UiO : Det juridiske fakultet

Cyberspace og DDoS-angrep: Navigering av rettslige utfordringer

Kandidatnummer: 676

Leveringsfrist: 2. mai 2023

Antall ord: 16084

Innholdsfortegnelse

1 INNLEDNING 1

1.1 Cyberkriminalitet og aktualitet 1
1.2 Forskningsspørsmålet 2
1.3 Metodisk tilnærming 3
1.4 Begrepsavklaring 5
1.4.1 En definisjonsbestemmelse eller ei? 5
1.4.2 Cyberkriminalitet? 5
1.4.3 Nøkkelbegreper 6

2 TJENESTENEKTANGREP 7

2.1 Hva er et tjenestenektangrep? 7
2.2 Hva er formålet med tjenestenektangrep? 8
2.3 Hvordan utføres tjenestenektangrep? 9

3 INTERNASJONAL REGELPRODUKSJON OG STRAFFEDOMSTOL 10

3.1 Konvensjon om cyberkriminalitet 10
3.2 Internasjonal straffedomstol 12

4 STRAFFERETTEN I CYBERSPACE 14

4.1 Grunnvilkår for straffeansvar 14
4.2 Eget kapittel i straffelovgivningen om cyberkriminalitet? 14

5 RELEVANTE STRAFFEBESTEMMELSER MOT DDOS-ANGREP 15

5.1 Straffeloven §§ 206 og 351 – Fare for driftshindring og skadeverk 15
5.1.1 Materiell rett 15
5.1.2 Anvendelsesområdet 16
5.2 Straffeloven § 192 – Anslag mot infrastrukturen 18
5.2.1 Formålet 18
5.2.2 Gjerningsbeskrivelsen 18

6 RELEVANTE STRAFFEBESTEMMELSER FOR UTFØRELSEN AV CYBERANGREP 19

6.1 Straffeloven § 204 – Innbrudd i datasystem 20
6.1.1 Internasjonal forpliktelse 20
6.1.2 Gjerningsbeskrivelsen 20
6.2 Straffeloven § 201 – Uberettiget befatning med tilgangsdata, dataprogram mv. 23

6.2.1 Internasjonal forpliktelse 23
6.2.2 Gjerningsbeskrivelsen 24

7 JURISDIKSJON OG STRAFFELOVENS STEDLIGE VIRKEOMRÅDE 27

7.1 Prinsippet om staters suverenitet i cyberspace 27
7.2 Internasjonal forpliktelse 28
7.3 Straffelovens stedlige virkeområde 29
7.3.1 Problemstilling 29
7.3.2 Tjenestenektangrep utført av en gjerningsperson i Norge - virkning i Norge .. 30
7.3.3 Tjenestenektangrep utført i Norge – virkning i utlandet. 31
7.3.4 Tjenestenektangrep utført fra utlandet – virkning i Norge. 32

8 TEKNOLOGINØYTRAL REGULERING 34

8.1 Regulering og teknologinøytralitet 34
8.2 Prinsippet om teknologinøytralitet 35
8.3 Uttrykk i straffelovgivningen 36

9 FORVENTET UTVIKLING FREMOVER 38

9.1 Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT ... 39
9.2 Riksadvokatens mål og prioriteringer for straffesaksbehandlingen i 2023 39
9.3 En FN-konvensjon for cyberspace 40

10 AVSLUTNING 42

LITTERATURLISTE 45

1 Innledning

1.1 Cyberkriminalitet og aktualitet

Den teknologiske utviklingen bidrar til at alle prosesser i samfunnet kan gå raskere, og påvirker samtidig selve endringshastigheten. Teknologien utfordrer sikkerhetsarbeidet blant annet gjennom nye måter å produsere, dele og lagre samfunnsviktig informasjon på. AI[1] forandrer livene våre for hver dag som går. Fra skriveverktøy til selvkjørende biler blir kunstig intelligens inkorporert i flere aspekter av livene våre. Mange mennesker er ikke klar over at flere av gjenstandene de anvender og samhandler med i hverdagen, for eksempel smarttelefoner, banktjenester og biler, på et eller annet nivå er automatisert. Internett er blitt den grunnleggende infrastrukturen i samfunnet, med et stort antall datanettverk knyttet sammen.

I dag anslås det at flere gjenstander er koblet til internett enn det er mennesker på jorda.[2] Vår avhengighet av digitale informasjonssystemer stiller krav om tidsriktige og dynamiske verktøy for å beskytte oss mot trusler i cyberspace. «Cyberspace» er betegnelsen på digitale flater, sammenkoblet av datasystemer og informasjonsressurser.[3]

Uttrykket «cyberspace» er også beskrevet i Europarådets konvensjon om cyberkriminalitet fra 2001[4]: «By connecting to communication and information services users create a kind of common space, called «cyber-space».».[5] Det er nettopp kriminaliteten som foregår i cyberspace som er tema for denne avhandlingen. Riksadvokaten avgjør hvert år hva slags kriminalitet som skal ha høyeste prioritet i straffesaksbehandlingen, og i år er cyberkriminalitet viet særlig oppmerksomhet. Saker om cyberkriminalitet skal prioriteres, og gis forrang ved ressursknapphet, og fagområdet har derfor høy aktualitet.

Vi opplever nye trusler, som for eksempel at datasystemer og infrastruktur i Norge kan angripes av anonyme aktører som befinner seg i andre land. Dessuten kan det være store avstander mellom handling og gjerningssted, når vi befinner oss i cyberspace. Til dette kan det sies at regulering av teknologi er en av vår tids store rettslige utfordringer.[6]

Cyberangrep er i ferd med å skape et nytt trussel- og risikobilde hvor våre viktige nasjonale interesser kan være truet. Det er derfor avgjørende med kriminalitetsbekjempelse for å hindre at samfunnet og enkeltindividet utsettes for kriminelle handlinger. Mange virksomheter

[1] AI: Eng: Artificial Intelligence; No: Kunstig intelligens.
[2] Curryer (2023).
[3] Nasjonal sikkerhetsmyndighet. (2017) s. 53.
[4] Ratifikasjon av Norge 30. juni 2006.
[5] Council of Europe. (2001) s. 2.
[6] Kaltenborn (2019) s. 151.

utsettes for reelle trusler knyttet til at det utstyret de bruker kan angripes, og som et resultat bli delvis styrt av uvedkommende. Det foreligger således et betydelig teknologisk press som kan utfordre sentrale samfunnsverdier. Imidlertid må hensynet til en effektiv kriminalitetsbekjempelse mot cyberkriminalitet avveies mot borgernes personvern og rettssikkerhet.

I juni 2022 ble Nasjonal sikkerhetsmyndighet (NSM) kontaktet av flere virksomheter som opplevde driftsforstyrrelser på sine nettsider. Årsaken viste seg å være et stort koordinert tjenestenektangrep fra den cyberkriminelle grupperingen, Killnet. Killnet er en av flere cyberkriminelle grupperinger som begår hacktivisme, og som siden Russlands invasjon av Ukraina har stått bak tjenestenektangrep mot land som støtter Ukraina. Grupperingen legger ut målene for angrep på sin telegram-kanal og ber følgerne utføre angrepet. Natt til 29. juni 2022 la grupperingen ut en liste med norske mål som utover dagen ble angrepet. Målene var blant annet nettsidene til politiet, UDI, BankID og NAV. Angrepet innebar å gjøre nettsidene ustabile eller helt utilgjengelig i korte perioder. Åpne kilder tilsier at motivasjonen for angrepet på generell basis var Norges støtte til Ukraina. I dagene etter angrepet la tilsvarende russiskvennlige grupperinger ut lister med flere mål de skulle angripe.[7]

Dersom angriperne lykkes med sine operasjoner, kan nedetid på nettsider være alvorlig, da det fremmer mistillit om myndighetenes evne til å beskytte befolkningen mot cyberangrep.

1.2 Forskningsspørsmålet

Temaet for denne avhandlingen er cyberkriminalitet.

Avhandlingen redegjør for følgende forskningsspørsmål:

> På hvilken måte er det rettslige rammeverket i norsk rett utformet når det gjelder cyberkriminalitet med særlig henblikk til en teknologinøytral strafferegulering.

Siden cyberkriminalitet er omfattende, og innebærer ulike kriminalitetstyper, vil fokuset i avhandlingen være på tjenestenektangrep, men det vil likevel være generell behandling av cyberkriminalitet som fenomen. For å besvare problemstillingen skal jeg i hovedsak redegjøre for gjeldende nasjonale strafferettslige bestemmelser mot cyberkriminalitet. Avhandlingen går inn på de mest relevante straffebestemmelsene i straffeloven, og hvordan disse regulerer cyberkriminalitet.

[7] Kripos (2023). s. 31.

Cyberkriminalitet kan være grenseoverskridende, og problemstillingen berører dermed også internasjonal rett, spesielt konvensjonen om cyberkriminalitet.[8] Konvensjonen omtales heretter Budapestkonvensjonen etter avtalens undertegningssted, Budapest. Masteroppgaven min redegjør for cyberoperasjoner med en forbindelse til utlandet, og om straffeloven får anvendelse i disse tilfellene. I forlengelsen av dette, vil oppgaven ta for seg hvorvidt det er et behov for endringer i rettslige rammeverk på et nasjonalt eller internasjonalt nivå, for å kunne bekjempe en større del av cyberkriminaliteten.

Når det gjelder teknologinøytral regulering, vil jeg se på hva uttrykket «teknologinøytralitet» betyr, og hvordan prinsippet om teknologinøytralitet virker inn på den strafferettslige reguleringen.

Avslutningsvis går jeg inn på politiets håndtering av cyberangrepene i praksis, og riksadvokatens fremtidige mål og prioriteringer i 2023 for cyberkriminalitet.
Oppgaven avgrenses mot kriminalitet i form av seksuallovbrudd, grov vold, drap og narkotika. Fokuset i oppgaven er ren cyberkriminalitet som rammer offentlige og private institusjoner som utfører kritiske samfunnsoppdrag, med eksplisitt fokus på tjenestenektangrep.

Bakgrunnen for at jeg ønsker å skrive om dette temaet, er at det stadig forekommer dataangrep mot både nasjonale og internasjonale aktører. Jeg har gjennomgående hatt interesse for skjæringspunktet mellom informasjonsteknologi og jus, og masteroppgaven var den passende anledningen til å kunne forske på cyberkriminalitet.

Cyberangrep er en ekstern trussel som har til hensikt å skade, forstyrre eller overbelaste datasystemet. NSM skriver i sin årsrapport for 2022 at krigsutbruddet i Ukraina har vist hvor viktig fokus på digital sikkerhet er, og dette gjør tematikken svært dagsaktuell. Cyberoperasjoner kan ramme ulike deler av samfunnet, eksempelvis strømnettet, flytrafikken eller veitunneler. Et vellykket dataangrep kan føre til at sårbar kritisk norsk infrastruktur står i fare for å slutte å virke, eksempelvis at hundretusener kan miste strømmen om angriperen bestemmer seg for det.

1.3 Metodisk tilnærming

For å besvare problemstillingen vil jeg anvende juridisk metode som et verktøy for å redegjøre gjeldende rett når det gjelder cyberkriminalitet. Avhandlingen tar for seg nasjonale lovtiltak om cyberkriminalitet, med særlig fokus på bestemmelser som regulerer tjenestenektangrep. Selv om fokuset er på norske rettsregler, må disse tolkes i lys av Norges folkerettslige forpliktelser, da cyberkriminalitet er et utpreget internasjonalt tema. Siden oppgaven tar for seg cyberkriminalitetens internasjonale aspekt, behandler jeg også straffelovens stedlige virkeområde. De

[8] Europarådets konvensjon av 23. november 2001 (konvensjon om datakriminalitet – ETS nr. 185)

alminnelige strafferettslige bestemmelsene i straffeloven tolkes og suppleres av andre relevante rettskilder, hovedsakelig forarbeidene til straffeloven og Budapestkonvensjonen.

Der hvor det finnes relevant høyesterettspraksis, blir disse fortløpende behandlet. Imidlertid foreligger det få rettsavgjørelser å se hen til, når det gjelder cyberkriminalitet som rettsområde, og dette gjenspeiles i avhandlingen min. En av grunnene til at det foreligger lite rettspraksis, kan være at cyberkriminalitet er et relativt nytt område som er i stadig utvikling og endrer seg raskt. Dessuten kan straffeforfølgningen av datakriminalitet være utfordrende, når man ikke får identifisert eller sporet gjerningspersonen, og dette vanskeliggjør å bringe saken for retten. En annen grunn kan være utfordringen med å sikre og innhente dokumentasjon og annet bevismateriale fra digitale informasjonssystemer, og dermed kunne bevise skyld i saker om cyberkriminalitet. Dermed er det begrenset med henvisninger til rettspraksis.

Budapestkonvensjonen er et internasjonalt regelverk som utgjør relevant bakgrunnsrett for denne avhandlingen. Konvensjonen må tolkes for å forstå meningsinnholdet, og fortolkningen skjer i tråd med Wien-konvensjonen om traktatretten.[9] Norge har ikke underskrevet eller ratifisert Wien-konvensjonen, men som andre ikke-parter til Wien-konvensjonen er Norge likevel bundet av de bestemmelsene som anses som folkerettslig sedvanerett, blant annet artikkel 31-33.[10]

Wien-konvensjonen om traktatretten artikkel 31 legger til grunn at en traktat må fortolkes «in good faith» i tråd med «the ordinary meaning», som bør tillegges traktatens ordlyd sett i sin «context» og i lys av traktatens «object and purpose». Ved enhver fortolkning må man derfor ta hensyn til samtlige momenter i en «single combined operation».[11]

Ordlydsfortolkning er første steget for å fastslå hvilken betydning konvensjonsteksten har ment å ha. Neste steg er å ta hensyn til hva slags traktat som tolkes når man fastslår «the ordinary meaning» av et ord. Siden Budapestkonvensjonen er en konvensjon som omhandler informasjons- og kommunikasjonsteknologi, må det tekniske og digitale aspektet tas i betraktning, og tolkes slik en person som er rimelig informert om hele meningsinnholdet ville tolket det. I tillegg skal det legges vekt på formålet med konvensjonen; bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

[9] Vienna Convention on the Law of Treaties (VCLT), trådte i kraft 27. januar 1980, 1155 UNTS 331, artikkel 2 første ledd.

[10] ICJ. *Kasikili/Sedudu Island (Botswana/Namibia)*, dom, 13. desember 1999, avsnitt 18.

[11] FNs folkerettskommisjon. (1966) s. 219.

For en aktiv tilegnelse av stoffet i denne masteravhandlingen er det innledningsvis hensiktsmessig å definere begrepene som brukes i masteroppgaven.

1.4 Begrepsavklaring

1.4.1 En definisjonsbestemmelse eller ei?

Flere av begrepene og uttrykkene i straffelovgivningen om cyberkriminalitet kan være vage og flertydige. Det presiseres likevel at det ikke foreligger noen definisjonsbestemmelse av cyberkriminalitet i straffeloven. Hensynet til klarhet og tilgjengelighet taler for en legaldefinisjon, men utfordringen ligger i å utforme presise og dekkende definisjoner som samtidig er føyelig nok.

Forarbeidene viser sprikende interesse for begrepsbruken. Datakrimutvalget gikk inn for bruk av legaldefinisjoner. Utvalgets mandat var begrenset til å gjelde kriminalitet begått med datateknologi, og definisjonene ble avgrenset i samsvar med dette. Justisdepartementet på sin side ønsket ikke legaldefinisjoner, da man fryktet at de kunne bli for rigide slik at straffebudene raskt ble utdaterte på grunn av teknologiutviklingen. Ved utforming av straffebudene søkte man heller å tilrettelegge for en dynamisk begrepsutvikling, og – så langt som mulig – for teknologinøytralitet.[12]

Imidlertid gjelder det et forbud mot analogi. Dette følger av legalitetsprinsippet nedfelt i Grunnloven (Grl.) § 96 og Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 7. Analogiforbudet gjelder selv om sterke reelle hensyn taler for anvendelse av straffebudet i det aktuelle tilfelle. Oppgaven avgrenses mot legalitetsprinsippet, og hvilken innvirkning dette har på lovgivningsutformingen.

1.4.2 Cyberkriminalitet?

Økende digitalisering av samfunnet medfører økning av kriminaliteten på digitale flater. Cyberkriminalitet forekommer som både alvorlig og mindre alvorlig kriminalitet. Uklarheter rundt begrepet cyberkriminalitet kan skape utfordringer, og det er uenighet rundt utformingen av begrepsapparater på dette området. Fenomenet omtales med ulike begreper som cyberkriminalitet, datakriminalitet og IKT-relatert kriminalitet. I avhandlingen brukes begrepene om hverandre, men meningsinnholdet er det samme. Videre antas det at forskjellige ord og uttrykk har forskjellig betydning når de forekommer i samme lov. Ellers ville lovgiver brukt ha brukt samme uttrykk.

[12] Ot.prp. nr. 22 (2008-2009) s. 21-22

«Datakriminalitet» defineres som kriminalitet som er rettet mot datasystemer og/eller datanettverk, eller kriminalitet der sentrale elementer av handlingsforløpet utføres ved hjelp av datasystemer og/eller datanettverk.[13]

De strafferettslige bestemmelsene som behandles i denne oppgaven, inneholder ord og uttrykk som «data», «dataprogram» og «datasystem», se lov 20. mai 2005 nr. 28 om straff (heretter straffeloven eller forkortet strl.) §§ 201, 204, 206, 351 annet ledd og § 371 bokstav b. Disse nøkkelbegrepene behandles nedenfor.

1.4.3 Nøkkelbegreper

1.4.3.1 «Data»

En naturlig språklig forståelse av «data» tilsier informasjon som kan lagres og bearbeides av datamaskiner. Betegnelsen er teknisk anlagt, men angir likevel ingen konkret anvisning på hva slags informasjon som omfattes av begrepet. Dermed tolkes uttrykket «data» vidt, og omfatter alle former for elektronisk informasjon. Dette kan inkludere tekst, tall, bilder, filer og andre former for informasjonslagring. Data kan lagres på forskjellige måter, og noen alminnelige måter å lagre data på er harddisker og skybaserte tjenester. Utover dette utvikles det stadig andre former for lagring av data, og dette kan gi opphav til nye rettslige utfordringer. Oppgaven avgrenses imidlertid mot utfordringer knyttet til lagringsmedium.

1.4.3.2 «Datasystem»

En naturlig språklig forståelse av «datasystem» tilsier enheter som kan utføre automatisk programstyrt databehandling. Ordlyden er vid, og kan omfatte enheter alt fra små nettbrett og smarttelefoner, til store omfattende systemer. Betegnelsen «datasystem» er teknologinøytral, og teknologinøytralitet behandler jeg senere i oppgaven. Det er dermed ikke avgjørende om innretningen er en del av et tradisjonelt datasystem eller en annen innretning som har tilsvarende funksjoner, men data i datasystemet må behandles av et dataprogram; altså være maskinlesbar. Teknologivalget avgjør ikke hvorvidt innretningen utgjør et datasystem.[14]

«Datasystem» er definert i Budapestkonvensjonen artikkel 1 bokstav a som «any device or a group of interconnected or related devices, one or more of which, pursuant to a program, perfoms automatic processing of data». Artikkelen definerer datasystem som en enhver innretning eller gruppe innretninger som er koblet sammen eller hører sammen, hvorav en eller flere utfører programmert, automatisk behandling av data.

[13] Innst. 360 S. (2020-2021) s. 1

[14] Schjølberg. (2017) s. 57

I forarbeidene til straffeloven 2005, er «datasystem» forklart som «enhver innretning, bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer.»[15] Dette tilsier at innretningen må kunne programmeres og utføre automatisk databehandling. Denne definisjonen samsvarer med Budapestkonvensjonens definisjon av «datasystem».

1.4.3.3 «Dataprogram»

Et dataprogram er en serie instruksjoner som beskriver hva en datamaskin skal utføre. Når programmet kjøres, utfører datamaskinen instruksjonene. Et dataprogram er dermed bestående av algoritmer som gir datamaskinen trinn for trinn-oppskrift på hvordan den skal løse ulike oppgaver. En algoritme er en sekvens av instruksjoner som beskriver hvordan man skal utføre en bestemt oppgave. Dataprogram kan variere fra enkle kalkulatorer til komplekse applikasjoner for å administrere store mengder data. Formålet er å automatisere oppgaver og løse disse mer effektivt.

2 Tjenestenektangrep

2.1 Hva er et tjenestenektangrep?

Et tjenestenektangrep eller DDoS-angrep[16] er en angrepsform som utelukkende rammer tilgjengeligheten til tjenesten, systemer eller de infrastrukturkomponenter som blir angrepet. Gjennom et slikt dataangrep angripes datasystem på en slik måte at det ikke kan brukes som tiltenkt.

Aktørene utnytter nettverk av allerede kompromitterte datamaskiner og andre enheter som en desentralisert ressurs til å overvelde målet med nettverkstrafikk. Mengden datatrafikk som må til for å gjennomføre et vellykket tjenestenektangrep, avhenger av trafikk- og responskapasiteten.[17] Tilgang til slike allerede kompromitterte nettverk selges av aktører med ekspertkompetanse som en tjeneste til mindre sofistikerte aktører. Det er dermed et enkelt og lett tilgjengelig angrepsmiddel som benyttes av et bredt spekter av aktører til forskjellige formål.[18]

Angrepet utføres oftest ved å overbelaste en eller flere ressurser, slik som kommunikasjonsprotokoll, applikasjon, nettverkskapasitet, maskinvare eller tilsvarende. Ellers kan angrepet også gjøres ved å utnytte svakheter i disse nettverks- eller applikasjonsprotokollene. Det kan også gjennomføres ved å skape feiltilstander som blokkerer en tjeneste eller funksjon, og som krever at utstyr eller tjenester må startes på nytt. Når en tjeneste er utilgjengelig, karakteriseres dette som nedetid. Selv om målene for distribuerte tjenestenektangrep vanligvis ikke blir

[15] Ot. prp. nr. 22 (2008-2009) s. 400
[16] Eng: Distributed Denial-of-service attack
[17] Kripos. (2023) s. 45.
[18] Kripos. (2023) s. 31

kompromittert, er kildene som genererer trafikk gjerne kompromitterte systemer. NSM sender ut varsler dersom de registrerer norske IP-adresser som utsettes for ondsinnet aktivitet, blant annet tjenestenektangrep.[19] Tjenestenektangrep med rekordstor datatrafikk får mye oppmerksomhet, men et angrep kan også rettes mot en flaskehals eller «single point of failure» hvor et system kan være sårbart for et angrep som bruker langt lavere trafikkvolum og dermed er vanskeligere å oppdage.[20]

Spørsmålet er om et tjenestenektangrep er ulovlig når det er nettsiden som ikke tåler den store mengden av trafikk.

Det er i utgangspunktet ulovlig å drive tjenestenektangrep, selv om nettsiden ikke tåler så mye trafikk. Dette henger sammen med at angrepet utgjør en kriminell handling med formål å forstyrre eller ødelegge data eller datasystemer. Hvis noen med vilje overbelaster en nettside med trafikk eller sender store mengder data for å hindre andre i å bruke siden, kan man bli straffet i henhold til gjeldende lovverk. Det er viktig å huske at det er eierne av nettsiden som bestemmer hvor mye trafikk siden skal tåle, og det er ikke opp til angriperne å avgjøre dette.

Bedrifter og virksomheter med tidskritiske prosesser er utsatte mål fordi nedetid kan være svært kostbart, og tjenestenektangrep kan medføre at kritisk infrastruktur blir satt ut av funksjon.[21] Den siste tiden har flere norske virksomheter vært rammet av dataangrep, eksempelvis ble nettsidene til Statistisk sentralbyrå og Nasjonal sikkerhetsmyndighet nylig utsatt for et tjenestenektangrep. Dette medførte at nettsidene ble tatt ned på grunn av det pågående angrepet.[22]

2.2 Hva er formålet med tjenestenektangrep?

Formålet med et tjenestenektangrep er gjerne oppmerksomhet snarere enn å påføre skade. Med andre ord er formålet ofte en signaleffekt, for eksempel ved å ramme nettsidene til en virksomhet. Hensikten kan være å fremprovosere uønsket atferd, enten hos brukerne av tjenesten som angripes eller i virksomheten som angripes.

Gjennom tjenestenektangrep kan virksomhetskritiske tjenester eller infrastruktur rammes, og tjenestenektangrepet kan være en del av et større sammensatt angrep. I løpet av den siste perioden har flere virksomheter også blitt offer for digital utpressing med løsepengevirus. Tjenestenektangrepet blir brukt som virkemiddel, hvor det fremsettes trusler om mer alvorlige angrep dersom det ikke utbetales løsepenger.

[19] Nasjonal sikkerhetsmyndighet. (2023) s. 21
[20] Nasjonal sikkerhetsmyndighet. (2023).
[21] Kripos. (2023) s. 16
[22] E24. (2023).

Til sammenligningsformål, var distribuerte tjenestenektangrep et av de vanligste cyberangrepene, sammen med phising og kartleggingsaktivitet. Phising, eller nettfisking på norsk, er en form for sosial manipulering, hvor en angriper forsøker å lure noen til å utføre en handling, for eksempel å gi fra seg sensitive opplysninger slik som passord eller annen personlig informasjon. Dette gjøres oftest ved å sende falske e-poster eller meldinger hvor avsender fremstår som en pålitelig kilde, eksempelvis et velrenommert foretak.[23] Kartleggingsaktivitet i cyberspace er prosessen med innsamling av informasjon om et spesifikt datasystem eller nettverk ved hjelp av ulike metoder. Formålet med innsamlingen er å kartlegge systemet som skal angripes, og identifisere eventuelle svakheter eller sårbarheter som kan utnyttes for å få uautorisert tilgang til systemet.[24]
Dersom det pågår vedvarende phising- og kartleggingsaktivitet mot norske aktører, tilsier dette at målene er attraktive, og en kartlegging av målene kan være en pekepinn mot et kommende cyberangrep.

2.3 Hvordan utføres tjenestenektangrep?

Cyberkriminalitet er ofte muliggjort av gjerningspersonenes mulighet til å opptre fordekt. Dette muliggjøres av anonymiseringsteknologier. Anonymiseringsteknologier lar en gjerningsperson operere med skjult identitet på tvers av landegrenser og jurisdiksjoner med ulik lovregulering. Ved å opptre anonymt knyttes ikke de straffbare handlingene til gjerningspersonene reelle identitet, og sjansen for straffeforfølgelse minker betraktelig. Tilgjengelige anonymiseringsteknologier vanskeliggjør i høy grad forebygging, avverging, etterforskning og straffeforfølgelse av tjenestenektangrep.[25] Teknologisk kompetente gjerningspersoner gjør etterforskningen av lovbrudd utfordrende. Tjenestenektangrep kan ofte forekomme fra utenlandske IP-adresser eller nettverk, og dette vanskeliggjør å identifisere og straffe gjerningspersonene.

Cyberkriminalitet blir ofte gjort mulig av kryptering, og VPN-tjenester er en type anonymiseringsteknologi som brukes ofte. Cyberkriminelle anvender VPN-tjenester[26] som gir tilgang til mellomtjenere[27] og ulike grader av kryptering av trafikk. Flere tilbyr ende-til-ende-kryptering for all trafikk mellom brukerens maskin og målene de kobler seg til via tjenestens mellomtjenere. VPN-tjenestene gir brukeren mulighet til å velge mellomtjenere i ulike land. Mellomtjenere kan eies eller leies gjennom egne tjenester eller et datasenter. For nettsider og tjenester brukeren kobler til vil brukernes utgangsadresse framstå som VPN-tjenestens mellomtjener. Dermed oppnår brukeren en viss anonymitet, i tillegg til at datatrafikken blir skjult gjennom

[23] Sunde. (2016) s. 52.
[24] Nasjonal sikkerhetsmyndighet. (2022) s. 21.
[25] Kripos. (2023) s. 20.
[26] VPN: Eng: Virtual Private Network; No: Virtuelt privat nettverk.
[27] Eng: Proxy Server

kryptering. Flere av VPN-tilbyderne krever lite eller ingen loggføring av kunders informasjon og bruk.[28] Dermed kan tjenestenektangrepet utføres uten at angrepet blir sporet. Tilgjengelige anonymiseringsteknologier vanskeliggjør dermed forebygging, avverging etterforskning og straffeforfølgning av tjenestenektangrep.

Det er derfor viktig å ha internasjonalt samarbeid og koordinering mellom ulike lands myndigheter for å kunne håndtere cyberangrep på en effektiv måte. Imidlertid kan dette bli utfordrende, da ulike land kan ha ulike lover og regler når det gjelder tjenestenektangrep, og at det derfor kan være utfordrende å finne en felles tilnærming til problemet på tvers av landegrenser.

3 Internasjonal regelproduksjon og straffedomstol

3.1 Konvensjon om cyberkriminalitet

Helt siden internett ble den grunnleggende infrastrukturen i samfunnet, har dette gitt opphav til en rekke juridiske problemstillinger. Cyberkriminalitet kjennetegnes ved at det enkelt kan begås på tvers av landegrenser. Det er økende konsensus om at det er nødvendig med globale retningslinjer for å bekjempe cyberoperasjoner og cyberkriminalitet. Av den grunn har det blitt iverksatt en stor og omfattende regelproduksjon vedrørende cyberkriminalitet.

Norge er medlem av FN, og har ratifisert FN-konvensjonen mot grenseoverskridende organisert kriminalitet.[29] Denne overenskomsten gir et rammeverk for samarbeid mellom land for å bekjempe organisert kriminalitet, inkludert cyberkriminalitet. Imidlertid avgrenses avhandlingen mot denne konvensjonen.

Videre er Norge også medlem i Europarådet og har ratifisert konvensjonen om cyberkriminalitet, som gir et rammeverk for å samarbeide om etterforskning og rettsforfølgelse av cyberkriminalitet, inkludert tjenestenektangrep. Budapestkonvensjonen utløste et hjemlig utredningsarbeid når det gjaldt straffe- og straffeprosesslovene. Konvensjonen ble vedtatt 8. november 2001 og undertegnet av Norge 23. november samme år, jf. kgl.res. 16. november 2001. Konvensjonen ble ratifisert 30. juni 2006 og trådte i kraft 1. oktober 2006.[30] Per februar 2023 hadde 68 stater ratifisert konvensjonen. Utviklingen i cyberspace skjer fort, og det er stadig behov for å se fremover og skape nye verktøy. Konvensjonen har derfor blitt supplert med to tilleggsprotokoller, hvorav den andre per februar 2023 er signert av 35 land.

Våre internasjonale forpliktelser for straffebestemmelser er beskrevet i denne konvensjonen, og hensynet til våre forpliktelser tilsier straffebestemmelser som tilkjennegir at alle former for

[28] Kripos. (2023) s. 21.

[29] United Nations *Convention against transnational organized crime* av 13. desember 2000 (CATOC).

[30] Europarådet. (2003).

cyberkriminalitet som nevnt i konvensjonen, straffes i Norge. Ved å slutte seg til konvensjonen forplikter dermed statene seg til å gjøre visse handlinger straffbare, som for eksempel datainnbrudd, dataskadeverk, ulovlig tilgjengeliggjøring av data og databedrageri. Med dette legger konvensjonen opp til en harmonisering av nasjonal rett på strafferettens og straffeprosessens område. Hensikten er å effektivisere mekanismene på internasjonalt nivå for bekjempelse av cyberkriminalitet og for utnyttelse av elektroniske bevis innenfor enhver form for kriminalitet. Budapestkonvensjonen er således mer enn et rettslig dokument; det er et rammeverk som tillater å dele erfaringer og skape relasjoner som forenkler samarbeid i spesifikke tilfeller, inkludert nødsituasjoner, utover de spesifikke bestemmelsene forutsatt i denne konvensjonen. Konvensjonen forplikter statene å samarbeide gjensidig for å gi rask hjelp i etterforskningen, og være tilgjengelige for kontakt hele tiden, syv dager i uken.[31]

Konvensjonen anvender et teknologinøytralt språk, slik at de materielle straffelovbruddene kan anvendes dynamisk i forhold til den teknologiske utviklingen i samfunnet. Dette for å sikre at nye former for skadelig programvare eller kriminalitet alltid er omfattet av denne konvensjonen. Imidlertid er konvensjonen om cyberkriminalitet basert på handlinger som i 1990-årene ble ansett å være uautoriserte og uakseptable slik at de burde straffesanksjoneres. Nye handlinger i cyberspace som utviklet seg etter 2001, kan også anses å være så uakseptable at det bør overveies en særskilt straffesanksjon, for eksempel tilfeller av identitetskrenkelse gjennom digitale handlinger, kriminalitet i sosiale medier eller terroristers bruk av internett og cyberangrep mot kritisk infrastruktur. Dette har ført til at Norge blant annet har vedtatt en særskilt bestemmelse om anslag mot infrastrukturen i straffeloven § 192.[32] Denne straffebestemmelsen behandles litt senere i oppgaven.

Utover dette er terminologien i konvensjonen om cyberkriminalitet fra 1990-tallet, som ikke nødvendigvis er passende terminologi for cyberspace i 2020-årene. Grunnet ulik terminologi har flere land allerede vedtatt eller forbereder endringer i straffelovgivningen som omfatter denne utviklingen. Konvensjonen anses ikke å være utdatert, men kan inneholde prinsipper som ikke tilfredsstiller cybersamfunnet av 2023. Det presiseres imidlertid at politiet og andre fagmiljøer mener at konvensjonen fremdeles holder mål som arbeidsverktøy, og dette indikeres av operativ etterforskning av cyberrelaterte straffesaker.[33]

Svært mange tjenestenektangrep vi står overfor, er globale og rutes gjennom flere land. I tilknytning til dette vil manglende samarbeid og avtaler mellom landene gjøre det nærmest umulig å etterforske og domfelle personer som står bak cyberkriminelle operasjoner. Den globale

[31] Schjølberg. (2023) s. 28.
[32] Schjølberg. (2023) s. 85.
[33] Møller. (2023)

politiske situasjonen for cybersikkerhet og cyberkriminalitet er fortsatt fastlåst.[34] Når tjenestenektangrep utføres fra utlandet, kan Norge inngå et internasjonalt samarbeid og anvende eksisterende avtaler og konvensjoner for å etterforske og straffeforfølge lovbrytere. Budapestkonvensjonen danner grunnlaget for internasjonalt samarbeid, siden nær sagt enhver straffesak har elementer av dataetterforskning.

Siden digitale tjenester anvendes på tvers av geografiske grenser og er globale i sin karakter, var det essensielt å legge til rette for en global oppslutning om konvensjonen. I tilknytning til konvensjonen ble det utarbeidet en forklarende rapport – «Explanatory report», som gir utfyllende merknader til problemstillingene som behandles i konvensjonsbestemmelsene.[35]

I forbindelse med undertegningen av konvensjonen nedsatte regjeringen et utvalg, Datakrimutvalget, som skulle avdekke hvilke lovtilpasninger som var nødvendige for ratifisering. Disse lovtilpasningene ble beskrevet i NOU 2003: 27 Lovtiltak mot datakriminalitet. Deretter fremmet regjeringen Ot.prp. nr. 40 (2004-2005), som på de fleste punkter fulgte opp utvalgets arbeid.

Som jeg kommer tilbake til senere i oppgaven, foreligger det òg mulighet for å straffe tjenestenektangrep gjennom nasjonal straffelovgivning, selv om angrepet er utført fra landet. Forutsetningen er at det er mulig å spore opp, identifisere og pågripe angriperen.

3.2 Internasjonal straffedomstol

Spørsmålet som behandles er hvorvidt det bør opprettes en spesialisert domstol for cyberkriminalitet.

Stadig flere stater og aktører har uttrykt et behov for en internasjonal straffedomstol, og dette behovet har blitt betegnet som «the missing link» i den globale rettshåndhevelsen av cyberkriminalitet.[36] En mulig årsak til at det ikke eksisterer en internasjonal straffedomstol mot cyberkriminalitet, er at cyberkriminalitet ofte er grenseoverskridende og kan involvere flere land. Det kan være vanskelig å forfølge saker når det er ulike jurisdiksjoner involvert. I tillegg kan det være utfordrende å holde tritt med den raske utviklingen av teknologi og cyberangrep.

Dersom det etableres en egen domstol for cyberkriminalitet, vil det kunne gi en mer effektiv håndheving av loven og sikre at de som er ansvarlige for cyberkriminalitet blir stilt til ansvar, uavhengig av hvor den straffbare handlingen fant sted. En spesialisert straffedomstol vil også

[34] Schjølberg. (2023) s. 182.
[35] Europarådet. (2001)
[36] Schjølberg. (2023) s. 228.

muliggjøre å utvikle spesialisert kunnskap om cyberkriminalitet som kan bidra til å bekjempe denne typen kriminalitet på en effektiv måte. I et samfunn med kontinuerlig digital transformasjon, er det avgjørende med en forståelse av de tekniske problemstillingene for å lykkes med saker som omhandler ny teknologi. For å kunne løse en sak må retten forstå hvordan en bestemt teknologi fungerer. Dette hjelper med å fastslå hvilke typer bevis som er nyttige, hvor raskt bevisene må sikres for å forhindre at går tapt, og hvordan de skal sikres. Domstolene vil med dette vite hvilke bevis som skal avvises som irrelevante, og være mer villige til å beordre sikring av elektroniske bevis. Dette bidrar til oppklaring i saken for domstolene, slik at avgjørelsen baserer seg på et riktig og fullstendig opplyst faktum.

I løpet av de siste årene har politi- og påtalemyndighet etablert enheter som spesialiserer seg på forbrytelser innenfor cyberspace. Det samme har flere advokatfirmaer foretatt seg, ved å opprette spesielle tverrfaglige arbeidsgrupper med fokus på nettkriminalitet. En slik utvikling har imidlertid ikke domstolene hatt. Dermed ender kompliserte saker som involverer de nyeste teknologiene hos dommere, som til daglig håndterer klassiske rettsområder. På den ene siden kan dommerne ha begrenset tid til å sette seg inn i alle aspekter ved en ny teknologi, noe som kan ha innvirkning på rettsavgjørelsen. På den andre siden krever imidlertid ikke alle tilfeller at den nye teknologen blir forklart i detalj. I utgangspunktet vil det være tilstrekkelig med et oversiktsbilde av de viktigste elementene og hendelsene blir avklart for dommeren. En god og grundig forståelse av cyberkriminalitet vil likevel føre til raskere og mer effektiv saksbehandling, og at saker tilknyttet cyberspace blir løst av en domstol med inngående kompetanse om teknologi.

Et forslag om en internasjonal domstol ble fremmet av Stein Schjølberg på FNs «Congress on Prime Prevention and Criminal Justice» i Bangkok i 2005. Det har blitt foreslått å organisere en domstol mot cyberkriminalitet med og som en del av Den internasjonale domstolen i Haag (ICJ). Spørsmålet er hvordan en spesialisert domstol for cyberkriminalitet kan skille seg fra Den internasjonale straffedomstolen i Haag.

Den internasjonale domstolen i Haag er det fremste judisielle organet i FN, og fungerer som verdens viktigste domstol. Hovedoppgaven til domstolen er å etterforske og straffeforfølge individer som har begått forbrytelser mot menneskeheten, krigsforbrytelser og folkemord. En spesialisert domstol for cyberkriminalitet vil ha en annen rolle og fokusere på ren cyberkriminalitet, slik som hacking, cyberangrep og løsepengevirus. Mens Den internasjonale straffedomstolen har en bredere jurisdiksjon, kan en cyberdomstol ha en mer spesifikk og avgrenset funksjon.

Avhandlingen går ikke nærmere inn på andre mulige organiseringer av en spesialisert domstol for cyberkriminalitet. Men en straffedomstol vurderes som vesentlig for å kunne straffeforfølge alvorlige tilfeller av angrep i cyberspace.[37]

4 Strafferetten i cyberspace

4.1 Grunnvilkår for straffeansvar

De alminnelige grunnvilkårene for straffansvar er regulert i straffeloven kapittel 3. For at noen skal kunne straffes, må fire vilkår være oppfylt: (1) handlingen må være lovstridig, (2) det må ikke foreligge noen straffrihetsgrunn, (3) gjerningspersonen må være tilregnelig og (4) og ha utvist skyld. Det kreves at en handling både objektivt og subjektivt må rammes av en straffebestemmelse.

I likhet med annen kriminalitet, er skyldkravet for cyberkriminalitet forsett. Dette fremgår av straffeloven § 21, som fremhever at straffelovgivningen bare rammer «forsettlige lovbrudd». Ordlyden tilsier at det er overtredelser av straffelovgivningen begått med viten og vilje, som er straffbare. En videre presisering av forsettskravet finner vi i § 22. Imidlertid gjelder forsettskravet bare så lenge «annet ikke er bestemt», jf. § 21. Dermed kan uaktsomhet i enkelte tilfeller være tilstrekkelig for å oppfylle skyldkravet.

Straffeloven rammer også medvirkning til cyberkriminalitet, eksempelvis i planleggingsfasen eller ved selve utførselen av handlingen. Rettsgrunnlaget for å straffe medvirkning til overtredelse er straffeloven § 15. Bestemmelsen omfatter alle bestemmelsene i straffelovgivningen, med mindre det tydelig er unntatt i den enkelte straffebestemmelsen.

Etter straffeloven § 16 er det straffbart med forsøk på cyberkriminalitet. Dette gjelder dersom straffebestemmelsen i straffelovgivningen kan medføre «fengsel i 1 år eller mer».

4.2 Eget kapittel i straffelovgivningen om cyberkriminalitet?

I forslaget til ny straffelov spesiell del har departementet lagt til grunn en stor del av Straffelovkommisjonens forslag til kapittelinndeling.[38] Departementet har gått inn for at bestemmelser som tar sikte på å beskytte informasjon og informasjonsutveksling fortrinnsvis samles i ett kapittel. Bestemmelsene i strl. kapittel 21 har derfor til felles at de først og fremst verner om informasjon og informasjonsutveksling. Det betyr at kapitlet ikke er forbeholdt typiske «datakriminelle» handlinger, men også omfatter handlinger som generelt truer informasjon og informasjonsutveksling i samfunnet. Det kan være handlinger som skjer uten bruk av teknologiske

[37] Schjølberg. (2023) s. 18.

[38] Ot.prp. nr.8 (2007–2008) s. 17-18

virkemidler, og som heller ikke retter seg mot datasystemer eller elektroniske kommunikasjonsnett, se eksempelvis strl. § 209 knyttet til taushetsplikt.[39]

Men det presiseres at også de øvrige kapitlene i straffelovens spesielle del inneholder enkeltbestemmelser som har en side til vern av informasjon og kommunikasjon. Videre i avhandlingen vil det redegjøres for bestemmelser fra straffeloven som er mest relevant i forhold til et tjenestenektangrep, og andre straffebestemmelser som kan være relevante i forbindelse med utførelsen av angrepet. Bestemmelsene presenteres ikke i henhold til straffelovgivningens kronologi, men etter problemstillingens relevans.

5 Relevante straffebestemmelser mot DDoS-angrep

5.1 Straffeloven §§ 206 og 351 – Fare for driftshindring og skadeverk

5.1.1 Materiell rett

Skadevoldende handlinger mot data og datasystemer, slik som tjenestenektangrep, kan straffes etter flere bestemmelser. Siden §§ 206 og 251 har dels overlappende virkeområde når det gjelder strafferegulering av DDoS-angrep, foretas det en løpende fortolkning av bestemmelsene nedenfor.

Straffebudet i § 206 rammer den som «uberettiget volder fare for avbrudd eller en vesentlig hindring» av driften av et datasystem. Dette kan gjøres ved å overføre, skade, slette, forringe, endre, tilføye eller fjerne informasjon, som i enkelte tilfeller vil kunne omfattes av bestemmelsen for skadeverk i straffeloven § 351.

En naturlig språklig forståelse av ordlyden tilsier at gjerningspersonen uten lovlig rett, gjennom ett eller flere av de opplistede fremgangsmåtene, medfører risiko for mulig stans i datasystemet eller en vesentlig blokkering i driften av datasystemet. Dermed får ikke bestemmelsene anvendelse på lovlige handlinger eller aktiviteter som utføres som del av drift, design, utvikling eller vedlikehold av datasystemer og nettverk.

Det er selve fareelementet som er gjort straffbart, og dette tilsier at overtredelsen av straffebudet er fullbyrdet allerede når faren er fremkalt, jf. ordlyden «volder fare for …». Et angrep på datasystemer kan bestå i at det iverksettes kapasitetskrevende prosesser på datasystemer som skaper fare for driftshindring eller avbrudd. Det som kreves, er en fare for et markert avvik fra datasystemers ordinære yteevne, og det er uten betydning om det er fare for langvarig eller kortvarig avbrudd eller vesentlig driftshindring. Imidlertid kan varigheten få betydning i vurderingen av om hindringen er vesentlig.[40]

[39] Ot. prp. nr. 22 (2008-2009) s. 20

[40] Schjølberg. (2017) s. 72

Driftsavbrudd av et datasystem er en alvorlig hendelse som kan medføre store økonomiske konsekvenser, i form av nedetid og utilgjengelighet. Det er dette vi ofte ser i form av tjenestenektangrep.

Skadeverksbestemmelsen § 351 er et skadestraffebud, hvor man straffer handlinger som «skader, ødelegger, gjør ubrukelig eller forspiller en gjenstand». En naturlig språklig forståelse av ordlyden tilsier at overtredelsen fullbyrdes idet skaden har manifestert seg på et vernet rettsgode, som for vårt vedkommende kan være data lagret på en dataserver eller et datasystem. Det avgjørende elementet i et skadestraffebud er at det begås en skade, ikke hvordan den begås.

Farestraffebud derimot krever ikke at handlingspersonens handling faktisk har ført til skade på gjerningsobjektet. Det er tilstrekkelig at handlingen kan medføre en skade; det vil si at det har oppstått en fare for det.[41]

Slik vi ser, er det noe overlappende gjerningsbeskrivelser mellom disse straffebestemmelsene. Foreløpig mangler vi rettspraksis som kan avklare bestemmelsenes saklige avgrensning, og vi må derfor hente veiledning fra forarbeidene. Etter rettspraksis har den alminnelige skadeverksbestemmelsen blitt anvendt som hjemmel for å straffe brudd på data og datasystem. Bestemmelsene om skadeverk (§ 351) og fare for driftshindring (§ 206) utvider straffeområdet ytterligere. Ved innføringen av § 351 annet ledd fikk data et selvstendig vern mot skadevoldende handlinger, og bestemmelsen omfatter både lagrede data og data under overføring.[42]

Paragraf 206 supplerer den alminnelige skadeverksbestemmelsen. Straffebudet rammer handlinger som før var tvilsomme hvorvidt skulle anses som skadeverk eller straffes for forsøk på skadeverk. Hovedbestemmelsen er altså § 351, og § 206 er et supplement.[43] Dette utledes også lovteknisk, da skadeverksbestemmelsen suppleres av § 206, fordi den slår ned på handlingen mens den er på farestadiet.

5.1.2 Anvendelsesområdet

Spørsmålet som oppstilles i denne delen av avhandlingen er hvordan de tre bestemmelsene – henholdsvis § 351 første og annet ledd, og § 206 – harmoniseres og dermed får sitt eget anvendelsesområde. Regulerer § 351 annet ledd alle digitale skadevoldende handlinger, både de som begrenser seg til å ramme data, og de som skader datasystemet?[44] Slik vi har sett på tidligere er

[41] Gröning, Husabø og Jacobsen. (2015). s. 176
[42] Ot.prp. nr. (2008-2009) s. 61 og 2.15.5. NOU 2007: 2 s. 153
[43] Ot.prp. nr. 22 (2008-2009) s. 63
[44] Sunde. (2016) s. 102

objektet for vern ulikt for de forskjellige leddene i § 351. Første ledd regulerer «gjenstand», som også innbefatter datasystem, sammenliknet med fortolkningen av «løsøregjenstand» i straffeloven § 343.[45]

De skadevoldende handlingene som reguleres etter annet ledd er tilsiktet objektet, «data». Virkeområdet for annet ledd er uberettigete endringer i data, og ikke et datasystem. Skadevoldende handlinger mot et datasystem vil kunne reguleres av første ledd, jf. ordlyden «gjenstand».

Videre er gjerningsbeskrivelsen i §§ 206 og 351 i stor grad sammenfallende. Begge bestemmelsene regulerer handlinger hvor man endrer, gjør tilføyelser til, skader, sletter eller ødelegger data. Hvis man følger begrepsbruken innenfor informasjonssikkerhet, hvor det differensieres mellom objekt- og datasikkerhet, bør § 351 første ledd reserveres for fysiske skadeverk mot datasystem, mens § 351 annet ledd bør ramme alle digitale krenkelser, både slike som må anses som skade på datasystemet, og slike som begrenser seg til å skade data uten konsekvenser for systemet.[46]

Et tjenestenektangrep er en angrepsmåte som i utgangspunktet skal ramme data i et datasystem, og gjøre innholdet i datasystemet utilgjengelig for brukerne av systemet. Dermed får ikke brukerne anvendt tjenesten som tiltenkt. Angrepet rammer altså tilgangen til datasystemet, og det kan drøftes hvorvidt datasystemet har blitt fysisk skadet av angriperne. Om et tjenestenektangrep ikke resulterer i noen form for fysisk skadeverk, er ikke angrepet regulert av § 351 første ledd. Dersom tjenestenektangrepet fører til fysiske skader på datasystemet, i form av datasystemets utilgjengelighet eller andre skadevirkninger, vil bestemmelsen likevel få anvendelse. Det presiseres at dette varierer fra angrep til angrep, hvor det avgjørende er realiteten og vurderingen av hvilke konsekvenser angrepet har medført.. Etter dette subsumeres skade på datasystemet under § 351 første ledd. Av forarbeidene fremgår det dessuten at § 351 første ledd kan bli supplert av § 206, som kun utgjør et supplement til § 351 første ledd. En driftshindring, slik som et DDoS-angrep, betegnes der som «systemskadeverk».[47]

Et annet relevant rettslig grunnlag for å sanksjonere tjenestenektangrep er § 351 annet ledd, dersom angrepet rammer data, og dette medfører bortfall av tilgang for brukerne av systemet. Dette kvalifiserer seg som en digital krenkelse, hvor bestemmelsen kommer til anvendelse. Det presiseres også at § 351 annet ledd har et selvstendig anvendelsesområde for dataendringer som ikke skader datasystemet eller volder fare for driftshindring. Bestemmelsen rammer også data under overføring, og har dermed et større nedslagsfelt.

---

[45] Rt. 2004 s. 1619 avsnitt 27

[46] Sunde. (2016) s. 103.

[47] Ot.prp. nr. 22 (2008-2009) s. 63.

Det vesentlige under subsumpsjonen, er å huske skillet mellom data og datasystemer, som igjen er bestemmende for hvilken bestemmelse som får anvendelse. Det lovgivningsmessige utgangspunktet uttrykt gjennom forarbeidene er at data og gjenstand prinsipielt – rettslig og faktisk – er ulike objekter. Dette kommer særlig til uttrykk i straffeprosessretten, hvor man behandler data som er et selvstendig objekt for beslag, jf. «ting» i straffeprosessloven § 203. Avhandlingen går ikke nærmere inn forskjellen mellom data og datasystem her.

5.2 Straffeloven § 192 – Anslag mot infrastrukturen

5.2.1 Formålet

Straffeloven § 192 finner vi i kapittel 20 om vern av den offentlige ro, orden og sikkerhet. Bestemmelsen viderefører straffeloven 1902 § 151b, og får tydeligere frem at datasystemer har et selvstendig vern mot sabotasje.[48] Bestemmelsen tilsvarer Straffelovkommisjonens utkast § 20-11 om sabotasje mot infrastrukturen.[49] Straffelovkommisjonen uttalte om straffeloven 1902 § 151 b, blant annet at bestemmelsens ordlyd er uklar, men bør ramme enhver ødeleggelse av informasjonssamling som volder omfattende forstyrrelser i forvaltningen eller samfunnslivet for øvrig, for eksempel ødeleggelse av et elektronisk system for betalingsformidling.

Siden flere stater har et særskilt straffebud som regulerer anslag mot infrastrukturen, tilsier internasjonale hensyn at Norge også har en slik bestemmelse.

5.2.2 Gjerningsbeskrivelsen

Straffeloven § 192 rammer den som volder omfattende forstyrrelse i den offentlige forvaltningen eller i samfunnslivet for øvrig. Bestemmelsen rammer kvalifiserte tilfeller, jf. ordlyden «omfattende». Ordlyden angir imidlertid ingen konkret terskel, og hva som skal regnes for omfattende forstyrrelse må bero på en skjønnsmessig vurdering. Det er imidlertid de virkelige alvorlige forstyrrelsene bestemmelsen tar sikte på, noe som også fremgår av strafferammen i straffebudet.[50] Ved mindre alvorlige forstyrrelser, må man ta i bruk bestemmelsene om skadeverk eller andre relevante grunnlag. Disse kommer jeg tilbake til senere i oppgaven. Hva som skal anses å utgjøre en «omfattende forstyrrelse» må baseres på en samlet vurdering, hvor varigheten, omfanget og virkningene av forstyrrelsene vil være avgjørende.[51] Oppgaven avgrenses mot hva som kreves konkret for å oppfylle vilkåret.

[48] Ot.prp. nr. 8 (2007-2008) s. 258-259 og s. 347
[49] NOU 2002: 4 s. 301-302
[50] NOU 1985: 31 s. 33
[51] Ot.prp. nr. 8 (2007-2008) s. 347.

Hvordan skaden er forårsaket, er bare overordnet beskrevet som «å ødelegge, skade eller sette ut av virksomhet». Både fysisk skade og skade som begås elektronisk omfattes. En mulig fremgangsmåte er utførselen av et DDoS-angrep som setter ut av funksjon et digitalt styringssystem, eller et skadelig datavirus som sletter SIM-kortdatabasen til en mobiloperatør.

Datasystemer reguleres både av bokstav a og b. For bokstav a fremgår det direkte av ordlyden, jf. «informasjonssamling», som også inkluderer dataanlegg. En naturlig språklig forståelse av ordlyden «informasjonssamling», kan tilsi at datasystemets formål er å registrere og samle opplysninger, eksempelvis Folkeregister eller Riksarkivets datasamling. Imidlertid har bestemmelsen lovteknisk to bokstavinndelinger, hvor bokstav a bedre skal få frem at dataanlegg generelt omfattes. «Informasjonssamling» i § 192 bokstav a omfatter således både digitale styringssystemer (SCADA), dataanlegg som har som formål å registrere og lagre opplysninger (f.eks. Folkeregisteret), tjenesteytende datasystemer (f.eks. Nasjonalt reseptregister) og datalagre (f.eks. nasjonalt masselager for databeslag i straffesaker). [52] Det avgjørende er datasystemets samfunnskritiske funksjon, ikke dets formål i seg selv.

Dersom en handling ligger utenfor forsettet, og dermed ikke var tiltenkt, men likevel oppfyller kravet til «omfattende forstyrrelse», jf. § 21, jf. § 21, blir det tale om grovt skadeverk, jf. § 352, jf. § 351. Dette kan bli aktuelt i tilfeller hvor gjennomføringen av et DDoS-angrep får mer vidtrekkende konsekvenser enn angriperen hadde forutsett. Slike utilsiktede virkninger må også være strafferegulert, slik at lovbrytere ikke slipper unna, ved å hevde at angrepet ikke skulle være så vidtfavnende.

6 Relevante straffebestemmelser for utførelsen av cyberangrep

Tjenestenektangrep kan variere fra hverandre, og dette kan utgjøre en rettslig utfordring, da ulike angrep kan være regulert av ulike straffebestemmelser. Slik vi har sett hittil, eksisterer det forskjellige lovhjemler for å straffeforfølge DDoS-angrep. Ikke minst er det viktig å bemerke at tjenestenektangrep er en cyberoperasjon med et hendelsesforløp, bestående av ulike stadier. DDoS-angrep inndeles hovedsakelig i en forberedelses-, utførelses- og sluttstadiet. Straffebestemmelsene som får anvendelse under straffeforfølgningen avhenger av hvilket stadium angrepet befinner seg på, og hva slags skade angrepet har medført. Dessuten utføres mange DDoS-angrep ved hjelp av datavirus eller annen skadelig programvare, og besittelse av slike programvarer er regulert av andre bestemmelser i straffeloven. Derav behandles de mest relevante straffebestemmelsene rundt overordnet cyberkriminelle operasjoner nedenfor.

[52] Sunde. (2016) s. 99

6.1 Straffeloven § 204 – Innbrudd i datasystem

6.1.1 Internasjonal forpliktelse

Straffeloven § 204 straffer den som bryter en beskyttelse eller ved annen uberettiget fremgangsmåte skaffer seg tilgang til et datasystem eller del av det.

Bestemmelsen gjennomfører Europarådets konvensjon om cyberkriminalitet artikkel 2 om datasystemers integritet og tilgjengelighet. Denne artikkelen fastsetter at medlemstater må vedta de lover og andre tiltak som er nødvendige for å straffesanksjonere uberettiget «access to the whole or any part of a computer system».

Artikkelen omfatter den rettsstridige tilgangen til eller inntrengningen i et datasystem, og omfatter både enkeltstående maskiner og elektroniske nettverk, jf. ordlyden av «any part». Hensynet til våre internasjonale forpliktelser, tilsier at det etableres en slik bestemmelse som straffeloven § 204. Formålet med bestemmelsen er å sikre at lagrede data ikke utsettes for uberettigede angrep, og bevare datasystemers konfidensialitet, integritet og tilgjengelighet.

Gjerningsmannen må ikke nødvendigvis ha gjort seg kjent med innholdet ved gjennomføringen av datainnbruddet. Det avgjørende er å ha skaffet seg tilgangen til datasystemet. Bestemmelsen beskytter også den kommersielle verdien av data når gjerningsmannen får en tilgang til data han ellers måtte ha betalt vederlag for, jf. Rt. 1994 s. 1610. Saken gjaldt produksjon og salg av piratfiltre som gjorde det mulig å ta inn TV 1000 uten samtykke fra rettighetshaveren. TV 1000 er en betalingsfjernsynskanal som sender TV-programmer over satellitt. I dommen kom man til at tilfeller hvor den datalagrede informasjon er tilgjengelig for allmennheten mot erleggelse av betaling, og den innlagte sperre bare har til formål å sikre at betaling ytes, også anses som datainnbrudd.

Paragrafen handler om «[i]brudd i datasystem» - ofte omtalt som «datainnbrudd». Lovgiver har imidlertid valgt å gå vekk fra uttrykket «datainnbrudd» for å få frem at straffebudet bare rammer uberettiget tilgang til lagrede data og ikke data under overføring.[53]
Oppgaven avgrenses mot handlinger hvor man ved å bryte en beskyttelse skaffer seg tilgang til informasjon som overføres ved elektroniske midler, og som reguleres av straffeloven § 205 b.

6.1.2 Gjerningsbeskrivelsen

Skadepotensialet ved innbrudd i datasystemer er stort. Ved bruk av automatisert verktøy er det mulig å bryte seg inn på tusenvis av dataservere over hele verden, mens en person ved alminnelige innbrudd bare kan bryte seg inn i ett bygg om gangen. Skadepotensialet og skadens omfang beror på hva slags datasystem det er skaffet tilgang til, eksempelvis om systemet

[53] Ot.prp. nr. 22 (2008-2009) s. 51

inneholder sensitive personopplysninger. Ved hjelp av et slikt innbrudd kan gjerningspersonen foreta tjenestenektangrep direkte i datasystemet, da angriperen besitter tilgang. Dette kan medføre en høyere grad av utfordring i å identifisere hvem som står bak et tjenestenektangrep.

6.1.2.1 Tilgang til datasystem

Etter § 204 er det straffbart å skaffe seg uberettiget tilgang til datasystem eller del av det. Om begrepet «datasystem» vises det til redegjørelsen i punkt 1.4.3.2. Innbrudd i datasystem kan være berettiget for eksempel hvis den sikkerhetsansvarlige har fullmakt til å forsøke å forsere en passordbeskyttelse for å teste systemsikkerheten. Testing med samtykke av den berettigete for å avsløre svakheter i sikkerhetssystemet medfører derfor ikke straffeansvar.[54] Det er den uberettigede tilgangen til datasystemet eller deler av det som er gjort straffbart her.

En alminnelig språklig forståelse av «tilgang» tilsier noe mer enn ytre observasjoner, f.eks. av innholdet på en dataskjerm. Den forklarende rapporten til Budapestkonvensjonen opplyser at «tilgang» betyr «the entering of the whole or any part of a computer system», jf. rapportens punkt 46. Det er uenighet hvorvidt en som uberettiget går inn på et kontor og leser informasjon på en pc-skjerm, kan anses å ha overtrådt bestemmelsen. Dette er en rettslig problemstilling som enda ikke er avklart gjennom rettspraksis, da grensene for hva som anses som «part of a computer system» ikke er trukket opp enda. Ved å ha logget seg på, eller på annet uberettiget vis trengt seg inn i datasystemet, er tilgang oppnådd. Da er handlingen fullbyrdet. Selv om dataene bare er gjort tilgjengelig for gjerningspersonen uten at han tilegner seg kunnskapen eller forstår innholdet i informasjonen, eller vet hvor informasjonen er lokalisert, er handlingen straffbar. Dette henger også sammen med den forklarende rapporten til Budapestkonvensjonen, om å erverve seg tilgang til «any part of a computer system».[55]

Det er heller ikke krav om at informasjonen må være lastet ned, for å oppfylle vilkåret om tilgang. Forsøk på å skaffe tilgang til passord eller andre innloggingsopplysninger uten tillatelse, kan utgjøre en straffbar handling, til tross for at man ikke skulle finne slike opplysninger, eller det overhodet ikke lar seg gjøre. Dermed er det straffbart å utforske et datasystem eller aktivisere sikkerhetssystemer eller adgangsprosedyrer, da dette kvalifiserer seg til å «bryte en beskyttelse» i et datasystem.

Videre må dataene man erverver være lagret i et lagringsmedium. Dersom de fremdeles er under overføring, reguleres forholdet av § 205 bokstav b om informasjon under overføring. Avhandlingen er avgrenset mot slik informasjon.

---

[54] Schjølberg. (2017). s. 55

[55] Schjølberg. (2017) s. 57

En handling som ved første øyekast fremstår utilsiktet og uskyldig, kan medføre betydelige økonomiske konsekvenser. Særlig ved mistanke om inntrengningen fra hackere kan det være nødvendig å gjennomgå datasystemer for å utelukke andre typer konsekvenser, eksempelvis overvåkning av informasjon, eller at datasystemer er ute av funksjon i et tidsrom. Av forarbeidene fremgår det at den som «uberettiget og med utgangspunkt i egen brukerkonto trenger seg inn på andres brukerkonti eller administrativt område på samme system, vil være omfattet, jf. «del av det»».[56] Departementet viser til at bestemmelsen i utgangspunktet bare verner informasjon indirekte ved å hindre tilgang til informasjonen, mens det som direkte straffes er den uautoriserte inntrengingen i systemet.

6.1.2.2 Beskyttelsesbrudd

Etter bestemmelsen må tilgangen være anskaffet ved å «bryte en beskyttelse». Dette vilkåret har en særlig viktig betydning for det strafferettslige vernet av datasystemer. Ved å oppstille et slikt vilkår om beskyttelse, forutsettes det at man i alminnelighet beskytter sine data ved sikkerhetstiltak som brukeridentifikasjon, passord, totrinnsverifisering eller lignede. Kravet styrker behovet for sikkerhetstiltak i cyberdomenet og reduserer faren for at det begås cyberkriminalitet. Informasjonen ligger ikke like tilgjengelig, når den er sikret gjennom et sikkerhetstiltak. Videre vil graden av beskyttelse varierer fra ett enkelttilfelle til et annet, og bero på skjønn. Bestemmelsen omfatter også tilfeller der beskyttelsen eksisterer for å sikre at den berettigede mottar vederlag for informasjonen som gjøres tilgjengelig i datasystemet.[57]

Det er imidlertid viktig å huske at ikke enhver form for sikkerhetstiltak er å karakteriseres som beskyttelse etter lovens ordlyd. Dersom data er åpen og tilgjengelig for alle, foreligger det ikke innbrudd i datasystemet. Straffelovrådet uttalte om dette: «Tanken bak bestemmelsen er at det primært hviler på innehaveren av anlegget å sørge for beskyttelse mot innsyn fra uberettigede. Først når det er tatt rimelige foranstaltninger i så måte, kan han kreve hjelp fra strafferettsapparatet.»[58]

Justisdepartementet uttalte i forarbeidene til straffeloven at: «Det er ikke et vilkår at innbruddet skjer ved å bryte en beskyttelse», jf. ordlyden av «eller på annen uberettiget måte». Siden brudd på beskyttelse anses å være et kjent typetilfelle, er dette særskilt nevnt i loven.[59] Hvis den som påberoper beskyttelse, har iverksatt tiltak slik at utenforstående forstår at informasjonen er begrenset i forhold til deling, må vilkåret beskyttelse anses å være oppfylt.

---

[56] Ot.prp. nr. 22 (2008-2009)

[57] Schjølberg. (2017) s. 58

[58] NOU 1985: 31 s. 31

[59] Ot.prp. nr. 22 (2008-2009) s. 403

6.1.2.3 Uberettiget fremgangsmåte

Straffeloven § 204 oppstiller også et annet alternativ enn beskyttelsesbrudd. Det fremgår av ordlyden at bestemmelsen også rammer den som «ved en annen uberettiget fremgangsmåte» skaffer seg tilgang til datasystem eller del av det. Dermed får ikke loven anvendelse på eksempelvis et tilfelle hvor den berettigete gir tillatelse til dataansvarlig til å forsøke å forsere en passordbeskyttelse for å kontrollere systemsikkerheten i en bedrift.

Justisdepartementet uttaler i forarbeidene til straffeloven at rettsstridsreservasjonen videreføres fra straffeloven 1902 § 145 annet ledd. Dermed vil rettspraksis om grensen mellom berettiget og uberettiget tilgang fortsatt være aktuell.[60]

Saken inntatt i Rt. 2012 s. 1669 gjaldt spørsmålet om domfellelse for hacking. Den reiste spørsmål ved tolkningen av straffeloven § 145 andre ledd om datainnbrudd, og om tiltalte hadde handlet i vinnings hensikt. Saksforholdet var at fornærmede ga sin pc og passordet for innlogging til tiltalte for at han skulle ordne opp i virusproblemer på maskinen. Tiltalte benyttet anledningen til å gå inn og kopiere privat informasjon på pc-en.

Førstvoterende konstaterte raskt at tiltalte gjennom sin handlemåte hadde fått tilgang til «data». Andre ledd rammet imidlertid bare den som «uberettiget skaffer seg adgang», og dette ble nærmere avgjort ved å se på bestemmelsens forhistorie. Konklusjonen ble «at det at tiltalte her har fått passord og PC og tilgang til å undersøke maskinen i sin helhet, må medføre at han ikke uberettiget har skaffet seg adgang til data som etter påloggingen lå åpne for ham». Det ble slått fast at han ikke hadde skaffet seg uberettiget tilgang til informasjon «ved annen uberettiget fremgangsmåte», jf. dommens avsnitt 26.

6.2 Straffeloven § 201 – Uberettiget befatning med tilgangsdata, dataprogram mv.

6.2.1 Internasjonal forpliktelse

Straffeloven § 201 er i hovedsak en ny bestemmelse om uberettiget befatning med tilgangsdata, dataprogram mv.

Bestemmelsen gjennomfører Europarådets konvensjon om cyberkriminalitet artikkel 6. Denne artikkelen fastsetter at medlemstater må vedta de lover og andre tiltak som er nødvendige for å fastslå blant annet «the production, sale, procurement for use, import, distribution or otherwise making available [...] a device, including a computer program […] computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed», jf. henholdsvis artikkelens punkt a.

[60] Ot.prp. nr. 22 (2008-2009) s. 403

Artikkelen får anvendelse på produksjon, salg, erverv for bruk, import, distribusjon eller tilgjengeliggjøring på annen måte når det skjer i den hensikt å begå en straffbar handling fastslått i samsvar med artikkel 2 til 5 i konvensjonen, som uautorisert testing og beskyttelse av datasystem.[61]

Å spre datavirus eller gjøre tilgjengelig et datasystem for uautoriserte og uvedkommende, kan bli meget omfattende og ukontrollert. Typiske virus med stort skadepotensiale, også kjent som malware, kan forårsake betydelig skade og ulempe.

Innretninger som datavirus og hackerverktøy har i utgangspunktet intet lovlig formål og anvendes for å begå straffbare handlinger. For å begrense disse handlingene er det utvetydig nødvendig å straffesanksjonere besittelsen av datavirus og hackerverktøy. Det er dermed viktig at straffeansvaret moderniseres, og også rammer forberedelseshandlinger foretatt med data, datasystemer og elektronisk kommunikasjon. Gjennom å straffesanksjonere alle former for spredning med tilgangsdata og hackerverktøy styrkes det videre arbeidet med å forebygge cyberkriminalitet. Dette er i overensstemmelse med våre internasjonale forpliktelser som tilkjennegir klare og utvetydige straffebestemmelser, slik at alle former for cyberkriminalitet straffes i Norge.[62]

Straffeloven § 201 oppfyller alle nevnte formål i Budapestkonvensjonen artikkel 6. Det er dermed straffbart dersom noen uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen «passord eller andre opplysninger som kan gi tilgang til databasert informasjon eller datasystem» eller «dataprogram eller annet», jf. bestemmelsens punkt a og b.

6.2.2 Gjerningsbeskrivelsen

Gjennom anvendelse av tilgangsdata eller dataprogram kan man få tilgang til data, foreta avlytting av informasjon, forårsake dataskadeverk og systemskadeverk. Dataprogrammer og andre digitale innretninger som er objektivt designet for eller tilpasset primært for å begå lovbrudd, eksempelvis datavirus og hackerverktøy, er typiske slike dataprogram. Typiske tilgangsdata er passord og innloggingskoder.

6.2.2.1 Straffeloven § 201 a

Straffeloven § 201 bokstav a omfatter den som uberettiget fremstiller, anskaffer, besitter eller gjør tilgjengelig for en annen passord eller andre opplysninger.

En naturlig språklig forståelse av «gjør tilgjengelig» tilsier det å overlate tilgangsdata til en annen, uavhengig av antallet som får som får tilgang til opplysningen. Spredningen kan skje

[61] Ajourført versjon av Straffeloven 2005, kommentarutgave av Matningsdal. Hentet 20.02.23.

[62] Schjølberg. (2017) s. 67

direkte, ved at selve passordet oversendes til en annen, eller indirekte, ved å spre en URL-adresse eller lenke til nettsider hvor passordet finnes, eller som angir på hvilken nettside opplysningen befinner seg.[63] Det er uten betydning hvor mange ledd man går gjennom, og om spredningen skjer med eller uten vederlag.[64]

Betegnelsen «passord eller andre opplysninger» er funksjonelt avgrenset og omfatter alle data som kan gi tilgang til fysiske eller logiske nivåer i et datasystem. Sammensetningen av tilgangsopplysningene er uten betydning, og kan dermed være bestående av tall, symboler eller bokstaver. Det er også uten betydning om dataene er kryptert. Bestemmelsen er ikke begrenset til å gjelde data brukeren selv taster inn i datasystemet, men omfatter også data som genereres maskinelt ved bruk av for eksempelvis irisavlesning, avlesning av fingeravtrykk eller stemmeregistrering.[65] Fremstilling av passord omfatter også passordknekking, som utføres maskinelt for å gjette passord.

Ordlyden av «anskaffer» tilsier en aktivitet hvor man får tak i passord eller andre opplysninger. Dermed omfatter ikke ordlyden en passiv mottakelse av passord eller andre opplysninger som man er uberettiget til. Det må altså overskrides en viss grense for aktivitet for å oppfylle vilkåret om anskaffelse. Dersom man bevisst aksepterer et tilbud om å motta tilgangsdata eller andre innloggingskoder, er dette en form for anskaffelse, og oppfyller vilkåret om aktivitet. Tilsvarende må antas å gjelde dersom man filmer inntasting av passord eller ved bruk av tastetrykkleser.[66]

6.2.2.2 Straffeloven § 201 b

Straffeloven § 201 bokstav b omhandler fremstilling, anskaffelse, besittelse eller gjøre tilgjengelig dataprogram eller annet som er særlig egnet som middel til å begå straffbare handlinger som retter seg mot databasert informasjon eller datasystem.

Bestemmelsen omfatter forskjellige befatninger med dataprogrammer og andre innretninger, slik som datavirus eller hackerverktøy, og som særlig er egnet til å begå straffbare handlinger som retter seg mot data eller datasystemer. Det kreves derfor at disse er utviklet eller tilpasset hovedsakelig i den hensikten å begå annen cyberkriminalitet.

Ordlyden av «annet som er særlig egnet som middel» er vid, og omfatter enhver logisk eller fysisk innretning som er egnet til å begå lovbrudd rettet mot databasert informasjon eller

[63] NOU 2003: 27 s. 59
[64] Schjølberg. (2017) s. 74
[65] NOU 2003: 27 s. 59
[66] Ot.prp. nr. 22 (2008-2009) s. 400

datasystem. Uttrykket «særlig egnet» angår ikke bare krav til at innretningen funksjonelt sett må være spesielt godt egnet, men også at dette må fremstå som innretningens mest fremtredende egenskap.[67] Databasert informasjon er informasjon selv om den ikke umiddelbart er tilgjengelig eller ikke er lesbar uten bruk av elektronisk utstyr.
Når det gjelder fremstilling eller produksjon av dataprogram eller annet som er særlig egnet som middel, er det typiske tilfellet en gjerningsmann som konstruerer et slikt dataprogram. Å anskaffe «dataprogram eller annet som er særlig egnet som middel» omfatter også tilfeller hvor dette er bestilt, men enda ikke levert.[68] Det kan eksempelvis være tale om en programvare til å overbelaste en server med datatrafikk, og derved iverksette et tjenestenektangrep. Programmet kan ha vært selvkonstruert eller bestilt fra en aktør.

Det siste alternativet består i å gjøre «dataprogram eller annet som er særlig egnet som middel» tilgjengelig for en annen. En alminnelig måte å tilgjengeliggjøre et dataprogram på er å selge det mot vederlag i en eller annen form. Distribusjon er også innbefattet, og innebærer en aktiv handling som det å videbringe dataprogram til andre. Et annet typisk tilfelle er å gjøre datavirus tilgjengelig på en nettside eksempelvis i form av datakobling, slik at andre kan bruke det. Det kan for eksempel anvendes til å utføre et DDoS-angrep. Av forarbeidene fremgår det at markedsføring også omfattes.

Videre er det straffbart å være i besittelse av et selvspredende dataprogram dersom besittelsen skyldes uberettiget fremstilling eller anskaffelse av dataprogrammet. Slike programmer betegnes også malware. Malware er fellesbetegnelsen på skadelige programmer og omfatter blant annet virus, ormer, spyware, adware og trojanske hester. I strafferettslig sammenheng er begrepet «besittelse» vært knyttet til fysiske gjenstander eller eiendom. Anvendelsen av betegnelsen på immaterielle objekter i datasystemer eller elektronisk kommunikasjon kan være utfordrende. Dette har særlig kommet til uttrykk i rettspraksis som angår besittelse av pornografi, og disse kan få tilsvarende betydning når det gjelder besittelse og oppbevaring av passord, datavirus og hackerverktøy på elektroniske lagringsmedier. Gjerningspersonen må ha rådighet over materialet, men besittelseskravet oppstiller ikke et krav om at lovbryteren må ha materialet fysisk hos seg, så lenge materialet er på et sted vedkommende selv kontrollerer.[69]

Besittelsens karakter er uten betydning. Det betyr at passord kan være nedskrevet for hånd, ligge lagret på et brukerområde på en datamaskin eller en skytjeneste som vedkommende har tilgang til. Besittelseskravet rammer også de tilfeller som har oppstått uforsettlig, men hvor

[67] Ot.prp. nr. 40 (2004-2005) s. 33
[68] Schjølberg. (2017) s. 70
[69] Schjølberg. (2017). s. 55

besitteren unnlater å slette passordet eller tilgangskoden etter å ha blitt oppmerksom på besittelsen.

Det følger av ordlyden at selvspredende programmer er programmer som sprer seg selv til andre maskiner og systemer når programmet først aktiveres, og spredningen er ukontrollert og ubegrenset. Selvspredende dataprogrammer er programmer som kopierer seg selv og derved sprer seg selv videre til andre datamaskiner. Ved å spre seg selv til stadig nye datamaskiner, kan slike programmer oppnå en rask spredning til svært mange datamaskiner, og potensielt utrette skade på disse.[70] Skaden kan bestå i konkrete funksjoner som programmet er instruert til, for eksempel sletting av filer. Selv om programmet ikke er programmert til å utføre en bestemt skade, så er selve funksjonen med å kopiere seg selv til andre datamaskiner en skade i seg selv. Et eksempel på anvendelsen av e-post som spredningsmekanisme. Viruset befinner seg i et e-postvedlegg til en alminnelig e-post, som deretter sendes ut alle kjente e-postadresser. Når vedlegget deretter åpnes av mottakeren, vil virusprogrammet kjøres på den aktuelle maskinen, og derved spre seg.

7 Jurisdiksjon og straffelovens stedlige virkeområde

7.1 Prinsippet om staters suverenitet i cyberspace

Prinsippet om enkeltstaters suverenitet innenfor sitt eget territorium ble etablert siden freden i Westfalen etter trettiårskrigen i Europa i 1648. Prinsippet ble inntatt i Folkeforbudet, «The Covenant of the League of Nations», som ble ratifisert i 1919 av 42 stater, og deretter av FN i 1945 i «The Chapter of the United Nations Article 1 and 2»,[71] som bekreftet prinsippet om territorial integritet.[72]

Staters suverenitet innebærer tradisjonelt at en selvstendig stat ikke uten eget samtykke kan begrenses i sin alminnelige handlefrihet. Prinsippet om staters suverenitet gjelder også i cyberspace. Enkeltstatene har sin suverenitet i behold over alle cyberaktiviteter innenfor statens suverenitetsområde. Dette prinsippet får også anvendelse for Norge, og Norge har som andre stater rett til å regulere all aktivitet i den digitale infrastrukturen i cyberspace som er lokalisert på eller fra norsk territorium.

I de senere årene er det spesielt rapporten «The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations» som drøfter grunnleggende prinsipper i cyberspace, deriblant suverenitet, statlig ansvar, menneskerettigheter og lovgivning. Rapporten ble publisert av

[70] NOU 2007: 2 s. 28

[71] https://www.un.org/en/about-us/un-charter/full-text Hentet 10.04.23.

[72] Schjølberg. (2023) s. 182.

Cambridge University Press i februar 2017. Rapporten presenterer prinsippene om den nasjonale suvereniteten i cyberspace.

Høyesterett har i kjennelsen inntatt i HR-2019-610-A en referanse til «Tallinn Manual 2.0». Saken gjaldt tredjemannsransaking, og spørsmålet var om politiet fra dataterminaler i selskapets kontorlokaler i Oslo kunne laste ned elektronisk materiale selskapet hadde lagret i utlandet, eller om slik tvangsbruk falt utenfor norske myndigheters jurisdiksjon. Rettsavgjørelsen viser utfordringen med å straffeforfølge cyberkriminalitet, når det begås på tvers av landegrenser.

Førstvoterende viser til «Tallinn Manual 2.0» og presiserer at manualen er utarbeidet med deltakelse fra en rekke internasjonale eksperter etter invitasjon fra «The NATO Cooperative Cyber Defence Centre of Excellence». Under den forklarende teksten til «Rule 11 – Extraterritorial enforcement jurisdiction» fremheves at det kan være vanskelig å avgjøre jurisdiksjonsspørsmålet «in cyber context», se avsnitt 12. Førstvoterende forstår rapporten dithen at det ekspertene – i favør av å godta territorial jurisdiksjon – blant annet legger vekt på om det aktuelle materialet «is meant to be accesible from the State concerned», se avsnitt 13, og om tilgang til materialet kan oppnås ved å anvende statenes tvangsjurisdiksjon overfor rettssubjekter som befinner seg i utlandet, se avsnitt 16 og 17.[73]

7.2 Internasjonal forpliktelse

Cyberkriminalitet reiser spørsmål knyttet til jurisdiksjon. Det er særlig cyberkriminalitetens internasjonale og grenseløse karakter som får betydning både i forhold til spørsmålet om hvor en handling skal anses begått, og hvorvidt gjerningspersonen skal kunne straffeforfølges i Norge.[74]

Budapestkonvensjonen artikkel 22 regulerer jurisdiksjon, og det står at hver part skal «adopt such legislative and other measures as may be necessary to establish jurisdiction» med hensyn til enhver straffbar handling fastslått «in accordance with Articles 2 through 11». Videre er det opplistet en rekke bokstavalternativer, som regulerer det stedlige virkeområdet til straffebud som er nevnt i artikkel 2 til 11.

Artikkel 22 nr. 1 bokstav a forplikter statene til å gjennomføre territorialprinsippet, jf. ordlyden «in its territory». Territorialprinsippet innebærer at statene skal kunne straffeforfølge handlinger som begås på statens territorium. Et dataangrep anses begått innenfor statens territorium når gjerningspersonen og eksempelvis datasystem som objekt, befinner seg der. Det samme

[73] HR-2019-610-A avsnitt 56.

[74] NOU 2007: 2 s. 139.

gjelder når hele eller deler av datasystemet som rammes av dataangrepet befinner seg på territoriet, til tross for at gjerningspersonen selv ikke befinner seg der.[75]

I artikkel 22 nr. 1 bokstav b står det at statene også skal kunne straffeforfølge «on board a ship flying the flag of that Party». Ordlyden tilsier at statene også kunne straffeforfølge handlinger som begås på skip som seiler under statens flagg. Det samme gjelder for «on board an aircraft registered under the laws of that Party», jf. artikkel 22 nr. 1 bokstav c. Dette omfatter dermed handlinger som begås på luftfartøy som er registrert i henhold til statens lovgivning. Etter artikkel 22 nr. 1 bokstav d skal statene også kunne straffeforfølge «one of its nationals» i utlandet, «if the offence is punishable under criminal law where it was commited» eller hvis overtredelsen «is commited outside the territorial jurisdiction of any State». Med dette reguleres adgangen til å straffeforfølge egne statsborgere for handlinger som begås i utlandet, forutsatt at handlingen også var straffbar i landet hvor den ble begått, eller dersom handlingen ikke ble begått innenfor territoriet til en stat.[76] Dermed kan eksempelvis dataangrep som begås av nordmenn i utlandet, straffeforfølges dersom det samme dataangrepet er straffbart i det landet hvor angrepet begås.

Videre påpekes det at artikkel 22 ikke forhindrer statene fra å etablere en mer vidtrekkende jurisdiksjon enn det som fremgår av konvensjonen, jf. artikkel 22 nr. 4. Vi kan trygt si at cyberkriminalitet kjenner ingen landegrenser, og utvikler seg raskt. Kriminelle, ofre og teknisk infrastruktur spenner over flere jurisdiksjoner, noe som gir mange utfordringer når det gjelder etterforskning og rettsforfølgelse. Det avgjørende i noen tilfeller kan være samarbeidet mellom flere stater. Dersom en handling etter omstendighetene dekkes av flere staters jurisdiksjon, skal statene så langt det er hensiktsmessig konsultere hverandre om hvor handlingen skal straffforfølges, jf. artikkel 22 nr. 5.

7.3 Straffelovens stedlige virkeområde

7.3.1 Problemstilling

Bestemmelsene i straffeloven av 2005 §§ 4-7 regulerer straffelovgivningens stedlige virkeområde. Hovedproblemstillingen i denne delen av masteravhandlingen er *hvor* dataangrepet må være foretatt for at det skal rammes av norsk jurisdiksjon, og kunne straffeforfølges ved norske domstoler.

[75] Explanatory report of the Convention on Cybercrime av 8. november 2001 punkt 233.
[76] NOU 2007: 2 s. 139.

Tilfellene som behandles i denne oppgaven er tjenestenektangrep:

- utført av en gjerningsperson i Norge, med virkning i Norge.
- utført i Norge, med virkning i utlandet.
- utført av en gjerningsperson fra utlandet, med virkning i Norge.

Problemstillingene har nær tilknytning til folkerettens regler med suverenitetsprinsippet, og hensynet til suverenitet tilsier at det bør utvises varsomhet med å strafforfølge i Norge for handlinger som begås på andre lands territorium.

7.3.2 Tjenestenektangrep utført av en gjerningsperson i Norge - virkning i Norge

Dersom det utføres et DDoS-angrep av en gjerningsperson som befinner seg på norsk territorium eller om bord på norsk skip eller luftfartøy, og angrepets mål er i Norge, er spørsmålet hvordan dette er strafferegulert.

Det at en stat kan regulere handlinger foretatt på territoriet, er selvsagt og følger av territorialprinsippet. Det gjelder landterritoriet, territorialfarvannet, luftrommet over land og sjø samt statens skip på de fri hav. Dette følger av straffeloven § 4 første ledd nr. 1; norsk straffelov får anvendelse på handlinger som er foretatt i riket, i samsvar med territorialprinsippet som statene er forpliktet til å gjennomføre etter Budapestkonvensjonen artikkel 22 nr. 1 bokstav a. Straffeloven er også gitt anvendelse på begrensende områder som norske skip og luftfartøy som befinner seg utenfor territorialgrensen, jf. alternativene opplistet i § 4 annet ledd.

En handling anses å være begått innenfor statens territorium når gjerningspersonen og objektet for den straffbare handlingen, eksempelvis datasystemet som angripes, befinner seg der. Det samme gjelder når hele eller deler av det datasystemet som berøres av den straffbare handlingen er plassert i territoriet selv om gjerningspersonen selv ikke befinner seg der, jf. den forklarende rapporten Budapestkonvensjonen artikkel 22.[77] Denne regelen baserer seg på territorialprinsippet; hver stat er forpliktet til å straffeforfølge kriminalitet som er etablert gjennom konvensjon og som begås på ens eget territorium. Dette skal kunne gjennomføres selv om gjerningspersonen ikke befinner seg på ens eget territorium.

Territorialprinsippet medfører at alle dataangrep foretatt i Norge, skal kunne straffeforfølges etter straffeloven. Straffeloven får dermed anvendelse, og tjenestenektangrepet kan straffeforfølges ved norske domstoler. Straffeforfølgning av cyberkriminalitet i territorialstaten er rimelig og hensiktsmessig. En utlending må forventes å gjøre seg kjent med stedets normer, og nærheten til datasystemer, vitner og øvrige bevis gir størst garanti for en effektiv straffeforfølgning.[78]

---

[77] Explanatory report of the Convention on Cybercrime av 8. november 2001 punkt 233

[78] Baumann, Stigen. (2018). s. 211.

Når det gjelder tjenestenektangrep, er det mulig å bestille et angrep til et fremtidig tidspunkt. På tidspunktet når angrepet gjennomføres, er det mulig at gjerningspersonen bak tjenestenektangrepet forlater Norge etter å ha bestilt angrepet, og ikke befinner seg i Norge når angrepet finner sted. Virkningen av angrepet inntreffer imidlertid i Norge. De fleste straffebestemmelser er stedsnøytrale, og behandler ikke denne problemstillingen nærmere. Problemstillingen må derfor vurderes etter straffelovens kapittel 1. Enkelte teknologinøytrale straffebud kan overtres på internett ved bruk av ytringer. Overtredelsen anses foretatt i Norge såfremt lovbryteren var i Norge da ytringen ble fremsatt.[79] Anvendt på vårt tilfelle; et tjenestenektangrep anses som foretatt i Norge såfremt lovbryteren var i Norge da tjenestenektangrepet ble bestilt. Dette gjelder selv om gjerningspersonen har beveget seg til utlandet når tjenestenektangrepet materialiserer seg, så lenge alt som var nødvendig for gjennomføringen av angrepet, ble foretatt fra Norge. Dermed vil handlingen bli vurdert som foretatt i Norge, jf. § 4.

7.3.3 Tjenestenektangrep utført i Norge – virkning i utlandet.

Trusselbildet i cyberspace blir stadig mer komplekst, og omfanget av kriminaliteten er stort. Av politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer, fremgår det at vi i tiden fremover vil se organiserte cyberkriminelle som opererer fra Norge, med fornærmede i både inn- og utland.

Fra foregående behandling i punkt 6.4.2, stiller det seg annerledes for dataangrep utført av en gjerningsperson i Norge med virkning i utlandet. Spørsmålet er om dataangrepet er «foretatt i Norge» når gjerningspersonen på gjerningstidspunktet er i Norge, men virkningene av dataangrepet inntreffer i utlandet, jf. § 4.

Det presiseres at spørsmålet ikke er løst av straffeloven § 7, som bare tillegger virkningen betydning som tilknytningspunkt til Norge når gjerningspersonen befinner seg i utlandet. Spørsmålet må besvares etter en tolkning av straffeloven § 4. Et dataangrep kan ha blitt forberedt og gjennomført i Norge, og da anses som forberedelsesfasene som foretatt i landet. Men når angrepet videre er gjennomført i Norge, må det vurderes som «foretatt» i Norge.

Det foreligger rettspraksis på et lignende tilfelle. Kjennelsen inntatt i Rt. 2004 s. 1619 gjaldt datakriminalitet hovedsakelig med virkning for datamaskiner som befant seg i utlandet, og reiste spørsmål om straffelovens stedlige virkeområde. Spørsmålet var om de straffbare handlingene som var utført fra Norge via internett, med virkning på datamaskiner i utlandet, var begått utenfor Norge. Saken gjaldt et tilfelle hvor gjerningspersonen «rootet» (trengte inn i som systembruker) på en maskin plassert i Finland. Deretter opprettet gjerningspersonen brukernavn

[79] Sunde s. 51

og passord til en tredjemann på maskinen, og var ved en rekke anledninger inne på maskinen og overførte filer til eller fra denne. Spørsmålet gjaldt datainnbrudd og ulovlig bruk, jf. strl. 1902 § 145 annet ledd og § 393, jf. § 12 første ledd nr. 1, nåværende §§ 204 og 343, jf. § 4. Forsvareren anførte at handlingene var foretatt i utlandet, siden beskyttelsesbruddene med passordene materialiserte seg på datasystemer i utlandet, og den ulovlige bruken gjaldt datasystemer som var å finne i Finland. Høyesterett la til grunn det samme som lagmannsretten; at dette var et tilfelle hvor de fysiske handlingene var utført i Norge. Det sentrale var at alle de nødvendige handlingene for å utføre den ulovlige bruken var foretatt i Norge. Dersom disse handlingene ikke hadde vært foretatt, hadde heller ikke virkningen i form av beskyttelsesbrudd og ulovlig bruk ha inntruffet på datasystemene i utlandet inntruffet. Med andre ord var handlingene i Norge avgjørende for virkningen som inntrådte i utlandet. Dermed kunne handlingene straffeforfølges etter norsk straffelov.

Dersom et tjenestenektangrep er bestilt gjennom en utenlandsk nettside med et utenlandsk toppnivådomene, kan dette reise spørsmål rundt hvorvidt angrepet er foretatt i Norge. Men selv om det er anvendt utenlandske domenenavn og tjenester er det tilstrekkelig med gjerningspersonens tilstedeværelse i Norge for å anse handlingen som foretatt i Norge, jf. § 4.

7.3.4 Tjenestenektangrep utført fra utlandet – virkning i Norge.

Spørsmålet videre er hvordan norsk straffelovgivning forholder seg til tjenestenektangrep foretatt i utlandet, men som får virkning i Norge. Norge er et attraktivt mål for kriminelle i utlandet, og gjerningspersoner som har rammet norske virksomheter har vært lokalisert i utlandet.

Det fremgår av straffeloven § 5 at denne bestemmelsen kommer til anvendelse utenfor virkeområdet til § 4 for en rekke opplistede alternativer. Bestemmelsen regulerer i hvilken utstrekning norsk straffelovning får anvendelse for handlinger foretatt utenfor norsk territorium eller andre områder og objekter som nevnt i § 4 annet ledd. Videre suppleres bestemmelsen av § 6, hvor lovgiver har gitt folkerettslige regler direkte anvendelse i norsk rett. Det understrekes imidlertid at dette utgjør et sekundært rettsgrunnlag, som er relevant overfor handlinger som ikke reguleres av §§ 4 eller 5. Avhandlingen avgrenses mot anvendelsen av §§ 5 og 6.

En profesjonalisering av cyberkriminalitet og tilknytning til utlandet er – med komplekse strukturer og samarbeid på tvers av landegrenser – likhetstrekk som går igjen i flere av kriminalitetstruslene i årets politiets trusselvurdering.[80] Alle former for cyberkriminelle verktøy og tjenester kan kjøpes på det åpne eller det mørke nettet, og dette muliggjør at ikke bare etablerte kriminelle aktører kan utføre tjenestenektangrep, men også uerfarne og mindre sofistikerte aktører blir kapable til å utføre slike angrep. Eksempelvis kan man bestille et tjenestenektangrep

[80] Kripos (2023) s. 8.

som andre utfører, eller kjøpe tilgang til skadevare for å gjennomføre et slikt angrep selv.[81] Scenarioet som behandles er at det utføres et tjenestenektangrep mot datasystemer som befinner seg i Norge; hvorav virkningene av tjenestenektangrepet inntreffer i Norge. Tjenestenektangrepet er imidlertid planlagt og utført av sentrale bakmenn og aktører som befinner i utlandet.

Spørsmålet som behandles er om dataangrepet er «foretatt» i Norge når gjerningspersonen på gjerningstidspunktet er i utlandet, men virkningene av dataangrepet rammer et datasystem i Norge.

Det relevante rettslige grunnlaget for å besvare spørsmålet er straffeloven § 7. Bestemmelsen regulerer hvor en straffbar handling skal anses som foretatt, altså forbrytelsens lokalisering når forbrytelsen har skjedde flere steder. En avklaring av dette spørsmålet er en forutsetning for å fastslå hvilken av reglene om straffelovgivningens geografiske rekkevidde som kommer til anvendelse. Rent lovteknisk og for systematikkens del burde § 7 vært plassert før §§ 4-6.

For at en handling foretatt i utlandet skal anses for å ha gjerningssted også i Norge, må to hovedvilkår være oppfylt: (1) straffbarheten har virkninger som «avhenger eller påvirkes av en inntrådt eller tilsiktet virkning» og (2) at virkningen enten har inntrådt på territoriet, eller at det var innenfor gjerningspersonens forsett at virkningen skule inntre på norsk territorium.

Lovens åpning for flere lokasjoner øker mulighetene betydelig for at en handling også blir regnet for å være foretatt på norsk territorium, i likhet med § 4.

Etter en naturlig språklig forståelse av «avhenger eller påvirkes av en inntrådt eller tilsiktet virkning», er det enklest å tenke at dette rammer fare- eller skadedelikter hvor utførelsen av den straffbare handlingen og resultatet av den ikke er sammenfallende i tid eller sted. Dette har likhetstrekk med et tjenestenektangrep som utføres fra utlandet mot et mål i Norge. For denne typen cyberkriminalitet er det naturlig at resultatet materialiserer seg et annet sted enn på datamaskinen som benyttes til å gjennomføre angrepet. En slik situasjon hvor aktivitet foregår på tvers av landegrenser, er normalt i cyberspace. Dette utfordrer premisset om fysisk nærhet mellom handling og konsekvens, som er underliggende for mange straffebestemmelser.

Når gjerningspersonen er i utlandet på gjerningstidspunktet, omfattes tjenestenektangrepet av norsk straffelovgivning såfremt virkningen av angrepet inntrådte eller var tilsiktet å inntre i Norge. Virkningen må være slik at straffbarheten «avhenger eller påvirkes» av den. Med dette menes at virkningen må være relevant i forhold til fullbyrdelsen. Dermed får ikke bestemmelsen anvendelse på en handling som er fullbyrdet og avsluttet i utlandet.

[81] Kripos (2023) s. 13

Det bemerkes i tredje delproposisjon til straffeloven at § 7 «ikke [er] knyttet til noen bestemt kategori straffebud». Videre i proposisjonen står det at bestemmelsen «må kunne anvendes når den inntrådte eller tilsiktede virkning knytter seg til en handling foretatt i et annet land».[82] Dette tyder på at vurderingstemaet er rent pragmatisk; spørsmålet gjelder kun om handlingen slik den artet seg, hadde en virkning i Norge relevant for fullbyrdelsen, eller om en slik virkning var tilsiktet.[83] Et tjenestenektangrep som rammer et datasystem på norsk territorium, omfattes følgelig av straffeloven, jf. § 7, jf. § 4 fordi den strafferettslige skaden faktisk inntrådte i Norge. Dersom tjenestenektangrepet ikke lykkes, anses dette som et forsøk, hvor virkningen av tjenestenektangrepet er tilsiktet fremkalt i Norge, jf. § 7.

Etter bestemmelsen regnes handlingen som foretatt der virkningen «er tilsiktet fremkalt». Nettverksbaserte handlinger kan ramme tilfeldig, og dette reiser spørsmålet om hvorvidt virkningen er «tilsiktet» å inntre i Norge, jf. § 7. Spørsmålet er relevant for generelle tjenestenektangrep utført mot flere datasystemer. Det tenkes at datasystemet gjerningspersonen i utgangspunktet skulle angripe befant seg i utlandet. Imidlertid klarer gjerningspersonen å angripe et datasystem i Norge uten at dette var planlagt eller tiltenkt. Forsettet omfatter det å begå den straffbare handlingen med et tjenestenektangrep, for eksempel å hindre tilgang til eller utførelse av en tjeneste. Gjerningspersonen er likegyldig til om datasystemet som rammes er norsk eller ikke-norsk. Hensikten med § 7 er å kunne drive straffeforfølgning når et tjenestenektangrep rammer et norsk mål. Hensynet gjør seg også gjeldende for tilfeldige krenkelser. I teorien er det lagt til grunn at «likestilt med tilsiktet er at virkningen faktisk har inntrådt».[84] Det gjelder således ikke noe krav om «stedsfortsett» når et norsk datasystem faktisk blir rammet. Løsningen bør være den samme ved straffbart forsøk etter ordlyden «tilsiktet». Noe annet ville innebære en ugunstig begrensning i rekkevidden av norsk straffelovgivning, og føre til bevismessige utfordringer for det subjektive vilkåret i forsøkstilfeller. Det antas dermed at bestemmelsen ikke krever at forsettet omfatter det forhold at rettsgodet eller datasystemet befinner seg i Norge. Det betyr at virkningen er «tilsiktet» fremkalt i Norge, jf. § 7, når datasystemet som utsettes for tjenestenektangrepet, er i Norge, selv om lovbryteren ikke hadde noen tanke for datasystemets lokalisering.

8 Teknologinøytral regulering

8.1 Regulering og teknologinøytralitet

Lovverket utfordres av den teknologiske utviklingen, og henger som regel etter. Det rettslige grunnlaget for internasjonalt juridisk samarbeid har ikke blitt utarbeidet i henhold til den

[82] Ot.prp. nr. 22 (2008-2009) s. 27.

[83] Sunde. (2016) s. 54.

[84] Ajourført versjon av straffeloven, lovkommentar av Matningsdal 2016. Punkt 4 note 1 til § 7. Bekreftet à jour per 1. juli 2022.

teknologiske utviklingen. Det kan ta lang tid å få informasjon fra utenlandske samarbeidspartnere, og dette kan føre til at sakene blir foreldet. Utfordringer i regulering, herunder framleie og bruk av mellomtjenere og VPN kan utgjøre juridiske sårbarheter som kan utnyttes til cyberkriminalitet. Imidlertid har lov om elektronisk kommunikasjon (ekomloven) fått nye bestemmelser som trådte i kraft 1. januar 2022. De nye bestemmelsene omhandler ekomtilbyderes lagringsplikt og vilkår for deling med politiet. Bestemmelsene pålegger ekomtilbydere å lagre identifiserende opplysninger om en abonnent i tolv måneder, kontra tidligere sletteplikt etter 21 dager. Politiet kan dermed kreve å få informasjon utlevert ved etterforskning av lovbrudd med en strafferamme over tre år. Denne lovendringen gjør identifisering av brukere noe enklere, og medfører at mer cyberkriminalitet kan etterforskes.[85]

8.2 Prinsippet om teknologinøytralitet

Ordet prinsipp stammer fra det latinske ordet, *principium,* som betyr «opprinnelse» eller «første årsak».[86] Et prinsipp er en grunnsetning eller grunnregel som man ikke bør bryte, og fungerer dermed som en skranke for hva som er tillatt. I jussen eksisterer det flere forskjellige prinsipper, for eksempel kontradiksjonsprinsippet, skyldprinsippet og legalitetsprinsippet. Når betegnelsen «teknologinøytralitet» anvendes i avhandlingen, siktes det til prinsippet om teknologinøytralitet.

Teknologinøytralitet anses å være en løsning på en rekke forskjellige problemstillinger som har oppstått som følge av digitaliseringen av samfunnet. Til tross for at teknologinøytralitet blir brukt hyppig i rettslige sammenhenger, er det fremdeles uklart hva man mener med begrepet. Det er viktig å ha et klart meningsinnhold av hva teknologinøytralitet er, og hva som kjennetegner en teknologinøytral bestemmelse, for å kunne kategorisere forskjellige bestemmelser under dette prinsippet. Først når meningsinnholdet er klart, vil prinsippet ha en funksjon i lovgivningsarbeidet og ved rettsanvendelsen. Bevisstgjøringen om at teknologinøytralitet har forskjellig meningsinnhold i ulike sammenhenger, er særlig nødvendig fordi det vises til teknologinøytralitet både når det gis føringer for hvordan lovbestemmelser skal utformes og når det gis føringer om hvordan bestemmelser skal forstås.[87]

Ved utformingen av straffebudene har man søkt å tilrettelegge for en dynamisk begrepsutvikling, og – så langt som mulig – for teknologinøytralitet.[88] Det innebærer at straffebestemmelsene som helhet er fristilt fra datateknologi. Man kan si at bestemmelsene stiller seg nøytral til

---

[85] Kripos. (2023) s. 32.

[86] «Prinsipp», *Wikipedia*, 11. august 2021, https://no.wikipedia.org/w/index.php?title=Prinsipp&oldid=21716571#cite_note-1. Hentet 22.03.23.

[87] Institutt for offentlig rett. «Teknologinøytralitet», Universitetet i Oslo, 14. desember 2022, https://www.jus.uio.no/ior/forskning/phdprosjekter/julfredrik/index.html.

[88] Ot.prp. nr. 22 (2008-2009) s. 21-22

fremgangsmåte. Reguleringen er dermed i overensstemmelse med det internasjonale teoretikere har uttalt som et vanlig mål for lovgiver i møte med informasjons- og kommunikasjonsteknologi: at den rettslige løsningen skal være lik «online» og «offline».[89] Teknologinøytralitet betyr at teknologier er likestilt, og at regelverket ikke skal gi fordeler ved bruk av bestemte teknologier. Dette ble illustrert av Datakrimutvalget i 2007 hvor utvalget uttalte at straffebudet er «på samme vis som de øvrige bestemmelser i lovforslaget, innholds- og teknologinøytralt».[90] Man fryktet at med teknologirelaterte ord og uttrykk i lovgivningen, ville dette kunne bli rigid, og føre til at straffebestemmelsene raskt ble utdaterte på grunn av teknologiutviklingen. Det er viktig å ha i bakhodet at truslene i cyberspace er sammensatte, og verktøyene som rettes mot oss er i stadig utvikling. Teknologi anses å være en betydelig driver for nesten alle kriminalitetsutfordringer og trusler mot norske verdier.

Tolkingen må derfor støttes på den språklige kontekst og veiledning i forarbeidene. I tillegg må formålsbetraktninger, herunder vern av datasikkerheten, anses relevant. Det kan ha betydning når man står overfor nye handlemåter eller endrete teknologiforhold. Straffebudenes fleksibilitet med en teknologinøytral utforming skal nettopp fange opp dette.[91]

Straffeloven tilstreber teknologinøytralitet, og i rettshåndhevelsen må man gjennomgående huske at ord og uttrykk som ved første øyekast fremstår som teknologirelaterte, kan ha et videre meningsinnhold; omfatte mer enn teknologiske forhold.

I denne avhandlingen har jeg redegjort for de alminnelige bestemmelsene om cyberkriminalitet i straffelovens kapittel 21. Jeg skal anvende noen typetilfeller fra straffeloven for å se hvordan teknologinøytralitet fremkommer i strafferettslig sammenheng.

8.3 Uttrykk i straffelovgivningen

I denne delen av avhandlingen vil jeg først analysere teknologinøytralitet i sammenheng med bestemmelsen om uberettiget befatning med tilgangsdata, dataprogram mv., jf. § 201. For dette formålet vil jeg ta utgangspunkt i uttrykkene, «databasert informasjon», «datasystem» og «dataprogram eller annet». Uttrykkene vil behandles fortløpende.

Til tross for at en bestemmelse er utformet generelt og teknologinøytralt, kan teknologiutviklingen medføre at bestemmelser blir uegnede og utdaterte etter noe tid. Det er dermed utfordrende å utvikle et regelverk som fullt ut og på lengre sikt, ivaretar bredden og kompleksiteten i

[89] Kaltenborn (2019) s. 154, jf. C. Reed: «When dealing with cyberspace, lawmakers often claim to be guided by the principle that there should be equivalence of legal treatment between online and offline activities.»

[90] NOU 2007: 2 s. 153.

[91] Sunde. (2016) s. 40-41

problemstillingene som følger med cyberkriminalitet. Etablering av en ordning eller et organ som jevnlig sørger for å avstemme regelverk og praktiske rettssikkerhetsmekanismer mot teknologiutviklingen bør derfor vurderes.[92]

Gjerningsbeskrivelsen i denne bestemmelsen handler om å gi tilgang til «databasert informasjon» eller «datasystem». I NOU 2007: 2 sondret Datakrimutvalget i lovutkastet § 10 mellom «data» og «databasert informasjon». Departementet fant ikke grunn til å operere med en tilsvarende sondring. Bakgrunnen for sondringen var at «data» blant annet omfatter enhver representasjon av informasjon som ikke er lesbar uten bruk av teknisk hjelpemiddel. Med «databasert informasjon» mente utvalget meningsinnholdet i data. Departementet fant heretter ingen grunn til å foreta en sondring mellom disse, og lot «databasert informasjon» omfatte både det utvalget betegnet som «data» og det utvalget betegnet som «databasert informasjon». [93]

Ved å bruke uttrykket «databasert informasjon» for både data og meningsinnholdet i data, utelukkes en teknologibasert regulering, og en teknologinøytral regulering fremheves.

Videre anvendes uttrykket «datasystem». Uttrykket anses for å være teknologinøytralt, og kan anses som et annet typetilfelle.[94] Etter Datakrimutvalgets oppfatning var datasystem teknologinøytralt. Utvalget anvendte begrepet, «IKT-system», men refererer til de samme innretningene i senere drøftelser der uttrykket «datasystem» anvendes: «Straffebudene i lovforslagene baserer seg på prinsippet om teknologi- og innholdsnøytralitet. Spørsmål om hva slags type «IKT-system» det er tale om og hva slags innhold dataene har, er ikke relevante for reglenes anvendelsesområde. Straffebudene omfatter «IKT-systemer», uansett om teknologien gjelder tele-, IT- og media (herunder kringkasting). Det samme gjelder innholdet. Om innholdet består av tekst, lyd, bilde eller dataprogram, er uten betydning.»[95]

Siden uttrykket er brukt i flere strafferettslige bestemmelser, jf. blant annet §§ 201, 201, 206 behandles det samlet her.

«Datasystem» var et nøkkelord i Datakrimutvalgets arbeid med teknologinøytrale straffebestemmelser. Begrepet «datasystem» er opprinnelig en oversettelse av det engelske uttrykket «computer system», og valget av ordlyd var foranlediget av lovarbeid som følge av at Norge tiltrådte Budapestkonvensjonen.[96] Uttrykket «datasystem» kom først inn i lovgivningen ved

[92] Sunde. (2021). s. 7.

[93] Ot.prp. nr. 22 (2008-2009)

[94] Eksempelvis karakteristikken av uttrykket «datasystem» i Prop. 106 L (2016-2017) s. 10.

[95] NOU 2007: 2 s. 59.

[96] Kaltenborn. (2019) s. 162, jf. NOU 2003: 27 s. 10. Uttrykket «datasystem» inngikk ikke i ordlyden i datainnbruddsbestemmelsen den gang.

innføringen av dagens straffelov. Frem til innføringen av begrepet har straffebudene mot datakriminalitet, vært utformet på forskjellige måter. En fellesnevner for bestemmelsene har vært at de på ulike vis har vært teknologinøytrale.

Etter en alminnelig språklig forståelse vil «datasystem» omfatte enhver innretning, bestående av maskinvare og data, som foretar behandling av data ved hjelp av dataprogrammer. Ordlyden er ikke tilsiktet en bestemt teknologiløsning, og teknologivalget er ikke avgjørende for hvorvidt noe en innretning utgjør et datasystem. Det intuitive etter ordlyds- og forarbeidstolkning vil være å anse personlige datamaskiner, nettbrett og mobiltelefoner som eksempler på datasystemer. Forarbeidene nevner dessuten datamaskiner som tilhører eller står i en bedrift, i den offentlige forvaltning, på internett, personal digital assistent (PDA), rutere, basestasjoner, kringkastingssendere osv.[97] En elementær forskjell fra forarbeidene til i dag, er at det har skjedd store fremskritt innenfor teknologien, og dette har gitt opphav til flere tekniske løsninger som vil omfattes av ordlyden.

Etter § 201 bokstav b første punktum er objektet «dataprogram eller annet». Etter en naturlig språklig forståelse innebærer dataprogram en serie instruksjoner som forteller datamaskinen hva den skal gjøre. Imidlertid er ordlyden vid, jf. «eller annet», og omfatter enhver logisk eller fysisk innretning som er egnet til å begå straffbare handlinger mot databasert informasjon eller datasystem. Gjennom en vid og åpen ordlyd i lovgivningen, kan det foretas en dynamisk rettshåndhevelse, siden man kan regulere flere problemstillinger som man på lovgivningstidspunktet ikke hadde tenkt på. Årsaken til dette kan være at utredningen var mangelfull eller at den den teknologiske utviklingen bringer med seg nye løsninger som ikke er lovregulert.

Det norske rettslige rammeverket for cyberkriminalitet er utformet for å være teknologinøytralt. Slik vi ser av noen utvalgte termer fra lovteksten og av sentrale lovbestemmer, er lovgivningen formulert slik at den kan håndheves uavhengig av hvilken teknologi som anvendes i et lovbrudd. Dette gir rettssystemet fleksibilitet til å håndtere nye og fremvoksende former for cyberkriminalitet.

9 Forventet utvikling fremover

Denne delen av avhandlingen omhandler det redegjorte situasjonsbildet, og hvordan man vurderer at cyberkriminalitetens utvikling blir fremover. Jeg vil først behandle Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT, for deretter å behandle Riksadvokatens mål og prioriteringer for straffesaksbehandlingen i 2023.

[97] NOU 2007: 2 s. 61.

9.1 Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT

Straffesaksbehandlingen skal bidra til redusert kriminalitet ved at straffbare forhold avdekkes og oppklares slik at skyldige effektivt kan straffeforfølges og ilegges adekvat reaksjon.[98] Riksrevisjonen har utarbeidet en undersøkelse om politiets innsats mot kriminalitet ved bruk av IKT i Dokument 3:5 (2020-2021), som ble oversendt Stortinget 2. februar 2021. Målet med undersøkelsen har vært å vurdere om politi- og påtalemyndigheten har oversikt over, etterforsker og oppklarer IKT-kriminalitet. Undersøkelsen baserer seg på tre kriminalitetsområder, og disse er: Internettrelaterte seksuelle overgrep, økonomisk IKT-kriminalitet (bedragerier og identitetskrenkelser) og ren IKT-kriminalitet (datainnbrudd og uberettiget befatning med tilgangsdata).[99]

Det avgjørende er at politiet har tilstrekkelige forutsetninger for å bekjempe cyberkriminalitet. Senest i årsrapporten for 2019 skriver Politidirektoratet at politiet mangler kompetanse til å møte utfordringene i cyberspace. Den pågående digitaliseringen utfordrer dermed politiets kompetanse, og utfordringene gjelder kompetanse på alle nivåer i politiet: basiskompetanse, spesialistkompetanse og påtalekompetanse.[100] Riksadvokaten har siden 2005 vært opptatt av at ren IKT-kriminalitet skal prioriteres, men dette ender opp med å bli nedprioritert.

Manglende kompetanse i politiets førstelinje medfører eksempelvis at tjenestenektangrep håndteres feil i den viktige initiale fasen. Elektroniske spor av angrepet sikres ikke riktig, og medfører igjen at det ikke iverksettes riktige etterforskningsskritt. Mye av kriminaliteten i cyberspace anses å være teknologikrevende, og det avgjørende er spesialistkompetanse, da dette vil kunne bekjempe utviklingen i cyberkriminaliteten. Dersom den digitale kompetansen styrkes i alle nivåer i politiet, vil dette kunne gi høyere oppklaringsprosent av cyberkriminalitet.

Videre bemerkes det at utfordringene i det internasjonale politisamarbeidet bidrar til at kriminelle unnslipper rettsforfølgning.

9.2 Riksadvokatens mål og prioriteringer for straffesaksbehandlingen i 2023

Tidligere har gjerningspersoner som har rammet norske virksomheter vært lokalisert i utlandet. Sannsynligvis vil vi i fremtiden registrere at organiserte cyberkriminelle opererer fra Norge, med fornærmede i både inn- og utland. Cyberkriminelle anvender ny teknologi raskt, og er også raske til å utnytte sårbarhetene de oppdager. Dermed finner cyberkriminelle stadig nye måter å

[98] Riksadvokaten. (2019). *Mål og prioriteringer for straffesaksbehandlingen i 2019 . politiet- og statsadvokatene*, rundskriv 1/19.

[99] Dokument 3:5 (2020-2021) s. 4

[100] Dokument 3:5 (2020-2021) s. 5

angripe på, og som ikke nødvendig ligner på forrige angrepstype. Siden ekomloven har fått nye bestemmer om lagring av IP-adresser, vil en slik endring mest sannsynlig føre til at flere gjerningspersoner vil benytte anonymiseringsteknologier som VPN. Kripos vurderer at det er sannsynlig at anonymiseringsmulighetene vil øke i tiden fremover med den teknologiske utviklingen.

De generelle målene for straffesaksbehandlingen er høy kvalitet, høy oppklaringsprosent, kort saksbehandlingstid og adekvat reaksjon. Riksadvokaten har det overordnede ansvaret for straffesaksbehandlingen, herunder ansvaret for å fastsette generelle mål og prioriteringer. Dette gjøres i et årlig rundskriv, hvor rundskrivet angir hvilke saker som skal gis forrang ved ressursknapphet, og omtaler dermed riksadvokatens sentrale styringssignaler.[101] I årets rundskriv er IKT-kriminalitet viet særlig oppmerksomhet.

Av rundskrivet fremgår det blant annet at politiets innsats når det gjelder kriminelle handlinger ved bruk av IKT må intensiveres. Det er vesentlig at påtalemyndigheten sørger for at det raskt og effektivt iverksetter etterforskning og sporsikring. Det må foretas en prioritering av informasjonsinnhenting og -deling til relevante internasjonale og nasjonale samarbeidspartnere, herunder Kripos, Økokrim og næringslivet, med formål om å avdekke, avverge eller stanse straffbare handlinger.[102] Ved et sammensatt trusselbilde, eller der sentrale samfunnsinstitusjoner blir utsatt for dataangrep, må det også iverksettes samarbeid med PST.[103] Internasjonalt rettslig samarbeid står også sentralt ved bekjempelse av denne type kriminalitet.

9.3 En FN-konvensjon for cyberspace

Det foreslås av flere aktører å iverksette samarbeid og dialoger om standarder og normer for handlinger og kommunikasjon i cyberspace innenfor rammen av FN-organisasjoner. Regionale og bilaterale samarbeid og avtaler vurderes ikke å være tilstrekkelig for en global cybersikkerhet og vern mot cyberangrep. Det bør derfor gjennomføres nye former for internasjonale lovtiltak på FN-nivå, for å kunne forebygge og bekjempe cyberkriminalitet. Spørsmålet er hvorfor en slik konvensjon er viktig.

Formålet med en ny internasjonal konvensjon bør være å dekke behovet for et effektivt internasjonalt samarbeid i forebygging og etterforskning av globale cyberangrep og annen cyberkriminalitet. Internasjonal koordinering og samarbeid er nødvendig for å kunne straffeforfølge cyberkriminelle handlinger. Et internasjonalt politisamarbeid medførte nylig i januar 2023 til at FBI i samarbeid med Europol og politi fra en rekke land – deriblant Norge – fikk stanset

[101] Riksadvokatens rundskriv 1/23

[102] Riksadvokatens rundskriv 1/23

[103] Riksadvokatens rundskriv nr. 4/2007

hackergruppen, «Hive». Siden juni 2021 hadde Hive angrepet mer enn 1500 ofre i over 80 land og mottatt over 100 millioner dollar fra utpressing. Ved hjelp av et internasjonalt samarbeid, fikk man kartlagt store deler av nettverket til Hive, og lagt ned infrastrukturen til slutt.[104] Det er derfor viktig at man raskt kan innlede et internasjonalt samarbeid i saker hvor handlingene foregår i flere land.

Formålet med en FN-konvensjon bør være å harmonisere landenes straffelovgivning om cyberkriminalitet. Den teknologiske utviklingen med cyberangrep mot enkeltlandenes kritiske infrastruktur viser nødvendigheten av å etablere standarder for straffebestemmelser i internasjonale regelverk. Konvensjonen må verne om fundamentale rettigheter innen personvern og menneskerettigheter og være i overensstemmelse med forpliktelsene i internasjonale lovverk om menneskerettigheter.[105]

Etter prinsippet om staters suverenitet kan ingen stat kreve suverenitet over cyberspace. «The Tallinn Manual 2.0» foretar en vurdering av viktige sider ved anvendelse av internasjonal lovgivning i cyberspace. Prinsippet om staters suverenitet bør få anvendelse blant annet på tilgang til data i henhold til nasjonale lovbestemmelser. I forlengelsen av dette må nasjonale stater kunne vedta tiltak som vurderes som nødvendig eller hensiktsmessige for cyberaktiviteter innenfor sitt nasjonale territorium, som også innebærer kabler for kommunikasjon av data til et annet lands territorium.[106]

Europarådet viser til at over 130 land har de siste ti årene revidert lovgivningen sin for å ta større høyde for cyberkriminalitet. Dette utgjør en økning på 100 % de siste ti årene. Utviklingen synliggjør behovet for en internasjonal avtale som kan supplere Budapestkonvensjonen. I 2019 vedtok FN en resolusjon hvor det ble bestemt at en slik avtale skal forhandles frem.[107] Arbeidet ble påbegynt i 2021 og er planlagt ferdigstilt i 2023. Vedtakelsen er planlagt i FNs generalforsmaling i februar 2024.

I motsetning til Budapestkonvensjonen blir dette den første globale konvensjonen om samarbeid og bekjempelse av cyberkriminalitet som tar sikte på å bli ratifisert av alle FNs 193 medlemsland. Utover det vil en ny konvensjon være et passende verktøy sett i forhold til utviklingen i cyberspace. Det kan bidra til å etablere en felles internasjonal standard for å håndtere cyberkriminalitet og sikre at statene samarbeider for å bekjempe kriminaliteten. Alt i alt vil dette

[104] Oslo politidistrikt. (2023).
[105] Schjølberg. (2023) s. 207
[106] Schjølberg. (2023) s. 207.
[107] Resolusjon A/RES/74/247 (2019).

kunne gi bedre beskyttelse til ofrene for cyberkriminalitet, da dagens moderne cyberlandskap har blitt endret gjennom de siste årene.

En slik konvensjon kan definere hvordan cyberkriminalitet skal forstås, og med dette sikre at landene på tvers av grenser, opererer med de samme definisjonene og meningsinnholdet i disse. Dette vil sikre en mer likartet praksis uansett hvor cyberkriminaliteten foregår. Imidlertid har det vært vanskelig å komme frem til en enighet om definisjonen av begrepet «cybercrime», og dette illustrerer en sprikende forståelse av grunnleggende termer i cyberspace. Utfallet av konvensjonen bør derfor være et viktig arbeidsverktøy som er enkelt å anvende og forstå for rettsanvenderne. Det antas at FN-konvensjonens endelige resultat vil være tilpasset Budapestkonvensjonen, uten at disse fungerer som konkurrenter. Budapestkonvensjonen vil innehva et mer operativt etterforsknings- og samarbeidsverktøy, med sine tilleggsprotokoller som er tilpasset moderne utfordringer.[108]

Det er vesentlig at cyberkriminalitetskonvensjonen kun regulerer «cyber dependent crimes», altså cyber-avhengige lovbrudd, og avgrenses mot «cyber enabled crimes», altså lovbrudd hvor digitale flater brukes som et verktøy for å gjennomføre den straffbare handlingen. Bakgrunnen for dette er at sistnevnte alternativ i utgangspunktet er tradisjonell kriminalitet, hvor det allerede eksisterer lovgivning. Dersom slik kriminalitet inkluderes i konvensjonen kan den raskt bli omfattende, og skape nye utfordringer knyttet til menneskerettigheter.

10 Avslutning

I Norge har vi fra 2019 til 2021 sett en tredobling i alvorlige cyberoperasjoner mot norske myndigheter og virksomheter. Antallet alvorlige og svært alvorlige hendelser har i 2022 vært på et tilsvarende nivå som i 2021.[109]

Norge er et av verdens mest digitaliserte land og står overfor store utfordringer i behovet for vern mot cyberkriminalitet. Det må derfor iverksettes tiltak for å kunne forebygge og verne landet mot cyberkriminalitet, derav tjenestenektangrep. De forebyggende tiltakene som i dag kan være vesentlige mot internasjonale cyberangrep og annen alvorlig cyberkriminalitet som opererer helt uavhengig av nasjonale landegrenser, kan deles inn i tre hovedområder. Det er for det første nødvendig å tilføre politi- og påtalemyndighet og institusjoner for cybersikkerhet kunnskap om utviklingen innen cyberkriminalitet. For det andre er det nødvendig å oppdatere eller innføre særskilte straffebestemmelser i de situasjonene hvor straffelovgivningen ikke gir et tilstrekkelig vern mot cyberkriminalitet. For det tredje er det nødvendig å utvikle

[108] Møller. (2023)

[109] Nasjonal sikkerhetsmyndighet. (2022) s. 9.

hensiktsmessige internasjonale cybersikkerhetstiltak for styring og kontroll av lagring og kommunikasjon av data og informasjon både nasjonalt og internasjonalt.[110]

Tjenestenektangrep skjer hele tiden, og er blitt et internasjonalt problem. Det at stadig flere aktører blir utsatt for tjenenestenektangrep viser skadepotensialet i denne slags cyberkriminalitet. De aller fleste tjenestenektangrep i Norge blir avverget av automatiserte sikkerhetsløsninger. Etter et tjenestenektangrep vil de aller fleste tjenere, tjenester og nettverk fungere som vanlig, uten at det må iverksettes noen ytterligere tiltak. Imidlertid varierer kompleksiteten på tjenestenektangrepene, og hvilke skadefølger angrepet medfører. Siden skadefølgene varierer, påvirker dette igjen håndhevingen av angrepet.

Det finnes flere tiltak man kan iverksette for å forhindre tjenestenektangrep. En måte er å øke kapasiteten på serveren eller nettverket, slik at det er i stand til å håndtere større mengder trafikk. Videre kan det være lurt å implementere et system som kan gjenkjenne og blokkere trafikk fra kjente tjenestenektangrep-tilkoblinger. I tillegg bør man sørge for å ha oppdatert programvare og sikkerhetsoppdateringer på serveren og nettverket for å redusere risikoen for sårbarheter. Og i tilfelle man rammes av et tjenestenektangrep, er det viktig å ha en beredskapsplan på plass, slik at man kan håndtere situasjonen så raskt og effektivt som mulig.

Dersom man ikke får sporet opp angriperen gjennom IP-adresse, kan det være vanskelig å identifisere og straffe gjerningspersonene bak et tjenestenektangrep. I slike tilfeller er det nødvendig å øke sikkerheten på serveren eller nettverket for å redusere risikoen for flere angrep i fremtiden. Det kan være lurt å etablere kontakt med en IT-sikkerhetsekspert eller en spesialist på tjenestenektangrep for å få hjelp til å identifisere og håndtere situasjonen. Dersom angrepet medfører økonomiske tap eller andre skader, kan det være mulig å gå rettslige skritt for å kreve erstatning.

Politiet kan ikke stoppe kriminalitet de ikke har kunnskap om at foregår. Dersom man opplever et cyberangrep som involverer kriminell aktivitet, eksempelvis hacking, nettsvindel eller utpressing, bør slike forhold anmeldes til politiet. Derfor må datakriminalitet, inkludert tjenestenektangrep rapporteres inn til politiet. Dette gjelder til tross for at man ikke har tapt penger eller data. Informasjonen gjennom denne rapportereringen bidrar i politiets etterforskning, og hindrer de kriminelle og reduserer skadevirkningene av kriminaliteten. Rapporteringen bidrar også til analyser av trender og informasjonskampanjer for å beskytte befolkningen og virksomhetene.[111] Hvis man derimot opplever et cyberangrep som kan true nasjonal sikkerhet, som for eksempel et angrep på kritiske infrastrukturer eller offentlige institusjoner, bør dette rapporteres til NSM. I tilfeller der man er usikker på hvem man skal rapportere til, kan man kontakte begge

[110] Schjølberg. (2023) s. 182.

[111] Oslo politidistrikt og Nasjonalt cyberkrimsenter. (2022). s. 1.

instansene for råd og veiledning. Det er imidlertid nødvendig å rapportere angrepet til relevante myndigheter eller organisasjoner, slik at de kan være oppmerksomme på situasjonen og bidra til å forebygge lignende angrep i fremtiden.

Litteraturliste

Litteratur

Cloudfare — Cloudflare. «What Is a Distributed Denial-of-Service (DDoS) Attack?» https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/. Hentet 13. mars 2023.

Curryer (2023) — Curryer, Emily. «IoT in 2023 and Beyond». TechInformed, 16. mars 2023. https://techinformed.com/iot-in-2023-and-beyond/.

Europarådet (2023) — Council of Europe. «Chart of Signatures and Ratifications of Treaty 185». https://www.coe.int/en/web/conventions/full-list. Hentet 4. februar 2023.

Europarådet (2001) — Concil of Europe. «Explanatory Report to the Convention on Cybercrime». 23. November 2001. https://rm.coe.int/16800cce5b. Hentet 6. februar 2023.

FNs folkerettskommisjon (1966) — FNs folkerettskommisjon. *Draft Articles on the Law of Treaties – with Commentaries*. 1966. Kommentar til Artikkel 27-28 s. 219 (avsnitt 8). https://legal.un.org/ilc/texts/instruments/english/commentaries/1_1_1966.pdf. Hentet 28. februar 2023.

E24 (2023) — «Dataangrep: Nettsidene til SSB og NSM er nede», 14. mars 2023. https://e24.no/i/RG4Qz5.

Gröning, Jacobsen og Husabø (2015) — Gröning, Linda, Jørn Jacobsen, and Erling Johannes Husabø. *Frihet, Forbrytelse Og Straff: En Systematisk Fremstilling Av Norsk Strafferett*. Bergen: Fagbokforl., 2015.

Haugen og Efjestad (2019) — Haugen, Finn, Jon Sverdrup Efjestad. *Strafferett – håndbok.* 5. Utg., Oslo: Cappelen Damm Akademisk, 2019.

Kaltenborn (2019) — Kaltenborn, Jul Fredrik. «Teknologinøytralitet og datakriminalitet – særlig om klassifiseringen av begrepet datasystem». Tidsskrift for strafferett 19, nr. 2 (28. juni 2019): 148–67. https://doi.org/10.18261/issn.0809-9537-2019-02-03.

Kripos (2023) — Kripos. «Politiets trusselvurdering 2023», 2023. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/politiets-trusselvurdering-ptv/politiets-trusselvurdering-2023.pdf

Matningsdal (2017) — Matningsdal, Magnus. *Straffeloven: Lov 20. Mai 2005 Nr. 28 Om Straff: De Straffbare Handlingene, Kapittel 17-31: Kommentarutgave.* Oslo: Universitetsforl., 2017.

Matningsdal (2015) — Matningsdal, Magnus. *Straffeloven: Lov 20. Mai 2005 Nr. 28 Om Straff: Alminnelige Bestemmelser: Kommentarutgave.* Oslo: Universitetsforl., 2015.

Müller (2017) — Müller, Amrei. «En kort innføring i folkerettslig traktattolkning». Jussens Venner 52, nr. 4 (6. september 2017): 222–59. https://doi.org/10.18261/issn.1504-3126-2017-04-02.

Møller (2023) — Jon Christian. «FNs cyberkriminalitetskonvensjon », 24. februar 2023. https://www.linkedin.com/pulse/fns-cyberkriminalitetskonvensjon-jon-christian-m%C3%B8ller/?originalSubdomain=no.

Nasjonal sikkerhetsmyndighet (2023) — Nasjonal sikkerhetsmyndighet. «Forebyggelse av tjenestenektangrep», 16. mars 2023. https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innen-for-digital-sikkerhet/forebyggelse-av-tjenestenektangrep.

Nasjonal sikkerhetsmyndighet (2023) — Nasjonal sikkerhetsmyndighet. «Risiko 2023». 2022. https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf.

Nasjonal sikkerhetsmyndighet (2022) — Nasjonal sikkerhetsmyndighet. «Nasjonalt digitalt risikobilde 2022». 2022. https://nsm.no/getfile.php/1311995-1664550278/NSM/Filer/Dokumenter/Rapporter/NDIG%202022.pdf.

Nasjonal sikkerhetsmyndighet (2022) — Nasjonal sikkerhetsmyndighet. «Risiko 2022». 2022. https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf.

Nasjonal sikkerhetsmyndighet (2017) — Nasjonal sikkerhetsmyndighet. «Helhetlig IKT-risikobilde 2017». 2017 https://nsm.no/getfile.php/133675-1592831718/NSM/Filer/Dokumenter/Rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf.

Politiet (2023) — Oslo politidistrikt. «Har bidratt til at hackernettverket HIVE er mørklagt». Politiet, 27. januar 2023. https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2023/01/27/hive/.

Politiet (2022) — Oslo politidistrikt og Nasjonalt cyberkrimsenter (NC3). «Den lille brosjyren om datasikkerhet». 9. mai 2022. https://www.politiet.no/globalassets/03-rad-og-forebygging/datakriminalitet/den-lille-brosjyren-om-datasikkerhet-no.pdf.

Reed (2010) — Reed, Chris. «Online and Offline Equivalence: Aspiration and Achievement». *International Journal of Law and Information Technology* 18, nr. 3 (1. oktober 2010): 248–73. https://doi.org/10.1093/ijlit/eaq006.

Schjølberg (2017) — Schjølberg, Stein. *Cyberkriminalitet.* Oslo: Universitetsforl., 2017.

Schjølberg (2023) — Schjølberg, Stein. *Cyberkriminalitet: Nasjonal og global utvikling*. 2. utg., Oslo: Universitetsforl., 2023.

Sunde (2021) — Sunde, Inger Marie. «Effektiv, tillitvekkende og rettssikker behandling av databevis.» 18. juni 2021. https://www.regjeringen.no/contentassets/13417a44276c4b4086fdcbabb2108455/utredning-databevis-2021.pdf.

Sunde (2019) — Sunde, Inger Marie. «Datakrimretten i 'fugleperspektiv'». Tidsskrift for strafferett 19, nr. 2 (28. juni 2019): 129–47. https://doi.org/10.18261/issn.0809-9537-2019-02-02.

Sunde (2016) — Sunde, Inger Marie. *Datakriminalitet*: *En Fremstilling Av Strafferettslige Regler Om Datakriminalitet.* Bergen: Fagbokforl, 2016.

Universitetet i Oslo (2022) — Institutt for offentlig rett. «Teknologinøytralitet». Universitetet i Oslo, 14. desember 2022. https://www.jus.uio.no/ior/forskning/phdprosjekter/julfredrik/index.html.

Wager (2022) — Wagen, Wytske Van Der, Jan-Jaap Oerlemans, and Marleen Weulen Kranenbarg. Essentials in Cybercrime: A Criminological Overview for Education and Practice. The Hague: Eleven, 2022.

Wikipedia (2021) — «Prinsipp». *Wikipedia*, 11. august 2021. https://no.wikipedia.org/w/index.php?title=Prinsipp&oldid=21716571#cite_note-1.

Lover

1814	Kongeriket Norges Grunnlov av 17. mai 1814 (Grunnloven)
1902	Lov 22. mai 1902 nr. 10 almindelig borgerlig straffelov (straffeloven 1902)
1981	Lov 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven)
1995	Lov 4. august 1995 nr. 53 om politiet (politiloven)
2005	Lov 20. mai 2005 nr. 28 om straff (straffeloven)
2010	Lov 28. mai 2010 nr. 16 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven)

Konvensjoner

Den europeiske menneskerettighetskonvensjonen	The European Convention on Human Rights. Rome 4 November 1950.
Wien-konvensjonen om traktatretten	The Vienna Convention on the Law of Treaties. Vienna 23 May 1969.
Konvensjon om datakriminalitet	Convention on cybercrime. Budapest 23 November 2001.

Forarbeider

NOU 1985: 31	Datakriminalitet
NOU 2002: 4	Ny straffelov Straffelovkommisjonens delutredning VII
NOU 2003: 27	Lovtiltak mot datakriminalitet Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi
Ot.prp. nr. 40 (2004-2005)	Om lov om endringer i straffeloven og straffeprosessloven og om samtykke til ratifikasjon av Europarådets konvensjon 8. november 2001 om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi (lovtiltak mot datakriminalitet)
NOU 2007: 2	Lovtiltak mot datakriminalitet Delutredning II
Ot.prp. nr.8 (2007–2008)	Om lov om endringer i straffeloven 20. mai 2005 nr. 28 mv. (skjerpende og formildende omstendigheter, folkemord, rikets selvstendighet, terrorhandlinger, ro, orden og sikkerhet, og offentlig myndighet
Ot.prp. nr. 22 (2008-2009)	Om lov om endringer i straffeloven 20. mai 2005 nr. 28
Meld. St. 37 (2014-2015)	Globale sikkerhetsutfordringer i utenrikspolitikken – Terrorisme, organisert kriminalitet, piratvirksomhet og sikkerhetsutfordringer i det digitale rom
Innst. 360 S. (2020-2021)	Innstilling fra kontroll- og konstitusjonskomiteen om Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT
Dokument 3:5 (2020-2021)	Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT

Rettspraksis

Nasjonal rettspraksis

Rt. 1994 s. 1610
Rt. 2004 s. 1619
Rt. 2012 s. 1669
HR-2019-610-A

Internasjonal rettspraksis

Botswana v. Namibia	*Kasikili/Sedudu Island (Botswana v. Namibia)*, International Court of Justice, Judgement, 13. desember 1999.