POLITIET
KRIPOS

ÅPEN

Trusselaktørers kontaktetablering med barn på internett

Etterretningsrapport

1. Hovedpunkter

- Det er *meget sannsynlig* at trusselaktører vil fortsette å kontakte barn på internett, at de hovedsakelig vil være menn og at gutter og jenter vil være utsatt.

- Det er *meget sannsynlig* at trusselaktører i all hovedsak tilnærmer seg barn på internett i den hensikt å begå seksuelle overgrep.

- Det er *meget sannsynlig* at trusselaktører vil bruke flere ulike plattformer for å kontakte barn på internett, både store og kjente plattformer som Snapchat og mindre utbredte plattformer, eksempelvis chatroulette-plattformer.

- Det er *sannsynlig* at bruk av ulike virkemidler, eksempelvis ros og forledelse, gjør det lettere for trusselaktører å komme i posisjon til å begå seksuallovbrudd mot barn på internett. Det er *mulig* at økt bevisstgjøring vil kunne redusere forekomsten.

- Det er *sannsynlig* at utviklingen innen anonymiseringsteknologi, kunstig intelligens og ende-til-ende-krypterte plattformer øker trusselaktørers handlingsrom. Det er *mulig* at KI vil kunne fungere som mottiltak.

2. Innhold

3. Bakgrunn

Det finnes en rekke plattformer på internett som benyttes av voksne til å komme i kontakt med barn. I mange av tilfellene ender kontakten med at barna blir utsatt for seksuelle overgrep, både fysiske og cyberstøttede[1]. Forskjellige plattformer er arena for ulike grupper barn og trusselaktørers framgangsmåter varierer. Det er utfordrende for politiet å til enhver tid ha oversikt over og rette innsats mot, de aktuelle problemområdene.

I juni 2023 bestilte ledelsen ved seksjon for seksuelle overgrep mot barn (SOMB) på Kripos en etterretningsrapport om trusselaktørers kontaktetablering med/tilnærming til barn på internett. Formålet med rapporten er å danne kunnskapsgrunnlag for framtidige prioriteringer og tiltak. Det gjelder både tiltak rettet mot trusselaktørene, forebyggende tiltak overfor barna og ansvarliggjøring av plattformene som muliggjør, eller i ytterste konsekvens tilrettelegger for, seksualisert kontakt mellom voksne og barn.

Etterretningsbehovet var et oppdatert situasjonsbilde av hvordan trusselaktører tilnærmer seg barn og hvilke virkemidler som benyttes i kontaktetableringen. I tillegg var det behov for informasjon om hvilke plattformer trusselaktørene bruker og hvorfor, hvilke barn som kontaktes og om kontakten med barna er tilfeldig eller utvalgt samt hva som er hensikten med kontaktetableringen og hva kontakten fører til. I tillegg var det ønskelig å registrere eventuelle endringer og utvikling.

Innhentingsperioden var fra 1. mai 2023 til 1. november 2023. Informasjonsgrunnlaget er uttrekk fra politiets egne registre, interne og eksterne rapporter, eksterne kilder som Nasjonalt kunnskapssenter om vold og traumatisk stress (NKVTS) og Medietilsynet samt innhenting fra åpne kilder på internett. Rapporten inneholder framtidsrettede vurderinger innenfor en tidsramme på seks måneder. Etter seks måneder vil vurderingenes konfidens avta.

3.1. Avgrensinger og forbehold

Rapporten er avgrenset til å omhandle barn under 14 år. Barn under 14 år har et særskilt vern i straffeloven, der bestemmelsene om overgrep mot barn under 14 år har høyere strafferamme enn for eksempel seksuell omgang med barn mellom 14 og 16 år. For barn under 14 år defineres all seksuell omgang som voldtekt. Kontaktetablering med barn rammer også den eldre aldersgruppen, men av hensyn til rapportens omfang, er disse utelatt.

Rapporten er videre avgrenset til voksne trusselaktører. Dette er personer over 18 år. Ettersom barna i rapporten er under 14 år vil ikke jevnbyrdighet i alder og utvikling gjøre seg gjeldende for personene i rapporten, da rettspraksis tilsier at terskelen for å frita for straff grunnet jevnbyrdighet i alder og utvikling vil være mellom tre og fire år.[2] [3] Andre eventuelle straffrihetsgrunner er ikke hensyntatt.

[1] Først benyttet i rapporten Cyberkriminalitet 2024 utgitt av Kripos. Erstatter begrepet kriminalitet støttet av datasystemer og betyr kriminalitet som fantes før det digitale rom oppstod, men som nå også kan støttes av eller gjøres enklere ved bruk av datasystemer.

[2] https://lovdata.no/lov/2005-05-20-28/§308

[3] https://www.domstol.no/globalassets/upload/hret/avgjorelser/2013/sak-2013-8-anonymisert.pdf

Informasjon hvor fornærmede er under 14 år og trusselaktør ikke er identifisert, er inkludert i datagrunnlaget. Det må her tas høyde for at trusselaktør kan være et barn. Informasjon hvor det fornærmede barnets alder og identitet ikke er kjent, er utelatt.

Noen av forholdene som er inkludert i datagrunnlaget kan ha skjedd før, men blitt rapportert i rapporteringsperioden.

3.2. Kontaktetableringsbegrepet

Det engelske ordet "grooming" er et mye brukt begrep om voksne trusselaktørers tilnærming til barn eller det å innynde seg hos barn. Grooming har mange ulike definisjoner og det varierer hva som legges i begrepet, men det har ofte blitt definert som en straffbar handling som går ut på at en voksen person avtaler et fysisk møte med et barn i den hensikt å begå et seksuelt overgrep. Grooming er derfor knyttet direkte til straffeloven § 306 *Avtale om møte for å begå seksuelt overgrep*.[4]

Begrepet kontaktetablering favner bredere enn grooming. Mye av kontakten mellom voksne og barn resulterer i andre former for seksuell utnyttelse enn den fysiske og er i stor grad digitalisert. I rapporten *Digitale seksuelle overgrep mot barn og unge – gjerningspersoner og fornærmede* utgitt av NKVTS brukes begrepet "seksuelle overgrep initiert via digitale medier". Med dette menes overgrep som er innledet via digitale medier uten at det har vært en grooming-prosess i forkant, hvor overgrepet kan skje fysisk eller digitalt.

I denne rapporten har Kripos valgt bort begrepet grooming på grunn av variasjonen i definisjonene og fordi flere av disse har begrensninger. Noe av kontakten mellom voksne og barn ender ikke med seksuallovbrudd eller andre straffbare forhold. Ved å bruke begrepet kontaktetablering må ikke intensjonen med voksnes tilnærming til barn på internett nødvendigvis være å begå seksuelle overgrep. Det kan være vel så relevant å se på de tilfellene hvor kontakten *ikke* ender med seksuelle overgrep, uavhengig av trusselaktørs intensjon. Noen ganger avklares heller ikke trusselaktørens intensjon, fordi kontakten mellom aktøren og barnet av ulike grunner avbrytes.

4. Kontaktetablering med barn på internett

Norske barn og unge har høy grad av digital tilstedeværelse. Foreldre oppga i en undersøkelse gjort av Medietilsynet at 85 prosent av barn i alderen ni til ti år har mobil og at nær sagt alle barn har mobil fra elleveårsalder.[5] I en annen undersøkelse gjennomført med barn i alderen ni til 18 år går det fram at nesten halvparten av norske niåringer bruker sosiale medier og 56 prosent av tiåringene. Fra tolvårsalder er minst ni av ti på sosiale medier.[6]

Med den teknologiske utviklingen og den økte bruken av digitale enheter er seksuelle overgrep mot barn på internett et omfattende samfunnsproblem i stadig vekst. Norsk politi mottar flere og flere tips for hvert år som går om norske gjerningspersoner som kontakter barn, utsetter dem for seksuell utpressing, skaffer seg overgrepsmateriale ved å få barna til å sende nakenbilder og -videoer eller begår cyberstøttede voldtekter.

[4] https://snl.no/grooming_-_strafferett, https://lovdata.no/lov/2005-05-20-28/§306

[5] Foreldre og medier 2022 – en undersøkelse om foreldres erfaringer med 1–17-åringers medievaner

[6] Barn og medier – en undersøkelse om 9–18-åringers medievaner

Politiet har i flere saker identifisert hundrevis av barn som har blitt utsatt for seksuallovbrudd over internett av samme gjerningsperson. Mange av barna har aldri fortalt noen om det de har opplevd.

4.1. Trusselaktørene

I politiets registre er det registrert flere titalls trusselaktører i rapporteringsperioden. Det er færre aktører enn det er barn, som betyr at én aktør ofte kontakter flere barn.

Den yngste trusselaktøren var 18 år mens den eldste var 64 år på tidspunktet for kontakten. Majoriteten av trusselaktørene var i alderen 18-29 år og utgjorde ca. 60 prosent. Det var én kvinne i datagrunnlaget.

Aktørene er bosatt over hele landet og har ulik sivilstatus, livssituasjon og bakgrunn. Det dreier seg derfor ikke om en homogen gruppe mennesker. Noen av aktørene er registrert med egne barn eller har tilgang på barn.

60 prosent av de identifiserte trusselaktørene er omhandlet med seksuallovbrudd mot barn fra tidligere og 37 prosent er domfelt for ett eller flere av disse forholdene. De fleste er domfelt for seksuelt krenkende atferd overfor barn under 16 år, enten i ord eller handling. I tillegg er det omtrent like høy forekomst av domfellelse for fremstilling av seksuelle overgrep mot barn eller fremstilling som seksualiserer barn, seksuell omgang med barn mellom 14 og 16 år og voldtekt av barn under 14 år.

4.2. Barna

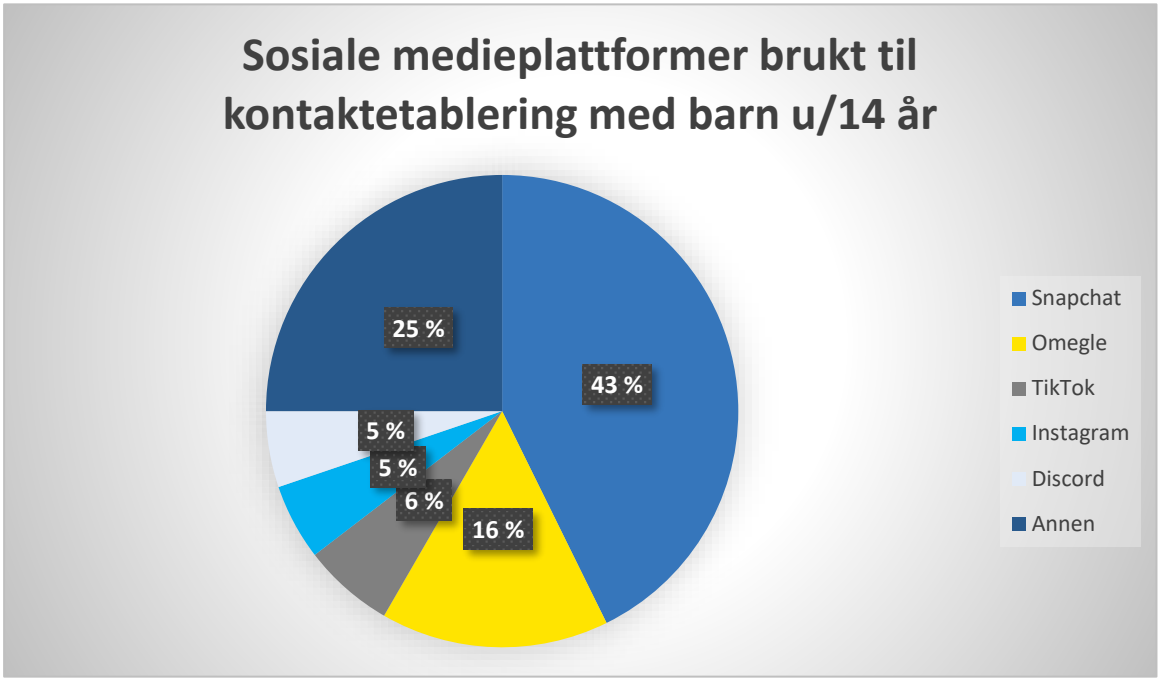
I aktuell periode er det i politiets registre registrert at rundt hundre barn under 14 år har blitt kontaktet av trusselaktører på internett. Jentene utgjorde ca. to tredjedeler og guttene én tredjedel.

Barna er bosatt over hele landet. For noen av barna hadde politiet informasjon om at de var i en særlig sårbar situasjon. Noen av barna hadde tidligere vært utsatt for vold eller seksuelle overgrep, andre hadde fysisk eller psykisk uhelse. Noen hadde en vanskelig familiesituasjon, eksempelvis foresatte med rusproblematikk. Andre igjen var underlagt barnevernet eller bodde på institusjon. Det er kjent at barn i en sårbar situasjon har høyere risiko for å bli utsatt for seksuell utnyttelse på internett. Mange barn i en sårbar situasjon har i tillegg færre tillitspersoner som kan ivareta dem i etterkant av at de har blitt utsatt for noe straffbart.[7]

4.3. Plattformene

Det framgår av datagrunnlaget at den mest brukte sosiale medieplattformen blant barn under 14 år samt plattformen trusselaktørene hyppigst benyttet seg av i sin kontaktetablering med barn, var Snapchat. På andreplass befant Omegle seg. I tillegg ble plattformene TikTok, Instagram og Discord brukt til kontaktetablering. Av spillplattformer var Fortnite og Roblox gjengangere. Det er også sett tilfeller av at trusselaktør sendte SMS til barn. For andre sosiale medier og spillplattformer er det kun registrert noen få tilfeller per plattform.

[7] https://www.politiet.no/globalassets/tall-og-fakta/seksuelle-overgrep-mot-barn/seksuell-utnyttelse-av-barn-over-internett.pdf



Figur 1: Plattformene som trusselaktører oftest benyttet til å kontakte barn.

Plattformene har ulik utforming, funksjonalitet og brukermasse. Det er lite informasjon om hvordan trusselaktørene kommer i posisjon til å kommunisere med barna på de forskjellige plattformene og om barna er utvalgte eller tilfeldige ofre. På noen plattformer må trusselaktør imidlertid sende en venneforespørsel for å kunne kommunisere med barnet, mens det på andre plattformer automatisk etableres kontakt.

4.3.1. Snapchat

Snapchat er en meldingstjeneste hvor man deler bilder og videoer med kontakter.[8] En slik melding kalles en "snap". På Snapchat er det mulig å legge til brukere fra kontaktlisten på telefonen, søke opp brukere og legge til brukere via funksjonen Quick Add, som gir venneforslag blant annet basert på venners venner.[9] Det er også mulig å starte samtaler med brukere man ikke er venn med. I kombinasjon med den store brukermassen medfører det mange muligheter for trusselaktører til å komme i kontakt med barn. I rapporteringsperioden er det sett eksempler på flere av kontaktmåtene. I tilfeller der kontakten mellom barn og trusselaktører flytter seg mellom ulike plattformer, ender kontakten i all hovedsak på Snapchat.

I Barn og medier-undersøkelsen av 2022 framgår det at åtte av ti barn mellom ni og 18 år benytter seg av Snapchat, og at det er det viktigste sosiale mediet blant unge.[10] Også undersøkelsene fra 2018 og 2020 viste det samme.[11] Omtrent halvparten av barna på barneskolen bruker Snapchat, mens på ungdomsskolen og videregående er andelen over 90 prosent.[12] Det er litt flere jenter sammenlignet med gutter som bruker Snapchat. Når

[8] https://snl.no/Snapchat
[9] https://help.snapchat.com/hc/en-us/articles/7012328615828-How-to-Add-Friends-on-Snapchat
[10] Barn og medier 2022 – en undersøkelse om 9–18-åringers medievaner
[11] Barn og medier-undersøkelsen 2018, Barn og medier 2020
[12] 9-11 år: Jenter 26%, gutter 22%. 12-14 år: Jenter: 91%, gutter 83%. 15-16 år: Jenter: 97%, gutter 91%. 17-18 år: jenter 96%, gutter 91%.

barna blir spurt hva de pleier å gjøre når noen legger dem til eller vil følge dem i sosiale medier, herunder på Snapchat, svarer nesten halvparten at de kun godtar forespørselen om de kjenner vedkommende, men 40 prosent svarer at de godtar forespørselen hvis de har felles venner. 15 prosent svarer at de godtar alle forespørsler.

I ett tilfelle startet trusselaktør en samtale med en jente uten at de var venner på Snapchat. Han spurte hvor gammel hun var, oppga deretter å være to år eldre enn henne og sendte videoer av at han befølte egen penis. Han etterspurte så bilder av jenta. Trusselaktør er ikke identifisert.

I et annet tilfelle har trusselaktør, en 42 år gammel mann, lagt til en jente på Snapchat. Da hun spurte ham hvem han var, oppga han at han legger til tilfeldige brukere. Han oppga til å begynne med at han var vesentlig yngre enn sin faktiske alder og fortsatte dialogen med jenta selv om hun sa hvor gammel hun var. Lenger ut i samtalen innrømmet han sin faktiske alder. Han ga henne komplimenter, ville se henne og forsøkte å ringe henne. Jenta fortalte om kontakten til en voksen tillitsperson som varslet politiet.

4.3.2. Omegle

Omegle var en amerikansk plattform som blant annet var forbundet med digital blotting og seksuell utnyttelse av barn på internett. Plattformens utforming tilrettela for kontakt mellom fremmede, inkludert mellom voksne og barn, og hadde mangelfull monitorering av chat og videochat. Mange straffesaker med norske ofre og gjerningspersoner har hatt sitt utspring i denne plattformen.

Omegle ble i november 2023 lagt ned uten forvarsel. Plattformens grunnlegger erklærte i et åpent brev på internett at Omegle var blitt brukt til kriminelle handlinger, men at plattformen også hadde møtt kritikk og motstand i så stor grad at det ikke lenger var mulig å opprettholde driften av nettstedet. Blant plattformens kritikere var myndigheter i flere land, inkludert norsk politi. Det eksisterer i dag en rekke lignende chatroulette-plattformer[13].[14]

I rapporteringsperioden ble flere barn utsatt for seksuell utnyttelse på Omegle. Blant annet besøkte to gutter i barneskolealder plattformen, hvor de kom i kontakt med en mannlig trusselaktør på videochat. Han snakket engelsk og satt naken foran webkameraet og onanerte. Trusselaktør skal så ha fått guttene til å dra ned buksene sine og vise penis.

4.3.3. TikTok

TikTok er et sosialt nettverk der brukerne kan dele korte videoer. Brukerne kan følge hverandre, kommentere hverandres videoer, dele videoer videre og kommunisere via direktemeldinger. Brukere med høy følgerskare kan også direktestrømme videoer. TikTok har økt substansielt i popularitet de siste årene og ble brukt av 73 prosent av norske barn mellom ni og 18 år i 2022. Det er færre barn fra ni til elleve år på TikTok enn det er på Snapchat, men bruken øker drastisk blant barn mellom 12 og 14 år. [15] [16]

[13] Chatroulette-plattformer kobler brukere vilkårlig sammen og baserer seg ofte på videochat med fremmede.

[14] Eksempler på chatroulette-plattformer er: OmeTV, Tinychat, Shagle, Chatroulette, EmeraldChat

[15] Barn og medier – en undersøkelse om 9–18-åringers medievaner

[16] 9-11 år: Jenter 7%, gutter 7%. 12-14 år: Jenter 71%, gutter 54%. 15-16 år: Jenter 95 %, gutter 81%. 17-18 år: Jenter 94%, gutter 82%.

I ett tilfelle har trusselaktør, en mann på 36 år, kontaktet en jente på TikTok og invitert henne ut på kaffe.

4.3.4. Instagram

Instagram er et sosialt medium for deling av bilder og video. Brukerne kan ha åpne eller lukkede profiler og følge hverandre. Brukere kan kommunisere via direktemeldinger, kommentere hverandres innlegg og dele innlegg videre. I tillegg til å publisere bilder og videoer kan man legge ut bilder og videosnutter i plattformens story-funksjon, som minner om story på Snapchat. Brukere kan også direktestrømme video.

I ett tilfelle har en jente mottatt en melding på Instagram fra en 28 år gammel trusselaktør som lurte på om han kunne få "komme i munnen" hennes.

4.3.5. Discord

Discord er en plattform som i utgangspunktet ble etablert for kommunikasjon mellom gamere i spill, men som har utviklet seg til å bli et sosialt medium som benyttes av langt flere enn bare gamere. Det finnes åpne og lukkede servere med få eller svært mange medlemmer og serverne er gjerne sentrert rundt ett hovedtema. Man kan invitere inn venner og kommunisere en-til-en eller i grupper, utveksle tekst, bilder, lyd og lenker. Discord brukes av 36 prosent norske barn i alderen ni til 18 år og i større grad av gutter enn jenter.[17]

I ett tilfelle har en jente blitt kontaktet av en 20 år gammel mann på Discord. Hun delte nakenbilder av seg selv etter forespørsler fra trusselaktør, som også har skrevet mange seksualiserte meldinger til jenta. Kontakten pågikk i flere måneder før jentas foreldre oppdaget kontakten.

Kripos har informasjon om at trusselaktører anser Discord-servere som omhandler gaming for å være gunstige steder å komme i kontakt med mindreårige gutter. Servere relatert til noen typer spill er mer aktuelle for de yngste guttene, mens andre er mer aktuelle for prepubertale gutter. Trusselaktører tenderer også til å finne seg servere med egne hobbyer/interesser som tema for lettere å kunne engasjere seg i dialog om temaet. Trusselaktører finner blant annet serverne ved å benytte seg av Discords "explore"-funksjon eller på nettsider som lister opp servere.

4.3.6. Spillplattformen Roblox

Roblox er en spillplattform hvor brukerne kan utvikle egne spill og spille spill laget av andre brukere. Roblox er i utgangspunktet gratis, men opererer med en egen valuta kalt Robux. Robux brukes for eksempel til å kjøpe klær og utstyr til egen avatar. I tillegg til å være en spillplattform er Roblox en sosial møteplass. Spillerne kan opprette kontaktlister, chatte med venner og chatte med spillerne i samme spill.

Kripos er kjent med at enkelte trusselaktører kommer i kontakt med barn på Roblox og flytter kontakten til Discord, hvor barna blir tilbudt Robux-gavekort i bytte mot seksualiserte bilder og videoer.

4.3.7. Spillplattformen Fortnite

Fortnite er en spillplattform som gir tilgang til forskjellige typer spill. Den fungerer også som et sosialt medium, hvor den gir mulighet for stemmechat og lar spillere legge

[17] Barn og medier – en undersøkelse om 9–18-åringers medievaner

hverandre til som venner. Plattformen har også tekstchat, men den er kun i "lobbyen" mellom spillrunder.

Kripos er kjent med at Fortnite brukes av trusselaktører til å komme i kontakt med barn.

Delvurdering: Det er *meget sannsynlig* at trusselaktører vil fortsette å kontakte barn på internett, at trusselaktørene i hovedsak vil være menn og at både jenter og gutter vil være utsatt. Det er *sannsynlig* at det vil være en noe høyere forekomst av jenter blant de utsatte barna. Det er *sannsynlig* at andelen sårbare barn som blir utsatt er høyere enn den andelen som framkommer i datagrunnlaget og at det skyldes mangelfulle opplysninger. Det er *meget sannsynlig* at det er store mørketall når det kommer til rapportering i saker om kontaktetablering og i forlengelsen av det, internettrelaterte overgrep mot barn.

Det er *meget sannsynlig* at Snapchat vil fortsette å være den dominerende plattformen i trusselaktørers tilnærming til barn på internett. Det begrunnes med at plattformen er overrepresentert i rapporteringsperioden og av de mest populære plattformene blant barn under 14 år. Det er *sannsynlig* at vi vil se en økt forekomst av nye/mindre kjente plattformer, men det er *lite sannsynlig* at disse vil ta over for Snapchat de neste seks månedene.

Selv om Omegle, som utgjorde en risiko for barns trygghet på internett, er lagt ned, er det *meget sannsynlig* at andre eksisterende eller framtidige chatroulette-plattformer vil være arena for seksuell utnyttelse av barn de neste seks månedene. **Delvurdering slutt**

5. Framgangsmåter i kontaktetablering

Trusselaktører som forsøker å oppnå kontakt med barn på internett benytter seg av mange ulike virkemidler.

5.1. Vanligste virkemidler

I rapporteringsperioden var et vanlig virkemiddel å utgi seg for å være yngre enn sin faktiske alder. I mange tilfeller spurte trusselaktør om barnets alder først og tilpasset egen alder deretter.

Det er også sett flere tilfeller av at trusselaktør utgir seg for å være jente, enten ved å oppgi det i brukernavn/visningsnavn og/eller chat, eller ved å spille av en video av en "falsk" jente istedenfor å benytte webkamera og videooverføring av seg selv i sanntid.

Kripos er kjent med at trusselaktører har god erfaring med å utgi seg for å være jenter og at mange anser det for å være en enkel og effektiv metode. Det gjøres blant annet ved å bruke bilder av ekte barn, noen ganger satt sammen til en "lokkevideo", eller ved å bruke videoopptak av ekte barn. Enkelte trusselaktører har ferdigheter til å få videoen til å framstå direktesendt, med mulighet for å hoppe til relevante deler av videoen hvor barnet gjør ulike handlinger. Noen trusselaktører benytter seg også av programvare som kan endre stemmen, eksempelvis ved få en voksen mann til å høres ut som en ung jente.

I motsetning til trusselaktører som går inn for å lure barna de kommuniserer med, har enkelte trusselaktører opplevd god respons ved å være åpne om at de er nettopp voksne, eksempelvis ved å formidle til unge gutter at man er en voksen, homofil mann.

Andre mye brukte virkemidler var å rose og gi komplimenter, eksempelvis for barnets utseende samt opptre vennskapelig og tillitvekkende. Enkelte trusselaktører innledet kjærestelignende forhold til barna og spilte på barnas følelser.

Andre trusselaktører tilbød barna penger for seksuelle tjenester, eksempelvis ved å foreslå å være barnets "sugar daddy"[18], og noen tilbød andre type goder som narkotika, alkohol eller tobakk.

Det er også sett eksempler på at trusselaktører framsatte trusler, var pågående og masete, eller spilte på barnets samvittighet og ga instruksjoner.

Delvurdering: Det er *meget sannsynlig* at å lure barna til å tro at de kommuniserer med jevnaldrende og/eller at de kommuniserer med en jente, både er utbredt og fører til at trusselaktør oppnår ønsket kontakt med barn. Det er *meget sannsynlig* at disse framgangsmåtene vil fortsette å være hyppig anvendt blant trusselaktører som ledd i å etablere kontakt med barn og utnytte dem seksuelt. **Delvurdering slutt**

6. Hva kontaktetableringen fører til

Trusselaktørers kontaktetablering med barn på internett kan føre til mange ulike seksuallovbrudd. Kontakten kan også ende før den utvikler seg til å bli straffbar.

Det framgår av informasjonsgrunnlaget at i ca. 84 prosent av tilfellene endte kontaktetableringen med seksuallovbrudd eller forsøk på seksuallovbrudd mot barn. Det utpeker seg derfor som overordnet motiv i trusselaktørers kontakt med barn på internett.

Seksuallovbruddene som forekom hyppigst var cyberstøttede, i form av seksualisert chat og digital blotting samt at trusselaktør skaffet seg, eller forsøkte å skaffe seg, materiale som seksualiserer barn. Det er registrert at jentene var noe mer utsatt for seksualisert chat og digital blotting og at guttene var noe mer utsatt for forespørsler om seksualiserte bilder og videoer.

6.1. Voldtekt

De mest alvorlige utfallene av trusselaktørers kontaktetablering var voldtekter av barn under 14 år. Det er både registrert cyberstøttede og fysiske voldtekter i rapporteringsperioden.

I en sak endte kontaktetableringen med fysisk voldtekt. En jente ble lagt til på en sosial medieplattform av en mannlig trusselaktør som utga seg for å være yngre. Han fant ut hvor fornærmede bodde og oppsøkte henne før han ved bruk av vold/fysisk makt voldtok henne.

[18] Sugar dating innebærer ofte at en eldre mann – kalt en sugar daddy – dater en ung person – i dette tilfellet et barn – og betaler for bl.a. seksuelle tjenester med gaver, penger eller andre former for goder.

I en annen sak endte kontaktetableringen med en cyberstøttet voldtekt. Den fornærmede gutten ble lagt til på Snapchat av en mannlig trusselaktør. Gutten forklarte at trusselaktøren var snill i begynnelsen, men begynte etter hvert å spørre etter nakenbilder. Han maste veldig på fornærmede som følte seg presset til å sende bildene. Det begynte med forespørsler om relativt uskyldige bilder før det eskalerte og til slutt endte med onaneringsvideoer og direktestrømming av onanering. Fornærmede har uttalt at han skammer seg over det som har skjedd og er redd for at det skal komme ut.

6.2. Seksuell utpressing

Et annet alvorlig utfall av trusselaktørers kontaktetablering med barn var seksuell utpressing. Det er i rapporteringsperioden sett eksempler på seksuell utpressing av barn under 14 år med både økonomisk og seksuelt motiv.

I ett tilfelle ble en jente kjent med en trusselaktør i spillet Roblox før kommunikasjonen ble flyttet til Snapchat. Trusselaktøren sendte jenta et bilde av et nærstående familiemedlem som han hadde funnet i sosiale medier og truet med at det ville skje noe med jentas familiemedlem dersom hun ikke sendte nakenbilder av seg selv. Jenta sendte et bilde, men trusselaktør ville ha flere bilder. Jenta varslet deretter foresatte, som tok kontakt med politiet.

I et annet tilfelle ble en gutt lagt til på Snapchat av trusselaktør via Quick Add. Gutten trodde han kommuniserte med en ung jente og sendte nakenbilder av seg selv til trusselaktøren. Kommunikasjonen ble så flyttet til Instagram, hvor trusselaktøren truet med å spre bildene til guttens venner og familie dersom han ikke kjøpte et gavekort til trusselaktør med en verdi på over 2000 kroner. Det fremkommer ikke hvilken type gavekort trusselaktør ba om.

6.3. Andre utfall

I ca 16 prosent av tilfellene foreligger det ikke informasjon om at kontakten mellom trusselaktør og barn endte med noe straffbart. I ett tilfelle har en trusselaktør som oppga å være 47 år kommet i kontakt med to jenter på Omegle før kontakten ble flyttet til Snapchat. Trusselaktøren ønsket å treffe jentene fysisk og inviterte dem ut på middag. I et annet tilfelle har en trusselaktør, en mann på 36 år, kontaktet en jente på TikTok og invitert henne ut på kaffe. I et tredje tilfelle har en trusselaktør, en 49 år gammel mann tidligere domfelt for seksuallovbrudd mot barn, kommunisert med fire elleveåringer på Teams.

Det er manglende opplysninger om hva som gjør at hendelsene ikke ender med noe straffbart. I flere av tilfellene framstår det tilfeldig ved at barnas foreldre oppdager kontakten og tar nødvendige grep. I andre tilfeller kan det være at barna avbryter kontakten av ulike årsaker.

Av Barn og medier-undersøkelsen framgår det at når barna blir spurt om de har blokkert noen i sosiale medier, inkludert på Snapchat, og hvorfor, er den vanligste årsaken fordi de har mottatt upassende innhold, som oftest fra en fremmed. Dette inkluderte blant annet nakenbilder og forespørsler om nakenbilder, kommentarer om barnets kropp og at den fremmede utgir seg for å være yngre enn sin faktiske alder.[19]

[19] Barn og medier – en undersøkelse om 9–18-åringers medievaner

Delvurdering: Det er *meget sannsynlig* at trusselaktører i all hovedsak kontakter/tilnærmer seg barn på internett i den hensikt å begå seksuelle overgrep. Dette underbygges av en høy forekomst av seksuallovbrudd som overordnet motiv og utfall. Det er *mulig* at det foreligger en skjevfordeling grunnet manglende kilder til informasjon som fanger opp tilfeller av kontaktetablering hvor barna ikke blir forsøkt seksuelt utnyttet.

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

7. Innvirkning på trusselaktørers mulighetsrom

Det er en rekke faktorer som innvirker på trusselaktørers mulighetsrom når de skal tilnærme seg barn på internett. Selv om eksempelvis både anonymiseringsteknologi og ende-til-ende-krypterte kommunikasjonsplattformer har flere legitime bruksområder, kan de også misbrukes av personer med uærlige hensikter. Samtidig kan ny teknologi bidra til å detektere og avverge ulike former for lovbrudd, herunder cyberstøttede seksuallovbrudd mot barn.

7.1. Anonymiseringsteknologi

Over tid har bruk av VPN- og proxy-tjenester[20] blant gjerningspersoner som begår cyberstøttede seksuallovbrudd bydd på utfordringer for politiet, blant annet fordi det vanskeliggjør eller umuliggjør identifisering av gjerningspersonene. En hovedutfordring er manglende regulering av VPN-tilbydere, som ikke omfattes av endringen i ekomloven fra 1. januar 2023, hvor internettilbydere ble pålagt å lagre informasjon om egne kunder i ett år.

Mange trusselaktører er opptatt av operasjonell sikkerhet og anonymitet på internett, men Kripos har informasjon om at meningene er delte hva gjelder bruk av VPN- og proxy-tjenester. På den ene siden mener noen at det gir tilstrekkelig beskyttelse, mens andre er av den oppfatning at man vil bli tatt dersom man ikke har omfattende tekniske kunnskaper og ferdigheter.

Det er utfordrende å få oversikt over omfanget av trusselaktører som benytter seg av VPN- og proxy-løsninger i sin kontaktetablering med barn. I tilfeller hvor sosiale medieplattformer avdekker og rapporterer mistenkelig kommunikasjon mellom voksne og barn, vil opplysninger om det potensielt straffbare forholdet eksempelvis meldes til National Center for Missing and Exploited Children (NCMEC) før videre rapportering til aktuelt lands myndigheter. All den tid trusselaktører velger å benytte seg av anonymiseringsteknologi som får IP-adressen til å framstå som at den tilhører et annet land, vil ikke informasjonen nødvendigvis tilfalle norsk politi. I de tilfeller politiet får informasjon fra privatpersoner kan det være vanskelig eller umulig å identifisere trusselaktøren(e).

[20] Proxy-nettverk består av flere servere som fungerer som mellomledd mellom internettbrukere og internett. Når internett-brukeren benytter en proxy-løsning skjules brukerens egentlige IP-adresse bak IP-adressen til mellomleddet. Målet for brukerens datatrafikk, for eksempel en nettside, vil på denne måten ikke regisrere brukerens egentlige IP-adresse. VPN-løsninger tar det samme oppsettet et steg videre ved å også kryptere datatrafikken mellom brukeren og mellomleddene. Det vil kun være mulig å se at datatrafikken kommer fra et VPN-nettverk.

7.2. Kunstig intelligens

I juni 2023 publiserte Kripos etterretningsrapporten *Generativ kunstig intelligens og cyberkriminalitet* som tar for seg mulighetene teknologien medfører for cyberkriminelle, inkludert seksuallovbrytere.

Kunstig intelligens (KI) gjør det enklere for trusselaktører å finne arenaer hvor barn oppholder seg på internett samt tilegne seg kunnskap om hvordan aktuelle spill- og kommunikasjonsplattformer fungerer. Videre finnes det KI-modeller som bruker dyp læring for å analysere og forstå skriftspråk, og som på den måten kan hjelpe trusselaktører med tilpasning av språk, ord og uttrykk i dialog med barn.[21] Generativ kunstig intelligens (GKI) gjør det i tillegg mulig å for eksempel generere bilder av falske barn som trusselaktøren kan utgi seg for å være i møte med barn på internett. Kunstig intelligente agenter (KI-agenter)[22] utgjør også en trussel dersom de misbrukes til cyberkriminelle formål, inkludert cyberstøttede seksuallovbrudd.[23] KI-agenter kan blant annet løse flere oppgaver simultant og vil gjøre det mulig å automatisere og effektivisere kontaktetableringsprosesser. En slik prosess vil kunne medføre at trusselaktører enklere plukker ut eller identifiserer barn som er ekstra utsatte for seksuallovbrudd på internett.

Samtidig kan KI benyttes til å skape forstyrrelser for trusselaktører. Både politi og samarbeidspartnere vil ved å utvikle og ta i bruk KI-verktøy for å detektere kontaktetablering med barn på internett, kunne avverge at de utsettes for seksuell utnyttelse. Politiet har eksempelvis samarbeidet med cybersikkerhetsfirmaet AIBA, som har utviklet et KI-verktøy som blant annet har til hensikt å stoppe trusselaktørers kontaktetablering med barn før dialogen rekker å utvikle seg til noe straffbart.[24]

Momio er en av flere plattformer som har tatt i bruk KI. Plattformen er utviklet av det danske IT-firmaet Momio Aps og er et kombinert spill og sosialt medium for personer under 18 år. På Momio kan brukeren sende og godta venneforespørsler, kommunisere i privat chat og i gruppechat. Brukere kan dele tekst, video og bilder i privat chat og på sider som er synlig for alle brukere av plattformen.[25]

Momio oppgir på sin nettside å være det tryggeste sosiale mediet for barn og har barns sikkerhet som fremste prioritet. Plattformen har en egen KI-moderator som sammen med et sikkerhetsteam monitorerer aktivitet på plattformen og setter inn tiltak når det anses nødvendig.[26]

---

[21] Large Language Models (LLM) er et eksempel på en slik type KI-modell

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

[23] Cyberkriminalitet 2024, utgitt av Kripos

[24] https://www.shifter.no/nyheter/henter-millioner-for-a-beskytte-barn-fra-grooming-pa-nett-og-overgrep/289729

[25] https://www.barnevakten.no/app/momio/

[26] https://www.company.momio.me/parents-safety

7.3. Ende-til-ende-krypterte plattformer

Bruken av ende-til-ende-krypterte meldingsplattformer[27] er stadig økende. I rapporten Cyberkriminalitet 2024 framgår det at plattformene skaper utfordringer for politiet og øker de cyberkriminelles handlingsrom. Dette gjelder også for trusselaktører som ønsker å komme i kontakt med barn på internett og utnytte dem seksuelt.

Teknologien gir trusselaktørene anonymisering og plattformene er like enkle å ta i bruk som andre sosiale medier. De er heller ikke kostbare. Meldingsplattformene sletter automatisk data og beskytter informasjonen i applikasjonene. For politiet kan det medføre at viktige spor går tapt.

Kripos har i løpet av 2023 observert at seksuallovbrudd som tidligere ble begått på åpne plattformer har flyttet seg til ende-til-ende-krypterte meldingsplattformer. Likevel er det kun observert få tilfeller av seksualisert kontakt mellom voksne og barn på slike plattformer, den foregår fremdeles hovedsakelig på åpne plattformer.[28]

Delvurdering: Det er *sannsynlig* at KI-verktøy vil bli brukt av trusselaktører til å komme i kontakt med barn på internett de neste seks månedene, både ved å tilegne seg kunnskap om arenaer barn bruker og ved tilpasning av språk. Det er *mulig* at trusselaktører også vil generere syntetiske bilder av barn som ikke finnes, for å forlede barn og utsette dem for seksuelle overgrep.

Det er *mulig* at KI-agenter vil bli tatt i bruk for å automatisere kontaktetablering med barn. Det er *mulig* at bruk av KI som ledd i å detektere trusselaktørers tilnærminger til barn på internett vil fungere som en motvekt og at det derfor ikke vil registreres en stor økning det kommende halvåret.

Det er *sannsynlig* at den økte bruken av ende-til-ende-krypterte meldingsplattformer og det faktum at flere plattformer konverterer til ende-til-ende-kryptering, vil medføre økt kontakt mellom trusselaktører og barn på plattformer med kryptert kommunikasjon i 2024. **Delvurdering slutt**

8. Overordnede vurderinger

Det er *meget sannsynlig* at trusselaktører vil fortsette å kontakte barn på internett, at trusselaktørene i hovedsak vil være menn og at både jenter og gutter vil være utsatt.

Det er *meget sannsynlig* at trusselaktører vil benytte flere ulike plattformer for å kontakte barn på internett, både store og kjente plattformer som Snapchat og mindre utbredte plattformer, herunder ulike chatroulette-plattformer.

Det er *sannsynlig* at virkemiddelbruk i sin helhet gjør at trusselaktører lettere kommer i posisjon til å begå seksuallovbrudd mot barn på internett. Det er *mulig* at økt bevisstgjøring hos barn, foresatte og kommunikasjonsplattformer rundt trusselaktørers

[27] Ende-til-ende-krypterte meldingsplattformer benytter seg av ende-til-ende-kryptering. Det vil si at det kun er deltakerne i en lukket gruppe som sender meldinger til hverandre som har tilgang til meldingene. Meldingene og filene krypteres før de sendes over nettverket med en nøkkel som bare deles mellom sender og mottaker. Også lyd- og videokommunikasjon kan krypteres fra ende-til-ende. Eksempler på slike plattformer er Telegram, Whatsapp og Signal.

[28] Cyberkriminalitet 2024, utgitt av Kripos

virkemiddelbruk vil kunne redusere forekomsten av kontakt med påfølgende seksuallovbrudd.

Det er *meget sannsynlig* at trusselaktører i all hovedsak kontakter/tilnærmer seg barn på internett i den hensikt å begå seksuelle overgrep.

Det er *sannsynlig* at utviklingen innen anonymiseringsteknologi, kunstig intelligens og ende-til-ende-krypterte kommunikasjonsplattformer vil bidra til økt mulighetsrom for trusselaktører i deres kontaktetablering med barn på internett. Det er *mulig* at KI vil kunne fungere som mottiltak og bidra til å avdekke, avverge og bekjempe kontaktetablering med og seksuell utnyttelse av barn.

9. Vedlegg

9.1. 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):

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