POLITIET
POLITIDIREKTORATET

Trusler og utfordringer innen IKT-kriminalitet (2017)

INNHOLD

RAPPORTENS FORMÅL OG OPPBYGNING

Denne rapporten er et av tiltakene i *Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet.* I et oppdragsbrev fra Justis- og beredskapsdepartementet til Politidirektoratet, datert 25. juni 2015, ble følgende oppdrag gitt:

> *Departementet ber Politidirektoratet ta ansvaret for å gjennomføre strategiens tiltak 2. Tiltaket innebærer at det skal utarbeides en særskilt, felles, årlig trusselvurdering for IKT-kriminalitetsfeltet innen Justis- og beredskapsdepartementets ansvarsområde som skal danne grunnlag for målrettet politiinnsats. Ved gjennomføringen av oppdraget, bes Politidirektoratet ta høyde for strategiens kapittel 4 om hovedutfordringer og hvordan disse kan møtes […].*

Begrepet IKT-kriminalitet omfatter i denne rapporten både
a) kriminalitet rettet mot datasystemer og
b) bruk av IKT som sentralt verktøy i utøvelsen av annen kriminalitet.[1]

Innen IKT-kriminalitet kan det være mange måter å oppnå ett og samme mål på, og samme form for IKT-kriminalitet kan brukes til å oppnå flere ulike formål. Til felles har IKT-kriminalitet at aktører ved hjelp av informasjons- og kommunikasjonsteknologi (IKT) påfører samfunnet skade eller tap.

Vi har valgt å fordele IKT-truslene på fire hovedkategorier som på ulikt vis synliggjør hvilke konsekvenser IKT-trusler har på samfunnet: Angrep på datasystemer (datainnbrudd og dataskadeverk), bedragerier og utpressing ved bruk av IKT, internett som marked for ulovlig varer og tjenester, og internett som arena trakassering, trusler og vold. Det er likevel ikke til å unngå at trusselen i enkelte tilfeller beveger seg over fra den ene kategorien til den andre.

I Del A, belyser vi aktuelle IKT-trusler. I Del B løfter vi frem felles utfordringer som går på tvers av de ulike truslene vi har beskrevet.[2]

Rapporten *Trusler og utfordringer innen IKT-kriminalitet (2017)* er skrevet av Kripos med støtte fra PST.

1 Europol (2017) bruker henholdsvis begrepene *Cyber-dependent crime* og *Cyber-facilitated crime* om disse to kategoriene.

2 Felles utfordringer kan mer eller mindre ses i sammenheng med det Europol (2017) betegner som «Cross-Cutting Crime Relevant Factors; factors that impact on, facilitate or otherwise contribute to multiple crime areas but are not necessarily inherently criminal themselves.»

HOVEDPUNKTER

Informasjons- og kommunikasjonsteknologi inngår i nesten alt vi foretar oss og blir en stadig viktigere del av samfunnet. I Norge blir stadig flere tjenester digitalisert, og nordmenn blir mer og mer eksponert for digitale løsninger. I 2016 rangerte World Economic Forum Norge som verdens 4. mest digitaliserte land, og vi er på 18. plass i bruk av IKT i offentlig forvaltning, opp seks plasser siden 2015.[3]

I Mørketallsundersøkelsen (NSR, 2016) fremkommer det at hele 44 % av respondentene har valgt å avstå fra å bruke tjenester på internett på grunn av frykt for datakriminalitet. I PWC Crime Survey (PWC, 2017) kommer det frem at norske virksomheter er mer bekymret for IKT-kriminalitet i 2016 enn de var i 2015.[4] «Dersom frykten for å ta i bruk digitale løsninger og tjenester blir stor, vil det bli en motkraft til den digitale omstillingen Norge er inne i» (Bjarte Malmedal, leder av NorSIS, ibid.).

Den økte frykten for datakriminalitet henger sammen med at IKT-trusselen har blitt større de siste årene. Ulike trusselaktører benytter seg i økende grad av digitale virkemidler for å nå sine mål.

IKT-trusselen stiger i takt med digitaliseringen av samfunnet og teknologiutviklingen

Mens fordelene ved teknologien er mange, følger det også en rekke trusler og utfordringer med den. Både statlige og ikke-statlige aktører vet å utnytte mulighetene teknologien gir til å utføre eller skjule sine (kriminelle) handlinger. IKT-kriminalitet er et begrep som favner et bredt spekter av kriminalitetsformer, ofre og gjerningspersoner.

Dataangrepene øker i frekvens og omfang både i Norge og Europa for øvrig, og faren for at den økende mengden sensitiv informasjon vi deler på internett kommer på å avveie og misbrukes har blitt større. Teknologiutviklingen har dessuten medført at fremmede stater og utenlandske kriminelle har fått bedre evne til å påvirke eller gjennomføre kriminalitet i Norge på stor avstand.

Flere fremmede etterretningstjenester med interesser i Norge har de senere årene brukt store ressurser på å utvikle kapasiteten innen digital spionasje, og Norge utsettes for etterretningsvirksomhet som kan ha stort skadepotensial.

Russland har utviklet sin evne til å gjennomføre digital sabotasje, for eksempel tiltak for å påvirke den politiske debatten eller svekke legitimiteten til politiske beslutningsprosesser. Dette innebærer spredning av desinformasjon, manipulasjon, propaganda og stimulering av sosial uro.

Kombinasjonen av at Norge er et velstående land og på verdenstoppen i internettbruk, gjør oss til attraktive mål for svindlere og personer som driver med utpressing. Internett gjør det lett for kriminelle å komme i kontakt med potensielle ofre, og IKT-verktøy kan bidra til å effektivisere svindel eller utpressing som baserer seg på sosiale manipulasjonsteknikker. Det foregår stadig mer utpressing og svindel over internett.

3 World Economic Forum (2016) *The Global Information Technology Report*. Side 16.

4 191 norske bedriftsledere, IT-ledere og sikkerhetsspesialister deltok i undersøkelsen. Undersøkelsen ble gjennomført av PWC med støtte fra NorSIS, Finans Norge og Bergen Næringsråd.

Den teknologiske utviklingen har bidratt til at tradisjonell kriminalitet kan utøves mer effektivt. Internett utnyttes i stadig større grad som kriminell markedsplass og kommunikasjonskanal. Teknologiutviklingen har i stor grad bidratt til at de kriminelle kan operere med lavere oppdagelsesrisiko.

IKT-kriminalitet kommer til å påvirke Norge og nordmenn i økende grad

Ettersom teknologien blir mer tilgjengelig og flere oppgaver og samfunnsfunksjoner flyttes over på nett, vil kriminalitet utført mot, eller ved hjelp av datasystemer bli en stadig større del av det totale kriminalitetsbildet.

Kunnskapsutviklingen blant trusselaktører innen IKT-kriminalitet skjer raskt, og terskelen for å utføre kriminelle handlinger eller fremme ekstreme holdninger er sannsynligvis lavere i den virtuelle verdene enn i den virkelige. Muligheten for anonymitet og kryptert kommunikasjon på internett kan ha bidratt til dette. På samme tid kan internettfora bidra til å normalisere og rettferdiggjøre kriminell adferd slik at flere begår handlinger de ellers ikke ville begått.

Utviklingen innenfor IKT-kriminalitet utfordrer politiets evne til å avdekke og etterforske kriminalitet

Det er viktig å utvikle kapasiteter og aktiviteter som kan demme opp for økende IKT-kriminalitet i samfunnet.

Utviklingen innenfor IKT-kriminalitet medfører at det blir stadig viktigere for politiet å få tilgang på lagret datatrafikk. IKT-utviklingen har derimot medført at det har blitt mer utfordrende for politiet å sikre spor og bevis i straffesaker. Manglende datalagring, sletting av lagrede data eller manglende samarbeid med tjenestetilbydere fører ofte til at spor og bevis ikke eksisterer eller er utilgjengelig når politiet har behov for informasjonen.

Et godt samarbeid med tjenestetilbydere og internasjonalt politi er ofte avgjørende for effektiv informasjonsinnhenting og etterforskning. Det er viktig med gode internasjonale kontaktpunkter og samarbeidsavtaler med tanke på internettrelaterte anmodninger og informasjonsbehov.

Kriminaliteten har blitt mer teknologidrevet, og den teknologiske utviklingen foregår i raskt tempo. Dette stiller store krav til politiets evne til å utvikle metoder og verktøy som kan bidra til å håndtere IKT-kriminalitet, for eksempel utfordringer knyttet til kryptering og anonymisering. Utviklingen stiller også større krav til teknologikompetanse og -utstyr både på grunnleggende og ekspert nivå i politiet.

Utviklingen innenfor IKT-kriminalitet utfordrer samfunnets evne til å forebygge, avdekke og anmelde IKT-kriminalitet

Utviklingen innenfor IKT-kriminalitet stiller høyere krav til datasikkerhet på alle nivåer i samfunnet. Det er viktig med gode tekniske sikkerhetsløsninger, men det er viktig å erkjenne at tekniske løsninger alene ikke kan løse alle utfordringer i denne sammenheng. Ofte spiller den menneskelige faktoren en avgjørende rolle når noen blir utsatt for IKT-kriminalitet. Det er derfor viktig å styrke sikkerhetskunnskapen og holdningene til sikkerhet på individnivå slik at den generelle sikkerhetskulturen i samfunnet blir styrket.

Mørketallene vedrørende IKT-kriminalitet er store. For at politiet skal få et bedre kunnskapsgrunnlag og være i stand til å målrette sin innsats, er det viktig at IKT-kriminalitet blir anmeldt på lik linje med annen type kriminalitet. Det er i denne sammenheng også viktig å legge til rette for at IKT-kriminalitet registreres på en effektiv og hensiktsmessig måte.

DEL A

AKTUELLE TRUSLER

A.1 Angrep på datasystemer – datainnbrudd og dataskadeverk

Med angrep på datasystem menes at noen får ulovlig tilgang til informasjon på datasystemer (brudd på konfidensialitet eller integritet), eller at datasystemer blir gjort utilgjengelig for rettmessig eier (brudd på tilgjengelighet).

Tyveri av informasjon, manipulering av informasjon, uautorisert destruksjon av data og hindring av normal drift av digitale tjenester er eksempler på kriminalitet som retter seg mot datasystemer. Alle datamaskiner tilkoblet internett er mulige mål for slik kriminalitet, og et angrep kan komme fra en hvilken som helst datamaskin i verden.

Angrep mot datasystemer har mange aspekter ved seg. Angrepene kan være rettet mot både personlige brukere, bedrifter, organisasjoner og staten. De ulovlige gjerningene begås av både statlige, statlig sponsede og ikke-statlige aktører, for eksempel vinningskriminelle grupper, konkurrerende bedrifter, ideologiske aktivister og ekstremist-grupper.

Innbrudd i datasystemer som resulterer i ulovlig tilgang til eller ulovlig formidling av private data eller immaterielle rettigheter øker i frekvens og omfang.[5] I Norge har NSM gjennom flere år sett en tydelig og jevn økning av antall målrettede dataangrep mot norske interesser, både offentlig og privat.[6] Dataangrep som ble avdekket i 2015 var større, mer avanserte og mer komplekse enn de var tidligere, og det er holdepunkter for å si at det er stor aktivitet fra trusselaktører mot Norge.

Avanserte trusselaktører er dessuten i stand til å infiltrere systemer og hente ut informasjon uten å bli oppdaget. «Angriperne utvikler sine teknikker raskere enn utviklingen av mottiltak. Dette er i praksis et våpenkappløp, og [NSM] forventer at slike angrep vil øke fremover.»[7]

Flere av aktørene har svært høy kompetanse og besitter store ressurser til utvikling, planlegging og gjennomføring av digitale innbruddsforsøk. Kripos har i 2017 innledet etterforskning mot flere personer som mistenkes for besittelse og spredning av ulike skadevarer. Noen av personene har også knytninger til andre hendelser som innbefatter distribuerte tjenestenektangrep (DDoS).

I en konkret undersøkelse ble det registrert mange norske brukere av en skanner- og/eller krypteringstjeneste. Det førstnevnte finner ut hvilke kommersielle antivirusprogrammer som detekterer at filen som blir testet inneholder programkode for skadevare. Krypteringstjenesten er designet for å endre programkoden i binærfilen til en skadevare, slik at den blir vanskelig for antivirusprogrammet å detektere.

Samtidig viser tall fra internasjonalt politisamarbeid at Norge ligger på et høyt internasjonalt nivå (nr.9 av 80 land) hva gjelder antall kjøpere av en konkret skadevare av typen Remote Access Trojan (RAT). Den kan gi kriminelle ulovlig tilgang til andres datamaskiner, blant annet ved å logge tastetrykk, hente ut informasjon (bilder, videoer og dokumenter) og kjøre kommandoer (flytte eller slette filer, ta skjermbilde, kontrollere webkamera samt lytte til datamaskinens mikrofon).

5 Europol (2017).

6 NSM (2017) *Risiko 2017: Risiko og sårbarheter i en ny tid. En vurdering av sårbarheter og risiko i Norge.*

7 NSM (2016) Risiko *2016: Kan risiko styres? En vurdering av sårbarheter og risiko i Norge.*

Mobiltelefoner fungerer i økende grad som mobile datamaskiner, og angrepene mot dem begynner å ligne på angrep mot datamaskiner.[8] I tiden fremover vil trolig skadevaretrusselen mot mobiltelefoner øke.

I Mørketallsundersøkelsen (2016) fremkommer det at over en fjerdedel av virksomhetene har opplevd uønskede sikkerhetshendelser det siste året. I PWCs cyber crime survey (2017) svarer 58 % av de norske respondentene at de har vært utsatt for datakriminalitet i løpet av de siste 12 månedene. 41 % svarer at angrepene medførte økonomiske tap for selskapet, og en fjerdedel indikerer selv at kostnadene overstiger en million norske kroner.

A.1.1 Skadevare og id-tyveri

Skadevare er i denne sammenheng ondsinnet programvare som typisk stjeler brukerdata, for eksempel kredittkortnummer, innloggingsinformasjon og personlig informasjon fra infiserte datamaskiner. Selskaper som oppbevarer betalingsopplysninger er attraktive mål for kriminelle, spesielt hotell- og detaljvarehandelen. Det er en økende trend at også andre typer data blir kompromittert, som for eksempel helseopplysninger.[9] Slike opplysninger kan utnyttes av kriminelle til mange ulike formål, for eksempel utpressing og mer målrettet svindel.

Flere norske virksomheter utsettes daglig for tusenvis av fiendtlige e-poster. Et selskap mottok for eksempel 6000 e-poster på en time, hvorav 1200 av disse var unike. Slike saker etterforskes sjelden, og i de tilfellene det iverksettes etterforskning, kommer den ofte for sent i gang. Dette kan skyldes flere forhold, blant annet at selskapene ofte ikke velger å anmelde hendelser fordi selskapene prioriterer avverging og skadebegrensning foran bevissikring.[10]

Angrepsteknikker som *nettfiske (**phishing og spear phishing**)* blir ofte benyttet for å stjele brukerdata. Mange som mottar e-post med vedlegg som inneholder skadevare, åpner denne slik at datamaskinen deres blir infisert. Angrepet kan komme i flere bølger, der skadevaren kan være skreddersydd og bli endret mellom angrepsbølgene. Dette gjør det krevende å oppdage og håndtere angrepene. Når en trusselaktør først oppnår fotfeste i et system eller nettverk, kan veien inn til verdifull og sensitiv informasjon i mange tilfeller være kort.

*Nettfiske i sanntid (**Real-time phishing eller RTP**)*[11] er fortsatt aktuelt i Norge, og det avdekkes stadig nye kampanjelignende RTP-angrep mot mål i Norge. Det er for eksempel avdekket flere tusen kompromitterte servere som har eller kan ha blitt benyttet til RTP, og i perioden september – desember i fjor, ble det oppdaget cirka 150 RTP-kampanjer. Et eksempel er RTP-kampanjen, «Skatteetaten», som hadde 25 banker som mål. Den samme grupperingen har også forsøkt å utgi seg for å være Apple for å få tak i kredittkortdata.

A.1.2 Løsepengevirus (ransomware)

Det siste året har det vært en markant økning i antallet løsepengevirushendelser i Norge, det vil si hendelser der ofrene får sine filer kryptert eller gjort utilgjengelige av gjerningspersoner som krever betaling for å dekryptere dem. Løsepengevirus kan ha store konsekvenser for næringsvirksomheter som ikke tar jevnlige sikkerhetskopier. Europol (2017) vurderer løsepengevirus som den største skadevaretrusselen med hensyn til konsekvenser for samfunnet; den overskygger trusselen fra *banktrojanere*[12] og annen skadevare som har til hensikt å stjele data.

8 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016.*

9 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016.*

10 For eksempel Aarø Njie, R. (2017) Kripos advarer:–Stor økning i datakriminalitet. *NRK* [Internett], 3.april. https://www.nrk.no/norge/kripos advarer_-_-stor-okning-i-datakriminalitet-1.13436174

11 For eksempel at bruker blir lurt til å logge inn eller legge inn sensitiv informasjon på en falsk nettside som etterligner den legitime nettsiden.

12 En trojaner er ondsinnet programvare som under falskt flagg har fått lov til å etablere seg i et datasystem. Den skaper skjulte bakdører inn i systemet ved å utnytte kjente sårbarheter.

55 % av de norske respondentene i PWCs cyber crime survey (2017) har i løpet av de siste 12 månedene blitt utsatt for [digital] utpressing. Kripos er for eksempel kjent med at et norsk selskap registrerte 200 forskjellige tilfeller av løsepengevirus i løpet av noen timer.

Det finnes en rekke ulike typer løsepengevirus, og aktørene som står bak kan være svært vanskelig å spore. Angrepet skjer som regel via epost som tilsynelatende ser legitim ut og som inneholder lenker eller vedlegg, for eksempel falsk epostfaktura fra mobiloperatører eller lenker til filer som ser ut til å være lagret i kjente skytjenester. Kripos observerer at virusene har blitt mer sofistikerte og at det har oppstått et marked der aktører som utvikler løsepengevirus, selger dem til andre som står for selve utpressingen. Det har dessuten blitt mer vanlig at betalingen kreves utført gjennom ***kryptovaluta***[13].

12. mai 2017 ble det kjent at skadevaren «WannaCry» spredde seg til datamaskiner over hele verden. Skadevaren skiller seg fra tidligere kjente løsepengeviruskampanjer ved at den sprer seg automatisk i nettverket ved hjelp av en kjent sårbarhet i programvare fra Microsoft. Kampanjen har ikke vært målrettet mot verken system, sektor eller region.[14] Det forventes at det kommer flere lignende angrep i fremtiden.

A.1.3 Angrep mot betalingssystemer

Etter en topp i 2012 har antallet vellykkede ***nettbankbedragerier*** gått ned. Bedrageriene gjennomføres med trojanere som infiserer offerets datamaskin via nettsider som offeret gjerne lures til å besøke, eller ved at offeret oppgir påloggingsinformasjon på en falsk nettside som utgir seg for å være nettbanken. Dermed får gjerningspersonene mulighet til å gjennomføre transaksjoner uten kontoeierens viten.[15]

Nedgangen i antall vellykkede bedragerier rettet mot norske nettbankkonti kan skyldes at bankene har innført bedre sikkerhetsrutiner og er blitt flinkere til å oppdage og stoppe mistenkelige transaksjoner. Selv om det har vært en markant nedgang i antall vellykkede bedragerier, bør ikke trusselen undervurderes. Bedrageriene har rettet seg mot mange forskjellige norske banker, og utvikling av nye teknikker, som bankene ikke oppdager, gjør at store beløp kan gå tapt. Bankene opplever at bedragerikampanjene rettet mot dem går i bølger. Det var i 2016 flere eksempler på at aktører utviklet angrepskode, testet og planla bedragerier mot norske banker.[16] Det er observert en økning i bruken av banktrojanere i andre land den siste tiden og det er sannsynlig at trusselen også mot norske banker vil øke i tiden fremover.

13 Kryptovaluta er en variant av virtuell valuta. Virtuell valuta er en «digital representasjon av verdi som hverken er utstedt av en sentralbank eller offentlig myndighet, og heller ikke nødvendigvis knyttet til en flat valuta, men er akseptert (...) som betalingsmiddel og kan overføres, lagres eller handles elektronisk». Virtuelle valutaer kan være mer eller mindre konvertible. Enkelte typer, som Bitcoin, kan uten vanskeligheter veksles til andre valutaer. Sentraliserte valutatyper styres av en tredjepart, som utsteder valutaen og fastsetter regler for bruken. Desentraliserte varianter benytter kryptografi for å generere nye valutaenheter og for å sikre kontroll over transaksjoner, og omtales gjerne som kryptovaluta. For kryptovalutaer foregår transaksjonene direkte, uten mellomledd. Bitcoin er en kryptovaluta, og er den virtuelle valutaen som har størst utbredelse (Justisdepartementet (2016:8) Nasjonal risikoanalyse hvitvasking og terrorfinansiering)

14 NSM (2017): Beskyttelse mot løsepengevirus/ransomware. NSM [internett], 15.mai. https://nsm.stat.no/aktuelt/beskyttelse-mot-ransomware/

15 Et nettbankbedrageri er en omfattende prosess som krever et større maskineri– fra utvikleren av programvaren der transaksjonene opprettes, til personer som kan ta ut penger og realisere gevinsten.

16 En norsk bank oppdaget eksempelvis mistenkelig aktivitet mot nettbankstrukturen deres som lignet på den kjente trojaneren Dyre. Dyre var en «crime as a service» trojaner som tidligere ble benyttet i suksessfulle phishing-kampanjer ovenfor banker. Trusselen forsvant etter at det ble gjennomført arrestasjoner i Russland i 2015.

Det har vært flere tilfeller av ***SWIFT-bedragerier*** i utlandet der svindlere har infiltrert systemet som overfører penger mellom finansinstitusjoner i ulike land (SWIFT – Society for Worldwide Interbank Financial Telecommunication). Spesielt vakte et stort datainnbrudd i sentralbanken i Bangladesh vinteren 2016 betydelig oppmerksomhet. Svindlerne lyktes i å lure banken til å overføre 81 millioner dollar fra Federal Reserve Bank i New York til en bank på Filippinene. Pengene ble videresendt fra banken på Filippinene til ulike kasinoer. Dette omtales som et av de største bankbedrageriene i historien. Svindlerne forsøkte opprinnelig å overføre en milliard dollar, men skrivefeil gjorde at enkelte transaksjoner ble stoppet.[17] Det er i tillegg kjent at det ble gjennomført et vellykket angrep mot banker i Ukraina våren 2016. På bakgrunn av at svindlere har lykkes i å gjennomføre bedragerier via SWIFT-systemet, er det sannsynlig at det vil komme flere forsøk og at noen vil lykkes.

Innføring av EMV (chip and PIN), geoblocking og andre sikkerhetstiltak har medført en reduksjon i ***fysisk kortsvindel*** (card-present fraud) i Europa. Svindel ved bruk av ***falsk kortinformasjon*** (card-not-present) har derimot blitt et større problem, spesielt med tanke på kjøp av fysiske varer og flybilletter, bilutleie og overnatting.[18] Kompromitterte kortdata er til salgs og lett å kjøpe på forum og markedsplasser på Internett. Det er dessuten «butikker» på *det mørke nettet*[19] som selger selvgenerert betalingskortinformasjon.[20]

Logiske angrep mot bankautomater er et økende problem i Europa. Det vil si at kriminelle benytter seg av elektronisk utstyr eller skadevare for å ta kontroll over en betalingsautomat. På den måten kan de ta ut penger eller stjele kortinformasjon. Det er også indikasjoner på at kriminelle grupper har begynt å manipulere eller kompromittere ***betalinger via det kortløse betalingssystemet NFC*** (Near Field Communication).[21] Dette demonstrerer hvor raskt kriminelle aktører kan tilpasse seg til og utnytte nye teknologiske løsninger og digitaliseringen av samfunnet.

A.1.4 Tjenestenektangrep

Distribuert tjenestenektangrep eller ***Distributed-Denial-of-Service (DDoS)***[22] er angrep som har til hensikt å hindre andre å få tilgang til en tjeneste, ressurs eller lignende på internett. Slike angrep er et yndet middel for å drive utpressing eller aktivisme, gi uttrykk for misnøye eller skjule andre former for datakriminalitet. Det koster norske og utenlandske virksomheter mye infrastruktur og arbeid for å beskytte seg mot slike angrep. Likevel utgjør DDoS angrep en viss risiko.[23]

DDoS angrep kan enkelt kjøpes på nett for små summer og gjør mange i stand til å påføre skade i millionklassen. Sakene er vanskelige å etterforske og peker ofte utenlands.

17 Quadir, S (2016) How a hacker's typo helped stop a billion dollar bank heist. *Reuters* [internett], 10.mars. http://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC

18 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016.*

19 Det mørke nettet blir også kalt *the dark web* eller the *dark net*. The dark web, er World Wide Web-innhold som befinner seg på *dark net* – et type nettverk (for eksempel Tor-nettverket) som bruker det åpne internettet, men som krever spesifikk software, konfigurasjon eller autorisasjon for å få tilgang. The dark web utgjør en liten del av deep web – innholdet på internett som ikke er indeksert av standard søkemotorer.

20 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016.*

21 Ibid.

22 Tjenestenektangrep gjennomføres ved at offerets datasystem utsettes for så stor datatrafikk eller belastning slik at legitim trafikk ikke kommer igjennom eller at systemet bryter sammen. Dette kan gjøres ved å styre flere maskiner (som samlet sett har større båndbredde enn offerets datasystem) til å være aktive mot offerets datasystem. Det kan også gjøres ved å utvikle og plante programmer som kopierer seg selv (virus), slik at offerets datasystem blir overarbeidet og til slutt stopper opp.

23 For eksempel Woolf, N (2016) DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian* [internett], 28. oktober. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

DDoS attacks continue to grow in intensity and complexity, with many attacks blending network and application layer attacks. Booters/stressers are readily available «as-a-service», accounting for an increasing number of DDoS attacks (Europol, 2016).

I det siste året har det vært i gjennomsnitt 750 tjenestenektangrep i måneden mot Telenors nett og kunder i Norge, Sverige og Danmark.[24] Til tross for dette har antall vellykkede tjenestenektangrep gått ned, sannsynligvis fordi norsk infrastruktur har blitt mer motstandsdyktig. Erfaringen i Norge er likevel at angrepene blir stadig kraftigere. De har også blitt billigere og enklere å gjennomføre. Telenor har sett angrep der samme kunde blir angrepet flere steder samtidig, eksempelvis på tjenester som leveres fra ulike datasentre. Denne typen angrep er ikke tilfeldig og utføres gjerne av en konkurrent eller noen som driver med utpressing.[25] Politiet etterforsket eksempelvis en sak hvor to IT-ansatte i 2013 utførte dataangrep imot sin egen arbeidsgiver og i 2015 mot et samarbeidende firma. De to personene ble i november 2016 dømt til elleve mnd. ubetinget fengsel hvorav cirka fire mnd. for dataangrepet.

Det har blitt mer vanlig at det trues med å gjennomføre tjenestenektangrep såfremt ikke offeret betaler løsepenger i form av vanlige pengeoverføringer eller overføring av *kryptovaluta*.[26] Det finnes kriminelle grupper som spesialiserer seg på å true virksomheter på denne måten.[27] Mange klarer å slå ut mindre nettverk i en kortere periode, men enkelte har ikke evnen til å gjennomføre så sterke angrep som de truer med.

A.2 Bedrageri og utpressing ved bruk av IKT

I takt med økningen i bruken av internett, øker omfanget av bedragerier via internett. Kombinasjonen av at Norge er et velstående land og på verdenstoppen i internettbruk, gjør oss til attraktive mål for svindlere.

Kriminelle bruker flere fremgangsmåter for å lure enkeltpersoner eller organisasjoner til å overføre penger eller informasjon til dem på falske premisser. Denne formen for svindel hviler tungt på sosiale manipulasjonsteknikker, og som regel spiller også IKT-verktøy en sentral rolle.[28] Dette kan være bruk av skadevare, falske profiler på internett, medbrakte kortterminaler, falske telefonnummer eller e-postadresser.

Gjennom sosial manipulasjon lures ofre til å oppgi sensitiv informasjon eller overføre penger til det de tror er en legitim mottaker. Informasjonen kan brukes til videre manipulasjon eller til andre former for kriminalitet, som identitetstyveri eller utpressing på internett. Disse forsøkene blir stadig mer presise og sofistikerte.

Aktører som bedriver bedragerier over internett, prøver stadig å finne nye måter å lure penger eller informasjon ut av ofrene sine på. Så snart en metode blir kjent for å fungere, kaster andre kriminelle seg på. Dette kan være én forklaring på hvorfor mengden bedragerier ofte går i bølger. Det betyr også at selv om man klarer å bekjempe én form for svindel, så forsvinner ikke trusselen fra tilpasningsdyktige aktører som står bak.

24 Næringslivets sikkerhetsråd (2016) *Mørketallsundersøkelsen*. Side 12.

25 Ibid.

26 Se fotnote 13.

27 «D4BC» og «Armada Collective» er eksempler på grupper som har truet norske virksomheter. Etter at politiet aksjonerte mot DD4BC, har det dukket opp nye aktører som prøver å kopiere dem.

28 Europol (2017).

A.2.1 Pengeoverføringer på falske premisser

Toppsjefsvindel (CEO fraud) foregår ved at som regel utenlandske personer kontakter ansatte i store internasjonale selskaper, utgir seg for å være en toppsjef i selskapet og ber dem overføre penger til en konto i utlandet. Både avsenders e-postadresse og navn fremstår som reelle for mottakeren. For å lykkes med slik kriminalitet må gjerningspersonene ha en viss innsikt i virksomhetens interne struktur.

> *A refined variant of spear phishing, CEO fraud, has evolved into a key threat as a growing number of businesses are targeted by organised groups of professional fraudsters. Successful CEO frauds often result in significant losses for the targeted companies (Europol 2016).*

Økokrim erfarer at trenden med toppsjefsvindel ble særlig merkbar i slutten av 2015 og begynnelsen av 2016 og vurderer at bedragerne nå for alvor innretter seg mot norske bedrifter. Mørketallene innenfor denne type bedragerier vurderes å være store. Norske bedrifter kan være fristet til ikke å anmelde, i frykt for å tape omdømme.[29]

Kripos kjenner til at en rekke norske selskaper har blitt utsatt for forsøk på toppsjefsvindel, og det anses som et økende problem. Ved ett tilfelle overførte et stort selskap over 500 millioner kroner, hvorav omtrent 100 millioner anses som tapt.[30] Det er gjort flere vellykkede forsøk på å svindle selskaper for store beløp på denne måten. Det utføres i tillegg mange små bedragerier der risikoen for å bli oppdaget er lav, mens den totale fortjenesten er høy.

Størstedelen av bedragerier som retter seg mot privatpersoner, begås nå via internett. ***Dating- og nigeriabedragerier*** mot norske borgere er fremdeles omfattende, og store summer sendes årlig ut av landet. I 2015 ble det registrert at 209 personer sendte ut 280 millioner kroner til antatte bedragere.[31]

Det har blitt mer vanlig at kriminelle tar kontakt med privatpersoner ved å fremstå som representanter for legale virksomheter, for eksempel brukerstøtte fra Apple o.l. ***Microsoftsvindel*** er spesielt aktuelt. Da fremstår gjerningspersonene som Microsoft-representanter når de kontakter privatpersoner på telefon eller e-post. De sier det er feil med PC-en til offeret og ber om personlige opplysninger for å rette opp feilen. Dersom offeret oppgir disse får gjerningspersonene muligheten til å overta PC-en deres. Enkelte oppdager først svindelen etter at pengene er trukket fra konto. E-postene fremstår som ekte, men dersom man besvarer e-postene går svarene til ulike andre e-post adresser. Bruk av private telefonnummer som har blitt klonet over internett kan også være aktuelt i denne sammenhengen. De fleste gjerningspersonene gjennomfører sannsynligvis kriminaliteten fra utlandet.

Getsvindel er også aktuelt, og modusen ligner på Microsoftsvindel. Svindlerne bruker sannsynligvis *klonede telefoner*[32] eller falske telefonabonnement, som er opprettet på bakgrunn av ID-tyveri, når de tar kontakt med offeret. I motsetning til ved Microsoftsvindel møter de fysisk på stedet for å stjele betalingskort, motta betaling eller utføre kortskimming ved bruk av medbrakt kortterminal.

29 Justisdepartementet (2016) *Nasjonal risikoanalyse hvitvasking og terrorfinansiering.*

30 Widerøe, R.J. og Solberg, T. (2017) Historien om «Operasjon Jackpot» – politi spilte direktør og rundlurte svindlere. *VG* [Internett], 20. mars. http://www.vg.no/nyheter/innenriks/krim/historien-om-operasjon-jackpot-politi-spilte-direktoer-og-rundlurte-svindlere/a/23951666/

31 Justisdepartementet (2016) *Nasjonal risikoanalyse hvitvasking og terrorfinansiering.*

32 En klonet telefon er en telefon som identifiserer seg som en annen telefon overfor telenettverket. Med andre ord vil det si at svindleren utnytter et annet telefonabonnement; det fremstår som at noen andre ringer (telefonnummer), og det er noen andre som betaler for samtalen. Dette gjøres ved at svindlerne får tak i serienummeret til en annen telefon for deretter å programmere det inn i sin egen. I mange tilfeller har utro tjenere i mobilbransjen skaffet dem serienummeret på nye telefoner som selges.

A.2.2 Barnelokking (grooming)

Kontaktetablering og utvikling av tillitsforhold til barn over internett, med formål om å avtale et fysisk møte kalles gjerne ***barnelokking***, eller ***grooming***.[33] Svært ofte ser imidlertid politiet at slik etablering og tillitsskapende kontakt kan finne sted, uten at formålet nødvendigvis er avtale om et fysisk møte. Med utviklingen av netteknologi, med bilder og video med høy oppløsning og direkte videochat, er dette i mange tilfeller tilstrekkelig for den som ønsker en seksualisert kontakt med barn. Politiet har i flere slike straffesaker avdekket at en enkelt overgriper har lyktes i å etablere en seksualisert kontakt med flere titalls eller hundretalls barn.

Voksne som ønsker en seksualisert kontakt med barn på nettet gjør ofte dette gjennom ulike chattetjenester. Den seksualiserte kontakten kan oppnås ved at gjerningspersonen gjennom en falsk nettidentitet manipulerer barnet til å bli overbevist om at det kommuniserer med en jevnaldrende. I flere saker har politiet sett at gjerningspersonen har opprettet flere nettidentiteter, og kontakter gjerne det samme barnet fra flere av identitetene, noe som forsterker manipuleringen. Med denne fremgangsmåten kan gjerningspersonene, på tross av en betydelig aldersforskjell, likevel evne å etablere et tillitsforhold med barn, som kan resultere i fysiske seksuelle overgrep.

A.2.3 Seksuell utpresssing (sextortion)

«Coercion and sexual extortion are increasingly being used to victimise children» (Europol, 2016). Seksuell utpressing på internett innebærer at seksualiserte bilder eller filmer brukes til å presse den som er avbildet for penger, til å sende mer materiale eller til å utføre seksuelle handlinger via direkteoverføring (webkamera) på internett eller i det virkelige liv. Produksjonen og delingen av det seksuelle materialet kan være frivillig, eller resultat av en manipulerende prosess i forkant. Ofte har man kun til hensikt å dele materialet med personer man stoler på, men det kan bli plukket opp av personer med kriminelle hensikter. Det selges dessuten bildepakker og guider for gjennomføring av seksuell utpressing på internett, der det reklameres med at det er lettjente penger.

Både profesjonelle aktører og enkeltpersoner driver seksuell utpressing, og utpresserens motivasjon kan være økonomisk eller seksuell. Særlig den seksuelle motivasjonen går igjen i mange anmeldelser for seksuell utpressing mot barn. Gjerningspersoner som manipulerer ofre til å ta seksualiserte bilder, kan utnytte et stort antall ofre, ofte mange titalls i samme periode. Det økonomiske utbyttet kan derfor være stort. Utpressingsbeløpene varierer fra et par tusen kroner til flere titallstusen kroner. Ofrene blir ofte bedt om å betale med *kryptovaluta*[34] eller via utenlandske betalingsforetak (Western Union, Moneygram o.l.). Det siste året er det registrert flere hendelser med seksuell utpressing i Norge, men mørketallene er sannsynligvis store. De som blir utsatt for slik utpressing kan, som ved andre typer seksuallovbrudd, ofte føle skam og skyldfølelse og dermed vegre seg for å anmelde forholdene til politiet.

I mange saker utviser gjerningspersonene en betydelig hensynsløshet. Konsekvensene kan derfor være svært store for de som blir utsatt for seksuell utpresning. I verste fall kan det være fare for liv og helse. Det er eksempler i utlandet på at personer har begått selvdrap etter å ha vært utsatt for denne type utpresning. Trolig har det også skjedd i Norge.

Den store mengden bilder og sensitiv informasjon på nettet gir grobunn for trusler og utpressing mot enkeltpersoner, og muligheten for å finne seksualiserte bilder og filmer på internett som kan misbrukes, blir stadig større. Det er stadig flere barn som

33 Straffeloven (2005) § 306: *avtale om møte for å begå seksuelt overgrep.*

34 Se fotnote 13.

bruker smarttelefoner, noe som gir dem tilgang til sosiale medier og kommunikasjonsapplikasjoner.

Samtidig har det blitt større aksept for å ta utfordrende seksualiserte bilder eller filmer av seg selv og distribuere dem ved hjelp av mobiltelefoner og/eller internett. Det forventes derfor en økning av tilsvarende saker i tiden fremover.

A.3 Internettmarked for ulovlige varer og tjenester

På *det mørke nettet*[35], kan kriminelle kommunisere tilnærmet anonymt, samt skaffe seg illegale produkter som kan brukes til kriminelle handlinger. Kriminelle utnytter eller etablerer markedsplasser på internett i økende grad i forbindelse med kjøp og salg av ulovlige varer og tjenester.[36] Internettmarkedet har dessuten aktualisert bruken av *virtuell valuta*, spesielt *kryptovaluta*.[37]

A.3.1 Ulovlig handel med bombekjemikalier

EU forordning 98/2013 ble implementert i Norge, 20. juni 2015, gjennom «Forskrift om håndtering av utgangsstoffer for eksplosiver». Denne innebærer et generelt forbudt mot salg av stoffer oppført på *liste en* (over gitte konsentrasjonsgrenser) for privatpersoner og virksomheter uten yrkesmessige behov. For stoffer oppført på *liste to*, er det krav om rapportering av mistenkelige transaksjoner, tyveri og svinn.[38] Før nytt lovverk trådte i kraft 20. juni 2015 var det eksempelvis fullt mulig for privatpersoner å handle kjemikalier på *liste en*.

Det finnes lite data for å anslå omfanget av ulovlig handel med kjemikalier på internett. Tollvesenet har ikke avdekket ulovlig import av kjemikalier som står oppført på *liste en* etter 1. januar 2016, men det avdekkes enkelte hendelser som involverer norske borgere som har bestilt forbudte kjemikalier fra norske leverandører uten yrkesmessig behov. Siden 1. januar 2016 har Kripos mottatt cirka 50 tips fra tollvesenet vedrørende betydelig og uforklarlig svinn og tyveri av bombekjemikalier eller mistenkelige transaksjoner i denne sammenheng.[39] I de fleste tilfellene finnes det ikke holdepunkter for å si at det har vært noe straffbart eller mistenkelig knyttet til importen.

I praksis er det vanskelig å handle forbudte kjemikalier innenfor EU etter at EU forordning 98/2013 trådte i kraft. Samtidig er det utfordrende å kontrollere hva privatpersoner bestiller fra land utenfor EU. Omfanget lavverdiforsendelser er på over en million forsendelser i året, og kravene til deklarering av lavverdiforsendelser er små. Det kan derfor ikke utelukkes at det handles kjemikalier på internett og at det forekommer smugling av kjemikaler skjult i pakker med falsk deklarering (f.eks. deklarert som urter).

A.3.2 Ulovlig handel med skytevåpen

Det er liten tvil om at ulovlige skytevåpen har blitt mer tilgjengelig via internett. Det har i 2016 vært enkelte straffesaker knyttet til denne typen ulovlig handel, der ulovlige skytevåpen og våpendeler har blitt importert fra utlandet for deretter å bli omsatt på åpne nettsider i Norge. Nordmenn har også forsøkt å kjøpe ulovlige våpen på markedsplasser på det *mørke nettet*[40]. Som regel sendes trolig våpen og våpendeler som handles på internett per post til mottagere i Norge.

35 Se fotnote 19.

36 Europol (2017).

37 Les fotnote 15.

38 Forskriften ligger under brann- og eksplosjonsvernloven. Utgangsstoffer for eksplosiver er også forbudt jfr. straffeloven §§ 190 og 191, men den viser videre til brann og eksplosjonsvernloven som definerer hvilke stoffer som er regulert. Forskriften nevner ikke liste eller vedlegg. Dette benyttes i EU forordningen (annex 1 og 2).

39 Noen av tipsene omhandler stoffer som står oppført på *liste to,* men i de fleste tilfellene er ikke kjemikaliene gjenstand for regulering.

40 Les fotnote 19.

Netthandel som modus medfører at den enkelte kjøper i mindre grad enn før er avhengig av å ha opparbeidet seg kontakter i kriminelle nettverk. Bruk av krypterte applikasjoner ved ulovlige transaksjoner kan i økende grad vanskeliggjøre bekjempelse av ulovlig erverv av skytevåpen gjennom internett.

Spredningen og tilgjengeligheten av ulovlige skytevåpen i Europa øker faren for at slike våpen benyttes i terroranslag. Pågående konflikter i EUs nærområder kan bli en kilde til våpen for ulovlig handel på nett. Det er også mulig at teknologisk utvikling i 3D-printing med metaller gjør at ulovlig våpenhandel på internett blir enda mer relevant.

A.3.3 Kjøp og salg av narkotika

Kjøp og salg av narkotika har beveget seg mer og mer over på elektroniske plattformer i de siste årene.[41] «Online marketplaces on the Darknet are now a key platform used to advertise and sell all types of drugs» (Europol, 2017).

Narkotikamarkedet på internett gir både kjøper og selger mulighet til å komme i kontakt med hverandre gjennom skjulte markedsplasser og på kryss av landegrenser. Med en forretningsmodell som ikke er avhengig av personlig kontakt eller fysiske møter, styrker de kriminelle evnen til å skjule sin identitet. Tilgangen til anonymitet og krypterte kommunikasjonstjenester på internett bidrar til å forsterke følelsen av egen trygghet.

Det har vært observert en stadig økning i narkotikaomsetningen via internett, spesielt fra tollvesenets side. Narkotikaen som kjøpes over internett distribueres i all hovedsak via postforsendelser.

I Norge rapporterer samtlige politidistrikter at kjøp og salg av narkotika over internett er en økende bekymring.[42] Dette eksemplifiseres godt i økningen i antall saker som omhandler nye psykoaktive stoffer (NPS) i perioden 2008-2016.[43] Disse stoffene blir i stor grad kjøpt og distribuert via internett.

Tilslag mot markedsplasser andre steder i verden har avdekket at personer i Norge både har kjøpt og solgt narkotika gjennom dem, og i 2016 siktet Kripos flere personer i nettverk som omsatte narkotika på internett.[44] Dersom myndighetene stopper et nettverk eller en markedsplass på internett, står som regel andre aktører raskt klare til å ta over narkotikahandelen.

Narkotika som selges over internett er ofte av høy kvalitet og/eller styrkegrad, og kjøper har et stort utvalg av produkter å velge blant.[45] I produkter med høy potens er brukerdosene lavere og det kan medføre en høyere risiko for feildosering. Dette er observert i forbindelse med NPS og *edibles*[46].

I følge FNs byrå for narkotika og kriminalitet (UNODC) er det sannsynlig at utviklingen i kjøp og salg over internett gjør narkotika tilgjengelig for nye brukergrupper og samfunn.[47] Kjøp og salg av narkotika over internett gjør det også mer sannsynlig at nye internasjonale trender og nye stofftyper når norske brukere raskere. Derfor er det meget sannsynlig at norske brukere vil fortsette å bruke internett som plattform for å kjøpe narkotika. Videre er det sannsynlig at kriminelle i større grad vil utnytte fordelene med elektroniske markedsplasser for å omsette narkotika i Norge.

41 EMCDDA (2016). Europeisk narkotikarapport.

42 Kripos (2017) Trendrapport 2017.

43 Kripos (2017) *Narkotikastatistikk 2016*.

44 Quist, C. (2016) 15 siktet i Norges største narkoaksjon på det mørke nettet. *VG* [Internett], 16.april. http://www.vg.no/nyheter/innenriks/krim/15-siktet-i-norges-stoerste-narkoaksjon-paa-det-moerke-nettet/a/23657196/

45 UNODC (2016) *World Drug report 2016*.

46 Spiselige produkter som inneholder narkotiske virkestoffer, ofte THC.

47 UNODC (2016) World Drug Report 2016.

A.3.4 Ulovlig salg av informasjon

Kriminelle stjeler ikke lenger bare kredittkortnummer, innloggingsinformasjon og personlig informasjon fra infiserte datamaskiner for sikre seg selv tilgang til betalingssystemer på internett.

I dag har informasjon fra datainnbrudd også blitt en viktig handelsvare for datakriminelle. Det er en trend at kriminelle i økende grad stjeler annen type data enn det som er nevnt ovenfor.[48] Slike opplysninger blir i økende grad tilegnet som steg for å utøve annen kriminalitet mer målrettet, for eksempel bedrageri, utpressing eller datainnbrudd.

Omsetning av informasjon fra datainnbrudd foregår ofte på internett. Kjøpere og selgere kan finne hverandre på markedsplasser og brukerfora som er tilrettelagt for denne type aktivitet. Aktuell type informasjon som har blitt avdekket til salgs på internett omfatter blant annet brukernavn og passord, epostadresser eller annen kontoinformasjon, brukermønstre, personnummer, kredittkortinformasjon, forretningshemmeligheter, åndsverk og sensitive/kompromitterende opplysninger av ulik art. Ofte er ikke de fornærmede klar over at informasjonen har kommet på avveie.

Konsekvensene av at sensitive opplysninger selges til uvedkommende kan være vidtrekkende. Denne formen for kriminalitet kan ramme enkeltpersoner hardt. Den kan også ses i sammenheng med kriminalitet som er svært samfunnsinngripende, for eksempel arbeidsmarkedskriminalitet, menneskesmugling, dokumentforfalskning, industrispionasje, politisk eller finansiell utpressing og svindel mot bedrifter. Tar man for eksempel i betraktning intellektuell eiendom, kan det å tilegne seg ulovlige data resultere i økonomiske tap som reflekterer flere års arbeid innen forskning og investeringer.[49] I tillegg kan tilliten til digitale løsninger reduseres.

A.3.5 Menneskehandel og menneskesmugling

Mennesker selges, kjøpes og utnyttes ulovlig via internett. Internett er en tilretteleggende faktor for menneskehandel og påvirker alle faser i menneskehandelen; fra rekruttering, transport og husing av ofre, til selve utnyttelsen og kontroll over ofrene. Menneskehandel og slaveri er gamle kriminalitetsformer, men de har fått nye dimensjoner gjennom rimelig og utbredt teknologi som enkelt benyttes via mobiltelefon.

Med økt bruk av internett har rekruttering, annonsering, salg og betaling for utnytting til prostitusjon, annen seksuell utnytting, tvangsarbeid og tvangstjenester i stor grad forflyttet seg fra gata til det digitale rom. Internett har også medført et økt antall kanaler for nedlasting og ulovlig deling av overgrepsmateriale. Dette gjelder ikke minst for menneskehandel til seksuell utnyttelse. I Norge har vi lite rettspraksis på feltet. I 2016 dømte imidlertid Bergen tingrett en person som bestilte seksuell utnyttelse av filippinske barn via internett for medvirkning til menneskehandel. Det er grunn til å forvente at vi vil se flere menneskehandelsaker med barn og internettrelaterte overgrep i tiden som kommer.

Økt bruk av internett til alle faser av menneskehandel vil trolig tilta i tråd med den teknologiske utviklingen og økt internettbruk globalt. Det antas også at teknologisk utvikling og innovasjon vil medføre nye og hittil ukjente former for seksuell utnytting, på samme måte som bruk av web-kameraer og sex-chats oppsto sammen med økt utbredelse av internett.[50]

48 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016*. Les også A.1.1

49 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016*.

50 Europol (2015) *Exploring tomorrow's organised crime*.

Kriminelle aktører kan komme i kontakt med og rekruttere et stort og økende antall potensielle ofre via ulike deler av internett, som sosiale medier og markedssider. Gjerningspersonene kan for eksempel forlede mennesker i en sårbar situasjon til å tro at de rekrutteres til ulike former for betalt arbeid i Norge. Menneskehandlerne og potensielle kunder oppnår kontakt og kommuniserer både på generelle plattformer og på spesielle chatte-rom, dating- eller eskortesider.

Menneskehandel kombineres ofte med annen alvorlig kriminalitet som bedrageri, dokumentforfalskning og menneskesmugling. Aktiviteten til menneskesmuglere fortsetter i stor grad å hvile på bruken av sosiale medier og kommunikasjon på internett. I enkelte tilfeller blir mindreårige smuglet til hensikt å produsere overgrepsmateriale som skal distribueres på internett.[51]

A.3.6 Seksuelle overgrep mot barn.

Internett er et sentralt verktøy for personer som søker å begå seksuelle overgrep mot barn:

> *The use of end-to-end encrypted platforms for sharing media, coupled with the use of largely anonymous payment systems, is facilitating an escalation in the live streaming of child abuse. Offenders target regions where there are high levels of poverty, limited domestic child protection measures and easy access to children. (Europol, 2016).*

Direkteoverførte overgrep, på engelsk kalt ***live streaming***, gjennomføres ved at en person sender en bestilling over internett med en beskrivelse av de seksuelle handlingene vedkommende ønsker at et barn skal utsettes for, i bytte mot betaling. Det er ofte små beløp som kreves for slike overgrep, noe som gjør at pengeoverføringene i seg selv ikke lett bringer mistanke om kriminelle handlinger. Det er også aktuelt at seksualforbrytere i etterkant av internettbestillinger reiser til landet der overgrepet fant sted, og selv forgriper seg på de samme barna.

Det er et fåtall straffesaker i Norge hvor det har vært pådømmelse for denne typen seksuelle overgrep, men per 2017 er flere saker under etterforskning. I sakene som er kjent for politiet er det i all hovedsak barn bosatt på Filippinene som har vært utsatt.

Direkteoverførte overgrep er vanskelig å avdekke da de overføres i sanntid og ikke er nødvendige å laste ned. Tilrettelegging for denne type overgrep krever lite kompetanse. Utviklingen på dette området har skjedd raskt, og direkteoverførte overgrep er ikke lenger i en startfase, men er blitt en etablert form for kriminalitet. Det forventes at omfanget vil øke, blant annet på grunn av nye og enklere muligheter for å strømme video på ulike sosiale medier og kommunikasjonsplattformer. Samtidig øker kapasiteten på internettlinjene i utviklingsland kontinuerlig, der hvor barn blir utsatt for slike overgrep. Det forventes en økning av tilsvarende saker i tiden fremover.

A.3.7 Overgrepsmateriale på internett

«Child Sexual Exploitation Material is increasingly produced for financial gain and distributed through the Darknet.» (Europol, 2017)

Personer som søker overgrepsmateriale på internett benytter seg ofte av ulike fildelingsprogrammer. Stort sett er dette fildeling via såkalte likemannsnettverk (peer-to-peer-nettverk eller P2P) som består av flere sammenkoblede brukere uten noen sentralisert styring. Disse programmene er enkle å bruke og gir lett tilgang til overgrepsmateriale.

51 Europol (2017).

Politiet har til enhver tid oversikt over mange personer som laster ned eller deler overgrepsmateriale. I perioden april 2016 til april 2017 observerte Kripos omlag 3000 unike IP-adresser i Norge som ble benyttet til å laste ned eller distribuere overgrepsmateriale.

Volumet overgrepsmateriale som er tilgjengelig på *det mørke nettet*[52] er økende.[53] Dette kan forklares med at mange som ønsker å dele overgrepsmateriale i større grad ønsker anonymitet og at det har blitt lettere å få tilgang til disse nettverkene. Det totale antallet personer som laster ned eller deler overgrepsmateriale, er trolig vesentlig større enn antall personer som er observert på de ulike åpne fildelingsnettverkene.

Anonymiseringstjenester bidrar ikke bare til å skjule fildelingen, men også til å øke sannsynligheten for at flere barn blir utsatt for fysiske overgrep. Inngangsbilletten til slike nettverk er i enkelte tilfeller at medlemmene selv bidrar med originalt materiale.

Generelt kan det å oppsøke overgrepsmateriale på internett være et første skritt mot fysiske overgrep, da kommunikasjon og deling av erfaringer og bilder mellom overgripere kan bidra til å normalisere den seksuelle interessen for barn, og dermed legitimere seksuelle fysiske overgrep. Mange av de som utfører seksuelle fysiske overgrep mot barn også overgrepsbilder tilgjengelig hjemme. I et uttrekk foretatt av Kripos i perioden 2013-2015 var totalt 912 personer mistenkt, siktet eller domfelt for besittelse av overgrepsmateriale. Av disse var 30 % i tillegg mistenkt, siktet eller domfelt for fysiske seksuelle overgrep mot barn under 16 år.[54]

A.4 Internett som arena for spredning av frykt, trusler og vold

Internett utgjør en unik arena fordi det er globalt, grenseløst og alltid tilgjengelig. Dette innebærer at brukere løpende kan være oppdatert på det som skjer nasjonalt og internasjonalt og at de kan nå eller skape en relasjon til andre personer som befinner seg på helt andre geografiske lokasjoner. Internett bidrar med andre ord til å skape samhold og fellesskap på bakgrunn av felles interesser.

Fremveksten av internett som kommunikasjonsplattform har gitt folk flest bedre anledning til å fremme egne meninger og synspunkter som offentlige ytringer. Ved hjelp av instrumenter på internett kan brukere opprette både åpne og lukkede grupper, direktemeldinger og publisere egne kommentarer.

Internett skaper dessverre også rom for aktører som påvirker storsamfunnet negativt, for eksempel nettsamfunn som representerer ekstreme holdninger. Der behøver ikke medlemmene å forholde seg til alternative holdninger, syn og perspektiver, noe som kan bidra til at medlemmene hisser hverandre opp. Dette kan bidra til å forsterke ytterpolene i samfunnet og legge til rette for straffbare handlinger i den virkelige verden, eksempelvis ordensforstyrrelser, skadeverk eller bruk av vold.

Over tid har det dannet seg en kultur og en norm for hva som er akseptabelt å ytre på sosiale medier, som avviker fra hva som er akseptabelt i resten av samfunnet. Mange mister hemningene når de beveger seg i det virtuelle rommet. Ytringsfriheten står sterkt, og hva som er lov eller ikke lov å ytre på internett er ofte drevet av en «indre justis».

52 Se fotnote 19.

53 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016.*

54 Kripos (2016) *Seksuelle overgrep mot barn under 14 år.*

Mange vet ikke at en ytring etter norsk rett er å regne som offentlig hvis den når 20–30 personer, uansett om den for eksempel er fremsatt på et privat nettforum som krever innlogging.

A.4.1 Vold, trusler og trakassering

Målrettede krenkelser på internett kan kalles digital mobbing eller nettmobbing. Mobberne er ofte anonyme, og det er gjerne flere av dem. Det er et økende problem at mobbere oppretter falske profiler på internett for å utgi seg for å være en annen eller den de mobber. Grunnlaget for de falske profilene er ofte åpent tilgjengelig informasjon, som navn, bilder, brukernavn og knytninger. Nettmobbing tar mange former, fra *trolling* der formålet er å erte eller terge, enkeltpersoner eller grupper, til målrettet psykisk vold over tid.

Regjeringsmedlemmer er spesielt utsatt for trusler og trakassering fra enkeltstående trusselaktører. Det ble i løpet av 2016 registrert en vedvarende strøm av mishagsytringer og trusler rettet mot regjeringen på internett, og en del av uttalelsene er svært grove og voldsforherligende. Opplevelsen av anonymitet på nettet kan bidra til sterkere språkbruk og mer aggressiv kommunikasjon.

Det vurderes som meget sannsynlig at denne type ytringer i sosiale medier vil fortsette i tilsvarende grad og med tilsvarende innhold i den kommende perioden. Imidlertid har økningen i oppfordringer til vold eller uttrykt voldsintensjon så langt ikke medført en økning i saker hvor PST avdekker en faktisk voldsintensjon. Antallet reelle trussel- eller voldshandlinger som PST håndterer årlig er fortsatt stabilt lavt.

Den siste tiden er det observert flere grupper på internett som motsetter seg offentlige myndigheter eller institusjoner. Enkelte støtter, oppfordrer eller utøver trusler og voldshandlinger for å nå sine mål. Disse kan kategoriseres som ***voldelige aktivister***. For eksempel er det en gruppe mennesker som aktivt motsetter seg barnevernet. De samler likesinnede, fronter sine kamper og organiserer aktiviteter på internett som blir iverksatt i den virkelige verden. Enkelte omtaler seg selv som «krigere» og uttrykker trusler mot ansatte i barnevernet eller barnevernet som institusjon. Både navn og bilder av barnevernsansatte blir publisert, og det oppfordres til represalier mot dem. Videoer av omsorgsovertagelser legges ut på internett, der barn, voksne og ansatte i både politiet og barnevernet blir identifisert. Identifiserte fosterforeldre får også represalier mot seg, og bilder og navn av barn som har blitt tatt hånd om av barnevernet blir lagt ut på internett i full offentlighet. I tillegg poster brukerne detaljerte skildringer av pågående saker mot barnevernet.

I 2016 ble flere skoler i Australia, Storbritannia, Japan og Frankrike utsatt for ***bombetrusler*** utført av hackere. Skoler i USA, Norge[55], Sverige, Guam og Nederland ble utsatt for lignende trusler i 2015. En russisk hackergruppe tok via Twitter på seg ansvaret for hendelsene i Frankrike, Japan, Nederland og Guam. Den russiske hackergruppen er imidler-tid også kjent for å tilby dette som en tjeneste (les: crime-as-a-service); at kunder kan kjøpe slike angrep ved å betale med *kryptovaluta*[56].

55 I Norge ble blant annet applikasjonen Jodel brukt til å fremsette bombetrusler mot flere norske skoler. Ettersom tjenesten ikke krever noen form for registrering, ble appen kjent som en «anonym» tjeneste. Etterforskning avdekket likevel hvem som sto bak, og gjerningspersonene var elever som ønsket seg en fridag på skolen. Den opplevde anonymiteten og reduserte oppdagelsesrisikoen syntes å være en viktig motivasjon.

56 Les fotnote 13.

Truslene ble fremsatt over telefon ved bruk av digitale forhåndsopptak, og de hadde fått tilgang til private telefonnummer som muligens har blitt klonet over internett.

A.4.2 Radikalisering og voldelig ekstremisme

Majoriteten av terrorangrep i Vesten de to siste årene er utført av soloaktører. Denne trenden vurderes å ville fortsette også i nærmeste framtid. Internett er en sentral driver når det gjelder radikalisering av soloaktører. Internett brukes bevisst som en propagandamaskin av organisasjoner som Al-Qaida (AQ) og ISIL, både i form av håndbøker, instruksjoner, moralsk støtte og inspirasjon gjennom publikasjoner som Inspire, Dabiq og Rumiyah. Gjennom propagandavirksomheten på nett kan organisasjonene fange individer som er på søken etter tilhørighet, både sosialt og ideologisk. Terrororganisasjoner som AQ og ISIL utnytter systematisk de sårbarhetene som er tilstede hos potensielle soloaktører, som er mottakelige for løfter om frelse og budskap hvor taperne blir helter. Gjennom publikasjoner av håndbøker som AQs «Safety and Security guidelines for Lone Wolf Mujahideen and small cells»[57] kan man finne både ideologisk tilhørighet, rettferdiggjørelse av terrorhandlinger og konkrete råd for å unngå å bli oppdaget.

Den raske veksten av sosiale medier og nye krypteringsløsninger gjør det mulig for personer uten fysiske nettverk å knytte seg til virtuelle nettverk. Internett er en arena hvor soloaktører kan bli radikalisert, og som virker som en forsterker for de som allerede er radikalisert. Soloaktører bruker internett i to henseender: for virtuell interaksjon og virtuell læring.

Virtuell interaksjon handler om å forsterke egne oppfatninger, søke legitimering for egne handlinger, drive propaganda- og rekrutteringsvirksomhet, i tillegg til å varsle det planlagte angrepet. Virtuell læring handler om å lese ideologisk materiale, vurdere og velge vold som løsning, målutvelgelse, angrepsplanlegging og forberedelsesvirksomhet samt å søke etter løsninger på problemer de møter underveis.[58] Aktører på internett bidrar med logistisk støtte og ekspertise for soloaktører der terrorceller kan benytte fysiske nettverk. Ifølge Gill (2015) lærte 42 prosent av soloterroristene i hans undersøkelse gjennom virtuelle kilder. Jo yngre soloaktøren er, jo mer sannsynlig er det at han eller hun bruker internett som plattform for læring og interaksjon.

Nye krypteringsløsninger på internett representerer en vesentlig sikkerhetsutfordring for sikkerhets- og etterretningstjenester internasjonalt. Det er for eksempel kjent at ekstreme islamister som opererer i Norge og utlandet, stadig blir mer sikkerhetsbevisste. Politiets sikkerhetstjeneste rapporterte i sin trusselvurdering for 2016 om økt bruk av lukkede fora og krypteringsverktøy i slike miljøer i Norge. Ekstreme aktører, om de opererer alene eller i grupper, har mulighet til å drive forberedelsesvirksomhet uten at dette er åpent synlig. Disse mulighetene blir systematisk utnyttet av ekstreme organisasjoner, hvor rekruttering i stadig større grad skjer på lukkede plattformer. Jo yngre soloaktøren er, desto viktigere vil internett være som arena for kunnskapstilegning, planlegging og inspirasjon.

57 En samling av 30 forelesninger av Abu Ubayda Abdullah al-Adm som er utgitt av al-Fajr Media Center.

58 Meloy & Gill (2015)

The extent to which extremist groups currently use cyber techniques to conduct attacks appears to be limited. There is currently little evidence to suggest that their cyber-attack capability extends beyond common website defacement. The availability of cybercrime tools and services, and illicit commodities (including firearms) on the Darknet provide ample opportunities for this situation to change (Europol, 2016).

A.4.3 Borgervern – fra Internett til aktiviteter på gata

I forbindelse med migrasjonsstrømmen mot Norge og Europa i 2015 og 2016, ble det som motreaksjon opprettet flere kritiske grupper på sosiale medier. Blant de som utmerket seg mest, var «Soldiers of Odin». Nordmenn rundt om i landet organiserte lokallag, og her var alt fra «Ola Nordmann» til tidligere straffedømte representert. Enkelte av disse medlemmene uttrykte støtte til voldshandlinger, både mot enkeltpersoner som myndighetspersoner og asylsøkerne generelt. På samme måte som i de barnevernskritiske gruppene, hauset de hverandre opp og terskelen for både hatefulle ytringer og voldsoppfordringer ble senket.

Mange av medlemmene mente at den norske sivilbefolkningen måtte beskyttes mot asylsøkerne og tok etter en stund til gatene for å patruljere rundt om i landet i ført hettegensere med symboler.

Offentlig uttalte gruppen at de ikke ville benytte maktmidler og at de ønsket å forhindre eller stoppe voldshandlinger eller andre straffbare forhold, blant annet ved å ta bilder og tilkalle politiet. Derimot er det alltid en fare for sammenstøt med andre grupper, når markante og svært så «høyrøstede» grupper tar til gatene for å utføre ordensoppgaver.

I lys av at flere av gruppens medlemmer er tidligere straffedømte, med tilknytning til kriminelle miljøer, var politiet bekymret for situasjonen.

Gruppen bidro med sin aktivitet på internett og med sin virksomhet i gatene til å forsterke ytterpunktene i samfunnet vårt. For eksempel opprettet islamister i Oslo «Allahs soldater» som tilsvar til «Soldiers of Odin».

A.5 Trusselen fra statlige aktører

Norge utsettes for etterretningsvirksomhet som kan ha stort skadepotensial. Norske naturressurser, NATO-medlemskap, interesser i Nordområdene, strategisk beliggenhet og attraktiv høyteknologisektor er faktorer som gjør at Norge er mål for etterretningsvirksomhet fra statlige aktører. Etterretningstrusselen mot Norge er høy. PST vet at Russland og Kina aktivt driver etterretningsvirksomhet i Norge. Disse aktørene utgjør de største truslene; imidlertid er det viktig å være oppmerksom på at andre land også driver etterretningsvirksomhet i Norge.

Formålet med etterretningsvirksomhet er først og fremst å understøtte eget lands politiske og økonomiske interesser, men også å planlegge for en eventuell konflikt eller krig i fremtiden. Statlige aktører bak etterretningsvirksomhet i Norge søker blant annet å innhente informasjon om norske forsvars-, sikkerhets, og beredskapsspørsmål og kritisk infrastruktur. Slik informasjon har særlig verdi for statlige aktører der sikkerhetspolitisk usikkerhet preger dagens forhold.

Statlige aktører forsøker også å påvirke politiske prosesser og drive industrispionasje. Aktørene forsøker å påvirke norske posisjoner i politiske beslutningsprosesser og forhandlinger til sin fordel. I slike tilfeller svekkes Norges forhandlingsposisjon, og det kan bli vanskeligere å få gjennomslag for norske interesser i internasjonal sammenheng. Industrispionasje fører til negative konsekvenser for enkeltbedrifter og svekker norsk konkurranseevne.

For å oppnå tilgang til verdifull informasjon benytter statlige aktører et bredt spekter av metoder. En av de mest sentrale metodene som benyttes er digital spionasje i form av nettverksoperasjoner. Statlige aktører benytter denne metoden hyppig, og med høy suksessrate. Dette er en rask og kostnadseffektiv metode med lav sannsynlighet for deteksjon, og det kan være vanskelig å spore en operasjon tilbake til en konkret aktør. I tillegg utføres operasjoner mot norske mål gjerne fra andre land, noe som medfører at operatørene står utenfor rekkevidden av norsk lov.

Arbeidet med å verve kilder finner i større grad sted i det digitale rom. Det er observert at etterretningstjenester innleder vervingsprosesser ved å knytte kontakter blant annet gjennom sosiale medier. Denne arenaen legger til rette for deling av personopplysninger, ikke minst opplysninger om kompetanse og arbeid. Dette er opplysninger som tjenestene kan bruke til å identifisere og kartlegge potensielle mål for en rekrutteringsoperasjon.

PST vet at russiske og kinesiske aktører aktivt gjennomfører nettverksoperasjoner i Norge til etterretningsformål. PST legger til grunn at Russland og Kina prioriterer å bruke betydelige ressurser på digital spionasje, og utvikler metoden til å bli ytterligere sofistikert slik at den kan gi høyere utbytte og foregå mer anonymt.

En rekke mål i statlig og privat sektor er særlig utsatt for nettverksoperasjoner. I statlig sektor er forsvars- og beredskapssektoren og politiske myndigheter prioriterte mål for etterretningsvirksomhet. Forsvaret, politiet, departementene, Stortinget, regjeringen og forskningsinstitusjoner og akademia er spesielt utsatt. Disse målene forvalter verdier som statlige aktører prioriterer høyt å få tilgang til fordi de direkte understøtter deres politiske og militære interesser. Nettverksoperasjoner mot statlige mål i Norge gjennomføres i ulikt omfang. Operasjoner kan rettes mot komplekse mål, slik som departementenes graderte eller ugraderte IKT-systemer, eller enklere mål, slik som enkeltpersoner med tilgang til sensitive opplysninger.

I 2017 var Utenriksdepartementet, Statens strålevern, en høyskole, Arbeiderpartiets stortingsgruppe, Forsvaret og Politiets sikkerhetstjeneste mottakere av målrettet e-post som inneholdt skadevare, såkalt *spearphishing-e-post*. Den russiske gruppen APT 29, som knyttes til russiske myndigheter, antas å stå bak angrepet. Denne type angrep er svært utbredt. Andre metoder som benyttes er *vannhullsangrep*[59], installasjon av skadevare på USB-pinner, anskaffelse av brukernavn- og passordinformasjon gjennom menneskelige kanaler eller falske e-poster, samt bruk av innsidere med tilgang til IKT-systemer.

Flere av etterretningstjenestene som opererer i Norge, har også som mål å skaffe seg eller plante lojale tjenere i prioriterte virksomheter. Disse kan eventuelt bruke sine legitime tilganger til å tilrettelegge for datanettverksoperasjoner fra innsiden. En slik kombinasjon av innsidevirksomhet og nettverksoperasjoner har et meget alvorlig skadepotensial.

59 Vannhullsangrep er skadevare gjemt på en ofte besøkt nettside.

I privat sektor er teknologiselskaper og IKT-tjenestetilbydere særlig utsatt for digital spionasje. Statlige aktører prioriterer å få tilgang til norske selskaper som produserer eller utvikler teknologi som andre stater har behov for gjennom digital spionasje. Flere land driver etterretningsvirksomhet mot leverandører av høyteknologi som samarbeider med for eksempel energisektoren og forsvarsindustrien. Teknologien som utvikles og produseres i disse sektorene er attraktiv av to hovedårsaker. For det første har flere stater ambisjon om å modernisere eller styrke sin forsvarskapasitet. I mange tilfeller må teknologi med militært bruksområde anskaffes i andre land dersom teknologien ikke kan anskaffes nasjonalt. For det andre har flere stater behov for norsk teknologi for å understøtte sine økonomiske interesser om å styrke eget næringsliv og konkurranseevne.

Norsk teknologi holder meget høy kvalitet, og statlige aktører – særlig Kina – søker derfor til Norge. For Kina er blant annet teknologi relatert til fornybar energi, grønn teknologi, bedre industriell produksjonskvalitet, utvikling av medisiner og romfartsteknologi spesielt etterspurt.[60] Slik industrispionasje bidrar til å svekke norsk næringsliv og konkurranseevne.

Russland utvikler sin evne til å gjennomføre digital sabotasje. I enkelte sammenhenger vil det innebære å iverksette tiltak for å påvirke den politiske debatten eller svekke legitimiteten til politiske beslutningsprosesser. Dette er tiltak som også kan iverksettes av etterretningstjenester som opererer mot Norge og norske interesser. Dette innebærer spredning av desinformasjon, manipulasjon, propaganda og stimulering av sosial uro.[61]

Digital sabotasje kan også utføres mot kritisk infrastruktur. Systemer innenfor kraftsektoren og elektroniske kommunikasjonssystemer er særlig utsatt for sabotasje. For eksempel kan sabotasje forstyrre eller undertrykke telekommunikasjon, kringkasting og internett.[62] Sannsynligheten for aktiv sabotasje mot Norge er lav, men det er et virkemiddel som kan benyttes i en eventuell konflikt eller krig.

PST vurderer at statlige aktører vil gjennomføre nettverksoperasjoner mot norske myndigheter, IKT-tjenestetilbydere, teknologimiljøer og aktører med ansvar for kritisk infrastruktur. PST forventer at operasjonene vil være avanserte og at disse vil bli ytterligere sofistikerte.

60 Etterretningstjenesten (2017) Fokus 2017. side 34.

61 Ibid, s.34. For eksempel ved å plante falske dokumenter, støtte nettrollaktivitet og bidra til falske nyhetsoppslag.

62 Ibid, s. 35.

DEL B

FELLES UTFORDRINGER

B.1 IKT-trusselen vil vokse i styrke og omfang

IKT-trusselen vil få et større og bredere nedslagsfelt. Flere aktører vil utnytte digitale sårbarheter for å oppnå politisk eller økonomisk vinning, og flere vil utnytte utviklingen innenfor IKT til å utøve annen kriminalitet mer effektivt. Det forventes også økt bruk av IKT til innhenting av informasjon om forhold i Norge som kan brukes av fremmede etterretningstjenester. Resultatet er at stadig mer kriminalitet vil finne sted helt eller delvis i det digitale rom. Med dette mener vi at politi og sikkerhetstjenester i fremtiden må forholde seg til flere og mer alvorlige dataangrep eller andre straffbare forhold der trusselaktørene tar i bruk IKT-verktøy som effektiviserer kriminelle handlinger.

IKT-verktøy og -metoder blir mer tilgjengelig for trusselaktører. Verktøy og metoder for å begå datakriminalitet krevde tidligere spesialkunnskap, men er nå blitt tilnærmet allment tilgjengelig og enkelt å benytte. Dette ses i form av utstrakt bruk av skadelig programvare som kriminelle enkelt kan anskaffe via internett. Også tjenester som krypterer data eller skjuler spor blir stadig mer brukervennlige og tilgjengelige. Dette åpner for mer effektiv og «sikker» samhandling mellom kriminelle og gjør det vanskeligere for politiet å spore aktiviteten tilbake til en trusselaktør.

De kriminelle vil ofte ha en fordel av at ny teknologi og nye metoder utvikles raskt ettersom politiet bruker tid på å tilpasse seg deres bruk av nye metoder og fremgangsmåter. Nye sikkerhetsteknologiske løsninger vil derfor være attraktive for kriminelle.

Kunnskapsutviklingen blant trusselaktører innen IKT-kriminalitet skjer raskt. Det er vanlig at de som driver med kriminell aktivitet på internett i stor grad lærer av hverandres feil. De deler relevant kunnskap om hvordan man beskytter seg selv på internett og hvordan man skal gjennomføre kriminaliteten mest mulig effektivt. Undersøkelser opp mot relativt unge personer som mistenkes for hacking tyder for eksempel på at de har hatt en rask kunnskapsutvikling som har gitt dem potensiale til å true samfunnets interesser.

Utviklingen innenfor IKT legger til rette for mer grenseoverskridende kriminalitet. Det digitale rommet er grenseløst, og fysisk avstand spiller en mindre rolle som begrensende faktor. I denne sammenheng kan ikke Norge dra like stor nytte av sin perifere geografiske beliggenhet. IKT-utviklingen har medført at kriminelle grupper og nettverk har kunnet utvide sine geografiske nedslagsfelt og operere over større avstander. IKT-utviklingen har med andre ord bidratt til at utenlandske kriminelle får bedre tilgang på kriminelle markeder og ofre i Norge.

Muligheter innenfor IKT påvirker holdninger og kultur, herunder etikk og moral. Terskelen for å utføre kriminelle handlinger ved bruk av datautstyr og/eller internett er sannsynligvis lavere enn ved annen kriminalitet. Teknologiske sikkerhetsanordninger har gjort det enklere å skjule sin egen identitet og aktivitet på nettet. Dette gir også kriminelle økt følelse av trygghet (les: lavere risikoopplevelse), og sannsynligvis er det lettere å distansere seg fra negative konsekvenser når handlingene foregår i det digitale rom der ofrene er «langt unna».

Internettfora kan bidra til å normalisere og rettferdiggjøre kriminell adferd. For personer med kriminelle hensikter er de ulike internettforaene en mulighet til å finne et fellesskap med likesinnede.

I slike fora, uten deltakere med kritiske motforestillinger, kan medlemmene forsterke hverandres holdninger og meninger. En «alle-gjør-det» mentalitet kan skape normative grensedragninger slik at hva som er akseptable handlinger avviker fra resten av samfunnet og at flere begår handlinger de ellers ikke ville begått. Det er også mulig at personer som opplever utenforskap kan søke tilhørighet i slike fora, og dermed oppnå anerkjennelse og status i det digitale rom dersom de gjennomfører IKT-kriminalitet som får oppmerksomhet i samfunnet.

B.2 IKT-utviklingen utfordrer politiets evne til å avdekke og etterforske kriminalitet

Mens informasjon om kommunikasjon tidligere kunne hentes inn fra relativt få kilder, som mobiltelefon og fasttelefon, bruker nordmenn i dag et mylder av ulike kommunikasjonstjenester. Dermed lagres informasjonen som skal til for å rekonstruere et hendelsesforløp på stadig flere steder. Utviklingen innenfor KT-kriminalitet medfører at det blir stadig viktigere å få tilgang på lagret datatrafikk.

Manglende datalagring, sletting av lagrede data eller manglende samarbeid med tjenestetilbydere fører ofte til at spor og bevis ikke eksisterer eller er utilgjengelige når politiet har behov for informasjonen. Tjenestetilbydere har ingen plikt til å lagre for eksempel trafikkdata, og flere teleleverandører har for eksempel sluttet å lagre opplysninger om IP-adresse da de ikke lengre har behov for dette i forbindelse med egen drift, for eksempel fakturering.

Politiet har i utgangspunktet ikke tilgang til brukerdata eldre enn 21 dager. Innhenting av IP-adresser brukt til pålogging hos utenlandske tjenester, som for eksempel Facebook og Google, tar ofte mer enn 21 dager. Derfor må norsk politi i mange tilfeller lete etter alternative beviskilder, noe som kan være ressurskrevende og føre til at flere enn nødvendig kommer i politiets søkelys. Samarbeid med tjenestetilbydere er avgjørende for effektiv informasjonsinnhenting. Mange internetttjenester nordmenn bruker faller derimot ikke inn under norsk jurisdiksjon. I land som USA er det opp til tilbyderne selv å bestemme hvordan de ønsker å samarbeide med utenlandsk politi, og erfaringsmessig er rettsanmodninger i mange tilfeller ikke en praktisk løsning, fordi behandlingstiden kan være på opptil ett år.

Det er en utfordring at aktører som er involvert i IKT-kriminalitet ofte befinner seg i forskjellige land og at enkelte kriminelle bevisst lagrer ulovlig innhold i andre jurisdiksjoner enn de selv befinner seg. Det er krevende å etterforske saker når serveren, eieren av serveren, kriminalitetsutøverne og ofrene er lokalisert i ulike land. Slike etterforskninger krever utstrakt internasjonalt samarbeid og tar gjerne lang tid. Det er derfor viktig å etablere gode internasjonale kontaktpunkter med tanke på internettrelaterte anmodninger og informasjonsbehov.

> *The use of encryption by criminals to protect their communications or stored data represents a considerable challenge for law enforcement, denying access to essential intelligence and evidence. This is a cross-cutting issue that affects all crime areas (Europol, 2016).*

Økt fokus på personvern og sikkerhet i samfunnet har bidratt til at det utvikles internettjenester som i økende grad tilrettelegger for anonymitet og kryptert kommunikasjon. Kriminelle har blitt flinkere til å utnytte disse tjenestene, men det er også en trend at kommunikasjonstjenestene gjør dette automatisk for dem.[63] Slik teknologi gjør det vanskeligere for politiet å avdekke kriminalitet på internett, herunder identifisere de kriminelle og hvor i verden de befinner seg. De kan for eksempel også koble seg på kafeers og naboers åpne eller lukkede nettverk eller manipulere informasjon som kan identifisere hvilken maskinvare som benyttes.

«The growing regularity of native encryption on mobile devices compounds this problem» (Europol, 2016). Fokuset på fysisk sikkerhet på datamaskiner og mobiltelefoner øker. Automatisk kryptering av lagringsmedier og tilgangskontroll med PIN-koder og fingeravtrykk gjør det stadig vanskeligere for politiet å få tilgang til bevis lagret på beslaglagte enheter. Videre gjør verifikasjonskoder og innloggingsvarsler det vanskeligere for politiet å få tilgang til brukerkontoer over internett.

Bruken av *virtuelle valutaer* har økt i Norge.[64] Samtidig har den virtuelle *kryptovalutaen* Bitcoin etablert seg som den vanligste valutaen i sammenheng med internettrelatert kriminalitet i Europa.[65] Økt bruk av kryptovaluta kan gjøre det vanskeligere å følge pengespor etter kriminell aktivitet.[66]

Det kan også skape nye muligheter for å følge pengespor i den offentlige transaksjonsloggen (blockchain), som ligger til grunn for desentralisert virtuell valuta. Ettersom transaksjoner kan utføres anonymt kan virtuelle valutaer utnyttes av kriminelle som driver med utpressing eller omsetning av ulovlige varer og tjenester på internett. Anonymiteten kan også utnyttes til hvitvasking og terrorfinansiering. Virtuelle valutaer fryktes brukt av ekstremister og terrorister for å opprettholde en anonym tilstedeværelse på nett og for å skjule store pengetransaksjoner.[67]

Politiet må vektlegge å utvikle bedre kapasitet for å avdekke og etterforske ulovlige aktiviteter på internett generelt, men kanskje spesielt med tanke på kriminell aktivitet på *det mørke nettet* og transaksjonsstrøm innenfor *virtuell valuta*. Her er det først og fremst myndighetene som må avdekke kriminalitet og opprette saker.

63 For eksempel Skype, Viber og WhatsApp, der man kan ringe med VoIP (Voice over IP) og sende tekstmeldinger. For én-til-én-kommunikasjon mellom kriminelle brukes tjenester som Jabber og ICQ (direktemeldingstjenester). Anonymiseringstjenester gjør at koblingen mellom internettbrukere og innholdet de laster ned og deler, blir mindre synlig. Bruken av mellomtjenere (proxy-tjenere) og tjenester for å være på *dark web* som Invisible Internet Project (I2P) og The Onion Router (Tor), øker også i omfang. Flere og flere nettsider krypterer nå alle data som går mellom nettsiden og de besøkende. Ved slik kryptering vil dataene, for eksempel e-postmeldinger, kunne lagres ukryptert av tilbyderen. Dette åpner for at tilbyderen kan utlevere informasjonen til politiet. En annen trend er at kommunikasjonstjenester som WhatsApp tilbyr ende-til-ende-kryptering, der selv ikke tilbyderen kan lese innholdet. Innholdet vil da kun være lesbart på datamaskiner og mobiltelefoner avsenderen og mottakeren bruker.

64 Justisdepartementet (2016). *Nasjonal risikoanalyse hvitvasking og terrorfinansiering*. Verdien av transaksjoner i valutaregisteret som antas å gjelde kjøp og salg av virtuell valuta med økte kraftig i perioden 2012 til 2014, fra totalt 4,1 mill. til 39,7 mill. NOK. Hovedtyngden var på kjøp og salg av kryptovalutaen, Bitcoin. I tillegg kommer nordmenns kjøp og salg via utenlandske vekslere, som ikke går via norske banker, og transaksjoner mellom Bitcoin-valutaer. Det er stor usikkerhet knyttet til hvor stor omsetningen av virtuelle valutaer mot kontanter er i Norge. Skatteetaten har estimert at den totale summen av transaksjoner med virtuelle valutaer økte fra 5,8 mill NOK i 2012 til 117,6 mill. i 2014.

65 Europol (2016) *The Internet Organised Crime Threat Assessment (IOCTA) 2016.*

66 Justisdepartementet (2016). *Nasjonal risikoanalyse hvitvasking og terrorfinansiering*. Virtuell valuta kan tilegnes ved hjelp av å stille datakraft tilgjengelig, men dette er både ressurs- og tidkrevende. Langt de fleste benytter derfor meglere. Meglere av virtuell valuta er ikke omfattet av hviTvaskingsloven per i dag, og det finnes også meglere av virtuell valuta som kjøper og selger valutaen mot kontanter. I 2014 ble det for eksempel også lansert en virtuell lommebok (applikasjon) som gir ytterligere anonymitet til transaksjoner med virtuell valuta, og gjør det i praksis umulig å avdekke hvem som har sendt penger til hvem.

67 POD (2015) *Politiets omverdensanalyse.*

Det er i det hele tatt viktig at det utvikles verktøy og metoder som kan demme opp for anonymiseringstjenester og kryptert kommunikasjon mellom personer som mistenkes å drive med ulovlig aktiviteter på internett.[68]

Når politiet skal etterforske IKT-kriminalitet må man ofte veksle mellom å bruke teknologiske metoder og tradisjonelle etterforskningsmetoder. Ofte må flere fagmiljøer integreres i etterforskningen, noe som er ressurskrevende. Utviklingen innenfor IKT-kriminalitet belyser behovet for å styrke teknologikompetansen i de operative miljøene, både i form av fagspesialister og at teknologikompetanse blir en større del av grunnleggende enkeltmannsferdigheter.[69]

B.3 IKT-utviklingen utfordrer samfunnets evne til å forebygge, avdekke og anmelde kriminalitet

Utviklingen innenfor IKT-kriminalitet stiller høyere krav til datasikkerhet på alle nivåer i samfunnet Norske virksomheter oppdager 80 % av de kjente sikkerhetstruende IKT-hendelsene ved tilfeldigheter eller på grunn av hendelsens direkte effekt på virksomhetens drift.[70] Dette tyder på at de fleste virksomheter ikke har nødvendige mekanismer på plass for å avdekke sikkerhetstruende hendelser og at den digitale kompetansen rundt sikkerhet og risiko ikke nødvendigvis øker i takt med eksponeringen. Trolig blir mange virksomheter utsatt for datakriminalitet uten å vite det.

Norske virksomheter oppgir at sikkerhetshendelsene i stor grad skyldtes tilfeldigheter eller uflaks, noe som tyder på at virksomhetene i liten grad oppfatter at angrepene er rettet spesifikt mot dem. Det kommer også fram at medarbeidere i 60 % av tilfellene gjorde feil som bidro til at sikkerhetshendelsene oppsto, og i cirka halvparten av tilfellene spilte manglende sikkerhetskompetanse en faktor.[71]

Selv om tekniske løsninger kan være gode, løser de ikke alle problemer. De beskytter for eksempel brukerne i liten grad mot ***sosial manipulasjon***. IKT-utviklingen har i større grad muliggjort svindel der svindlerne evner å fremstå som andre enn de er. Det kan være vanskelig å verifisere avsenderen av en e-post fordi e-postadressen fremstår som lik eller tilnærmet lik den legitime adressen. Falske telefonabonnement som er opprettet på bakgrunn av ID-tyveri, eller bruk av telefonnummer som har blitt klonet over internett, er også utfordringer i denne sammenheng. På disse måtene kan kriminelle lure mottakeren til å utbetale penger eller åpne et infisert vedlegg eller en lenke som leder til en infisert nettside, noe som muliggjør et datainnbrudd.

Kripos erfarer at folks evne til å være kritiske og vurdere ekthet kan være relativt dårlig når informasjonen kommuniseres på internett. Dette kan være fordi den teknologiske utviklingen skjer raskt og at man ikke er helt fortrolig med den.

Mørketallsundersøkelsen (NSR, 2016) viser at få anmelder datakriminalitet: 9 % av virksomhetene som utsettes for angrep tar saken videre til politiet.

68 Politi Toll Nordensamarbeidet (2016).
69 Ibid.
70 Næringslivets sikkerhetsråd (2016) *Mørketallsundersøkelsen.*
71 Ibid.

Firmaet, Mnemonic (ibid:8), mener i denne sammenheng sikkerhetsbransjen bør ta et oppgjør med unødvendig hemmelighold. «[…] dersom det norske IT-sikkerhetsmiljøet visste hva hele miljøet samlet vet kunne langt flere angrep vært forhindret.» Det vurderes for øvrig at mørketallene også er store hva gjelder IKT-kriminalitet som retter seg mot enkeltindivider.

For at politiet skal få et bedre kunnskapsgrunnlag og være i stand til å målrette sin innsats, er det viktig at IKT-kriminalitet blir anmeldt på lik linje med annen type kriminalitet. Selv om en sak blir henlagt på grunn av manglende bevis kan det være informasjon om modus og øvrige spor som kan bidra til å styrke politiets kunnskapsgrunnlag, herunder styrke politiets evne til å etterforske IKT-kriminalitet på et senere tidspunkt. Det er i denne sammenheng viktig å legge til rette for at IKT-kriminalitet registreres på en effektiv og hensiktsmessig måte.

Politidirektoratet
Juni 2017

Design og trykk: Kripos