til feil vurdering av motivasjonen bak handlingen. Aktøren, Ola Normann, ville basert på en slik antagelse kunne bli klassifisert som en seksuallovbryter, ikke en uklassifisert aktør der motivasjonen er noe annet enn seksuell tilfredsstillelse. Eksemplet viser hvorfor det er nødvendig å identifisere alle aktørnivåene for å presist vurdere trusselen.

I tilfeller der samme aktør kan beskrives med flere aktiviteter, roller eller profiler samtidig (eksempelvis multikriminelle og gråsoneaktører), kan det se slik ut:

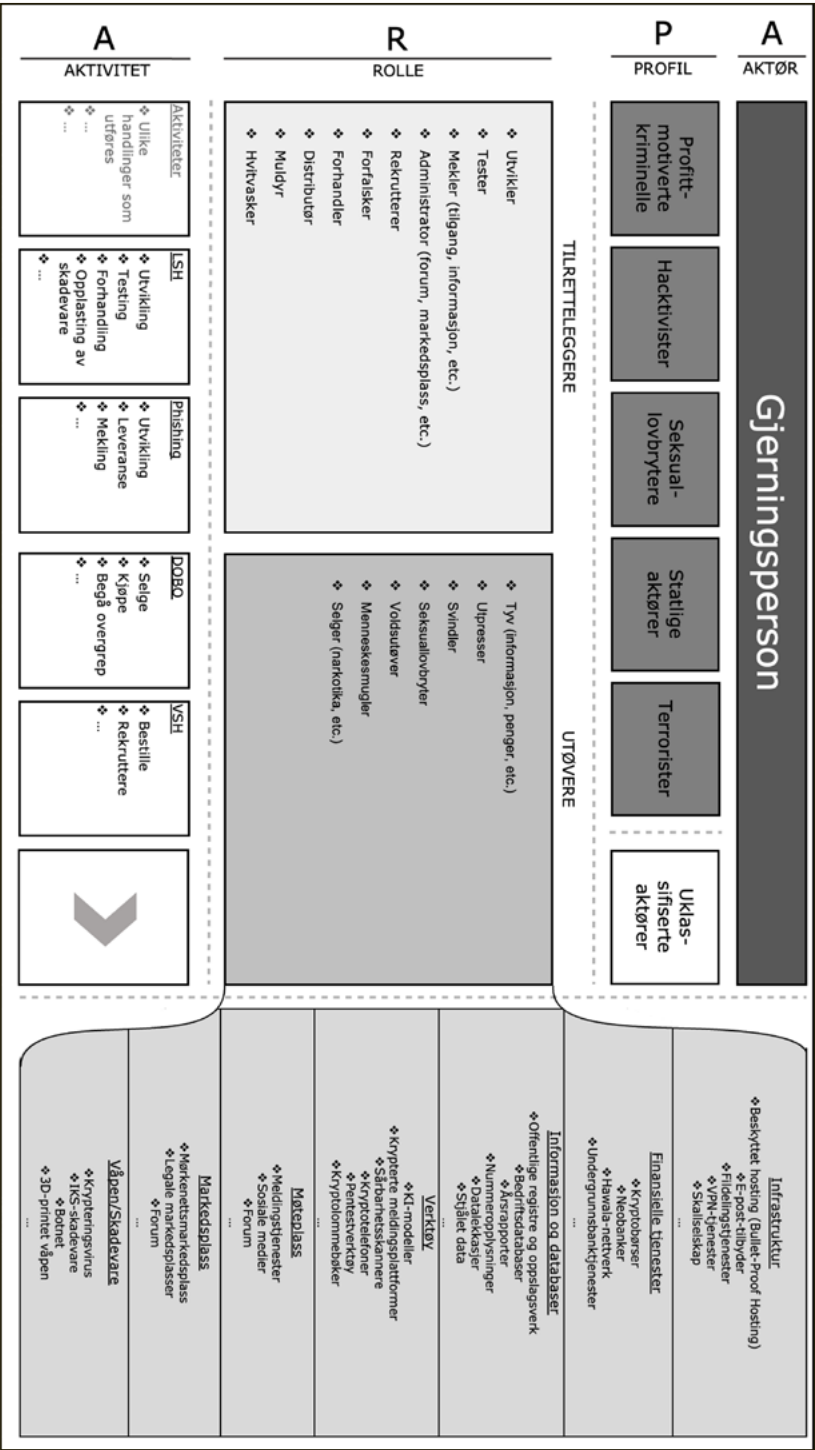
Multikriminell:

- (A) Rekruttering av utøvere
- (R) Menneskesmugler; Tilrettelegger DOBØ
- (P) Profittmotivert kriminell
- (A) Ola Normann

Gråsoneaktør:

- (A) Sårbarhetssøking
- (R) Hacker
- (P) Aktivist/terrorist
- (A) Ukjent

⁸¹ For mer om kultmedlemmer, se side 82–85.



Figur 4: ARPA-rammeverket. Modellen leses nedefra og opp, fra aktivitet til aktør. Modellen er utviklet av Kripos og inspirert av A. J. Greimas⁸².

ARPA-rammeverket bidrar med en ny nivåinn-
deling av aktører og tydeliggjør hva hvert nivå
omfatter. I tillegg bidrar rammeverket til å kart-
legge ulike aktiviteter og roller (tilretteleggere
og utøvere), noe som kan gi beslutningsstøtte
i prioritering av saker. Kripas inviterer andre
politienheter, offentlige myndigheter og private
virksomheter som arbeider med ulike trusler til
å bidra i det videre kartleggingsarbeidet for å
identifisere sentrale aktiviteter og roller på tvers
av kriminalitetstområder.

Profittmotiverte kriminelle

Kommersielle aktører

Tradisjonelle kommersielle aktører kan ha en
kriminell side. Slike kommersielle aktører vil
kunne ha samme grunnleggende motivasjon
som profittmotiverte kriminelle, normalt penger
og innflytelse, men skiller seg ved at kjernevirk-

somheten skjer innenfor økonomiske foretak
som tilsynelatende opererer innenfor samfun-
nets forventninger og regulatoriske krav.

Lovbrudd begått av kommersielle aktører
innebærer hovedsakelig 1) utnyttelse av midler-
tidige smutthull som har oppstått som følge av
teknologisk utvikling eller svakheter mellom ulike
jurisdiksjoner; eller 2) å selge varer eller tjenester
som er ulovlige i seg selv for å a) profittoptimali-
sere egen kjernevirksomhet, eller b) tilrettelegge
for kriminell virksomhet. Dette omfatter varer og
tjenester i gråsonen mellom lovlig og ulovlig,⁸³
såkalte flerbruksvarer⁸⁴, og tradisjonell organisert
kriminalitet og økonomisk kriminalitet.⁸⁵

Profittmotiverte kriminelle aktører som utnyt-
ter økonomiske foretak – for eksempel skall- og
frontselskaper eller virksomheter brukt som
fasade for å hvitvaske kriminelt utbytte – inngår
i utgangspunktet ikke i denne kategorien. I noen

82 Greimas, A. J. (1984). *Structural semantics: An attempt at a method*. Etera.

83 Enten ved at en aktør kalkulert utnytter et smutthull i lovverket, at deler av virksomheten er lov-
lig mens andre deler er ulovlig, eller at produktet kan være ulovlig i én kontekst, men lovlig i en
annen. Eksempler er KI-modeller som kan generere ulovlig innhold, verktøy for å omgå digitale
rettighetssystemer, droner med særlige spesifikasjoner, samt private etterretnings- og sikker-
hetsselskaper som går for langt i virkemiddelbruken.

84 Flerbruksvarer er varer som i utgangspunktet er sivile, men som også har viktige militære an-
vendelser. Begrepet brukes her i utvidet forstand til også å inkludere kriminell anvendelse. Eng:
Dual Use Items, Technology and Services.

85 Økokrim. (2022). *Trusselvurdering 2022*. s. 61. <https://www.okokrim.no/getfile.php/5017571.2528.q7zikspuaagqs/%C3%98kokrim+trusselvurdering+2022.pdf>

tilfeller er det likevel vanskelig å trekke klare skillelinjer.⁸⁶ I enkelte land er det ikke uvanlig at ansatte i myndighetsapparatet eller private foretak også har posisjoner i kriminelle organisasjoner og veksler mellom rollene. Dette bidrar til uklare grenser mellom kommersielle aktører og statlige aktører, og andre profittmotiverte kriminelle.

Noen eksempler på roller som kan tilfalle kommersielle aktører er overvåkingstjenester⁸⁷, forhandlere ved cyberangrep med løsepengevirus (LPV)⁸⁸, samt tilbydere av digital infrastruktur⁸⁹ eller tjenester⁹⁰ som tilrettelegger for eller tilslører kriminalitet.

Kriminelle som begår utpressing

Cyberrettet utpressing kan foregå på flere måter og i ulike konstellasjoner. I tiden etter 2010 har den vanligste formen for utpressing foregått

ved at kriminelle benytter seg av et såkalt *RaaS kit*⁹¹, med ulike tilhørende støttetjenester som tilbys i et LSH-nettverk. Dette har utviklet seg til en av de mest utbredte forretningsmodellene for cyberrettet utpressing gjennom de siste femten årene.

Selv om de fleste LSH-nettverk ofte er sentrert rundt bruk av en form for skadevare med krypteringsfunksjon, baserer ikke lenger alle LSH-nettverk seg på bruk av kryptering. Gjennom de siste fem årene har det blitt stadig vanligere for cyberkriminelle å begå utpressing basert på datatyveri og trusler om publisering av virksomheters data, uten at det gjennomføres kryptering. I slike tilfeller kan det være noe upresist og misvisende å omtale slike kriminelle konstellasjoner som løsepengevirus som handelsvare (LSH), ettersom skadevaren som

86 Ibid. s. 61.

87 Tilbydere av høyteknologiske cybervåpen som eksempelvis kommersiell spionskadevare som er underlagt lisensplikt, men som omgår eksportkontroll eller sanksjoner. Eng: *Private Surveillance og Commercial Spyware*.

88 Tilbydere av forhandlingstjenester som inngår skjulte avtaler eller driver utbyttedeling med løsepengevirusaktører. Eng: *Ransomware/Extortion Negotiation og Cyber Extortion Incident Response*.

89 For eksempel beskyttet Hosting (eng: *Bulletproof Hosting*) og VPN- og proxy-tjenester.

90 For eksempel IP-stressere (også kjent som eng: *DDoS-for-Hire*), fildelingstjenester, ende-til-ende-krypterte meldingsplattformer og epost-tilbydere.

91 Et RaaS kit, også omtalt som «panel», kan forstås som en programvare med ulik funksjonalitet. (*RaaS*, kort for *Ransomware-as-a-Service* på engelsk, er løsepengevirus-som-handelsvare, forkortet LSH, på norsk.) RaaS kit lar kriminelle begå cyberrettet utpressing, uavhengig av ferdigheter, mot at den kriminelle deler en prosent av profitten med eieren av RaaS kit'et.

A close-up photograph of a hand clicking a white computer mouse. The mouse is positioned over a circular image of the Earth, showing continents and oceans. The background is dark. A white text box with a double-slash icon is overlaid on the image.

// Nær sagt hvem som helst med
internettilgang kan slutte seg til
et USH-nettverk . //



gir den kriminelle mulighet for kryptering ikke lenger er til stede. Utpressing som handelsvare (USH) foreslås som et utvidet begrep som favner både tradisjonelle LSH-nettverk og de kriminelle konstellasjonene som bedriver andre former for cyberrettet utpressing, men som fortsatt opererer i rammen av kriminalitet som handelsvare (KSH). Det sentrale poenget er at programvaren og måten den benyttes på er flyktig og skiftende, mens menneskene bak handlingene og deres intensjoner står seg over tid.

Nær sagt hvem som helst med internetttilgang kan slutte seg til et USH-nettverk. Selv om to eller flere kriminelle inngår i samme USH-nettverk, eller tar i bruk samme LSH-skadevare, betyr ikke dette at de automatisk utgjør en definert cyberkriminell gruppe⁹². Bruk av en bestemt LSH-variant sier i seg selv lite om den enkelte kriminelle, vedkommendes kapabiliteter eller motivasjon. Affilierte⁹³ kan veksle mellom ulike USH-varianter samtidig, noe som utfordrer politiets evne til å gjenkjenne gjerningspersoner på tvers av cyberangrep, skadevaretyper og grupperinger eller nettverk.

I forbindelse med en etterforskning av datinnbrudd begått i Norge avdekket Kripas at gjerningspersonen hadde benyttet fire ulike LPV-varianter om hverandre, samtidig som det var indikasjoner på at aktøren også benyttet en femte LSH-variant. Gjerningspersonen er videre knyttet til cyberangrep mot i overkant av 130 virksomheter utenfor Norge, og har lyktes med å innkreve nærmere 50 millioner kroner i løsepenger fra ofrene. Eksempelet illustrerer at én enkelt kriminell kan være affiliert med og benytte seg av flere LPV-varianter samtidig.

Kripas erfarer at tradisjonelle LSH-grupperinger i ulik grad opererer som åpne eller lukkede nettverk. Tidligere analyser av løsepengevirus-grupperingen *HIVE* viste at denne besto av en sentralstyrt kjernegruppe, med en restriktiv tilnærming til fordeling av oppgaver, og som selektivt rekrutterte nytt personell inn i kjerne

92 En cyberkriminell gruppe er en samling av enkeltindivider som samarbeider for å oppnå et felles mål gjennom å begå cyberkriminalitet.

93 En affiliert er en person som har en forretningsmessig forbindelse til en LSH/USH og som benytter seg av skadevaren denne leverer.

gruppen. Gruppen hadde en diskre tilnærming til rekruttering av affilierte i cyberkriminelle forum. Til sammenligning ser man at eksempelvis grupper som *Lockbit* gradvis fikk en mer åpen profil, hvor alle som betalte for tilgang fikk mulighet til å benytte seg av Lockbit løsepengevirus. Konsekvensene av dette ble at Lockbit tiltrakk seg affilierte som var uerfarne og som begikk operasjonelle feil. Dette bidro videre til å svekke Lockbits profesjonelle profil og omdømme.

Fragmentering i USH-økosystemet har skjerpet kampen om å tiltrekke seg affilierte. Enkelte USH-nettverk markedsfører seg som bedre enn sine konkurrenter for å maksimere rekruttering og inntekter. En sentral del av denne markedsføringen er å ramme store og profilerte virksomheter for å skape maksimal oppmerksomhet. Flere LSH-grupperinger har en tydelig medieprofil og uttaler seg i redaktørstyrte medier. Rasjonalet bak denne utviklingen baserer seg på oppfatninger om at beryktede LSH-skadevarer får økt forhandlingskraft overfor fornærmede gjennom omdømme. Det er også eksempler på at LSH-grupperinger skaper et bilde av seg selv som en kapabel aktør ved å antyde at de har angrepet betydningsfulle virksomheter, uten at det er klart at de faktisk har gjort dette. Slik promotering av meritter og retorikk kan legge ekstra press på den fornærmede i en forhandlingssituasjon, samt bidra til å tiltrekke seg talenter (affilierte) til sin kjernegruppe. Det er i tillegg rapportert om en tilstrømning av yngre kriminelle

som viser høyere risikovillighet, prestasjonsjag og søken etter medieoppmerksomhet. Dette har ført til flere omstridte hendelser, nye konstellasjoner og løse sammenslutninger på tvers av USH-økosystemet.

Med bakgrunn i etterforskning og internasjonalt politisamarbeid har Kripas kartlagt i overkant av 400 kriminelle med ulike knytninger til det cyberkriminelle økosystemet. Arbeidet har hovedsakelig tatt utgangspunkt i etterforskninger der det er begått ulike kombinasjoner av datainnbrudd, datatyveri/kryptering og utpressing, både i Norge og internasjonalt. Flesteparten av aktørene som er omhandlet i kartleggingen har en form for tilknytning til en eller flere LSH-varianter. Også personer med andre og mer perifere roller i det cyberkriminelle økosystemet er kartlagt.

Fram mot og gjennom året 2025 har kartleggingen ledet til identifisering av en betydelig andel cyberkriminelle, hvor enkelte av disse også er blitt etterlyst internasjonalt. Arbeidet har gitt verdifulle innsikter i ulike mekanismer og dynamikker i det cyberkriminelle økosystemet.

Den identifiserte gruppen kriminelle består utelukkende av menn, hvorav flesteparten er i aldersspennet 20 til 40 år. De fleste har opprinnelse fra Russland og Ukraina, men også personer fra en rekke andre nasjonaliteter er representert i datagrunnlaget. Et gjennomgående fellestrekk er at de fleste behersker russisk språk og benytter dette i kommunikasjon med andre de samarbeider med. Enkelte har formell utdanning i IT-relaterte fag, mens de fleste

Med bakgrunn i etterforskning og internasjonalt politisamarbeid har Kripos kartlagt i overkant av 400 kriminelle med ulike knytninger til det cyberkriminelle økosystemet.

ser ut til å mangle formell utdanning. Det er indikasjoner på at de eldste i den identifiserte gruppen har bedrevet ulike former for cyberrettet kriminalitet over flere år, og at de begynner å involvere seg i LSH da denne kriminalitetsformen gjennomgikk et taktskifte i forbindelse med framveksten av kryptovaluta i årene etter 2009.

Kriminelle som begår utpressing med løsepengevirus er opptatt av hva myndigheter og sikkerhetsbransjen foretar seg for å motvirke og bekjempe cyberkriminalitet. I tillegg er de bevisste på hvordan konkrete USH-grupperinger omtales og vurderes i offentlige trusselvurderinger. Dette kommer eksempelvis til uttrykk ved at de deler og diskuterer innhold i ulike trusselvurderinger og nyheter om politiaksjoner, og tiltak mot cyberkriminelle.

Kripas har sett enkelte eksempler på at cyberkriminelle bestemmer seg for å gå videre til andre LPV-varianter når de opplever at én variant får for mye oppmerksomhet fra myndigheter. Dette står imidlertid noe i kontrast til internasjonale utviklingstrekk de senere årene, hvor man ser tendenser til at visse USH-nettverk aktivt forsøker å skape blest om egne LSH-nettverk.

Delvurderinger

Kriminelle aktører som begår cyberrettet utpressing er i hovedsak drevet av et ønske om profitt. Kripas legger til grunn at profittmotiverte cyberkriminelle vil fortsette å utvikle sine handlemåter og tilpasse seg mottiltak i jakten på økonomisk fortjeneste i 2026 og videre. Ved cyberrettet utpressing er kriminelle aktører avhengige av å benytte et pressmiddel, henholdsvis stjålet data eller kryptering av virksomhetens systemer. Det er *lite sannsynlig* at dette vil endre seg i 2026.

Profittmotiverte seksuallovbrytere

Profittmotiverte seksuallovbrytere er aktører som begår seksuallovbrudd mot barn, men som er motivert av et ønske om økonomisk vinning. Kripas observerer i hovedsak tre ulike profittmotiverte seksuallovbrytere: (1) Selgere av direkteoverførte bestillingsovergrep (DOBO-selgere), (2) utpressere og (3) aktører som selger overgrepsmateriale. Samtlige begår seksuallovbrudd, men på ulike måter.

DOBO eksisterte ikke før det digitale rom oppstod, og teknologien har medført at barn i risikoland nå blir solgt og utsatt for overgrep både fysisk og digitalt. DOBO-selgere er oftest filippinske kvinner med egne, mindreårige barn. De kan være både tilretteleggere som organiserer og formidler direkteoverførte fysiske overgrep

mot egne og andres barn, og de kan være utøvere av overgrepet – ofte er kombinasjonen av tilrettelegger og over griper tilfelle.⁹⁴ Som beskrevet på side 39 under kapittelet om normalbildet, selges DOBO til seksuelt motiverte norske menn.

Det er ikke registrert at norske aktører selger DOBO av norske barn, hverken til norske eller utenlandske kjøpere. Det er imidlertid kjent for Kripos at norske gjerningspersoner har solgt seksualisert materiale av egne barn til seksuelt motiverte aktører. I tillegg har cyberdomenet skapt rom for et marked hvor barn og unge selger egenprodusert seksualisert materiale av seg selv og andre til seksuelt motiverte aktører. Barna kan tenke på det som lettjente penger, uten å være klar over potensielle konsekvenser det kan få for dem i framtiden, eller hvilken risiko det kan medføre. Bildene kan få evig liv på internett og deles mellom seksuelt motiverte aktører, og barna kan selge bilder og videoer til aktører med et alvorlig voldspotensial som kan utgjøre en betydelig fare.

Som det framgikk av fjorårets cyberkriminalitetsrapport, er profittmotiverte seksuallovbrytere som begår seksuell utpressing av norske barn oftest aktører fra Filippinene, Nigeria og Elfenbenskysten. De er i mindre grad organiserte enn tidligere antatt, og kriminaliteten er

forholdsvis enkel å gjennomføre, i tillegg til lav oppdagelses- og straffeforfølgelsesrisiko.⁹⁵ Som tidligere nevnt er det ikke registrert betydelige endringer i normalbildet, selv om det er registrert en marginal økning i antall norske utpressere og i antall mindreårige jenter som er ofre for kriminaliteten.

Salg av overgrepsmateriale er, i motsetning til de to overnevnte kriminalitetstypene, lovbrudd som i gjerningsøyeblikket ikke rammer barnet direkte, men som allikevel kan medføre gjentatte krenkelser mot offeret. Kripos er kjent med at norske seksuallovbrytere kjøper overgrepsmateriale av både norske og utenlandske profittmotiverte aktører, og det er registrert både kjøp og salg av autentisk og syntetisk overgrepsmateriale. Som det framgår av normalbildet er det imidlertid vanligst at aktører som har befattning med overgrepsmateriale utveksler slike bilder og videoer med likesinnede uten noen form for betaling. Det er ikke kjent om de norske aktørene både er seksuelt motiverte og motiverte av profitt, eller eventuelt i hvilken utstrekning kombinasjonen forekommer.

Cyberdomenet har skapt et utvidet univers for profittmotiverte aktører, også seksuallovbrytere. Mulighetene er stadig flere og aktørgruppen ekspanderende, og Kripos observerer

94 Kripos. (2023). *Direkteoverførte bestillingsovergrep (DOBO)*. s. 5. <https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/direkteoverførte-bestillingsovergrep-dobo.pdf>

95 Kripos. (2025). *Cyberkriminalitet 2025*. s. 7.

at de kriminelle kontinuerlig utvikler sine metoder og framgangsmåter. Sekkeposten kriminalitet som handelsvare har allerede et mangfoldig repertoar av kriminelle tjenester til salgs. Kripas omtalte i fjor at utviklingen innen kunstig intelligens kan medføre automatisering og oppskalering av kontaktetableringsprosesser.⁹⁶ Kanskje vil også kontaktetablering som handelsvare (eng: *Grooming as a Service*) være å finne på markedet i framtiden.

Delvurderinger

En av de sterkeste driverne for cyberkriminalitet er et ønske om profitt, og aktørene er tilpasningsdyktige i sin utførelse av kriminaliteten. Også en del seksuallovbrudd mot barn kan begås med hensikt om å oppnå en økonomisk vinning. Seksuell motivasjon er en sterk drivkraft som profittmotiverte aktører vil kunne utnytte for å tjene penger. Kriminalitetsutøvelsen kan spre seg i et ubegrenset antall retninger, og det er *sannsynlig* at profittmotiverte aktører vil finne nye måter å oppnå en økonomisk vinning på ved å begå ulike former for seksuallovbrudd. Det er *mulig* at dette vil kunne ses i form av kriminalitet som handelsvare.

Om forholdet mellom cyberkriminelle og statlige aktører

Grunnet den spente geopolitiske situasjonen verden nå befinner seg i og det kommende totalforsvarsåret, har Kripas valgt å se på kompleksiteten rundt statlige aktører og deres involvering i cyberkriminalitet. Det er særlig i cyberdomenet at ulike former for samvirke mellom statlige aktører og kriminelle aktører forekommer.

Cyberkriminalitet kjennetegnes ofte av at gjerningspersonen innledningsvis er ukjent for politiet, og det er gjennom etterforskning at aktørene bak et lovbrudd avdekkes. Politiet må derfor ha kunnskap om hvordan statlige aktører gjør seg gjeldende i det cyberkriminelle økosystemet, slik at etterforskningen kan overføres til andre etater hvis etterforskningsmandatet endrer seg underveis.

Stormaktsrivalisering og internasjonale konflikter tåkelegger allerede uklare skillelinjer mellom statlige aktører og cyberkriminelle aktører. Dette gjelder spesielt skillelinjene mellom statlige aktører, hacktivist og profittmotiverte cyberkriminelle. I norske etterretnings- og sikkerhetstjenesters trusselvurderinger for 2026 fastslås det

96 Kripas. (2025). *Cyberkriminalitet 2025*. ss. 48–50.

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.

For å forstå samvirket mellom statlige og cyberkriminelle aktører fullt ut, må man også forstå at det finnes grader av statlig tilknytning. For å unngå feilaktig attribusjon til andre land, benyttes Norge som eksempel for å beskrive dette. Man kan snakke om *norske aktører*, *norsk-statlige aktører*, *norsk-statlig tilknyttede aktører* og *pro-norske aktører*. Førstnevnte inkluderer aktører som er fra Norge eller eier et norsk pass. Det er ikke gitt at en *norsk aktør* har knytning til den norske staten. *Norsk-statlige aktører* er aktører som representerer den norske staten. Begrepet *norsk-statlig tilknyttede aktører* brukes i tilfeller hvor det er tilstrekkelige indikatorer på at det eksisterer en knytning mellom den cyberkriminelle og den norske stat. Sistnevnte omtales dersom aktøren selv har gitt uttrykk for å være pro-Norge. Ved bruken av begrepet *pro-norske aktører* er ulike former for kontakt med den norske stat verken bekreftet eller kan utelukkes.

Figur 5: *The Spectrum of State Responsibility*, Atlantic Council. Oversatt av Kripos.

at statlige aktører benytter kriminelle stedfortredere⁹⁷ for å oppnå statens ulike målsetninger.^{98, 99}

Stater er ikke avhengig av geografisk nærhet til de cyberkriminelle for å nyttiggjøre seg av dem. En stat kan bruke kriminelle som opererer i eller kommer fra andre land enn den respektive staten.

Cyberdomenet er en arena som gir svært gode forutsetninger for å operere fordekt. Dette vanskeliggjør arbeidet med å identifisere og straffe-førløge cyberkriminelle, og gjør det utfordrende å få innsikt i samvirket mellom cyberkriminelle og statlige aktører. Atlantic Councils rammeverk (*Spekteret av statlig ansvar*, Figur 5) lister opp ti nivåer av statlig ansvar for cyberangrep begått av kriminelle. Modellen omfatter alt fra statlige

bidrag til å stoppe en kriminell handling (nivå 1) til at staten utfører cyberangrepet selv (nivå 9) eller gjennom en integrert tredjepart (nivå 10). Kjennskap til dette spekteret er viktig sett i lys av trusselbildet fra statlige aktører slik dette er beskrevet av norske etterretnings- og sikkerhetstjenester. Rammeverket beriker det cyberkriminelle situasjonsbildet og kan benyttes til å tolke tilfeller av cyberrettet kriminalitet spesielt.

Det eksisterer ulike grader av samvirke og *krysspollinering* blant 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.

De siste år har en rekke saker avdekket eller gitt grunn til sterk mistanke om statlig involvering i cyberkriminelle operasjoner og angrep, både i Norge og Europa. I deler av Europa har det vært en økning i cyberangrep de siste år, hvor

97 Kriminelle stedfortredere (proxy-aktører) er personer eller organisasjoner uten formell tilknytning til etterretnings- og sikkerhetstjenester eller andre myndighetsorganer, som vitende eller uvitende utfører kriminell aktivitet på oppdrag fra, eller til støtte for, myndigheter. Aktiviteten kan være politisk, ideologisk eller økonomisk motivert. Kilde: PST. (2025). *Nasjonal Trusselvurdering 2025*. s. 12. https://www.pst.no/globalassets/2025/nasjonal-trusselvurdering-2025/nasjonal-trusselvurdering-2025_no_web.pdf

98 PST. (2026). *Nasjonal trusselvurdering 2026*. ss. 12–13, 16–18, 22–23. <https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2026%20-%20N0%20-%20Utskriftsvennlig%20v4.pdf>

99 Etterretningstjenesten. (2026). *Fokus*. ss. 27–29. <https://www.etterretningstjenesten.no/publikasjoner/fokus/fokus-pa-norsk/Fokus2026%20-%20N0%20-%20Utskriftsvennlig%20v4.pdf>



Cyberdomenet er en arena som
gir svært gode forutsetninger for
å operere fordekt.

mange vurderes til å ha hatt en kombinasjon av strategiske¹⁰⁰ og økonomiske motivasjoner. Også norsk industri og offentlige virksomheter har jevnlig blitt truffet av cyberangrep. Blant annet har disse vært rettet mot havner og landføringspunkter for gass, energi og kommunikasjon de siste år.

Det er ulik grad av frivillighet blant de cyberkriminelle til å operere med eller på vegne av en stat. Det kan også endres over tid. Eksempelvis kan et samarbeid i utgangspunktet være frivillig, men senere utvikle seg til et mer tvangspreget forhold der en av partene sitter på informasjon eller maktmidler som gjør det vanskelig for den andre å trekke seg ut.

Redegjørelsen i dette kapittelet underbygger det norske etterretnings- og sikkerhetstjenester har stadfestet: at kriminelle stedfortredere er en del av statlige aktørers virkemiddelbruk.¹⁰¹ Dette kommer særlig til uttrykk i det digitale domenet, hvor spesielt cyberrettet kriminalitet er like egnet til å understøtte kriminelle motiver som statlige målsetninger. Forståelsen av figur 5 som viser den statlige involveringen i cyberkriminalitet er viktig for å tolke hendelser, forstå kontekst og sammenhenger, og gjennom dette forsterke politiets evne til å oppdage avvik fra normalen, varsle og skadebegrense så mye som mulig.

100 For å anskaffe informasjon om sivil og militær teknologi. Kilde: Etterretningstjenesten. (2025).

Fokus. s. 14 <https://www.regjeringen.no/contentassets/6290dec36c374ee191e5c7dbbal8a258/fokus2025-no-weboppslag-v3.pdf>

101 Grensene mellom digitale og fysiske trusler kan være vanskelige å definere. I dette landskapet ser man også såkalte sammensatte eller hybride trusler. Sammensatt virkemiddelbruk handler om at statlige aktører som ønsker å ramme andre stater på andre måter enn væpnet konflikt, bruker en rekke ulike metoder og virkemidler for å understøtte egne strategiske målsettinger. For eksempel kan fordekke påvirkningsoperasjoner og desinformasjon bidra til å destabilisere demokratier gjennom å svekke befolkningens tillit til sentrale samfunnsinstitusjoner. På denne måten kan for eksempel autoritære regimer søke å skape kaos eller påvirke politiske beslutninger i et annet land til sin fordel. Kilde: Stortingsmelding 13 (2024–2025). *Forebygging av ekstremisme: Trygghet, tillit, samarbeid og demokratisk motstandskraft*. Kultur- og likestillingsdepartementet. <https://www.regjeringen.no/no/dokumenter/meld.-st.-13-20242025/id3092713/?ch=3>



Selv om skadeomfanget hittil har vært begrenset, viser utviklingen at hacktivistene tilpasser metoder og verktøy for å oppnå større effekt.

Hacktivister

Hacktivisme er en hybridform som kombinerer politisk eller ideologisk motivert aktivisme med cyberkriminalitet, og utgjør en vedvarende trussel mot norske verdier og interesser. Fenomenet omfatter mer enn tjenestenektangrep, og inkluderer også informasjons- og datatyveri, lekkasje og spredning av stjålet informasjon, samt annen digital kriminalitet utført med politisk eller ideologisk motivasjon.

Enkelte grupper opererer i grenselandet mellom aktivisme og profittmotivert kriminalitet, der økonomiske gevinster kan brukes til å finansiere hacktivistisk virksomhet. Angrepsformen domineres av tjenestenektangrep, som brukes for å skape oppmerksomhet, uro og svekke tilliten til samfunnsinstitusjoner eller påvirke opinion.

I Norge har pro-russiske grupper blant annet gjennomført tjenestenektangrep og gjort uautoriserte endringer i industrielle kontrollsystemer. En hendelse i Bremanger, der styringssystemet til en demning ble kompromittert, og 500 liter vann ble sluppet ut hvert sekund i fire timer, illustrerer hvordan slike aktører kan demonstrere evne til å ramme kritisk infrastruktur. Det er også observert tydelige knytninger mellom den russiske stat og cyberkriminelle som gjennomfører cyberangrep for å samle informasjon knyttet til norsk teknologi og våpen.

Selv om skadeomfanget hittil har vært begrenset, viser utviklingen at hacktivistisk tilpasser metoder og verktøy for å oppnå større effekt. Fenomenet framstår dermed som både

et kriminalitetsproblem og et sikkerhetspolitisk virkemiddel, med gråsoner mellom ytringsfrihet, ulovlig påvirkning og grader av statlig støtte.

Det er flere kjente tilfeller av personangrep mot folkevalgte politikere, inkludert deep-fake-pornografi mot Italias statsminister Giorgia Meloni og de britiske politikerne Priti Patel og Penny Mordaunt. Pro-russiske *Killnet* manipulerte i 2022 et bilde av utenriksminister Anniken Huitfeldt og lanserte kampanjen «Good morning Norway All squads at battle» med tjenestenektangrep mot norske offentlige portaler og sykehus.

Seksuallovbrytere med seksuelt motiv

Som beskrevet under normalbildet for cyberstøttede seksuallovbrudd mot barn har teknologi utviklet seg til å bli en integrert del av kriminalitetsområdet. Det er viktig å forstå at det dreier seg om kriminalitet begått av mennesker *mot* mennesker, og at lovbruddene i vesentlig utstrekning fører til fysiske konsekvenser, selv om de begås ved hjelp av teknologi. En enkelt aktør kan begå både cyberstøttede og fysiske overgrep. Det kan skje i form av en rekke ulike lovbrudd begått mot samme barn eller separat og mot forskjellige barn. Det er derfor utfordrende å skille mellom aktører som begår fysiske lovbrudd og aktører som begår cyberstøttede lovbrudd da gruppene delvis glir over i hverandre.



Ikke alle aktører med en seksuell motivasjon er pedofile eller har en seksuell interesse for barn. Seksuell interesse utvikles over tid på lik linje med andre interesser, det samme gjelder for seksuelle forstyrrelser.

Gjerningspersonene som begår cyberstøttede seksuallovbrudd mot barn utgjør en stor og sammensatt gruppe og rammer svært mange norske barn årlig. Aktørene har ulike motiver, utfører seksuallovbrudd på forskjellige måter og benytter seg av flere digitale arenaer. Det er likevel slik at de fleste av dem, i likhet med aktører som begår tradisjonelle seksuallovbrudd, er drevet av et ønske om seksuell tilfredsstillelse – til tross for at noen opplever en viss avstand til ugjerningen når de kan gjemme seg bak en skjerm.

Seksuelt motiverte gjerningspersoner er aktører fra alle landsdeler, samfunnslag og i alle aldre, men det er en klar overvekt av mannlige aktører, og de fleste av dem er unge – tenåringer og menn i tju- og trettiårene¹⁰². Unn-

taket er DOB0-kjøpere: menn med en vesentlig høyere gjennomsnittsalder enn andre menn som begår cyberstøttede seksuallovbrudd.¹⁰³

Det er en overvekt av jenter blant de registrerte ofrene, som samsvarer med overvekten av mannlige registrerte seksuallovbrytere og at det er flest personer med heterofil orientering i samfunnet.¹⁰⁴ Samtidig er det nødvendig å presisere at det også finnes kvinnelige overgripere i kategorien seksuelt motiverte aktører. Det foreligger særdeles lite forskning på kvinners seksuelle preferanser overfor barn – dette på et område som samlet sett er lite belyst i forskningslitteraturen.

Ikke alle aktører med en seksuell motivasjon er pedofile eller har en seksuell interesse for barn.¹⁰⁵ Seksuell interesse utvikles over tid

102 Politiet. (2024). *Politiets straffesaksbehandling 2024*. s. 60. <https://www.politiet.no/globalassets/tall-og-fakta/strasak/2024/politiets-straffesaksbehandling-2024.pdf>

103 Kripos. (2023). *Direkteoverførte bestillingsovergrip (DOB0)*. s. 6.

104 Statistisk sentralbyrå. (2021, 26. januar). *Seksuell orientering i befolkningen etter alder (18–79 år)*. <https://www.ssb.no/444196/seksuell-orientering-i-befolkningen-etter-alder-18-79-ar.prosent>.

105 Nasjonalt kunnskapssenter om vold og traumatisk stress. (2023). *Digitale seksuelle overgrep mot barn og unge*. Rapport 3/2023. s. 44. <https://www.nkvts.no/content/uploads/2024/01/NKVTS-Rapport-3-2023-Digitale-seksuelle-overgrep-mot-barn-og-unge.pdf>

på lik linje med andre interesser, det samme gjelder for seksuelle *forstyrrelser*¹⁰⁶. Hva et menneske tenner på kan med andre ord endre seg. Kombinasjonen av å se på pornografi og å få utløsning eller orgasme forsterker en tenning. Dersom man ser på pornografi som er skadelig, eksempelvis pornografi som forestiller en overfallsvoldtekt, kan det gjøre at man utvikler en tenning for dette. Det samme gjelder også for overgrepsmateriale – både ekte og syntetisk. Eksponering for pornografi – eller overgrepsmateriale – kan dermed forsterke og videreutvikle seksuelle interesser og forstyrrelser, i tillegg til å være normaliserende og tillatende.¹⁰⁷

Pedofili er både en seksuell orientering og en psykiatrisk diagnose, og regnes som en seksuell utviklingsforstyrrelse som er medfødt eller etablert i løpet av et menneskes første tre leveår. Tiltrekningen til barn kan gjøre seg gjeldende allerede i slutten av barneskole- eller begynnelsen av ungdomsskolealder. Selv om det foreligger mørketall, anslås det at 1–2 % av befolkningen er pedofile. En kan være både pedofil og samtidig heterofil eller homofil, altså være tiltrukket av barn med et bestemt kjønn. Å være pedofil er ikke ensbetydende med å være kriminell. Det går an å være pedofil uten å begå overgrep, og det går an å være en seksuallovbryter uten å være pedofil.

106 Seksuelle forstyrrelser kjennetegnes av at de medfører intense og vedvarende impulser som er egodystone (tanker, følelser eller handlinger som oppleves som fremmede, uønskede eller i strid med ens verdier og selvilde) og/eller skader andre, direkte eller indirekte, ved at man handler på impulsene. Kilde: Psykologspesialist Svein K. G. Øverland under foredrag for politiansatte. Øverland, S. K. G. (2024, 13. november). *Fortid, framtid, trender, tanker*. Stine Sofies Stiftelse, Grimstad.

107 Nasjonalt kunnskapssenter om vold og traumatisk stress. (2023). *Digitale seksuelle overgrep mot barn og unge* (Rapport 3/2023). s. 47.

En undergruppe av paraplyen seksuelt motiverte aktører, blir seksuelt opphisset av å påføre ofrene sine ydmykelse og smerte. Et slikt tenningsmønster kalles seksuell sadisme¹⁰⁸. Da er det ikke nødvendigvis viktig for aktøren hvem offeret er – om det er en voksen eller et barn. Samtidig vil barn i kraft av å være barn være mer sårbare for utnyttelse enn de fleste voksne, og i så måte enklere ofre. Gruppen er vesentlig mindre enn andre seksuelt motiverte aktører, men er like relevant og utgjør på lik linje med andre aktører en trussel mot barn. Aktørgruppen er også forbundet med annen alvorlig tilleggsproblematikk som ruslidelser, personlighetsforstyrrelser og psykopati.^{109, 110}

Fellesnevneren for de hittil omtalte aktørene er at motivasjonen handler om *tenning*. Når det gjelder mindreårige aktører som begår overgrep mot andre barn, er det mange andre faktorer som også gjør seg gjeldende. Det amerikanske ressurscenteret National Center on the Sexual Behaviour of Youth (NCSBY) peker på fire grunnleggende elementer¹¹¹ for utvikling av problematisk seksuell atferd¹¹²:

1. Sårbarhets- og risikofaktorer
2. Familiære utfordringer
3. Modellering av tvang
4. Modellering av seksualitet

108 Seksuell sadisme tilsvarer (eng:) *coercive sexual sadism disorder (CSSD)*, en ny diagnose i ICD-11, og må ikke forveksles med frivillig seksuell sadisme mellom samtykkekompetente voksne (bedre kjent som S/M eller BDSM). Det nye sykdomsklassifiseringssystemet ICD-11 er enda ikke implementert i Norge, men skal ifølge Helsedirektoratet erstatte ICD-10 i 2028–2029.

109 Nasjonalt kunnskapssenter om vold og traumatisk stress. (2023). *Digitale seksuelle overgrep mot barn og unge* (Rapport 3/2023). s. 54–55.

110 Lunde, A. L. (2017). Å nyte andres smerte. *Tidsskrift for Norsk psykologforening*, (7), ss. 619–621. <https://www.psykologtidsskriftet.no/artikkel/2017as07ae-A-nyte-andres-smerte>

111 De fire faktorene er: (eng:) 1) *Youth vulnerabilities and risks*, 2) *Family adversity*, 3) *Modeling of coercion*, 4) *modeling of sexuality*. Kilde: National Center on the Sexual Behavior of Youth. (2025). *Understanding and Serving Adolescents with Problematic Sexual Behavior: Engaging Youth, Caregivers and Communities*. Dallas.

112 Eng: *Problematic Sexual Behaviour (PBA)*. Se tekstboks på neste side.

Skadelig seksuell atferd (SSA) brukes ofte som paraplybegrep for både problematisk seksuell atferd (PSA) og skadelig seksuell atferd i norsk kontekst.

Skillet mellom problematisk og skadelig seksuell atferd ligger i at skadelig atferd involverer krenkelser, trusler, tvang eller en betydelig maktubalanse, mens problematisk atferd kan være utviklingsmessig upassende eller sårende, men uten samme grad av alvorlig krenkelse eller skade.

Norges regionale ressursentre om vold, traumatisk stress og selvmordsforebygging (RVTS) er inne på det samme i sin beskrivelse av årsaker til atferden. Det kan handle om (1) egenskaper ved barnet som resulterer i impuls-handlinger (for eksempel en ADHD-diagnose) og uheldig eksperimentering med seksualitet. Det kan også dreie seg om (2) følelsesmessig, fysisk eller seksuelt misbruk eller omsorgssvikt.

I tillegg kan det ha sammenheng med hva barnet har observert, for eksempel (3) vold og tvang utført av en forelder mot en annen, eller at (4) voksne har hatt sex foran barnet.

Barn og unge har i stor utstrekning tilgang til teknologi og seksuelt medieinnhold som pornografi, ofte uten tilsyn fra voksne, som kan påvirke deres seksuelle utvikling. Forskning viser at eksponeringen kan medføre økt risiko for problematisk seksuell atferd, sammenlignet med ungdom som ikke blir eksponert for slikt innhold.¹¹³ Dette samsvarer med barn og unges opplevelse av at pornografi i liten grad formidler viktige verdier som samtykke og gjensidighet, og at pornografi har ført til deltakelse i seksuelle handlinger de unge opplevde som grenseoverskridende, smertefulle og krenkende.¹¹⁴ Medieoppslag har videre framlagt dokumentasjon på en økning i risikofylt praksis, som kvelertak under sex, hvor tendensen knyttes til pornografi. Samlet peker dette på et komplekst samspill mellom teknologisk tilgjengelighet, eksponering for seksuelt innhold og ungdoms seksuelle utvikling – både sunn og usunn. Mindreårige seksuallovbrytere bidrar

113 Mori, C., Park, J., Racine, N., Ganshorn, H., Hartwick, C., & Madigan, S. (2023). Exposure to sexual content and problematic sexual behaviors in children and adolescents: A systematic review and meta-analysis. *Child Abuse & Neglect*, 143, Article 106255. <https://doi.org/10.1016/j.chia-bu.2023.106255>

114 Redd Barna Norge. (2021). *Et skada bilde av hvordan sex er: Ungdoms perspektiver på porno*, ss. 20–26. https://resourcecentre.savethechildren.net/pdf/rapport_et_skada_bilde_av_hvordan_sex_er_ungdoms_perspektiver_pay_porno.pdf

dermed til at gruppen seksuelt motiverte aktører blir ytterligere kompleks.

Selv om det går an å utvikle en seksuell interesse for barn gjennom eksponering for overgrepsmateriale, vet man ikke om det er en sammenheng mellom bruk av overgrepsmateriale og det å begå overgrep mot barn. Det man imidlertid vet noe om, er at bruk av overgrepsmateriale er den sterkeste indikasjonen på en seksuell interesse for barn, enten den er medfødt (pedofili) eller utviklet over tid (seksuell interesse/forstyrrelse). tillegg vet man at mange aktører som er domfelt for seksuelle overgrep mot barn, også har hatt befatning med overgrepsmateriale.

Politiets primærstrategi er å forebygge kriminalitet. Det er dermed politiets jobb å forebygge at barn blir utsatt for seksuelle overgrep. For å forebygge seksuallovbrudd mot barn, må vi forstå hvilke drivkrefter som får gjerningspersonene til å begå overgrep – både hva som skyldes en indre motivasjon og hva som kan tilskrives ytre påvirkning. Det finnes ikke et enkelt, utvetydig svar på dette, og det eksisterer mange kunnskapshull. Samtidig vet vi en del om hvilke mekanismer som gjør seg gjeldende, og kan slå fast at dette ikke er et problem som kan løses av politiet alene. Det er behov for mer forskning, økt kunnskapsdeling, videreutvikling av behandlingstiltak, lover og regler som holder tritt med teknologisk utvikling og fornyet seksualundervisning når det kommer til sunn seksuell utvikling og atferd.

Delvurderinger

Seksuelt motiverte aktører er en mangfoldig gruppe mennesker med sammensatte og nyanserte motivasjoner og preferanser. Aktørene utgjør derfor en stor og uoversiktlig trussel som er utfordrende å håndtere. Gjerningspersonene benytter i økende grad digitale muliggjørere for å etablere kontakt, gjennomføre og dokumentere overgrep mot barn, samt ivareta anonymitet, skjule aktivitet og effektivisere steg i kriminalitetsutøvelsen. Det er *meget sannsynlig* at teknologien fungerer som en akselerator for seksuelt motiverte aktører, og det er *meget sannsynlig* at forekomsten av overgrep mot barn vil opprettholdes i det kommende året.

Mindreårige som begår seksuallovbrudd mot barn tilfører ytterligere kompleksitet til aktørgalleriet, hvor utvikling av seksuelt problematisk og skadelig atferd har en rekke årsaker. Det er imidlertid *sannsynlig* at tilgang på teknologi, høy grad av eksponering for seksuelt medieinnhold og manglende kontrollmekanismer fører til at flere mindreårige vil begå seksuallovbrudd mot barn enn tidligere.

Den globale framveksten av syntetisk overgrepsmateriale øker den totale mengden tilgjengelige bilder og videoer som viser seksuelle overgrep mot barn. Det er *mulig* at en slik økt tilgjengelighet i kombinasjon med økt distanse fra ekte¹¹⁵ barn som blir utsatt for ekte overgrep fører til at flere personer utvikler en seksuell interesse for barn. Det er *mulig* at eksponering for overgrepsmateriale gjør at aktører med en seksuell interesse for barn tar steget fra å se på overgrep til å begå egne overgrep, både digitalt og fysisk.

Uklassifiserte aktører

Denne kategorien omfatter aktører som ikke naturlig faller inn under de øvrige profilene, eller der motivasjonen foreløpig er ukjent. Enkelte kan handle ut fra personlige drivkrefter som spenning, nysgjerrighet eller hevn. Andre kan begå kriminelle handlinger simpelthen fordi de har teknisk evne til det og ønsker å bevise noe for seg selv eller andre. På denne måten kan de eksempelvis oppnå status i digitale miljøer. Kategorien viser at ikke alle cyberkriminelle følger tydelige mønstre. Bedre oversikt over denne

gruppen kan redusere risikoen for sorte svaner – altså uforutsette, ukjente fenomener.

Kultmedlemmer / The Com – ekstreme voldelige nettsamfunn

I denne rapporten har Kripos valgt å omtale aktører som inngår i ekstreme, voldelige nettsamfunn *kultmedlemmer*. Som nevnt på side 29 og 47–48, er dette et fenomen som først ble registrert i Norge i 2022, og hvor det er registrert en økning i 2025, både nasjonalt og internasjonalt. Kultmedlemmer er, basert på Kripos' nåværende innsikt, plassert under profilen uklassifiserte aktører. Det skyldes at kultmedlemmenes motivasjon framstår uklar og sammensatt. Det er imidlertid noen likhetstrekk som går igjen og danner et generelt bilde av aktørene.

Selv om kultmedlemmer kjennetegnes av å ha gjennomgått en form for radikaliseringsprosess og noen av dem har utviklet et ekstremistisk tankegods, drives de i utgangspunktet ikke av hverken politiske eller religiøse mål, selv om noen har knytninger til høyreekstreme miljøer. De drives av såkalt *nihilistisk* voldelig ekstremisme, som baserer seg på et generelt hat mot samfunnet hvor målet er å skape kaos og sosial ustabilitet. Nettverkene er ofte organisert rundt karismatiske ledere, som i andre kulturer og sekter.

¹¹⁵ Grunnlagsmodeller som genererer syntetisk overgrepsmateriale har på et tidspunkt tatt utgangspunkt i ekte barn, både barn som har blitt utsatt for overgrep og barn som ikke har det. Med *ekte* menes her faktiske bilder og videoer av faktiske barn.

Kripos er også kjent med at de fleste kultmedlemmer søker aksept, tilhørighet, popularitet og anerkjennelse. Jo mer ekstrem man er og jo mer alvorlige handlinger man får ofre til å begå, desto høyere status oppnår man blant andre kultmedlemmer. Det framstår av den grunn som at mange av aktørene ønsker å ta del i et fellesskap og å bli sett, og at isolasjon, utenforskap og annerledeshet dermed kan være faktorer som enten får aktørene til å søke seg til nettsamfunnene eller gjør dem enklere for andre aktører å rekruttere. Det er ikke kjent hvorvidt aktørene selv forstår hva de motiveres av eller har et bevisst forhold til dette. Det er sett tilfeller av at ofre blir til gjerningspersoner som deretter finner nye ofre. I mange tilfeller deles det veiledninger om hvordan kultmedlemmer skal gjøre forberedelser, identifisere ofre, lure og manipulere ofre og deretter presse dem til å begå alvorlige handlinger. Forberedelsene innebærer ulike tiltak for å heve operasjonssikkerheten og gjøre det vanskelig for politiet å identifisere dem. Kripos er kjent med at brukernavn aktørene benytter ofte er uten

Følgende endringer i barn og unges atferd kan indikere at de er utsatt for påvirkning fra farlige nettmiljøer:

Hemmelighold om nettaktiviteter – skjuler skjermen når noen nærmer seg, bruker flere eller anonyme kontoer.

Tilbaketrekking og isolasjon – tilbringer overdreven mye tid alene, distanserer seg fra familie og venner.

Følelsesmessige plager – har plutselige humørsvingninger, virker engstelig eller deprimeret.

Interesse for skadelig innhold – viser interesse for vold, mørke temaer, ekstremistiske ideologier eller grafisk materiale.

Endringer i språk eller symbolbruk – bruker ukjent slang, ekstremt språk, koder eller symboler som kan være knyttet til ekstreme nettmiljøer.

Skjuler fysiske tegn på skade – går med klær som dekker over for selvskading, bitemerker, brannskader, utskjæringer, eller andre skader eller markeringer.

geografiske kjennetegn, og det er vanlig at kultmedlemmer kommuniserer på engelsk. I tillegg har Kripos observert at gruppene i liten grad samles i nasjonale fellesskap, som gjør at nettverkene nesten utelukkende er internasjonale.

Politiet får informasjon som avdekker personer knyttet til ekstreme, voldelige nettsamfunn gjennom ordinære tips om deling av overgrepsmateriale, for eksempel fra NCMEC. Det er ofte uklart innledningsvis om personen det tipses om er en gjerningsperson eller om det er et offer som har blitt truet eller presset til å dele overgrepsmateriale av seg selv.

Gjerningspersonene er primært gutter i alderen 12–25 år. Dette gjelder også for de norske aktørene. I flere av de norske sakene er det registrert at svært alvorlig kriminalitet innenfor volds- og seksuallovbrudd har blitt begått eller har vært under planlegging.

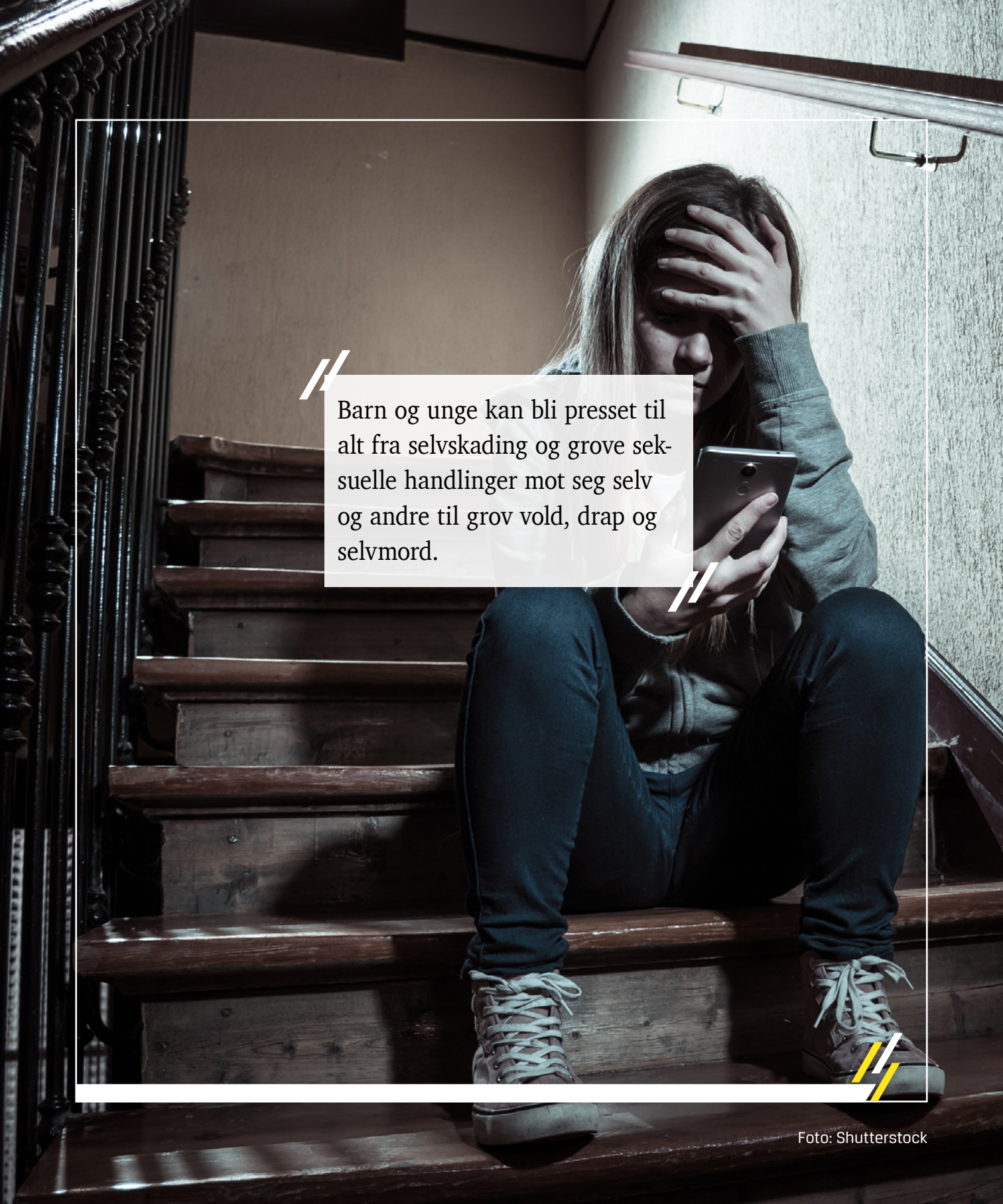
Fenomenet er bekymringsverdig da det kan være vanskelig å avdekke og kan få svært alvorlige konsekvenser. Barn og unge kan bli presset til alt fra selvskading og grove seksuelle handlinger mot seg selv og andre til grov vold, drap og selvmord. Det er viktig at både politiet og samfunnet for øvrig er kjent med at ekstreme, voldelige nettsamfunn eksisterer, og vet hvilke faresignaler man skal være på utkikk etter.

Delvurderinger

Kultmedlemmers motivasjon framstår utydelig og er *sannsynlig* sammensatt, som gjør trusselen vanskelig å identifisere, avdekke, etterforske og forebygge. Det er *sannsynlig* at en rekke kultmedlemmer heller ikke selv vet hva de motiveres av, men det er samtidig *sannsynlig* at de ønsker en form for anerkjennelse og tilhørighet, som driver dem til å begå handlinger de normalt ikke ville gjort.

Kultmedlemmer er opptatte av operasjons-sikkerhet, kommuniserer oftest på engelsk og benytter i stor grad krypterte plattformer. I tillegg er organiseringen av nettverkene uoversiktlig, de har forgreininger over hele kloden og er stadig ekspanderende. Det er derfor *sannsynlig* at politiet vil ha utfordringer med å identifisere kultmedlemmer som begår kriminalitet mot norske barn og unge.

Det er *sannsynlig* at en del av aktørene er sårbare for påvirkning og dermed lettere å manipulere og radikalisere. Det er imidlertid også *sannsynlig* at en del av aktørene er tiltrukket av det normbrytende, og derfor *mulig* at de like gjerne kunne blitt involvert i grupperinger som driver pedo-hunting eller rekruttert av kriminelle nettverk til bestillingsvold, som ekstreme, voldelige nettsamfunn.

A young woman with long brown hair is sitting on a set of wooden stairs. She is wearing a grey hoodie, dark blue jeans, and brown sneakers with white laces. Her right hand is covering her face, and her left hand is holding a black smartphone. The background is a plain wall with a metal handrail. The lighting is dramatic, with strong shadows.

// Barn og unge kan bli presset til alt fra selvskading og grove seksuelle handlinger mot seg selv og andre til grov vold, drap og selvmord. //

Prosesser og metoder innen cyberkriminalitet

I dette kapittelet ønsker Kripos å redegjøre for cyberkriminelle *angrepsfaser* og *målutvelgelsesprosesser*. Figur 6 tar for seg roller og muliggjørere og projiserer dem innenfor cyberrettet og cyberstøttet kriminalitet, samt kriminalitet som foregår utenfor det digitale rom (slik det framkommer i figur 1). Man får da en bedre oversikt over kriminalitetens forskjellige avhengigheter til det digitale rom, og figur 6 utvider dermed det analytiske rammeverket.

Angrepsfaser og virkemidler

Angrepsfasen i et cyberangrep bør forstås som en prosess med flere delmål, beslutningspunkter og involverte aktører. Grad av målretthet, sofistikasjon, motivasjon og intensjon kan variere gjennom hele prosessen, avhengig av aktøren og motivet bak handlingen.

Som illustrert i Figur 3 på side 56 (*Cyberkriminalitetens ontologi*) må kriminelle aktører som regel gjennom flere steg (delmål) for å oppnå sitt endelige mål.¹¹⁶ Derfor kan cyberrettet kriminalitet sammenlignes med en stafett – ikke en sprint – der stafettpinnen bytter hånd

flere ganger før endemålet nås. Underveis er det flere beslutningspunkter der trusselaktøren tar beslutninger basert på informasjonen vedkommende har tilegnet seg fram til det punktet. Beslutningene påvirker hvordan angrepet utvikler seg videre.

Stegene i angrepsfasen varierer ut fra hvilken type kriminalitet som begås, aktørenes handlemåter og motiv. Likevel har politimyndigheter og private sikkerhetsselskaper gjennom etterforskninger avdekket generelle likhetstrekk i angrepsfasene ved blant annet cyberangrep med løsepengevirus,¹¹⁷ bedragerier¹¹⁸ og seksuallovbrudd¹¹⁹.

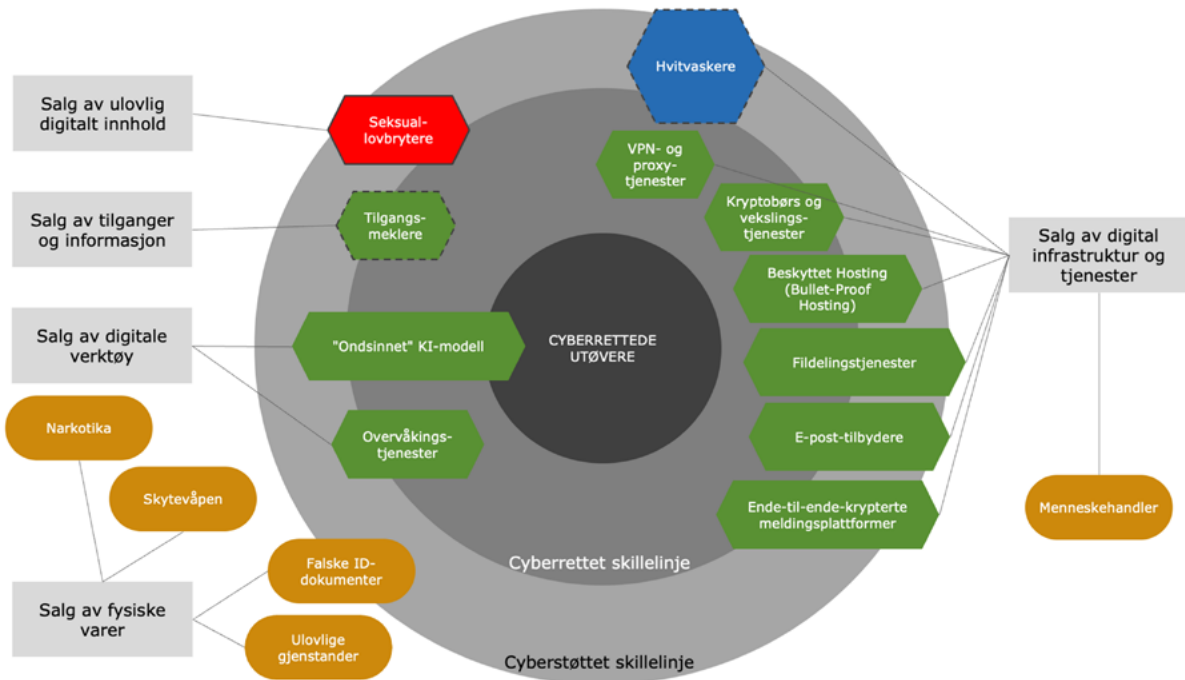
Kartlegging av beslutningspunkter, delmål og involverte aktører i en angrepsfase gir relevant innsikt i samhandlingsdynamikkene mellom de ulike aktivitetene og rollene som ble presentert i Figur 4 (*ARPA-rammeverket*) på side 60. Denne innsikten avdekker muligheter for forstyrrelser og målrettede tiltak, og må vurderes i lys av sammensatt virkemiddelbruk og statlige aktørers interesse for informasjon som omsettes av kriminelle.

116 Europol. (2025). *Internet Organised Crime Threat Assessment (IOCTA)*. ss. 13–15.

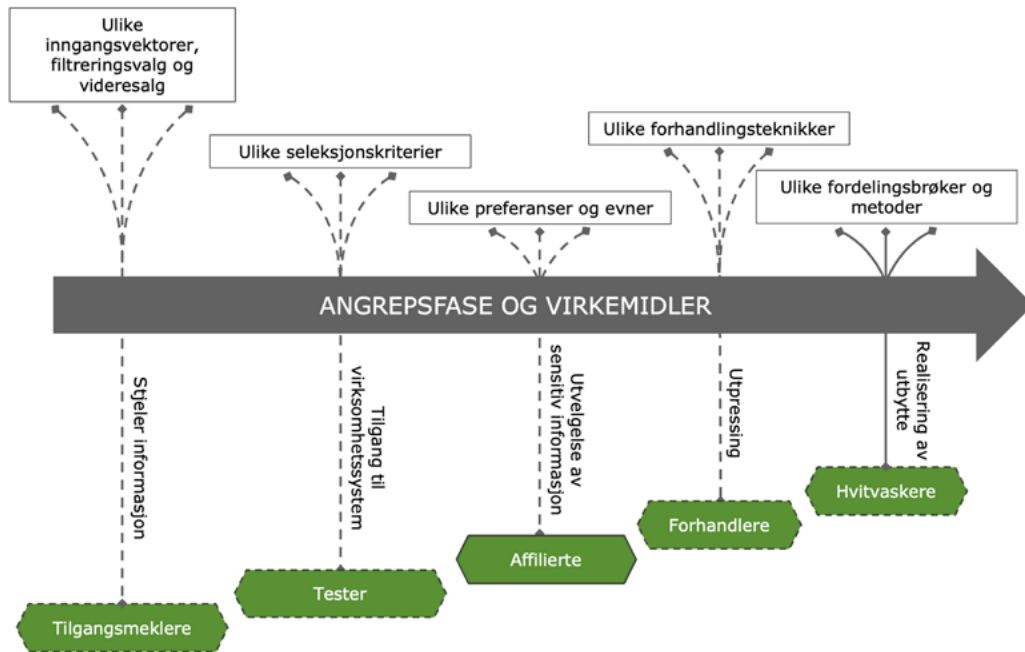
117 For eksempel illustrert av Europol gjennom Cyber Kill Chain® og MITRE ATT&CK®.

118 For eksempel illustrert gjennom Fraud Kill Chain, Check Fraud Kill Chain og Financial Fraud Kill Chain.

119 For eksempel illustrert av Kripos gjennom modellen *Typiske framgangsmåter for kontaktetablering med barn* i rapporten *Cyberkriminalitet 2025*, s. 81.



Figur 6: Avhengigheter til det digitale rom. Modellen illustrerer at vi finner de samme rollene og muliggjørerne i både cyberrettet og cyberstøttet kriminalitet. Plasseringen indikerer i hvilken grad rollen eller muliggjøreren ansees som cyberrettet (nest innerste sirkel), cyberstøttet (ytterste sirkel) eller utenfor det digitale rom (området utenfor sirkelen). Sistnevnte faller utenfor definisjonen av cyberkriminalitet, men er inkludert i modellen for å vise at det er kort avstand mellom det digitale og fysiske domenet. I tilfeller der samme rolle eller muliggjørere overlapper flere sirkler, betyr dette at ulike kvaliteter ved rollen/muliggjøreren kan plasseres på flere steder langs det cyberkriminelle spekteret. Sekskanter er roller (tilretteleggere og utøvere) og ellipser er muliggjørere. Tilretteleggere er markert med en stiplet kantlinje og utøvere med en heltrukken linje. Det som hovedsakelig faller utenfor det digitale rom er illustrert i oransje. Av det som befinner seg i det digitale rom er roller, illustrert i rød, og muliggjørere, illustrert i grønn. Muliggjøreren «Ondsinnnet» KI-modell overlapper den innerste sirkelen (digitale utøvere) for å illustrere at KI-agenter har potensial til å fungere som selvstendige utøvere uten menneskelig involvering. Modellen er utviklet av Kripas.



Figur 7: Eksempel på angrepsfase for et cyberangrep uten krypteringsvirus. Modellen viser fem beslutningspunkter (tekstbokser over prosesspilen) og fem delmål/endemål (tekst under prosesspilen). De stiplede linjene er delmål, den heltrukne linjen er endemål. De grønne symbolene nederst knytter målsetninger og beslutninger til de involverte aktørene (sekskant med stiplet linje er tilretteleggere og sekskant med heltrukken linje er utøvere). Forløpet spenner fra valg av inngangsvektor (beslutningspunkt) som tilgangsmekleren (involvert aktør) benytter for å stjele informasjon (delmål), til hvordan utbyttet skal hvitvaskes og fordeles (endemål) mellom involverte aktører. Ved hvert beslutningspunkt påvirker ulike preferanser og kriterier hvordan angrepet utvikler seg. Enkelte beslutningspunkt kan derfor være høyt målrettede, andre mer opportunistiske. Tilsvarende kan noen delmål/endemål utføres med høyteknologiske, cyberrettede virkemidler, mens andre med lavteknologiske og cyberstøttede virkemidler. Modellen er utviklet av Kripas.

Figur 7 illustrerer et eksempel på hvordan angrepsfasen kan se ut.

En cyberrettet angrepsprosess kan starte ved flere beslutningspunkter, men starter som regel med et datainnbrudd. Slike datainnbrudd har utviklet seg fra relativt enkle operasjoner med få delmål til komplekse forløp med en rekke delmål (tiltak) for å omgå sikkerhetsmekanismer hos brukeren. Den økte vanskelighetsgraden har bidratt til større spesialisering og arbeidsfordeling blant de kriminelle aktørene og på den måten skapt nye roller og aktiviteter i det cyberkriminelle økosystemet. På den annen side kan én og samme person utfylle alle rollene og gjennomføre hele angrepsprosessen alene. En slik helhetlig tilnærming, der den samme aktøren utfører alle delmål fra start til slutt, er uvanlig innen cyberrettet, men vanligere innen cyberstøttet – eksempelvis noen typer seksuallovbrudd.

Kripos erfarer at ulike informasjonsmeklere¹²⁰ bruker de samme virkemidlene og handlemåtene, men selger informasjon eller tilganger til ulike kjøpere. For eksempel kan en informasjonsmekler (1) selge store, usorterte datapakker av lavere kvalitet på kriminelle markedsplasser, (2) selge tilganger til virksomheter som er attraktive mål for løsepengevirusaktører, eller (3) selge informasjon av interesse for en statlig aktør gjennom åpne eller lukkede kanaler. Hvert

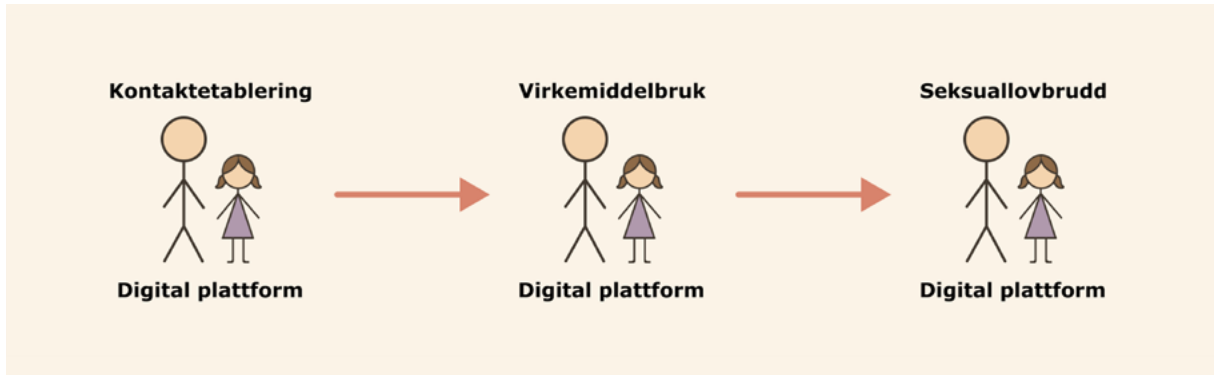
av disse tilfellene innebærer ulike relasjoner, samarbeidsmekanismer, kommunikasjonsplattformer og involverte aktører.

Målutvelgelse og kontaktetablering – cyberstøttede seksuallovbrudd

Cyberstøttede seksuallovbrudd mot barn favner flere ulike lovbrudd, og det er forskjell på hvilke som rammer barn *direkte* – eksempelvis ved at gjerningspersonen skriver seksualisert til et barn på en sosial medieplattform – eller *indirekte* – som at to aktører utveksler overgrepsmateriale de har skaffet seg på internett. Dette delkapittelet vil ta for seg seksuallovbrytere som direkte utsetter barn for cyberstøttede seksuallovbrudd, uavhengig av aktørens profil, den grunnleggende motivasjonen.

Når det gjelder seksuallovbrudd mot barn er det vanligst at alle delmålene mot endemålet begås av samme gjerningsperson. Prosessen fra kontakt opprettes til et seksuallovbrudd er fullbyrdet, gjennomføres ofte av én og samme aktør. Kripos erfarer også at aktørers tilnærming til barn i de fleste tilfeller er tilfeldig, selv om det forekommer at aktører ser seg ut et bestemt barn. Gjerningspersonene benytter seg ofte av en kvantitativ framgangsmåte, eksempelvis ved å legge til en rekke brukere på Snapchat, eller ved å logge seg på en chatroulette-plattform og bevege seg fra den ene videosamtalen til

¹²⁰ Informasjonsmeklere er mennesker som kjøper og selger informasjon.



Figur 8: En forenklet framstilling av framgangsmåten som benyttes av aktører som ønsker å etablere kontakt med og utsette barn for seksuallovbrudd. Ses i sammenheng med figur 13 på side 81 i *Cyberkriminalitet 2025*. Modellen er utviklet av Kripas.

den andre for å lete etter potensielle ofre.

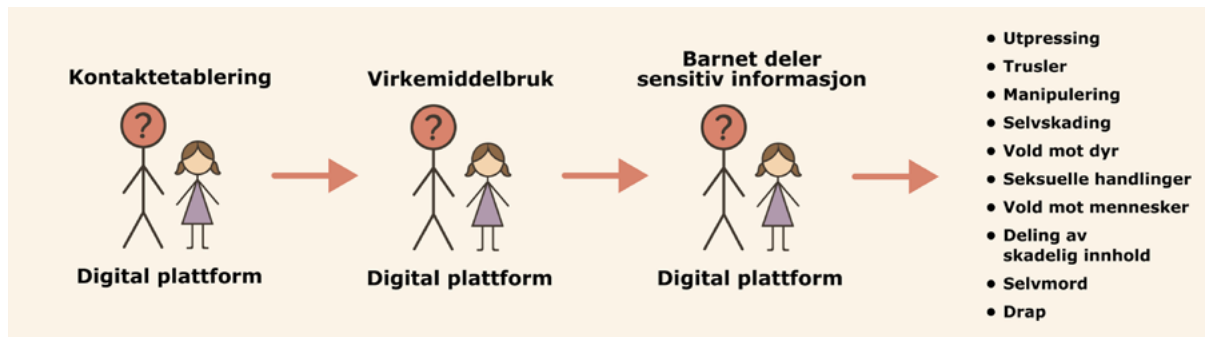
Samtidig er mange seksuallovbrytere preferansedrevne¹²¹ – de har gjerne noen foretrukne karakteristikker de ser etter i målutvelgelsesfasen. Flere aktører som er drevet av seksuell motivasjon oppsøker eksempelvis aktivt arenaer som er populære blant barn i en viss aldersgruppe. Dersom aktøren er tiltrukket av prepubertale gutter, kan aktøren for eksempel delta i en server på Discord sentrert rundt et videospill som spilles av mange gutter i foretrukket alder.

Blant mer målrettede aktører er kultmedlemmer som aktivt leter etter sårbare barn og unge. Det går fram i en rapport av Europol om ekstreme, voldelige nettsamfunn¹²² at disse ofrene

framstår som enklere å manipulere og oppnå tillit hos enn andre personer. Mindreårige mellom 8 og 17 år som eksempelvis sliter med depresjon eller selvmordstanker, barn og unge som tilhører LHBTQ+-miljøer og barn med minoritetsbakgrunn, er særlig utsatte. Det er registrert at kultmedlemmer blant annet benytter nettbaserte støttegrupper og selvhjelpssamfunn som arena for å finne ofre. De bygger tillit, samler inn personlig informasjon om barnet, flytter kommunikasjonen til en kryptert kommunikasjonsplattform og bruker den personlige informasjonen til å presse og true barnet til alvorlige handlinger som grov selvskading eller seksuell omgang med seg selv eller andre. Barnet presses deretter til å

¹²¹ Preferanse refererer til en hva en person foretrekker i valget mellom flere ting.

¹²² Europol. (2025). *The rise of online cult communities dedicated to extremely violent child abuse*.



Figur 9: En forenklet framstilling av kultmedlemmers framgangsmåte for å etablere kontakt med sårbare barn og unge og hva ofrene utsettes for eller presses til å gjøre. De ulike utfallene helt til høyre er ikke uttømmende. Modellen bygger på figur 12 på side 76 i Cyberkriminalitet 2025, som viser eksempler på faser i seksuell utpressing med seksuelt og økonomisk motiv. Modellen er utviklet av Kripas.

dokumentere handlingen og dele materialet med kultmedlemmet, ofte som ledd i en rekke andre alvorlige handlinger. Det er også informasjon om at aktører rekrutterer nye medlemmer til nett-samfunnet. Disse begynner gjerne som ofre og presses eller forledes til å rekruttere nye ofre på et senere tidspunkt.

Noen aktører har en opportunistisk tilnærming til kriminaliteten ved at de begår overgrep når muligheten byr seg, uten at det framstår som den opprinnelige intensjonen. Et eksempel på dette er DOBO-kjøpere som får tilbud om å kjøpe direkteoverførte overgrep mot jenter når de egentlig var ute etter direkteoverført pornografisk innhold av voksne kvinner. En annen form for opportunistisme gjelder profittmotiverte utpressere som hovedsakelig går etter voksne

menn med betalingsevne. Dersom utpresseren oppnår kontakt med en mindreårig gutt, vil utpresseren allikevel forlede gutten, få ham til å dele et nakenbilde av seg selv og deretter presse ham for penger.

Teknologi gir aktører som begår cyberstøttede seksuallovbrudd mot barn et utvidet handlingsrom. Som nevnt i tidligere utgaver av rapporten, sørger digitale muliggjørere for at aktører lettere kan skjule sin identitet, enklere kan forlede barn, har flere arenaer å nå barn på og kan ramme flere barn raskere. I tillegg gjør fravær av kontrollmekanismer det mulig for aktøren å begå overgrepene. I et cyberrettet perspektiv kan man si at det eksisterer ingen brannmur, alternativt eksisterer den, men den er ikke konfigurert – det er noen porter som står åpne.

Manglende kontrollmekanismer gjelder både *sikkerhet og trygghet*¹²³. Det kan være alt fra den respektive plattformens evne til å beskytte barn mot kriminalitet på egen plattform – sikkerhet – til foreldres involvering i barnas liv og aktiv bruk av tilgjengelig foreldrekontrollfunksjon på den aktuelle plattformen – trygghet.

Målutvelgelse – cyberrettet kriminalitet

Dette delkapittelet bygger videre på eksemplet i Figur 7. Tilgangsmekleren kan i første steg av angrepsfasen skaffe påloggingsinformasjon eller tilganger gjennom eksempelvis phishing¹²⁴ mot store e-postdatabaser eller via ondsinnede nettsider som rangerer høyt i søkemotorer¹²⁵. Disse metodene innebærer å kaste ut vide nett for å treffe flest mulig internettbrukere. Tilgangsmekleren kan for eksempel videreselge pålog-

gingsinformasjon (brukernavn og passord), eller skaffe tilganger ved å installere skadevare¹²⁶ som innlemmer brukernes datamaskin i et botnet¹²⁷.

I begge tilfeller kan en tilgangsmekler verdivurdere materialet etter ulike seleksjonskriterier. Påloggingsinformasjon kan for eksempel sorteres etter toppdomene, navn og passordstyrke. Tilganger via kompromitterte datamaskiner vurderes etter mer tekniske kriterier som informasjonskapsler, IP-adresse, operativsystem, datamaskinnavn, digitale lommebøker og om maskinen har antivirus. Med gitte filtreringsvalg kan de kompromitterte systemene deles inn i kategorier. For eksempel (1) høyverdimål, (2) vanlige brukere og (3) uinteressante systemer. Tilgangsmekleren kan da tilby nedlasting av løsepengevirus til «høyverdimål», installere

123 Bruken av de engelske begrepene *security* og *safety* i cyber-kontekst innebærer en forskjell mellom *security* (sikkerhet), som beskytter data og datasystemer fra tilsiktede trusler som hacking og skadevare, og *safety* (trygghet), som beskytter mennesker fra utilsiktet skade eller risiko.

124 I dette tilfellet kunne tilgangsmekleren sendt ut en mail og fått internettbrukeren til å klikke på en ondsinnet lenke eller laste ned et vedlegg.

125 Kjent som søkemotorforgiftning. Eng: *SEO Poisoning*.

126 Som regel en dropper. En dropper er en type dataprogram som er utviklet for å installere (eng: *to drop* – å slippe) andre skadevarer på et datasystem, gjerne innlastere (eng: *Loader*) og informasjonsstjeler (eng: *Stealer*). Det blir stadig vanligere at én skadevare kombinerer flere funksjoner. Dropperen inkluderer vanligvis ikke ondsinnet kode, da dataprogrammet er laget for å unngå sikkerhetsmekanismer (eksempelvis antivirus) på fornærmedes datamaskin.

127 Botnet er et nettverk av kompromitterte datamaskiner og andre internetttilkoblede enheter som er infisert med skadevare og som dermed kan fjernstyres ulovlig.



informasjonsstjeler hos «vanlige brukere» og forkaste «uinteressante systemer».

Det er naturlig at tilgangsmeklere som kaster ut vide nett, benytter kvantitative seleksjonskriterier for å håndtere store datamengder. Dersom påloggingsinformasjon eller tilganger selges videre til en USH-gruppering, er det ofte kvalitative seleksjonskriterier som styrer neste steg. Eksempler på kriterier hos en USH-gruppering kan være virksomhetsrelaterte¹²⁸, sårbarhetsrelaterte¹²⁹, sikkerhetsrelaterte¹³⁰, politiske

forhold¹³¹, samt grunner til å *ikke* ramme enkelte virksomheter¹³². Disse kriteriene kan raskt endre seg, og ulike begrensninger kan gjelde for affilierte som benytter en LSH-skadevare, og for LSH-skadevarens kjernegruppe. I et tilfelle hvor tilgangen er skaffet via et tredjepartsangrep¹³³ eller verdikjedeangrep¹³⁴, endrer målutvelgesprosessen seg betydelig. Samlet understreker dette utfordringer med trusselvurderinger som er basert på skadevaretype alene.

Kripas har ingen opplysninger som tilsier at

128 For eksempel omsetning, registreringsland, antall ansatte og bransje, samt sannsynligheten for at virksomheten vil forsøke å unngå offentlig omtale og omdømmetap.

129 For eksempel sektorspesifikke og bransjespesifikke sårbarheter, eller sårbarheter i felles teknologisk infrastruktur.

130 For eksempel sannsynligheten for at virksomheten anmelder saken til politiet, og om politiet vil prioritere saken med etterforskningsressurser.

131 For eksempel økt etterspørsel etter tilganger til israelske og amerikanske virksomheter i kjølvannet av krigen i Gaza.

132 Enkelte LSH-grupperinger har eksplisitte føringer for hvem som ikke skal rammes, eksempelvis veldedige organisasjoner som arbeider for barn, helseforetak, energisektoren, skoler og militær sektor. Begrunnelsen kan være frykt for straffeforfølgelse eller interne moralske føringer.

133 Tredjepartsangrep innebærer at en aktør 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.

134 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.

norske virksomheter er utsatt for løsepenge-virusangrep *fordi* de er norske. Dette utelukker ikke at enkelte norske virksomheter kan være utvalgte mål, men Kripas kjenner ikke til tilfeller der norske virksomheter i seg selv har vært et seleksjonskriterium for profittmotiverte USH-nettverk. Det motsatte er imidlertid observert for hacktivist, som også kan bruke krypteringsvirus og begår datatyveri.

Det er krevende å fastslå hva som faktisk har skjedd under et cyberangrep og hvordan fornærmede er rammet uten å etterforske forholdet. I etterforskningen er politiets hovedfokus å identifisere gjerningspersonen – ikke å rekonstruere tenkningen bak målutvelgelsesprosessen. Som del av den innledende etterforskningen følger politiet sporene tilbake til utgangspunktet. Der som politiet ser at eksempelvis påloggingsinformasjon eller systemtilganger er samlet inn med et *vidt nett*, kan angrepet bli tolket som opportunistisk. Å følge sporet bakover fra åstedet til utgangspunktet beskriver imidlertid bare hvor dataen kom fra – ikke hvordan gjerningspersonen tenkte og hvilke valg gjerningspersonen tok underveis, som det går fram av beslutningspunktene i angrepsfasen (Figur 7). Hensikten med å beskrive angrepsfasen er å redegjøre for forløpet fra valg av inngangsvektor til utnyttelse og målrealisering, ofte med flere involverte aktører, beslutningspunkter, preferanser og avveininger. Cyberangrep som framstår å springe ut fra en opprinnelig bred og opportunistisk tilgang, kan ha vært ledsaget av målret-

tede valg på flere stadier i angrepsprosessen. Etterforskningssporet gir ofte et bakoverblikk på informasjonens opphav, mens forståelse av angrepsfasen og trusselaktørens grad av målrettethet krever et foroverblikk på beslutningene som formet veien fram til endemålet.

Kriminelle nettverks bruk av digitale muliggjørere

Som nevnt har den teknologiske utviklingen gitt kriminelle nettverk et nasjonalt og globalt handlingsrom til å utvide sin virksomhet. Internett fungerer som en markeds plass for alt fra narkotikahandel til kjøp av kriminelle tjenester. Gjennom sosiale medier og krypterte plattformer kan nettverkene nå et langt større publikum, rekruttere nye deltakere og selge varer og tjenester anonymt uten fysisk kontakt. Teknologien har gjort det meget enkelt for utenlandske aktører å etablere seg i Norge, hvor spesielt svenske nettverk har gjort sitt inntog den siste tiden.

Kriminelle nettverk utnytter i økende grad teknologiske plattformer til å rekruttere personer til å utføre ulike oppgaver i sin virksomhet – som transport, oppbevaring og salg av narkotika, samt hvitvasking av penger. Rekrutteringen skjer både åpent og skjult, og det er avdekket forsøk på å rekruttere personer innenfor yrker med tilgang til informasjon, varer eller tjenester som kan misbrukes.

Kriminelle nettverk har tradisjonelt hatt en sterk og hierarkisk struktur med tydelig leder-

skap og rollefordelinger. Framveksten av KSH i det digitale rom har gjort strukturen mer fragmentert og fleksibel hos enkelte kriminelle nettverk – spesielt nettverk som er sterkt digitaliserte. Aktører samarbeider i større grad på tvers av nettverk og landegrenser, hvor profitt tillegges mer vekt enn lojalitet.

Denne utviklingen har likheter med det cyberkriminelle økosystemet, hvor spesialisering og kjøp av tjenester og kompetansebasert samarbeid er grunnleggende. Mens de cyberkriminelle nettverkene er fullstendig digitale, opererer kriminelle nettverk i et hybridrom hvor det fysiske og digitale kombineres.

Den største ulikheten er at cyberkriminelle kan operere globalt uten å forlate datamaskinen, mens de tradisjonelle kriminelle nettverkene er avhengig av lokal tilstedeværelse og fysisk gjennomføringsevne i områdene der de opererer. Teknologi fungerer derfor primært som en styrkemultiplikator for eksisterende kriminalitet, og ikke en erstatning for fysisk kapasitet. Teknologien brukes som digital muliggjørere for å effektivisere logistikk, rekruttere personer i lokale roller, kommunisere trygt og redusere oppdagelsesrisikoen for bakmenn.

Delvurderinger

Det er *meget sannsynlig* at kriminelle nettverk kommer til å fortsette å integrere teknologiske hjelpemidler for å effektivisere driften og maksimere profitten i sin ulovlige virksomhet. Det er *mulig* at dette på sikt kan viske ut skillelinjer mellom kriminelle nettverk og cyberkriminelle nettverk, da kriminelle nettverk i stadig økende grad blir avhengige av digitale muliggjørere for å optimalisere virksomheten.

Utviklingen av vold som handelsvare

Utviklingen av KSH har gitt kriminelle nettverk anledning til å overføre konseptet til vold som handelsvare (VSH)¹³⁵. Gjennom digitale plattformer kan kriminelle nettverk nå ut til et bredt publikum – særlig unge, sårbare personer – som lokkes, forledes, motiveres eller presses til å utføre volds handlinger på vegne av det kriminelle nettverket.

Spesielt svenske kriminelle nettverk som nylig har etablert seg i Norge, bruker sosiale medier aktivt for å appellere til sårbare unge. Gjennom rap-musikk, symbolbruk og bilder som glorifiserer gjengkultur, vold og fryktkapital, skaper de en attraktiv og normalisert framstilling av den kriminelle livsstilen.

135 Kripos. (2025). *Vold som handelsvare – En beskrivelse av fenomenet*. https://www.politiet.no/globalassets/tall-og-fakta/kriminelle-nettverk/2025-10-16-a-vold-som-handelsvar---kripos_.pdf

The background is a dark blue gradient. In the center, a human hand is shaking a digital wireframe hand. The background is filled with various faint icons: a skull and crossbones, a play button, a warning triangle, a downward arrow, a padlock, a shield, and a magnifying glass. A white text box with a double-slash icon on the left and right sides is positioned over the handshake.

Teknologien brukes som digital muliggjører for å effektivisere logistikk, rekruttere personer i lokale roller, kommunisere trygt og redusere risikoen for bakmenn.

Motivasjonsfaktorer for rekrutterte ungdommer:

Innledningsvis: Løfte om raske penger, spenning og status tilknyttet gjengens varemærke frister unge sårbare til å ta kontakt. Rekruttererne viser fram luksus, makt og tilhørighet som den unge kan bli en del av.

Underveis: Gjennom forledningsprosessen observeres det at fellesskapet og lojaliteten blir viktigere enn selve pengene. Rekruttererne bygger et avhengighetsforhold og får den unge til å føle seg unik og betydningsfull for nettverket. Fristelsen av økonomisk gevinst tones kraftig ned i denne prosessen – mens følelsen av å ha en rolle i fellesskapet dominerer.

Resultat: I realiteten er det få eksempler på at unge faktisk mottar den lovede betalingen etter fullført oppdrag, og det er lite som tyder på at de oppnår reell økt status i miljøet. Ungdommene ender opp som den tapende part og brukt som engangsressurser.

Flere sårbare unge mennesker lar seg inspirere av virkemidlene og sosiale medier blir brukt som rekrutteringsarena for de kriminelle nettverkene. Mens forledningen foregår på sosiale medier¹³⁶, foregår ofte utlysingen av voldsoppdrag, planlegging og koordinering på krypterte kommunikasjonsplattformer¹³⁷.

En tydelig trend det siste året er at rekrutteringen til voldsoppdrag har utvidet seg fra krypterte til åpne plattformer som sosiale medier, noe som utvider rekrutteringsgrunnlaget. Samtidig med denne utviklingen har det vært en økning i voldsoppdrag i Norge. I 2025 har politiet registrert et tosifret antall bestilte voldshandlinger som er gjennomført i Norge, og et tilsvarende antall har blitt avverget. Dette illustrerer hvor viktig teknologien er for virksomheten til de kriminelle nettverkene.

Unge sårbare rekrutteres via sosiale medier

Det er ofte unge, sårbare personer som påtar seg voldsoppdrag for kriminelle nettverk – som også virker å være den faktiske målgruppen. Eksempelvis argumenterer rekruttererne med at de ikke trenger å bekymre seg for straff etter som de er under kriminell lavalder.

136 TikTok, Snapchat og Instagram er mest utbredt.

137 Eksempelvis Signal, Telegram og Zangi.

Rekrutteringsprosessen kan gå svært raskt. Enkelte ganger er det snakk om få dager fra kontakten innledes til ungdommen står med våpen i hånden. Noen ganger rekrutteres personer uten at det foreligger et konkret oppdrag på daværende tidspunkt. I slike tilfeller kan det gå noe tid før utøveren aktiveres, men dette skyldes fortrinnsvis oppdragsmangel, ikke manglende vilje og motivasjon hos utøveren. I mellomtiden holdes utøveren «varm» gjennom digital kommunikasjon, hvor utøveren får høre hvor viktig vedkommende er og at nettverket trenger «soldater» som er lojale og fryktløse. Slik opprettholdes motivasjonen fram til målet for oppdraget blir lokalisert.

Teknologien har muliggjort denne formen for KSH, hvor bakmenn kan operere fra transittland uten utleveringsavtale med Norge og likevel fjernstyre kriminaliteten i detalj. Teknologien spiller en avgjørende rolle – fra rekruttering og planlegging til gjennomføring av voldsoppdrag. Etter utførelsen brukes nyhetsartikler, film fra hendelsen eller annen omtale av oppdraget som propaganda i sosiale medier for å bygge fryktkapital, styrke nettverkets omdømme og rekruttere nye utøvere. Uten teknologiske hjelpemidler ville den hurtige etableringen av kriminelle nettverk i Norge eller fjernstyring av voldshandlinger vært mulig i samme omfang.

Delvurderinger

Det er *sannsynlig* at unge utøveres motivasjon i like stor grad handler om tilhørighet og sosial status i det kriminelle nettverket som økonomisk vinning.

I 2025 er det registrert et rekordhøyt antall bestilte voldsoppdrag via sosiale medier og krypterte kommunikasjonsplattformer. Det er *meget sannsynlig* at voldsoppdrag vil fortsette å forekomme i Norge i 2026.

Dersom nordiske myndigheter lykkes i å pågripe bakmenn, blant annet gjennom internasjonalt samarbeid, pågripelser i utlandet og utleveringsavtaler, er det *sannsynlig* at dette vil redusere omfanget av voldsoppdrag i Norge.



Ventet utvikling 2026

I etterretningsrapportene *Cyberkriminalitet 2024* og *2025* delte vi inn vurderingene i tre kategorier: *trusselen mot enkeltpersoner*, *virksomheter* og *samfunnet*. Økt sammenkobling gjør imidlertid at nivåene glir over i hverandre. En trussel mot enkeltpersoner kan spre seg inn i virksomhetsnettverket, og konsekvensene av angrepet på virksomheter kan få konsekvenser for samfunnet. Sårbarhetene og avhengighetene går derfor på tvers av nivåene. En kompromittert mobiltelefon kan være inngangen fra individ til samfunn. I motsatt retning kan omfattende trusler mot mange enkeltpersoner gi samfunnsmessig konsekvens.

Trusselen mot enkeltpersoner

Det er *sannsynlig* at vi vil se en videreutvikling av menneske-maskin-grensesnittet¹³⁸, også innenfor kriminalitet som handelsvare, med det resultat at brukerterskelen ytterligere reduseres, samtidig som verktøyenes kompleksitet og ytelser økes. Den økte profesjonaliseringen og spesialiseringen av kriminalitet som handelsvare vil *sannsynlig* være nok en driver for denne

utviklingen. Videre er det *sannsynlig* at en slik utvikling vil senke inngangsbarrieren for nye kriminelle, og at særlig barn og unge blir forsøkt rekruttert til å utføre enklere, men ofte risikoutsatte oppgaver på vegne av andre.

Profittmotivet står sterkt blant mange av aktørene i det cyberkriminelle økosystemet, og de kriminelle videreutvikler stadig sine metoder og framgangsmåter. Det er *mulig* at økningen innenfor og utviklingen av kriminalitet som handelsvare, slik som vold som handelsvare (VSH), også vil kunne gjøre seg gjeldende innenfor seksuallovbruddsfeltet, all den tid det også finnes profittmotiverte aktører som begår seksuallovbrudd.

Det er *sannsynlig* at kunnskapsgapet om digitale trusler og sikkerhet som eksisterer mellom privatpersoner og virksomheter vil øke, som følge av at kriminelle kontinuerlig tilpasser seg mottiltak og utvikler nye og mer utspekulerte metoder. Trusler fra det digitale domenet blir stadig mer kompleks og kompliseres ytterligere av KI sin svarte boks¹³⁹. De færreste private vil ha interesse, tid, krefter og kompetanse til å

¹³⁸ Eng: *Human-Machine Interface (HMI)*.

¹³⁹ KI sin svarte boks er begrepet som brukes for hva som inne i et KI-system. Det er umulig for leseren å vite hva som foregår inne i systemet, derav uttrykket «svart boks».

ivareta egen sikkerhet. Samtidig blir den private og profesjonelle sfæren stadig mer sammenvevd, og man utfører gjerne arbeidsrelaterte oppgaver på sin private mobil/PC.

Privatpersoner som ønsker å ivareta egen digital sikkerhet må kjøpe sikkerhetsløsninger av troverdige profesjonelle leverandører. De som ikke gjør dette vil være svært sårbare for digitale trusler. Det er *sannsynlig* at dette kunnskapsgapet vil være størst blant de yngste og eldste i samfunnet, i tillegg til sårbare grupper. Det er videre *sannsynlig* at ubeskyttede privatpersoner blir mer attraktive mål for cyberrettet kriminalitet og informasjonsinnsamling.

Manglende modenhet i møte med teknologi vil *sannsynlig* også gjøre barn og unge mer sårbare for seksuell utnyttelse. Seksuelt motiverte aktører benytter i økende grad digitale muliggjørere for å etablere kontakt, gjennomføre og dokumentere overgrep mot barn, samt ivareta anonymitet, skjule aktivitet og effektivisere steg i kriminalitetsutøvelsen. Det er *meget sannsynlig* at teknologien fungerer som en akselerator for seksuelt motiverte aktører, og det er *meget sannsynlig* at forekomsten av overgrep mot barn vil opprettholdes i 2026.

Det er *meget sannsynlig* at det vil være en økning i saker som knyttes til ekstreme, voldelige nettsamfunn i 2026, og at norske barn og

unge både vil være gjerningspersoner og ofre. Det er *sannsynlig* at flere norske gjerningspersoner og ofre vil utføre alvorlige handlinger som følge av involvering i nettsamfunnene, og utsette seg selv og andre for alvorlig fare.

Trusselen mot virksomheter

Det er som regel vanskeligere å utføre destruktive cyberangrep enn forstyrrende cyberangrep¹⁴⁰, da fysisk eller logisk ødeleggelse ofte fordrer dyp kunnskap og forståelse for hvordan systemet fungerer. Basert på dette er det *sannsynlig* at et eventuelt destruktivt cyberangrep mot norske virksomheter eller kritisk infrastruktur vil bli utført av en aktør med innsideinformasjon eller betrodd systemtilgang.

Det er *lite sannsynlig* at destruktive cyberangrep blir utført av profittmotiverte kriminelle i løpet av det neste året. Samtidig er det *sannsynlig* at USH-nettverk vil ramme norske virksomheter som direkte eller indirekte understøtter kritiske samfunnsfunksjoner eller kritisk infrastruktur.

Det er *lite sannsynlig* at hacktivistene alene, uten støtte fra statlig aktør, er i stand til å gjennomføre destruktive cyberangrep mot norsk kritisk infrastruktur.

Det er *mulig* at økt bruk av moderne sikkerhetsmekanismer¹⁴¹ og bedre ivaretagelse av

140 Eng: *Disruptive Cyber Attacks*.

141 Eksempelvis (eng:) *Endpoint Detection and Response (EDR)*.

grunnleggende sikkerhetshygiene vil føre til mer bruk av ulike former for sosiale manipulasjonsteknikker og innebygde funksjoner¹⁴² i den fornærmedes systemer og mindre bruk av skadevare.

Dersom ellers lovlige, internasjonale digitale leverandørkjeder forstyrres er det *mulig* at cyberkriminelle aktører vil benytte muligheten til å opprette tilsynelatende legitime virksomheter for å fylle eventuelle vakuum. Dette skyldes at det er *sannsynlig* at høyt press for å fylle hull i forsyningskjeden medfører lavere kritisk vurdering av nye aktører. Dersom dette skulle inntreffe er det *mulig* at disse aktørene også får økt aksess til norske virksomheter. I et slikt tilfelle, og i tilfeller hvor norske virksomheter rammes, er det *sannsynlig* via tredjepartsangrep.

Det er *sannsynlig* at nye USH-grupperinger bestående av unge cyberkriminelle vil ta i bruk nye metoder, med særlig vekt på sosial manipulasjon, offentlig kommunikasjon og markedsføring, samt bruk av kunstig intelligens i utførelsen av kriminaliteten. Det er *sannsynlig* at unge cyberrettede kriminelle aktører er mindre forutsigbare i sine målvalg og ikke følger de samme typiske handlemåtene som mer etablerte løsepengevirusgrupperinger har gjort de siste fem årene.

Det er *meget sannsynlig* at virksomheters implementering og bruk av KI-agenter vil ut-

nyttes av kriminelle. Det er videre *sannsynlig* at KI-agenter som blir brukt av norske virksomheter vil hjelpe cyberrettede kriminelle som er på innsiden av virksomhetens nettverk, med raskere å finne fram til sensitiv informasjon og trykkpunkter som kan benyttes av den kriminelle i en utpressingssituasjon.

Trusselen mot samfunnet

Hacktivisme utgjør en voksende trussel mot personer med en høy posisjon i samfunnet, eksempelvis en representant for politiske syn eller verdier. Det er eksempelvis flere kjente tilfeller av personangrep mot folkevalgte politikere. Teknologisk utvikling støtter målrettede, mer raffinerte og skalerbare angrep som *mulig* vil heve terskelen for å delta i det offentlige ordskiftet.

Angrep mot demokratiske symboler og prosesser ved at politisk og ideologisk motiverte aktører hindrer tilgang til informasjon, misbruker politiske symboler og merkevarer eller endrer meningsinnhold som virkemiddel med mål om å spre budskap og svekke tillit viser at hacktivistene retter seg mot demokratiske institusjoners troverdighet og legitimitet. Det er *sannsynlig* at slike symbolmanipulasjoner og desinformasjonskampanjer vil øke i omfang og raffinement i 2026 og i det videre, særlig i tilknytning til valg og politiske konflikter.

Kripos har tidligere vurdert at KI-generert

¹⁴² Eng: *Living Off The Land (LOTL)*.

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 opprettholdes for 2026 og videre.

Det er *sannsynlig* at KI-generert programkode vil føre til en relativ økning i antall sårbarheter i programvare, også en stund etter at KI-modeller blir bedre enn mennesker til å avdekke sårbarheter i programkode. Det er videre *sannsynlig* at KI-generert kode med sårbarheter forplanter seg i programvare med åpen kildekode og at dette vil bli utnyttet av kriminelle.

Aktører som begår seksuallovbrudd, uavhengig av motivasjon, utgjør en trussel mot de aller mest sårbare i samfunnet – barna våre. På et overordnet nivå utgjør også disse aktørene en trussel mot samfunnet, omfanget av lovbruddene og konsekvensene de påfører barna tatt i betraktning. Det er *sannsynlig* at den samlede trusselen fra aktører som begår seksuallovbrudd vil øke i 2026, særlig gitt økningen i The Com-relaterte saker i Norge og profittmotiverte aktørers evne og vilje til å finne nye måter å tjene penger på. Det er videre *sannsynlig* at økt tilgang på og økning i omfang av teknologiske muliggjørere, i kombinasjon med manglende kontrollmekanismer, gjør barn både mer utsatte

for overgrep og for å utvikle en seksuelt problematisk eller skadelig atferd eller annen avvikende atferd, som i ytterste konsekvens kan gjøre dem til utøvere av kriminalitet selv.

Det er *sannsynlig* at KI bidrar til å presse ned prisene på flere digitale varer og tjenester som tilbys på kriminelle markeds plasser, eksempelvis *phishing kit*¹⁴³ og digitale verktøy som benyttes til å begå kriminalitet.

Det er *mulig* at flyktninger og migranter fra Ukraina til Norge vil føre med seg teknisk kompetanse som kan ha markedsverdi for norske kriminelle nettverk. Det er videre *sannsynlig* at norske kriminelle nettverk aktivt vil forsøke å rekruttere cyberrettede kriminelle aktører for å øke kapabiliteter innen eksempelvis rekognosering, overvåking og operasjonell sikkerhet.

Det er *meget sannsynlig* at kriminalitet som handelsvare (KSH) fører til mer ressurskrevende etterforskninger som følge av en økt avstand mellom bakmenn og utøvere, bruk av anonymiseringsteknologi og at tradisjonell lokal aktørkunnskap svekkes som følge av flere involverte parter og det digitale domenets særegenhet.

143 Phishing kit er en ferdigstilt pakke med ulike programvareverktøy som gjør det enkelt for cyberkriminelle, uavhengig av tekniske ferdigheter, å gjennomføre en phishing-kampanje.



Vedlegg

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

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, eksempelvis seksuell utpressing som ikke er en egen paragraf i straffeloven. 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 er en samlebetegnelse for alle cyberkriminelle aktører og består av: (1) aktørene som begår kriminaliteten, altså aktørlandskapet, (2) miljøet der kriminaliteten finner sted, altså det digitale rom, og (3) utenforliggende 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.

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

Handlemåte benyttes om en bestemt framgangsmåte 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 **handling**, 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.

Hendelse 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 vilde 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 lyktes eller ikke. Eksempler på hendelser kan inkludere skanning av åpne porter i et nettverk, kartlegging av sårbarheter i en programvare og forsøk på rekruttering av insidere.

Aksjon, eller politiaksjon, er et polisizært 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.

Teknologi

Begrepet **teknologi** omfatter kunnskap, metoder og verktøy som mennesker bruker for å løse problemer og dekke behov. I denne rapporten refererer teknologi til moderne teknologi (mobiltelefoner, datamaskiner, kunstig intelligens) og usynlig teknologi (programvare, internett, algoritmer).

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 fysiske rom». I rapporter utgitt av Kripos er det digitale rom helheten av datasystemer, nettverk, enheter og programvare hvor cyberkriminalitet begås.

System er en ordnet sammenstilling av deler til en helhet som løser en oppgave. I denne

rapporten viser system til enten teknologiske systemer eller sosiale systemer. **Teknologisk system** er en menneskeskapt og samlet helhet med en indre sammenheng og logisk ordning som jobber sammen i et digitalt kommuniserende økosystem. Et teknologisk system består av ulike komponenter, relasjoner og koblinger mellom komponentene. Eksempler inkluderer datasystemer, OT-systemer eller virksomhets-systemer. **Sosialt system** er relativt varige relasjoner mellom individer, grupper, institusjoner eller mellom ulike sosiale systemer der gruppedeltagerne står i et gjensidig definert forhold til hverandre. Et sosialt system inkluderer prosesser som bidrar til å ivareta, regulere, endre eller fornye systemene, som for eksempel språk, verdier, normer eller lover. Eksempler inkluderer det cyberkriminelle økosystemet, cyberkriminelle nettverk eller grupper.

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 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 tett integrert for å oppnå et overordnet mål.¹⁴⁴ 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 feltstyr, kontrollsystemer og applikasjoner. Eng: Industrial Control Systems (ICS).

Virksomhetssystem er en 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), kundeservice-systemer (CRM) og dataanalyse (BI).

KI-system er en samlebetegnelse for ulike program- og maskinvarer som utfører handlinger, fysisk eller digitalt, basert på tolkning og behandling av strukturerte eller ustrukturerte data, i den hensikt å oppnå et gitt mål.¹⁴⁵ **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).

144 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., ss. 96–100). Imra International.

145 Kommunal- og moderniseringsdepartementet. (2020). *Nasjonal strategi for kunstig intelligens*. s. 9. Regjeringen.

Andre KI-systemer kan også utvise **agentiske egenskaper** uten nødvendigvis å bli omtalt som KI-agenter. Disse egenskapene inkluderer mål (eng: objectives), handlinger (eng: actions), minne (eng: memory) og refleksjon (eng: rethink).

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 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.

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.

-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 eller databasemoduler.

Flerbruksvarer er varer som i utgangspunktet er sivile, men som også har viktige militære anvendelser. Begrepet brukes her i utvidet forstand til også å inkludere kriminell anvendelse. Eng: Dual Use Items, Technology and Services.

Arvede systemer er gamle og ofte utdaterte systemer som er sårbare for utnyttelse, fordi de ble utviklet i en annen tid under andre sikkerhetsforhold. Eng: Legacy systems.

Botnet er et nettverk av kompromitterte datamaskiner og andre internettilkoblede enheter som er infisert med skadevare og som dermed kan fjernstyres ulovlig.

KI sin svarte boks er begrepet som brukes for hva som er inne i et KI-system. Det er umulig for brukeren å vite hva som foregår inne i systemet, derav uttrykket «svart boks».

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.

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 etter-spør 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.

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 internettjenester. 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.

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.¹⁴⁶

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 «løsepen-

146 Straffeloven. (2025). Kap. 1, § 20 første ledd bokstav a. *Lov om straff* (LOV-2025-06-20-86). Lovdata. https://lovdata.no/dokument/NL/lov/2005-05-20-28/KAPITTEL_1-3#KAPITTEL_1-3

gevirusaktører». **Trusselaktør** brukes der det ikke er mulig eller ønskelig å indikere aktørens profiltilhørighet, og innbefatter statlige aktører og terrorister, i tillegg til enkelte cyberkriminelle personer og 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.

Cyberkriminell gruppe er en samling av enkeltindivider som samarbeider for å oppnå et felles mål gjennom å begå cyberkriminalitet.

Kriminelle nettverk (KN) er et samlebegrep på miljøer, gjenger, grupperinger eller sett av individer som er knyttet sammen gjennom kriminalitet. De kriminelle knytningene kan være av både kortvarig og langvarig karakter, involvere alle typer kriminalitet og nettverkene kan ha større eller mindre grad av struktur og organisering.¹⁴⁷

Cyberkriminelle nettverk (CKN) er en samling av enkeltindivider og/eller grupper som samarbeider, er gjensidig avhengige eller utveksler varer eller tjenester for å begå cyberkriminalitet.

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

Tilretteleggere er personer som i kraft av sin tilgang og kompetanse medvirker til kriminalitet eller sørger for at kriminaliteten tilsløres.

Utøvere (kriminalitetsutøvere) er de som begår kriminalitet mot enkeltpersoner eller virksomheter. En aktør kan både være en tilrettelegger og en utøver – avhengig av situasjonen.

Muliggjørere er teknologiske verktøy, digital infrastruktur og fysiske hjelpemidler.

Affiliert er en person som har en forretningsmessig tilknytning til en LSH-gruppering og som benytter seg av løsepengevirus som handelsvare. Eng: Affiliate.

Tilgangsmeklere brukes som en betegnelse for cyberkriminelle som selger stjølet informasjon og ulovlig aksess til datasystemer. Tilgangsmeklere 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

147 Lunde, A. (2021, 24. august). *Kriminelle nettverk innen økonomisk-, arbeidslivs-, og miljøkriminalitet*. Økokrim, s. 1. <https://www.okokrim.no/kriminelle-nettverk-innen-oekonomisk-arbeidslivs-og-miljoekriminalitet.6353115-411472.html>

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

Kriminelle stedfortredere (proxy-aktører) er personer eller organisasjoner uten formell tilknytning til etterretnings- og sikkerhetstjenester eller andre myndighetsorganer, som vitende eller uvitende utfører kriminell aktivitet på oppdrag fra, eller til støtte for, myndigheter. Aktiviteten kan være politisk, ideologisk eller økonomisk motivert.¹⁴⁸

Kapasiteter henviser til kriminelles kvantifiserbare 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. Motiv 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 slutttilstand.

Kriminalitetsutøvelse

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 utøvet 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.

Utpressing som handelsvare (USH) er et begrep som favner både tradisjonelle løsepengevirus-som-handelsvare-nettverk (LSH-nettverk) og de kriminelle konstellasjonene som bedriver andre former for cyberrettet utpressing, men som fortsatt opererer i rammen av kriminalitet-som-handelsvare (KSH).

Cyberrettet utpressing er i denne rappor-

148 PST. (2025). *Nasjonal Trusselvurdering 2025*. s. 12.

ten 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 hacktivistene eller skadeverk på kritisk infrastruktur.

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 som destruktive cyberoperasjoner, her omtalt som digitalt skadeverk. Cyberangrep¹⁴⁹ er straffbare etter norsk straffelov.

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. **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 utnyttas på et senere tidspunkt. **Tredjepartsangrep** innebærer at en aktør 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.

Angrepskjeden refererer til et rammeverk

149 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 [...]». Kilde: Forskrift om restriktive tiltak mot cyberangrep. (2021). § 6, vedlegg A, artikkel 1, punkt 2. *Forskrift om restriktive tiltak mot cyberangrep* (FOR-2021-05-11-1459). Lovdata. <https://lovdata.no/dokument/SF/forskrift/2021-05-11-1459>

utviklet av Lockheed Martin for å identifisere og forhindre datainnbrudd og uønsket aktivitet i et nettverk. Rammeverket identifiserer hvilke steg en trusselaktør må utføre for å lykkes med å kompromittere et datasystem. Eng: Cyber Kill Chain™.

Destruktivt angrep er hovedsakelig cyberangrep som kun har til hensikt å ødelegge eller sabotere for virksomheters drift. Denne typen angrep utføres typisk ved bruk av skadevaretyper som permanent sletter eller ødelegger data og har naturligvis et stort skadepotensiale. Destruktive cyberangrep benyttes normalt i sabotasjeaksjoner. **Forstyrrende angrep**, eksempelvis cyberangrep med bruk av løsepengevirus, skiller seg fra destruktive angrep ved at de påfølgende ødeleggelsene er konsekvenser fremfor mål i seg selv. Det er som regel vanskeligere å utføre destruktive cyberangrep enn forstyrrende cyberangrep, da fysisk eller logisk ødeleggelse ofte fordrer dyp kunnskap og forståelse for hvordan systemet fungerer.

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.

Digitale bedragerier er en samlebetegnelse for en rekke ondsinnede aktiviteter utført via digitale plattformer med hensikt å manipulere, bedra eller stjele fra enkeltpersoner eller virksomheter.

Det er bruken av teknologi som skiller digitale bedragerier fra andre typer bedragerier.

Doxxing/doxing (eng.) er offentliggjøring av personlig/sensitiv informasjon om et individ eller en organisasjon.

Voice-phishing er en type phishing der cyberkriminelle bruker telefonoppringninger (og potensielt taleteknologi) for å manipulere ofre til å avsløre sensitiv informasjon.

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 framstille 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.¹⁵⁰

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.

Sammensatt virkemiddelbruk handler om at statlige aktører som ønsker å ramme andre stater på andre måter enn væpnet konflikt, bruker en rekke ulike metoder og virkemidler for å understøtte egne strategiske målsettinger. For eksempel kan fordekte påvirkningsoperasjoner og desinformasjon bidra til å destabilisere demokratier gjennom å svekke befolkningens tillit til sentrale samfunnsinstitusjoner. På denne måten kan for eksempel autoritære regimer søke å skape kaos eller påvirke politiske beslutninger i et annet land til sin fordel.¹⁵¹

Annet

Kompleksitet beskriver systemer med mange gjensidige avhengige elementer og relasjoner,

der samspillet er ikke-lineært og vanskelig å forutse. Helheten får da framvoksende egenskaper og atferd som ikke kan forklares ved å summere delene. Organisatorisk kompleksitet oppstår når ansvar er fragmentert og organiseringen er uoversiktlig.

Utløser er hendelser, utsagn, observasjoner og lignende som setter i gang en prosess. Eksempler inkluderer krig og konflikter, idrettsarrangementer, folkeavstemninger og prisutdelinger.

Sammensatte eller hybride trusler handler om at aktører, for eksempel stater, benytter seg av alle sine tilgjengelige virkemidler for å nå sine mål. Ofte benyttes metoder som påvirkning, tvang og fysisk skade for å så tvil i befolkningen, undergrave samhold, manipulere andre staters interesser, svekke demokratiske institusjoner og påvirke handlefriheten vår. Dette foregår gjerne i det skjulte for å unngå direkte konflikt.

Med **sikkerhet** menes beskyttelse av data og datasystemer fra tilsiktede trusler som hacking og skadevare, mens **trygghet** betyr beskyttelse mennesker fra utilsiktet skade eller risiko. Eng: security (sikkerhet) og safety (trygghet).

150 Straffeloven. (2025). Kap. 26, § 311. *Lov om straff* (LOV-2025-06-20-86). Lovdata. https://lovdata.no/dokument/NL/lov/2005-05-20-28/KAPITTEL_2-11#%C2%A7311

151 Stortingsmelding 13 (2024–2025). *Forebygging av ekstremisme: Trygghet, tillit, samarbeid og demokratisk motstandskraft*. Kultur- og likestillingsdepartementet. <https://www.regjeringen.no/no/dokumenter/meld.-st.-13-20242025/id3092713/?ch=3>

Figuroversikt

Figur 1

Begrepskartet for cyberkriminalitet. Side 11

Figur 2

Økosystemet for cyberstøttede seksuallovbrudd. Side 38

Figur 3

Cyberkriminalitetens ontologi. Side 56

Figur 4

ARPA-rammeverket. Side 60

Figur 5

Spekteret av statlig ansvar. Side 72

Figur 6

Avhengigheter til det digitale rom. Side 87

Figur 7

Eksempel på angrepsfase for et cyberangrep uten krypteringsvirus. Side 88

Figur 8

En forenklet framstilling av framgangsmåten som benyttes av aktører som ønsker å etablere kontakt med og utsette barn for seksuallovbrudd. Side 90

Figur 9

En forenklet framstilling av kultmedlemmers framgangsmåte for å etablere kontakt med sårbare barn og unge og hva ofrene utsettes for eller presses til å gjøre. Side 91



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 inter-

nasjonalt politisamarbeid og ansvarlig for politiets nasjonale etterretningsproduksjon.

Nasjonalt cyberkrimsenter (NC3) ved Kripos bekjemper cyberrettet og cyberstøttet kriminalitet, sistnevnte 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 anmeldes til lokalt politi. Er du usikker på om forholdet er straffbart eller har du informasjon du ønsker å dele med oss?

Tips oss om cyberstøttede
seksuallovbrudd

Ta gjerne kontakt gjennom NC3 sine tipsmottak.

Tips oss om cyberrettet
kriminalitet



Kripos

Postadresse: Postboks 2094 Vika, 0125 Oslo

Besøksadresse: Nils Hansens vei 25, 0667 Oslo

Kontakt: 23 20 80 00 / kripos@politiet.no