Rapport

Kunnskapsoversikt cyberkriminalitet

Forfattere:

Per Håkon Meland, Nina Møllerstuen Bjørge, Marte Høiby, Stine Skaufel Kilskar

Rapportnummer:

2023:01331 - Åpen

Oppdragsgiver:

Justis- og beredskapsdepartementet

SINTEF Digital
Postadresse:
Postboks 4760 Torgarden
7465 Trondheim

Sentralbord: 40005100

info@sintef.no

Foretaksregister:
NO 919 303 808 MVA

Rapport

Kunnskapsoversikt cyberkriminalitet

EMNEORD
Cyberkriminalitet
Datakriminalitet
Begreper
Omfang
Måling
Kunnskap

VERSJON
1.0

DATO
2024-03-08

FORFATTERE
Per Håkon Meland, Nina Møllerstuen Bjørge, Marte Høiby, Stine Skaufel Kilskar

OPPDRAGSGIVER
Justis- og beredskapsdepartementet

OPPDRAGSGIVERS REFERANSE

PROSJEKTNUMMER
102027997

ANTALL SIDER
54

SAMMENDRAG
På oppdrag fra Justis- og beredskapsdepartementet har SINTEF gjennomført en systematisk litteraturstudie for å adressere forskningsspørsmål knyttet til begreps-definisjoner og hvordan man kan måle omfang av fenomenet cyberkriminalitet. Denne rapporten presenterer en systematisk kunnskapsoversikt som svarer på disse spørsmålene. Litteraturen er tydelig på at det ikke finnes en entydig definisjon av hva cyberkriminalitet er, men et fellestrekk er at de omtaler ulovlige handlinger både ved hjelp av eller rettet mot datamaskiner, nettverk eller annen digital teknologi. Siden dette favner såpass bredt, er det anbefalt å bruke mer spesifikke begreper når man skal forstå og operasjonalisere cyberkriminalitet, herunder måling av omfang. Vår anbefaling er å benytte en nyetablert taksonomi fra litteraturen for å beskrive de mange måtene å begå forbrytelser med og mot teknologi. Samtidig bør en eller flere straffbare handlinger knyttes opp imot Budapest-konvensjonen sin klassifisering, som er det mest anerkjent rammeverket for lovbrudd.

UTARBEIDET AV
Per Håkon Meland
SIGNATUR

KONTROLLERT AV
Geir Kjetil Hansen
SIGNATUR

GODKJENT AV
Maria Bartnes
SIGNATUR

RAPPORT NR.	ISBN	GRADERING	GRADERING DENNE SIDE
2023:01331	978-82-14-07159-7	Åpen	Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
0.5	2023-11-06	Versjon for referansegruppe
0.6	2023-11-21	Utkast klargjort til oppdragsgiver
0.7	2024-01-21	Nytt utkast klart til oppdragsgiver
1.0	2024-03-08	Ferdigstilt rapport

Sammendrag

Cyberkriminalitet er et uoversiktlig fenomen i stadig endring. Selv om det er en allmenn oppfatning om at det blir mer av det, er det vanskelig å si noe konkret om hvor mye og hvor raskt. Mange vil også hevde at cyberkriminalitet ikke skiller seg særlig fra tradisjonell kriminalitet, men at det snakk om «gammel vin i nye flasker». På oppdrag fra Justis- og beredskapsdepartementet, har SINTEF gjennomført en systematisk litteraturstudie for å adressere forskningsspørsmål knyttet til begrepsdefinisjoner og hvordan man kan måle omfang av fenomenet. Denne rapporten presenterer en systematisk kunnskapsoversikt som svarer på disse spørsmålene. Første del av undersøkelsen har vært å utvikle en protokoll som sikrer at hele prosessen er eksplisitt, transparent, standardisert, oppdaterbar, replikerbar og mindre utsatt for forskningsbias. Gjennom søk i anerkjente litteraturdatabaser og videre filtrering gjennom en seleksjonsprosess kom vi fram til et representativt utvalg på 55 fagfellevurderte artikler og 29 artikler fra grå litteratur. Disse er publisert i løpet av de fem siste årene fram til søketidspunkt. Fra dette utvalget har vi har gjort en grundig ekstrahering og syntetisering av innholdet for å svare på forskningsspørsmålene. Vi har også undersøkt og hentet data fra de mest fremtredende kildene i utvalget og slik inkludert anerkjente publikasjoner fra tidligere år. Denne kunnskapsoversikten viser derfor til langt flere kilder enn det sentrale utvalget.

Litteraturen er tydelig på at det ikke finnes en entydig definisjon av hva cyberkriminalitet er. Bare innenfor vårt utvalg av 55 fagfellevurderte artikler ble det brukt 32 forskjellige definisjoner. Ingen av definisjonene dominerte i stor grad, men de fleste var semantisk sett ganske like. De aller fleste omtaler ulovlige handlinger både ved hjelp av eller rettet mot datamaskiner, nettverk eller annen digital teknologi. Siden dette favner såpass bredt, er det anbefalt å bruke mer spesifikke begreper når man skal forstå og operasjonalisere cyberkriminalitet. Dessverre finnes det ikke noen komplett taksonomi eller et rådende klassifiserings-rammeverk for cyberkriminalitet, men det overordnede skillet mellom type I, angrep mot datamaskiner, og type II, angrep ved bruk av datamaskiner, er helt klart det som dominerer i utvalget vårt. I praksis er det en glidende overgang mellom disse avhengig av hvor involvert teknologien er. Det er også vanlig å betegne en type III-dimensjon, som sier noe om det er velkjent eller ny type teknologi som benyttes. Vår anbefaling er å benytte en nyetablert taksonomi fra litteraturen for å beskrive de mange måtene å begå forbrytelser med og mot teknologi. Samtidig bør en eller flere straffbare handlinger knyttes opp mot Budapest-konvensjonen sin klassifisering, som er det mest anerkjent rammeverket for lovbrudd.

En måte å måle omfanget av cyberkriminalitet på er å bruke data fra politiets ulike register. Dette gir imidlertid bare et bilde av de sakene som blir kjent for politiet, og ikke alle de sakene som faktisk skjer. Vi har sett forholdvis få eksempler på dette i vårt utvalg. I nyere publikasjoner er det vanligere å måle omfanget av ulike typer cyberkriminalitet ved hjelp av undersøkelser som for eksempel spør folk eller organisasjoner om de har vært utsatt for hendelser og hva slags konsekvenser det har hatt. Dette gir også bare et delvis bilde, fordi ikke alle vil svare ærlig eller huske alle hendelsene. Andre kilder til omfang inkluderer rapporter fra sikkerhetsselskaper, men mange forfattere stiller spørsmål ved metode og kredibilitet i disse knyttet til blant annet selskapenes forretningsmessige interesser. Det er også store avvik mellom hva som undersøkes og omfanget undersøkelsene hevder å kunne måle. I denne rapporten gir vi oversikt over metoder, omfangsresultater, samstemthet og utfordringer knyttet til målinger i litteraturen. Mange studier viser at selv om tradisjonell kriminalitet er på vei ned, vokser cyberkriminalitet med større takt og har andre økonomiske konsekvenser. Dermed øker det totale kriminalitetsbildet.

Til slutt gir vi anbefalinger og premisser for målinger av cyberkriminalitet i Norge. Vi har sett på om det er undersøkelser og data fra utlandet som kan overføres hit, og beskriver også eksisterende Norske undersøkelser for å kartlegge hvilke typer cyberkriminalitet disse allerede dekker.

Innholdsfortegnelse

BILAG/VEDLEGG

1 Introduksjon

> *«Even if cybercrime to some extent represents old wine in new bottles, its scale and variety imply that we are dealing with an awful lot of wine in very many, differently shaped and capacious bottles»*
> - Bert-Jaap Koops [1]

Cyberkriminalitet, eller datakriminalitet som tidligere var den mer vanlige betegnelsen, er et uoversiktlig fenomen i stadig endring. Her i Norge har Riksrevisjonen [2] påpekt at uklarhet rundt begrepet har skapt utfordringer, slik som mangel på effektive strategier og tiltak på området. Internasjonalt mener FN [3] at uten en klar definisjon, blir rapportering av hendelser på tvers av byråer, jurisdiksjoner og stater en kompleks og uklar øvelse. Vi har i dag ingen internasjonal konsensus på hvordan man skal definere og måle cyberkriminalitet [4], og det er derfor vanskelig å gi gode estimater på hvor stort problemet virkelig er og hva som skiller cyberkriminalitet fra tradisjonell kriminalitet. Mange typer cyberkriminalitet var (analoge) kriminelle handlinger før Internetts tidsalder, men har utviklet seg til å bli cyberfenomener og på en måte fått en ny vår. Andre typer kriminalitet har oppstått sammen med teknologien.

I 2022 fikk SINTEF fra Justis- og beredskapsdepartementet i oppdrag å kartlegge kunnskapen om datakriminalitet som fenomen og prøve å si noe om omfanget av datakriminalitet i Norge. Denne rapporten er en systematisert kunnskapsoversikt over ny og relevant fagfellevurdert forskning på dette området, og fokuserer på de overordnede spørsmålene:

- *Hvilke begrepsdefinisjoner av datakriminalitet finnes det i litteraturen, og hvordan operasjonaliserer ulike studier begrepene som brukes?*
- *Hvordan måles omfanget av datakriminalitet etter ulike begreper slik de er definert i eksisterende studier?*

Det er ønskelig å gjennomføre måling av cyberkriminalitetsomfang i Norge, men før man kan måle må man ha en klar idé om hva man måler, hvordan og hvorfor. Denne kunnskapsoversikten danner et slikt grunnlag for en slik gjennomføring.

Vi har analysert fagfellevurdert litteratur fra hele verden for å forstå fenomenet cyberkriminalitet i en global kontekst. Det har ikke vært et mål for denne kunnskapsoversikten å lage en ny, norsk språkdrakt for de begrepene som benyttes internasjonalt, så vi benytter derfor i stor grad mange engelske begreper hentet fra litteraturen. Vi har derimot prøvd å gi begrepene en forklaring og kontekst som kan være et grunnlag for å etablere eller identifisere passende norske begreper på sikt.

Som en del av dette prosjektet har vi engasjert en referansegruppe med representanter fra ulike politidistrikt, Nasjonalt cyberkrimsenter (NC3) ved Kripos, CERT-miljø (*Computer Emergency Response Team*), bank og finanssektoren, konsulenter fra sikkerhetsindustri og juridiske eksperter. Referansegruppen har gitt innspill på preliminære funn og deltatt i nyttige diskusjoner knyttet til dette arbeidet, og fortjener en stor takk.

1.1 Uønskede begreper

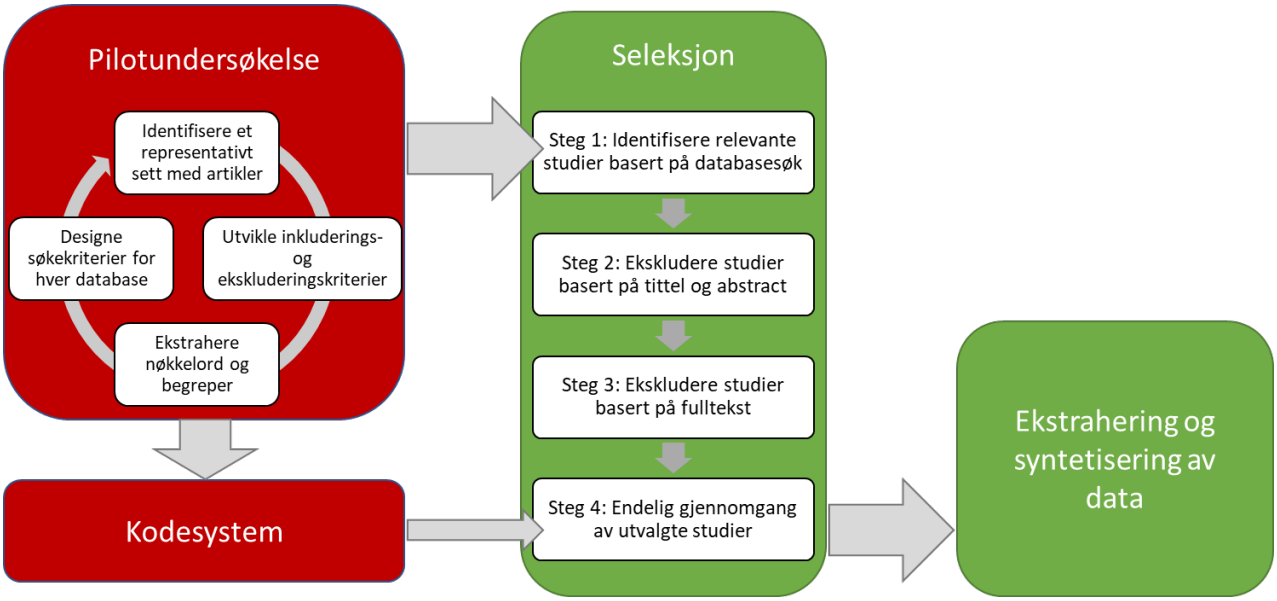
En viktig presisering er at denne kunnskapsoversikten ikke representerer forfatternes meninger om hva som er de riktige begrepene å bruke. Derimot gjengir vi og sammenstiller de ulike begrepene som litteraturen bruker. Et konkret innspill fra referansegruppen har vært at enkelte begreper som litteraturen benytter er sterkt uønskede. Dette gjelder først og fremst begrepet «*child pornography*» / «barnepornografi», hvor det heller bør brukes «seksualiserte skildringer av barn», «overgrepsmateriale», «overgrep mot barn» eller lignende. Vi har registrert at justiskomiteen i en innstilling til Odelstinget fra 2004-2005 [5] allerede da ville

ha slutt på bruken av dette begrepet. En god del år senere, i 2018 [6], gikk også Domstoladministrasjonen ut mot bruken av begrepet i rettssaker, og Bjørn-Erik Ludvigsen fra Kripos uttalte at bruk av begrepet regnes som uprofesjonelt. Ludviksen gjentok samme beskjed på Facebook-siden til Kripos i 2021 [7]. Begrepet har vist seg å være seiglivet, og dessverre har vi sett samme uheldige tendens i litteraturen. Begrepet brukes fremdeles i nyere oversikter over typer cyberkriminalitet eller i definisjoner. I denne kunnskapsoversikten gjengis begrepet der det opptrer som del av litteraturen i sitat, mens vi i egen tekst benytter andre norske begreper. Vi støtter ambisjonen om å unngå begrepet i videre definisjoner og operasjonalisering. I nyere litteratur ser vi imidlertid gjentagende bruk av et alternativt begrep med forkortelsen CSAM, som står for «*Child Sexual Abuse Material*».

1.2 Forskningsmetode

For å lage denne kunnskapsoversikten har vi benyttet en metode for systematisk litteraturstudium (*systematic literature review* (SLR)). Kort fortalt er dette en anerkjent metode for å systematisk sammenstille kunnskap fra litteraturen, med opprinnelse fra det medisinske fagfeltet. Når man gjennomfører et slikt studium, lager man og følger en tydelig definert protokoll som gjør undersøkelsen eksplisitt, transparent, standardisert, oppdaterbar, replikerbar og mindre utsatt for forskningsbias. Detaljene fra protokollen er utelatt fra denne kunnskapsoversikten, men protokollen ligger som vedlegg for den som ønsker innsyn.

Gangen i vår SLR er gjengitt i Figur 1. En pilotundersøkelse har dannet grunnlag for å utvikle selve protokollen. Det vil si spesifisering av inkluderings- og ekskluderingskriterier for litteraturen, identifisering av sentrale nøkkelord og begreper, og utvikling av e søkestrenger for ulike indekseringsdatabaser. Et annet resultat av pilotundersøkelsen har vært et kodesystem som er brukt for å klassifisere tekstlig innhold i artiklene.

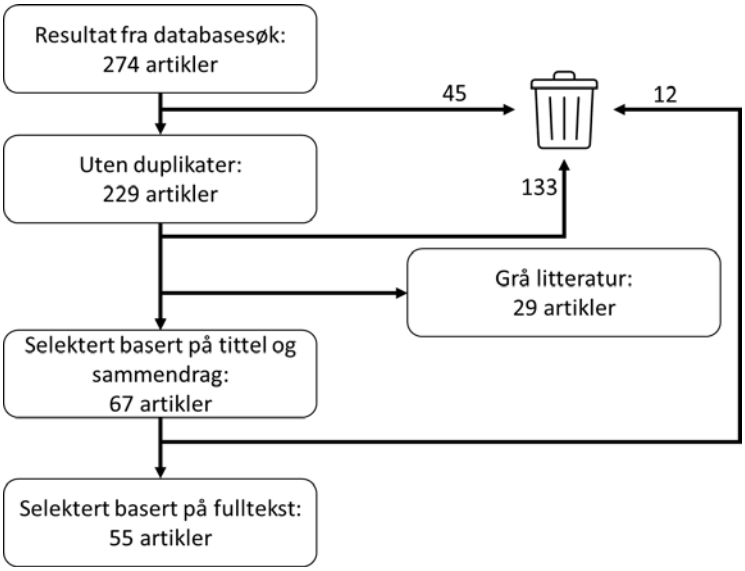


Figur 1. Planlegging og gjennomføring av SLR

Seleksjonsfasen går ut på å filtrere artiklene man har funnet i databasene til man har igjen et utvalg som er i henhold til inkluderings- og ekskluderingskritertene. De mest sentrale inkluderingskriteriene har vært at utvalget må ha hovedfokus på vårt tema og være fagfellevurderte publikasjoner fra anerkjente publikasjons-kanaler. Vi har inkludert både *primærstudier,* som er arbeid med originale empiriske data, og *sekundær-studier,* som er oversiktsartikler basert på andres arbeid. Vi har også valgt å inkludere enkelte typer særlig relevant grå litteratur. Dette gjelder bøker eller bokkapitler utgitt av kommersielle forlag uten at de er

fagfellevurdert, men som likevel er indeksert av litteraturdatabaser. Det samme gjelder enkelte typer rapporter og avhandlinger.

Vi begrenset tidsperspektivet i søkestengene brukt mot indekseringsdatabasene til de siste 5 årene (fra 1.januar 2017). Publikasjoner som ikke har hatt mye gjennomslag i form av siteringer/omtaler har blitt ekskludert, men her gjorde vi unntak for helt ferske publikasjoner. Kort oppsummert startet vi med 274 artikler etter søk i åtte ulike indekseringsdatabaser. Etter fjerning av duplikater og gradvis mer detaljert analyse (se Figur 2) endte vi opp med utvalg på 55 artikler som var fagfellevurderte og 29 artikler fra grå litteratur.



Figur 2. Seleksjonsprosess etter databasesøk.

Fra dette utvalget har vi har gjort en grundig ekstrahering og syntetisering av innholdet for å svare på forskningsspørsmålene. Som en del av syntetiseringsprosessen har vi også undersøkt og hentet data fra de mest sentrale kildene vårt utvalg baserer seg på (såkalt «*snowballing*»). Dermed fanger vi opp anerkjente publikasjoner fra tidligere år og gjør at denne kunnskapsoversikten viser til langt flere kilder enn det sentrale utvalget.

Vi har lyst til å nevne at i 2022 publiserte Phillips et al. [8] en litteraturstudie med et lignende formål og metodisk tilnærming som i vårt oppdrag. De har på samme måte som oss analysert definisjoner og klassifiseringer av cyberkriminalitet. I vårt studium har vi hatt et noe annerledes, større og nyere utvalg enn hva Phillips et al. har brukt, og vi har under syntetiseringen av våre funn sett på om vi kan forsterke tidligere resultater og om vi finner mangler eller feil. Phillips et al. er heller ikke det eneste metastudiet vi har benyttet, men er det som overlapper mest med vårt.

1.3 Rapportens struktur

Strukturen i de neste kapitlene er basert på forskningsspørsmålene. Kapittel 2 omhandler definisjoner og begrepsbruk fra fagfellevurdert litteratur, mens kapittel 3 fokuserer på kunnskap knyttet til måling av omfang. I kapittel 4 presenterer vi en del metadata om litteraturutvalget vårt, og i kapittel 5 henter ut sentrale relevante funn i grå litteratur som ble identifisert under seleksjonsprosessen. Kapittel 6 inneholder konklusjoner og anbefalinger.

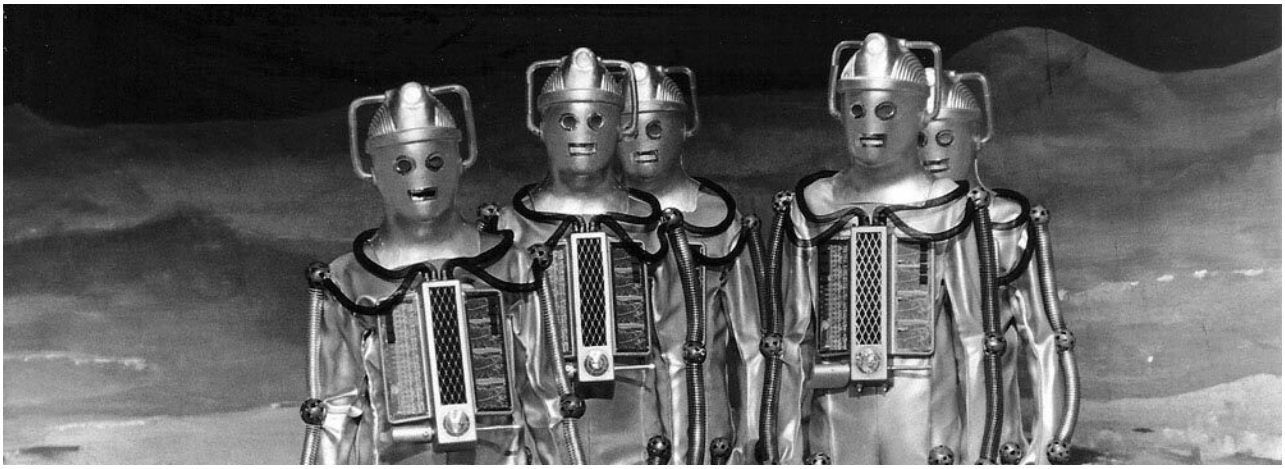
2 Definisjoner og begrepsbruk

I den engelskspråklige litteraturen har det blitt brukt mange ulike begreper for cyberkriminalitet, noe vi også tok høyde for da vi søkte etter litteratur. På overordnet nivå har typisk begrepene «computer crime», «data crime», «cyber crime» (inkludert «cybercrime»), «virtual crime», «digital crime», «high-tech crime» og «Internet crime» blitt brukt mye om det samme konseptet ([8], [9]), men dette har endret seg over tid. McGuire [10] har studert hvordan begrepet «cybercrime» har gått fra å bli et relativt lite brukt begrep til det dominerende over tid. For eksempel, i årene 1995-2000 var «computer crime» det klart mest brukte i litteraturen, mens etter den tid har «cyber crime» / «cybercrime» tatt over. Denne utviklingen har vært gjenspeilt i Norge også, og vi benytter derfor i hovedsak *cyberkriminalitet* når vi omtaler dette fenomenet i denne kunnskapsoversikten.

Før vi gir oss i kast med å se på definisjoner for cyberkriminalitet, er det greit å forstå opphavet til ordet «cyber». Neste seksjon gir en kort innføring.

2.1 Hva er cyber?

«Cyber» er et nokså gammelt begrep, og har hatt litt ulik betydning oppgjennom historien [11]. Opprinnelsen er det gamle greske ordet «kubernētēs» (κυβερνήτης), som betyr *styrmann* (for skip). Nærmere vår tid, på 1940-tallet, navnga matematikeren Norbert Wiener fagfeltet for kontroll- og kommunikasjonsteori *cybernetics* (Norsk: *Kybernetikk*). Sentralt i dette fagfeltet er robotikk, og begrepet «cyber» ble mer allment populært da robotrasen «cybermen» dukket opp i TV-serien Dr. Who på BBC i 1966 (se Figur 3).



Figur 3. Cybermen fra BBC-serien Dr Who. Tillatelse for bruk av bildet er gitt av L. Williams fra The Dr Who site.

«Cyber» ble senere knyttet mer mot datateknologi gjennom populærkultur, spesielt science fiction-boken *Neuromancer* fra 1982 av William Gibsen, hvor begrepet «cyberspace» ble introdusert. I dag brukes «cyber» gjerne som et prefix for noe som har noe med Internett å gjøre, slik som «cyberwar», «cyberterrorism», «cybersex», «cybersecurity» og selvfølgelig «cybercrime».

2.2 Hva er cyberkriminalitet?

I litteraturen benyttes mange ulike definisjoner av begrepene knyttet til konseptet cyberkriminalitet. Det er mange publikasjoner som trekker opp nettopp dette fenomenet som et problem. Fra vårt utvalg skriver for eksempel Nouh et al. [12] *«there have been several arguments in the literature over the exact definition of cybercrime with no single universal definition»* og tilsvarende fra Broadhead [13] *«there is no single, universally adopted definition of cybercrime»*. Furnell og Dowling [14] har skrevet en innsiktsfull artikkel som

belyser denne problematikken, og argumenterer for at det store antallet definisjoner er resultat av at problemet er dynamisk og endrer seg over tid. Det er en økende tendens til at alle dårlige opplevelser på nett betegnes som cyberkriminalitet, inkludert mobbing, stalking og trakassering. I litteraturen er den mest konsistente oppfatningen at cyberkriminalitet er et paraplybegrep for et bredt spekter av kriminalitet tilknyttet den digitale sfære [15].

Hva er problemet med et paraplybegrep? Svaret på det kommer for eksempel fram i De Paoli et al. [9] sin artikkel fra 2021. De gjennomførte en intervjustudie av spesialister ved datakriminalitetssentre i ulike Europeiske land (inkludert Norge), og selv om begrepet «cybercrime» var godt kjent, ble det heller brukt mange alternative begreper innenfor samme enhet («Internet crime», «IT crime», «high-tech crime», «digital crime» og «technology crime»). Dette har ført til utfordringer knyttet til statistikk for anmeldelser og etterforskning. Den generelle anbefalingen fra denne artikkelen er å ta bedre i bruk begreper fra Budapestkonvensjonen [16], som vi kommer tilbake til senere i denne rapporten.

I Tabell 1 har vi samlet definisjoner og definisjonskilder for «cybercrime» brukt i vårt litteraturutvalg. Vi har sortert tabellen på årstall for definisjonen. Det er bemerkelsesverdig at 55 artikler som er publisert innenfor samme femårsperiode refererer til 32 forskjellige definisjoner. Vi ser på dette som et klart forsterkende bevis på en manglende omforent definisjon.

Tabell 1. Definisjoner av "cybercrime" brukt i litteraturutvalget

Definisjoner	Brukt av
“a crime that is committed with the use of a computer through a communication device or a transmission media called the cyberspace and global network called the internet“ Sackson (1996) [17]	Awhefeada og Bernice [18]
“any crime that may occur through a computer system or network, within a computer system or network, or against a computer system or network” United Nations (2000) [19]	Babanina et al. [20]
“computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks” Thomas and Loader (2000) [21]	Akdemir et al. [22]
“the term cybercrime does not actually do much more than signify the occurrence of a harmful behaviour that is somehow related to a computer” Wall (2001) [23]	Phillips et al. [8]
“any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them.” Oxford Dictionary of Law (2002)	Cordova et al. [24]
“Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime” Pati (2003) [25]	Goni [26]
“‘the criminal use of any computer network or system on the Internet; attacks or abuse against the systems and network or system on the Internet; attacks or abuse against the systems and networks for criminal purposes; crimes and abuse from either existing criminals using new technology; or new crimes that have developed with the growth of the Internet” Heimans (European Commission) (2004) [27]	Srivastava et al. [28]
“any unauthorized, or deviant, or illegal activity over the Internet that involves a computer as the tool to commit the activity and a computer as the target of that activity” Moitra (2005) [29]	Luknar [30]
“any crime that is facilitated or committed using a computer, network, or hardware device” Gordon and Ford (2006) [31]	Graham et al. [32], Luknar [30], De Paoli et al. [9], Conway og Hadlington [33], Lazarus et al. [15], Ratten et al. [34]
“a crime committed on a computer network” Brenner (2006) [35]	Somer [36]
“criminal acts committed using electronic communications networks and information systems or against such networks and systems.” European Commission (2007) [37]	Cordova et al. [24], Nouh et al.[12], Chandra og Snowe [38], Akdemir et al. [22], Anderson et al. [39]
“a crime that is enabled by or targets computers” Clay (2007) [40]	Awhefeada og Bernice [18]

Definisjoner	Brukt av
“the transformation of criminal or harmful behaviour by networked technology.” Wall (2007) [41]	Cordova et al. [24], Shan-A-Khuda og Schreuders [42]
“a criminal activity in which computers or computer networks are the principal means of committing an offense or violating laws, rules, or regulations” Kshetri (2009) [43], [44]	Akdemir et al. [22], Srivastava et al. [28]
“any illegal act that involves a computer, its systems, or its applications” CENGAGE Learning (2010) [45]	Amro [46]
“crime in which computer networks are the target or a substantial tool ” Koops (2010) [1]	Akdemir et al. [22]
“Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)” Halder og Jaishankar (2011) [47]	Goni [26], Azad et al. [48]
“crimes committed at a distance, with significant difficulties concerning the determination of the place of perpetration of such an offence, carried out by electronic means, in a digital sphere” Pradillo (2011) [49]	Luknar [30]
“criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime” ISO 27032 (2012) [50]	Chandra og Snowe [38]
“Cyber Crime means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them” South African Cybercrime Law (2012) [51]	Goni [26]
“Cybercrime is a crime in the so-called cyberspace” (oversatt fra Russisk) Nomokonov og Tropina (2012) [52]	Almazkyzy og Esteusizov [53]
“the use of information resources and (or) the impact on them in the informational sphere for illegal purposes” (oversatt fra Kinesisk) Shanghai Cooperation Organization (SCO) Agreement (2013), gjengitt fra [54]	Akdemir et al. [22]
“criminal activity making use of computers and the Internet” Gerry og Moore (2015) [55]	Mendoza [56]
“a criminal act of which the target is computer information” (oversatt fra Russisk) Commonwealth of Independent States Agreement (2016), gjengitt fra [57]	Akdemir et al. [22]
“crime committed over the Internet which might include hacking, defamation, copyright infringement and fraud” Ajayi (2016) [58]	Mohammed et al. [59]
“any crime that is committed using a computer or network, or hardware device” Symantec Corporation (2017) [60]	Cordova et al. [24]
“this term is understood to cover criminal conduct that affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet users.”Weissser, ukjent kilde (2017)	Cordova et al. [24]
“any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT)” Europol (2017) [61].	Broadhead [13], Ratten et al. [34]
“an intended illegal act involving the use of computers or other technologies” The American Institute of CPAs (AICPA) (2017) [62]	Chandra og Snowe [38]
“an act that uses computer technology to commit a crime.” Chandra og Snowe (2020) [38] (egen definisjon)	Chandra og Snowe [38]
“the use of a computer as an instrument to further illegal ends, …” Encyclopedia Britannica (2023) [63]	Awhefeada og Bernice [18]
“Crime or a crime committed using computers or the internet.” Oxford English Dictionary (2023) [64]	Goni [26]

Semantisk sett er ikke disse definisjonene veldig forskjellige. I hovedsak ser vi noen forskjeller knyttet til rollen til datamaskiner, nettverk og Internett, hva som er naturen til den kriminelle aktiviteten og hvem som er målet for aktiviteten. Noen definisjoner er bredere og mer inkluderende, mens andre setter søkelys på spesifikke aspekter knyttet til cyberkriminalitet. Andre aspekter ved definisjonene vi har lyst til å fremheve er:

- De aller fleste dekker ulovlige handlinger både med og mot datateknologi, mens et mindretall er mer fokusert på angrep mot teknologien.

- Mens de tidlige definisjonene omtalte først og fremst datamaskiner og nettverk, har de senere et bredere spekter av teknologi (Internett, mobiltelefoner, maskinvare, cyberspace).
- I vårt utvalg har vi sett en generell trend hvor mange av forfatterne gjerne stiller flere definisjoner opp mot hverandre i samme artikkel.
- Det brukes definisjoner fra nesten alle år mellom 2000-2017, altså ingen klar konsentrasjon, selv om våre to mest brukte stammer fra henholdsvis 2006 og 2007.
- Korte definisjoner er mer populære enn lange.
- Vi har også sett at samme forfatter er kilde til ulike definisjoner med noen års mellomrom, se for eksempel Wall (2001 og 2007).
- Forfattere har en tendens til å sitere definisjoner fra andre forfattere fra samme geografiske region. For eksempel referer Almazkyzy og Esteusizov [53] fra Romania til en definisjon i den russiske artikkelen av Nomokonov og Tropina [52], Goni [26] fra India refererer til Pati [25] som også er fra India og Mohammed et al. [59] fra Nigeria referer til Ajayi [58] som er fra Kenya. I litteraturstudiet til Phillips et al. [8] trekkes det fram at de dominerende definisjonene er fra den vestlige verden, og kan derfor ikke sees å være globale.

Akdemir et al. [22] gjennomførte en undersøkelse publisert i 2020 for å finne de mest populære definisjonene av «cybercrime» brukt av artikler indeksert av Google Scholar og ProQuest, og kom fram til at Thomas og Loader (fra 2000, [21]) og Gorden og Ford (fra 2006, [31]) var de mest brukte. Detaljene om denne undersøkelsen og utvalget er ikke godt beskrevet, men resultatet stemmer delvis med vårt. Vi så bare ett eksempel på en artikkel som brukte definisjonen til Thomas og Loader, mens Gordon og Ford var den mest siterte hos oss, altså:

«any crime that is facilitated or committed using a computer, network, or hardware device»[1]

Hos oss kom Europakommisjonen sin definisjon fra 2007 like bak på en andreplass med:

«criminal acts committed using electronic communications networks and information systems or against such networks and systems».

Likevel er det det lett å se at det er ingen som er klart dominerende i dette feltet.

Vi ba en *large language model* (LLM) lage en syntetisering basert på definisjonene brukt av utvalget vårt og fikk følgende resultat: *«Cybercrime refers to illegal activities involving computers, networks, or digital technology, which can harm individuals, organizations, or society. It includes offenses like hacking, fraud, and copyright infringement».* En norsk oversettelse av dette kan være: *«Cyberkriminalitet refererer til ulovlige aktiviteter som involverer bruk av datamaskiner, nettverk eller digital teknologi, som kan skade enkeltpersoner, organisasjoner eller samfunnet. Dette inkluderer lovbrudd som hacking, svindel og brudd på opphavsrett»*. Om denne definisjonen er bedre eller dårligere enn hva som allerede finnes tar vi ikke stilling til her, men vi ser at også denne definisjonen er såpass bred at vi trenger noen mer spesifikke operasjonelle begreper. Dette ser vi nærmere på i neste avsnitt.

2.3 Hvilke mer spesifikke begreper brukes i litteraturen?

Siden «cybercrime» er et såpass diffust begrep er det vanlig å bruke mer spesifikke begreper for typer av cyberkriminalitet. En taksonomi er et system for å klassifisere noe, og har ofte en hierarkisk struktur hvor innholdet er organisert i grupper eller typer. I litteraturen finnes det flere taksonomier som forsøker å organisere begreper på ulike nivåer knyttet til cyberkriminalitet. Somer [36] publiserte i 2019 en oversikt

[1] Gordon og Ford sier faktisk at det beste hadde vært om begrepet «cybercrime» hadde blitt slettet fra leksikon, men siden det er vanskelig å få til har de altså laget sin egen definisjon.

over slike taksonomier[2], og peker på at selv om det er mye overlapp mellom disse, er det klare forskjeller som skyldes ulik logikk for oppbygning. Noen taksonomier er basert på tradisjonell kriminalitet, andre baserer seg på teknologi, trusselaktører og angrepstyper, mens noen igjen er basert på juridiske forhold. Vi går her gjennom de viktigste typene som er omtalt i vårt utvalg.

2.3.1 To dimensjoner

Det er først og fremst to hovedkategorier av cyberkriminalitet som benyttes i litteraturen og ellers, nemlig «cyber-enabled» og «cyber-dependent» ([13], [65], [14], [42], [4], [59], [8]). Den første omhandler tradisjonell kriminalitet som kan forsterkes gjennom bruk av datamaskiner og datanettverk, mens den andre tar for seg kriminalitet som bare kan gjennomføres ved hjelp av datamaskiner og datanettverk. Opprinnelsen til denne distinksjonen ser ut til å komme fra en bakgrunnsartikkel [19] til FN sin workshop om data-kriminalitet i år 2000. Begrepene som ble brukt i denne artikkelen var da *Computer crime in a narrow sense («computer crime»)* (som tilsvarer «cyber-dependent») og *Cyber crime in a broader sense («computer-related crime»)* (som tilsvarer «cyber-enabled»). Skillet mellom «cyber-dependent» og «cyber-enabled» brukes også i INTERPOL sin *National Cybercrime Strategy Guidebook* utgitt i 2021 [66]. Her i Norge har vi tilsvarende oppdeling med «kriminalitet mot datasystemer» og «kriminalitet støttet av datasystemer» i Kripos sin rapport *Cyberkriminalitet 2023* [67], men det finnes også eksempler på benevnelsene «cyber-muliggjort»/ «fasilitert» (som tilsvarer «cyber-enabled») og «cyber-avhengig» (som tilsvarer «cyber-dependent»). I denne rapporten bruker vi «cyber-enabled» and «cyber-dependent» i uoversatt form.

Andre (for eksempel Lallie et al. [68]) refererer til tilsvarende overordnede to-delte kategorisering brukt i den britiske *CyberCrime – prosection guidance* [69]. Det er også verdt å nevne tilsvarende oppdeling med «computer as a target» og «computer as a tool» fra en mye sitert artikkel av Gordon og Ford fra 2002 [70]. Senere har også Gordon og Ford [31] foreslått å konseptualisere cyberkriminalitet som et spektrum, hvor Type I «technology crime» (tilsvarer «cyber-dependent») befinner seg på en side, mens Type II «people crime» (tilsvarer «cyber-enabled») befinner seg på den andre (se Figur 4). Man plasserer da mer spesifikke typer kriminalitet et sted mellom disse ytterpunktene avhengig av hvor sentral teknologi er for gjennom-føringen.

Figur 4. «The continuum of cybercrime», slik foreslått av Gordon og Ford [31].

I en utvalgsartikkel [71] fra 2022 har vi også sett noen som prøver seg med begrepene «computer-assisted» og «computer-focused» cyberkriminalitet, men vi ser ikke helt hva nytt dette tilfører. Det finnes også eksempler på forfattere [36] som eksplisitt sier at de ikke regner «cyber-enabled crime» som cyber-kriminalitet, altså at bare *ren* «cyber-dependent crime» er cyberkriminalitet.

2.3.2 Tre dimensjoner

Utover «cyber-enabled» og «cyber-dependent», finnes det ikke noen definitiv (internasjonalt akseptert og konsistent brukt) klassifisering av cyberkriminalitet [14]. Det er derimot ingen mangel på forsøk, og det

[2] Altså en taksonomi over taksonomier for cyberkriminalitet.

finnes mange eksempler på ulike taksonomier og grupperinger i litteraturen. For eksempel er en tidlig klassifisering fra Wall sin bok fra 2007, *Cybercrime: The transformation of technology in the networked age* [41], mye sitert. Han identifiserer tre kategorier:

- **Computer integrity crime («crime against machines»):** for eksempel hacking og tjenestenektangrep, i praksis det samme som cyber-dependent.
- **Computer asssisted crime («crime using machines»):** knyttet til svindel eller tyveri, i praksis det samme som cyber-enabled.
- **Computer content crime («crime in the machines»):** knyttet til ulovlig innhold på datamaskiner eller i kommunikasjon, eksempelvis ulovlig pornografi eller hatefulle ytringer.

En tilsvarende klassifisering ble også definert av Europakommisjonen i 2007 i deres *Towards a general policy on the fight against cyber crime* [37]:

- **Traditional crime on electronic networks**, som inkluderer svindel eller forfalskning over elektronisk kommunikasjon og informasjonssystemer.
- **Illegal content**, som inkluderer publisering av ulovlig innhold slik som overgrepsbilder eller rasistiske ytringer.
- **Crimes unique to electronic networks**, for eksempel angrep mot informasjonssystemer, tjenestenekt eller hacking.

Denne klassifiseringen har blant annet blitt brukt av Anderson et al. sin hyppig siterte artikkel *Measuring the cost of cybercrime* [72] først presentert i 2012 og på nytt i oppfølgingsartikkelen *Measuring the changing costs of cybercrime* [39] fra 2019[3].

Phillips et al. [8] trekker fram to utvidelser til to-klassifiseringssystemene som ikke er fanget opp i utvalget vårt. Den første var en utvidelse til «cyber-dependent» og «cyber-enabled», hvor Wall [73] definerte «cyber-assisted» kriminalitet som en tredje kategori i 2005. Denne skal favne kriminelle handlinger hvor det er litt tilfeldig at teknologi benyttes i kriminelle handlinger, for eksempel kriminell kommunikasjon gjennom en eller annen app. Vi bemerker at denne kilden knapt har vært sitert og begrepet er lite brukt. Den andre utvidelsen gjelder Gordon og Fords spektrum med Type I og Type II. Her foreslo Sarre et al. [74][4] i 2018 en Type III kategori for å dekke cyberkriminalitet som anvender relativt fersk teknologi, som kunstig intelligens, automatiske bot'er og selvlæring.

For å undersøke sammenhengen mellom kjønn og cyberkriminalitet, har Ibrahim [75] og Lazarus [76] utviklet det de kaller *the tripartite cybercrime framework* (TFC). Her deles cyberkriminalitet opp i tre kategorier basert på motivasjon [15]:

- ***Socio-economic cybercrime,*** definert som datamaskin- og/eller internettbasert ervervelsen av økonomiske fordeler ved hjelp av falske påstander, etterligning, manipulasjon, forfalskning eller annen bedragersk framstilling av fakta, som for eksempel nettsvindel, kredittkortsvindel, nettkorrupsjon og kjærlighetssvindel.
- ***Psychosocial cybercrime,*** som refererer til digitale kriminelle handlinger som primært er drevet av psykologiske motiver for å forårsake sjokk, nød eller skade på en person, der økonomisk gevinst ikke er det primære målet. Dette inkluderer cyberstalking, nettmobbing og online trakassering.
- ***Geopolitical cybercrimes,*** som inkluderer cyberkriminalitet som er av grunnleggende politisk karakter og involverer statlige aktører (og ikke-statlige aktivister) og/eller deres representanter som

[3] Til sammen har disse to artiklene rundt 1000 siteringer, og den sistnevnte er den nest mest siterte artikkelen i utvalget vårt.
[4] Denne ble identifisert av våre søk og er godt sitert, men ble utelatt da den ikke er fagfellevurdert.

engasjerer seg i handlinger som cyberspionasje eller skadevare-baserte angrep for å forstyrre en nasjonal kritisk infrastruktur.

Årsaken til denne noe overlappende oppdelingen er at det er ulike proporsjoner på hvor hardt ulike kjønn rammes av ulik type cyberkriminalitet. For eksempel blir kvinner hardere rammet av «hevnporno» enn menn, mens nettsvindel oppleves omtrent likt av begge kjønn. Eksempler på noen typer cyberkriminalitet knyttet til disse kategoriene og operasjonelle engelske definisjoner vises i Tabell 2.

Tabell 2. Eksempler på operasjonelle definisjoner av typer cyberkriminalitet, gjengitt fra Lazarus et al. [15].

Type cyberkriminalitet	Kategori	Operasjonelle definisjoner
Cyberbullying	Psychosocial	*Bullying is intentional, aggressive behaviour, carried out repeatedly against a victim, whereas with cyberbullying, the power imbalance between bully and victim and the repetitiveness of the behaviour typically involved in traditional bullying are often missing from the equation.*
Revenge porn	Psychosocial	*Revenge porn is defined as non-consensual sharing of sexually explicit images and/or videos, whether self- or other-generated, with an underlying motivation linked to revenge.*
Online fraud	Socio-economic	*Online fraud refers to the computer and/or Internet-mediated acquisition of financial benefits by false pretence, impersonation, manipulation, counterfeiting, forgery or any other fraudulent representation of facts.*

Fra Somer [36] sin undersøkelse kan vi også legge til en tre-deling foreslått i Ghernaouti sin bok fra 2013 [77], hvor målet er å skille cyberkriminalitet fra handlinger mer knyttet til krig og terrorisme:

- **Cyberkriminalitet mot mennesker**, som ærekrenkelse, svindel, identitetstyveri og brudd på personvern.
- **Cyberkriminalitet mot verdier/aktiva**, som datatyveri, piratkopiering av programvare, forfalskning, overvåkning og spionering, manipulering av informasjon, tyveri av åndsverk (IP).
- **Cyberkriminalitet mot nasjoner**, som kan involvere destabilisering, informasjonskrig og angrep mot kritisk infrastruktur.

2.3.3 Flere dimensjoner

Europarådets klassifisering av ulovlige handlinger knyttet til cyberkriminalitet er også godt representert i litteraturen. Denne *Convention on Cybercrime,* ofte omtalt som *Budapestkonvensjonen*, ble skrevet i 2001 [16] og trådde i kraft i 2004, og kan sees på som et rammeverk for å etablere nasjonale lover og juridisk samarbeid på tvers av landegrenser. Klassifiseringen er ifølge McGuire [10] den viktigste og globalt mest anerkjente forståelsen av cyberkriminalitet. Per i dag er den ratifisert av 68 land[5], inkludert Norge. Klassifiseringen av lovbrudd, med utvidelser fra 2003 [79], er vist i Tabell 3. Norsk oversettelse av begreper er basert på de norske versjonene av konvensjonen [80] og tilleggsprotokollen [81] fra Lovdata.

[5] Det er verdt å merke seg er at Russland har protestert mot konvensjonen på bakgrunn av den truer nasjonal suverenitet, og prøver å presse gjennom en erstatning via FN [78].

Tabell 3. Europarådets *Convention on Cybercrime* (Budapestkonvensjonen) grupperer straffbare handlinger knyttet til cyberkriminalitet

Straffbare handlinger	Norsk oversettelse
A: Offences against the confidentiality, integrity and availability of computer systems and data	Straffbare handlinger som rammer datasystemers og dataenes fortrolige karakter, integritet og tilgjengelighet
Article 2 Illegal access	Ulovlig tilgang
Article 3 Illegal interception	Ulovlig oppfanging av data
Article 4 Data interference	Inngrep i dataenes integritet
Article 5 System interference	Inngrep i driften av et datasystem
Article 6 Misuse of devices	Misbruk av innretninger og tilgangsdata
B: Computer-related offences (forgery, fraud)	Straffbare handlinger knyttet til datamaskiner
Article 7 Computer-related forgery	Datarelatert falsk
Article 8 Computer-related fraud	Datarelatert bedrageri
C: Content-related offences	Straffbare handlinger knyttet til innhold
Article 9 Offences related to child pornography	Straffbare handlinger knyttet til barnepornografi[6]
D: Offences related to infringements of copyright and related rights	Straffbare handlinger knyttet til krenkelser av opphavsrett og nærstående rettigheter
Article 10 Offences related to infringements of copyright and related rights	Straffbare handlinger knyttet til krenkelse av opphavsrett og nærstående rettigheter
E: Acts of a racist and xenophobic nature committed through computer systems	Kriminalisering av rasistiske og fremmedfiendtlige handlinger begått i et datasystem
Article 3 Dissemination of racist and xenophobic material through computer systems	Spredning av rasistisk og fremmedfiendtlig materiale via datasystemer
Article 4 Racist and xenophobic motivated threat	Rasistisk og fremmedfiendtlig motivert trussel
Article 5 Racist and xenophobic motivated insult	Rasistisk og fremmedfiendtlig motivert fornærmelse
Article 6 Denial, gross minimisation, approval or justification of genocide or crimes against humanity	Fornekting, grov bagatellisering, godtakelse eller rettferdiggjøring av folkemord eller forbrytelser mot menneskeheten
Article 7 Aiding and abetting	Medvirkning

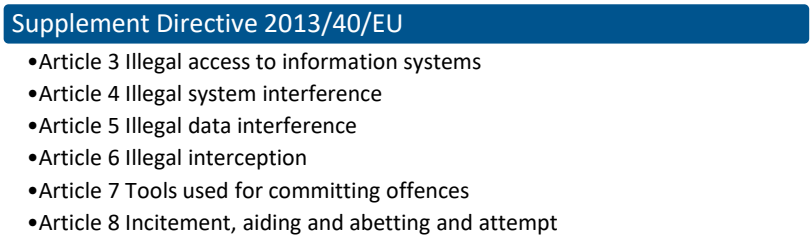
Som påpekt av Broadhead [13], er ikke kategoriseringen til Budapestkonvensjonen ment å være uttømmende, og den raske utviklingen av cyberkriminalitet gjør det lite hensiktsmessig å operere med en streng klassifisering. Europarådets klassifisering har også blitt kritisert for å være utdatert [22], [82], og for ikke å fange opp nye fenomener slik som *spamming*, *cyberbullying/trolling, cyberstalking* og *grooming* i god nok grad. Paoli et al. [4] mener at konseptet «cyber extortion» (vanligvis knyttet til ransomware) ikke er godt nok dekket av konversjonen. Fra vårt utvalg har også Tsakalidis og Vergidis [83] og senere Tsakalidis et al. [84] foreslått en del direkte utvidelser og endringer til Budapestkonvensjonen, blant annet følgende tilleggspunkter:

- Identity theft (under B)
- Trademark-related offences (under D)
- Pornographic material (under C)
- Religious offences (under C)

[6] Som omtalt i seksjon 1.1 bør begrepet erstattes med «seksualiserte skildringer av barn».

- Cyberbullying (under C)
- Illegal gambling and online games (under C)
- Phishing (ny kategori *Combinational offences*)
- Cyber laundering (ny kategori *Combinational offences*)
- Cyberwarefare (ny kategori *Combinational offences*)
- Terrorist use of the Internet (ny kategori *Combinational offences*)

I 2013, publiserte Europaparlamentet og Rådet for Den europeiske union (også kjent som Unionsrådet eller Ministerrådet) et direktiv [85] for å koordinere europeisk lovgivning for straffbare handlinger knyttet til angrep mot informasjonssystemer. Dette direktivet var basert på Budapestkonvensjonen, men inneholdt et mer minimalistisk sett med kategorier slik vist i Figur 5. Siden fokus var på informasjonssystemer, er det tydelig at denne begrenser seg til «cyber-dependent» kriminalitet eller angrep mot informasjonselementer som lagres eller overføres mellom datasystemer.



Figur 5. Europaparlamentets og Rådet for Den europeiske union sin minimalistiske definisjon av straffbare handlinger knyttet til angrep mot informasjonssystemer

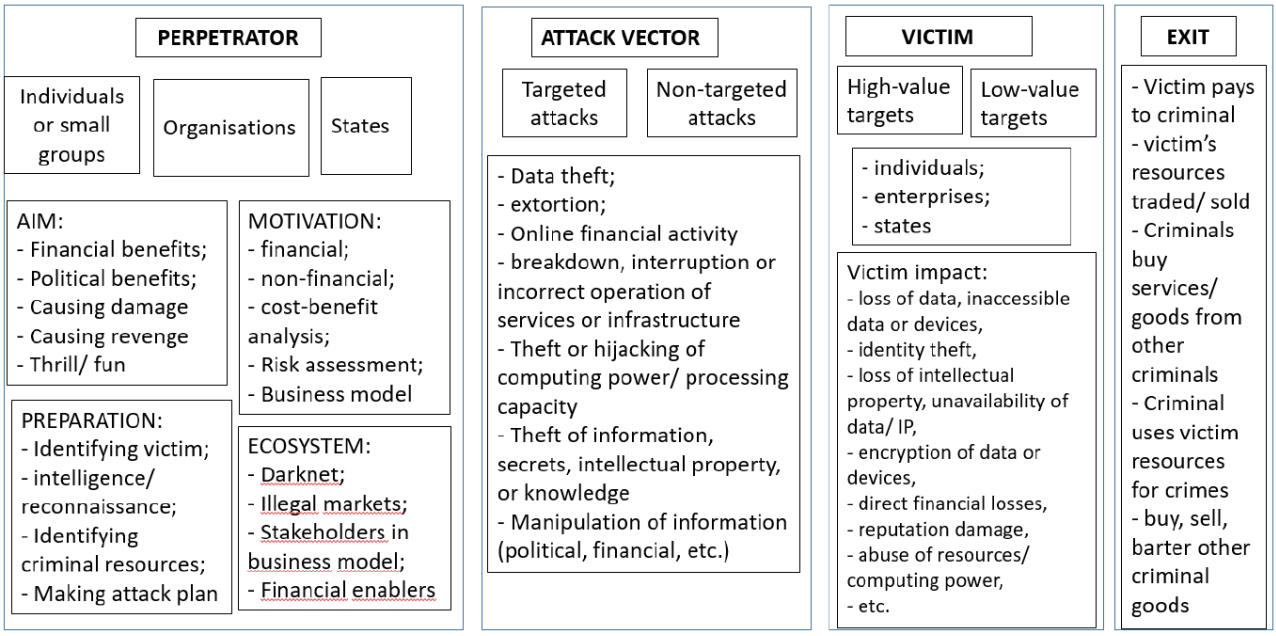
Den britiske *CyberCrime – prosecution guidance* [69], som sist ble oppdatert i 2019, har en bredere og bedre dekning av mange av de nye fenomenene sin klassifisering sammenlignet med Budapestkonvensjonen. I litteraturen ser vi at studier fra Storbritannia (for eks. [68]) gjerne referer til denne. Vi vet også at *the European Data Protection Board* (EDPB) foreslo i 2021 [86] noen konkrete utvidelser til det neste tillegget til Budapestkonvensjonen. Disse er knyttet til personvernbrudd.

Noen forfattere (Cordova et al. [24]) grupperer konsepter i forhold til angripernes mål, for eksempel om det er mot individer eller organisasjoner, for så å bruke mer tradisjonelle begreper som trakassering eller vandalisme. For eksempel, om aktiviteten er rettet mot individer, kan dette igjen spesifiseres om det er mot den bestemte personen eller personens eiendeler:

- **Mot person:** Trakassering gjennom e-post, cyberstalking, spredning av obskønt materiale på internett, ærekrenkelse, hacking og uanstendig eksponering
- **Mot eiendeler:** Datavandalisme, overføring av datavirus, Internett-inntrenging, uautorisert kontroll over datamaskinsystemer og hacking.

Somer [36] lister opp en god del andre taksonomier i sin oversikt, for eksempel en hentet fra boken *the UN Manual on the prevention and control of computer related crime* (1994), samt en god del som går på mer teknologiske aspekter ved cyberkriminalitet. Felles for disse er at de er relativt gamle, og vi har heller ikke sett disse referert til i litteraturen. Somer påpeker at siden cyberkriminalitet er under konstant utvikling, er det vanskelig å ta i bruk noen av de eksisterende taksonomiene for å forstå fenomenet. Derfor foreslår også Somer sin egen variant hvor man beskriver en slags reise (eller prosess) for den kriminelle handlingen, hvor man identifiserer gjerningsperson (*perpetrator*), angrepsteknikk (*attack vector*), offer (*victim*) og avslutning (*exit*) innenfor hver sin dimensjon slik vist i Figur 6. En slik modell kan øke forståelsen av de kriminelle handlingene. Denne kunnskapen kan brukes til å fokusere etterforskning og velge blant motvirkende tiltak,

for eksempel holdningskampanjer, lovendringer, utvikling av ny teknologi, endre adferd hos potensielle offer og overvåkning. Merk at Somer ser bort fra «cyber-enabled crime», og kun tar for seg «cyber-dependent crime».



Figur 6. Somer sin fire-dimensjonale taksonomi for kriminelle «reiser». Figur er gjengitt med tillatelse fra forfatter.

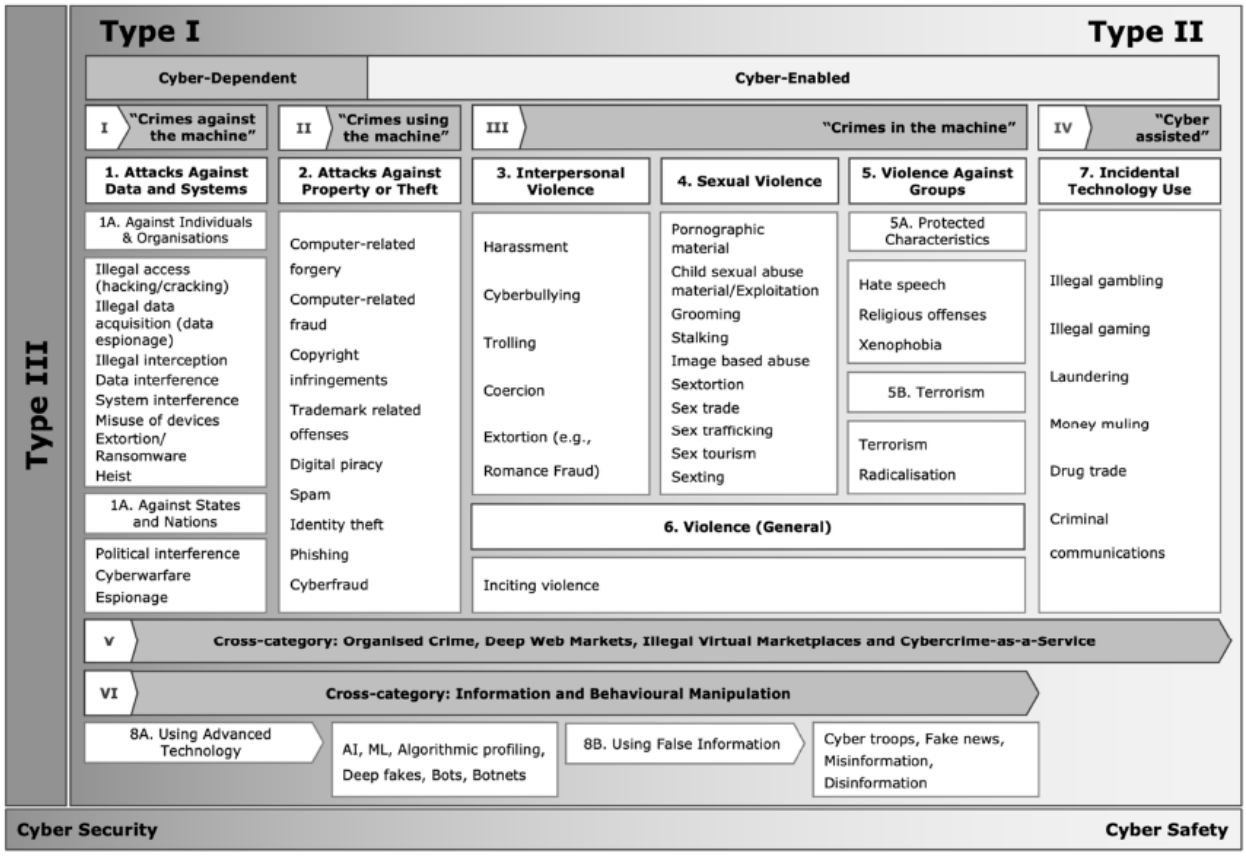
Praktisk utprøving av Somer sin taksonomi og metode for å modellere cyberkriminalitetsprosesser er ikke dokumentert i selve artikkelen, men finnes beskrevet i hennes doktorgradsavhandling fra 2022 [87]. Kort fortalt ble utprøvingen gjennomført med politi fra Estland, Tyskland og Storbritannia, samt cybersikkerhets-studenter ved et Universitet i Estland. Totalt 255 deltagere fikk opplæring og ble observert under pilotforsøk, samt fulgt opp med spørreskjema, diskusjoner i fokusgrupper og semistrukturerte intervju. Responsen fra de fleste deltagerne viste at dette var en nyttig tilnærming, spesielt knyttet til trening og etterforskning. Også Tsakalidis et al. [83] har laget en tilsvarende struktur for å beskrive cyberkriminalitetshendelser, da delt opp i:

- **Hendelsesbeskrivelse:** Som er fritekst.
- **Lovbrudd** (*identified offence*): Hvor underkategoriene er en utvidet versjon av Budapest-konvensjonen.
- **Gjerningsperson** (*offender*): Hvor det skilles på ulike kategorier av individer (bøller, terrorister, innsidere, osv.) og større entiteter (organisasjoner, stater).
- **Tilgangsbrudd** (*access violation*): Som er delt i fysisk tukling, lokal tilgang til datamaskin og fjern-tilgang.
- **Mål** (*target*): På overordnet nivå skille mellom individuelle mål (ulike typer misbruk, som økonomisk, seksuelt, fysisk, mentalt og IKT) eller samfunnet (infrastruktur, nasjonale tjenester).
- **Offer** (*victim*): Hvor det skilles på individ, organisasjon og nasjon.
- **Skade** (*harm*): Som er konsekvensen mot individer (følelsesmessig skade, tap av liv eller eiendom), systemer eller bare delvis/påbegynt skade.

Felles for både Somer og Tsakalidis et al. sine strukturer er at slike beskrivelser er ganske omfattende og mye av informasjonen vil ofte være utilgjengelig. Cyberhendelser er ofte diffuse av natur; det er vanskelig å med

sikkerhet si hvem som står bak, hva som har skjedd, om offeret var tiltenkt mål og hva kortsiktig og langsiktig konsekvens vil være for ulike offer.

Phillips et al. [8] viser også til flere taksonomier for cyberkriminalitet som er brukt opp gjennom årene, men vi har ikke sett at disse har hatt noe særlig gjennomslag. De gir også eksempler på taksonomier som spesialiserer seg på enkelte typer kriminalitet, som *Luxembourg Guidelines* [88] for ulike typer overgrep mot barn. I det tilfellet dekker klassifiseringen ikke bare overgrep som skjer over Internett. På samme måte som Somer, har også Phillips et al. kommet fram til at eksisterende taksonomier ikke holder mål, og at det derfor er best å lage sin egen. Det er verdt å merke seg at denne artikkelen har flere anerkjente forfattere (spesielt Mary Aiken, Stefano Caneppele og Julia Davidson) som har publisert mange artikler innenfor kriminologi over mange år, og tilnærmingen fremstår kanskje som mer solid enn Somer. Phillips et al. sin klassifisering er vist i Figur 7, og er egentlig et forsøk på å slå sammen flere eksisterende taksonomier. På øverste nivå bruker de Gordon og Ford [31] sin glidende skala mellom Type I («cyber-dependent») og Type II («cyber-enabled») langs den horisontale aksen, og så Sarre et al. [74] sin Type III dimensjon langs den vertikale aksen (enkel/dagligdags teknologi øverst, sofistikert teknologi nederst). Som eksempler på Type III nevner Phillips et al. bruk av avansert teknologi som kunstig intelligens, maskinlæring (underkategori av KI), spredning av falsk informasjon, desinformasjon og falske nyheter. Dette er temaer som i liten grad er dekt i utvalget vårt, selv om Jeong [89] nevner at KI bidrar til manipulasjon, svindel og dype forfalskninger («*deepfakes*»). I samme studie omtales også bruken av falske nyheter.



Figur 7. Klassifisering fra Phillips et al. [8]. Figur er gjengitt med tillatelse fra kontaktforfatter.

Inne i figuren gjør de det litt unødvendig forvirrende ved å nok en gang bruke romertall (I-VI) for underkategorier av typer, delvis basert på Wall [41] sine dimensjoner. Underkategori I omhandler *kriminalitet mot datamaskinen*, og inkluderer blant annet spredning av virus, å ta kontroll over datasystemer, datainnbrudd

og tjenestenektangrep. Denne typen cyberkriminalitet er nevnt hyppig i vårt utvalg [8], [18], [24], [26], [36], [68], [71], [83], [90], [91]. Phillips et al. klassifiserer dette innenfor om det er mot individer eller stater, der det i vårt utvalg knyttes mest til individer gjennom offerstudier.

I underkategori II, *kriminalitet ved bruk av datamaskiner*, klassifiserer Phillips et al. som angrep mot eller tyveri av eiendom, og er utbredt dekt i vårt utvalg. Dette er også cyberavhengig kriminalitet, men dreier seg i større grad om svindelforsøk, forfalskning, piratkopiering, spredning av spam, identitetstyveri og lignende med bruk av datateknologi [8], [9], [15], [18], [26], [32], [36], [39], [42], [59], [90], [91], [92], [93], [94], [95], [96].

Underkategori III dreier seg om *kriminalitet som foregår i datamaskinen*, og setter søkelys på mellom-menneskelig vold i cyberdomenet. Her inngår hendelser som trakassering og mobbing på nett, tvang, trolling og romantisk svindel [4], [10], [17], [22], [23], [40], [96] [107]. Kriminalitet i maskinen omhandler også blant annet seksuell vold, som overgrepsmateriale, *stalking*, *grooming* eller annen ulovlig seksuell adferd i cyberspace. Type kriminalitet nevnt i utvalget vårt dreier seg om overgrepsmateriale mot voksne og barn, og er nevnt i følgende studier [4], [10], [17], [21]–[23], [28], [33], [40], [54], [58], [96], [105], [108], [110]. Vold mot grupper i cyberdomenet er lite nevnt av utvalget, men to studier nevner hatefulle ytringer [8], [90], hvorav bare Phillips et al. [8] nevner religiøs vold. I motsetning er cyberterror nevnt av en rekke studier i utvalget [8], [18], [24], [36], [71], [93], [94], [97].

Underkategori IV betegnes som *cyber-assistert*, og omhandler kriminalitet som gjøres med tilfeldig teknologibruk. Her inkluderer Phillips et al. ulovlige gambling og spilling, hvitvasking, salg av narkotiske stoffer og online kriminelle nettverk. Disse temaene er i liten grad dekt i det innsamlede utvalget, mens salg av narkotiske stoffer er nevnt i to studier [8], [71].

Underkategoriene V og VI går på tvers av den horisontale aksen ettersom de kan inneholde elementer fra alle over eller stå for seg selv. Nederst på den horisontale aksen har de inkludert nødvendigheten av typen beskyttelsestiltak, altså at til venstre må man tenke «cyber security», mens til høyre mer i retning «cyber safety».

3 Omfang

3.1 Måling av omfang i studiene

Rundt halvparten av artiklene fra utvalget har måling av omfang som problemstilling helt eller delvis. For å måle omfang av cyberkriminalitet kan en rekke ulike metoder benyttes. Befolkningsundersøkelser, offer-studier, casestudier og metastudier er eksempler på metoder som benyttes i litteraturen.

Noen studier benytter data samlet inn av større befolkningsundersøkelser eller samler inn og sammenfatter eksisterende datasett fra ulike kilder for å få tilstrekkelig datagrunnlag til å kunne si noe om omfang. Metastudier kan på samme måte avhjelpe utfordringer knyttet til innsamling av data, ved at en benytter eksisterende studier for å si noe om forskningen på feltet. Cyberkriminalitet er utfordrende å måle fordi det er et svært omfattende og uavgrenset fenomen og fordrer store systematiske undersøkelsesmetoder og datasett. I tillegg forblir mange hendelser uoppdaget eller aldri registrert, noe som gir hull i dataene, samt at cyberkriminelle gjerne forfalsker sine spor, som kan gi feil dataene.

Befolkningsundersøkelser er ofte større nasjonale eller internasjonale spørreundersøkelser som blant annet kan si noe om en befolknings internettvaner, holdninger til cyberkriminalitet eller hvor stor andel av en befolkning som er utsatt for kriminalitet. I noen tilfeller kan disse identifisere utvalg som kan undersøkes videre for å finne tendenser innenfor en gruppe, som eksempelvis ofre for kriminalitet. Videre undersøkelser

rettet inn mot slike grupper går under kategorien offerstudier, og undersøker for eksempel hvordan viktimiseringen innvirker på dem og hvordan de eventuelt responderer. Offerstudier er altså undersøkelser rettet mot individer eller grupper i befolkningen, som sammenfatter disses opplevelse av et fenomen eller hendelser og kan si noe om hvordan det oppleves å bli utsatt for eksempelvis kriminalitet.

Måling har i stor grad søkelys på viktimisering (gjennom bl.a. befolkningsstudier) og analyser av tall for rapportering og anmeldelse. Det er ofte antagelser om mørketall, og en betydelig utfordring ved å måle omfang er derfor knyttet til manglende rapportering og anmeldelse. Kriminalitet som påfører verditap synes å i større grad anmeldes mens trakassering, særskilt seksuell trakassering, sjeldnere rapporteres eller anmeldes [23]. Det antas at underrapportering skyldes manglende kunnskap om rettigheter og hva som er lovbrudd, og stigma knyttet til seksuell trakassering og såkalt kjærlighetssvindel. Rapporteringsgraden ser generelt ut til å øke i takt med kriminalitetens alvorlighetsgrad, men økningen er noe mindre for hendelser i cyberrommet enn ikke-cyberrelaterte hendelser [31]. Utfordringene ved rapportering og mørketall fremstår todelt, der (manglende) anerkjennelse i statsapparat, næringsliv og rettssystem later til å være én del av det, og kunnskap om rettigheter knyttet til cyberkriminalitet i befolkningen en annen.

Kvalitative metoder er gjerne ikke best egnet for måling av omfang. Likevel, kan personer med særskilt erfaring eller ekspertkompetanse på et smalt felt være gode kilder for å si noe om utbredelse av et fenomen innenfor gitte forhold ved hjelp av intervjuer, casestudier og tematisk analyse. Disse metodene treffer smalere enn de ovenfornevnte, men kan like fullt si noe om omfanget av cyberkriminalitet ut ifra relevante saker eller kompetanse som sammenfatter kunnskap som ikke er tallfestet.

I alt beskriver litteraturen et omfang i bred målestokk, som anslag om *økonomisk tap* eller *psykososiale konsekvenser* for individer og samfunn. Der måling i seg selv er tema for forskningen, begrunnes det blant annet med stadige og raske endringer i det «digitale offerbildet» samt manglende universelle definisjoner og konsensus om konseptet cyberkriminalitet [98]. I det videre fremlegges en oversikt over hvilke metoder som er benyttet for å måle ulike størrelser av omfang av cyberkriminalitet i utvalget (Tabell 4). Deretter følger mer inngående beskrivelser av de publikasjonene som vi mener bidrar med betydelig empiri til kunnskap om omfang, og en vurdering av metodene som er benyttet.

Tabell 4. Oversikt over litteratur i utvalget som omhandler måling av omfang

Publikasjon	***Hva* måles?**	***Metode* for måling**
Abdulai [99]	Frykt for å bli offer for cyberkriminelle handlinger.	Offerstudie, online spørreundersøkelse blant studenter ved et universitet i Canada. 462 respondenter. Binær logistisk regresjon brukt for å forutsi frykt for cyberviktimisering sett i sammenheng med tidligere viktimisering og sosioøkonomisk bakgrunn.
Akdemir et al. [22]	Undersøkelse av politiets utfordringer med håndtering av økonomisk cyberkriminalitet i UK, spesielt når handlingene skjer over landegrenser.	Tematisk analyse av data fra semistrukturerte intervju med politi (10) i cyberkriminalitets-avdelinger og eksperter i IT-avdelinger (3) hos lokale myndigheter.
Amro [46]	Effekter av cyberkriminalitet på individer i Palestina – følelser og konsekvenser.	Spørreundersøkelse, 300 individer.
Anderson et al. [39]	Total samfunnsøkonomisk kostnad og utvikling fra 2012 til 2019 av ulike typer cyberkriminalitet: 1) tradisjonelle kriminalitetstyper som svindel eller falsk, men datarelatert, 2) publikasjon av ulovlig innhold og 3) kriminalitet unik for elektroniske nettverk.	"Best mulig grunnlag" (best-efforts basis). Data fra ulike kilder. Den samfunnsøkonomiske kostnaden er summen av direkte tap (inkl. kriminell vinning/ fortjeneste), indirekte tap og kostnader knyttet til forebygging.

Publikasjon	*Hva* måles?	*Metode* for måling
Ardiansyah og Amri [100]	Juridiske begreper og cyberkriminalitetsfenomener under COVID-19-pendemien i Indonesia. Omfang av ulike typer cyberangrep.	Kvalitativ studie. Analyserer ulike fenomener fra sekundære datakilder som bl.a. nettbaserte nyhetsmedier og journaler.
Breen et al. [98]	Cyberviktimisering knyttet til seks typer cyber-kriminalitet blant amerikanere: Bank- eller kreditt-kortsvindel, manglende levering av kjøpte varer, utpressing, svindel knyttet til forskuddsgebyrer, uteblivelse av betaling og overbetalingssvindel.	Befolkningsundersøkelse, total n= 11 953 som besvarte nettbaserte spørreskjema.
Broadhead [13]	Total kostnad i millioner USD av cyberkriminalitet for virksomheter for syv land i hhv 2016 og 2017, samt prosentvis økning mellom årene, årlig kostnad per industri 2017, samt hva kostnadene er forbundet med for 2015, 2016 og 2017.	Bruker tall fra en undersøkelse av Ponemon Institute – deskriptive data av faktiske kostnader pådratt enten direkte eller indirekte som følge av faktiske detekterte cyberangrep. Data for 2017 fra respondenter fra 254 virksomheter i 15 sektorer i syv land.
Correia [101]	Få mest mulig ut av rapporteringsdata om nett-kriminalitet og svindelkriminalitet: en casestudie av *UK Action Fraud* (AF).	To studier basert på utvalg av AF-data knytet til kriminalitetsrapporter fra Walisisk politi mellom 2014 og 2020: 1) Sårbarhet og gjentakende viktimisering basert på 17 049 kriminalitets-rapporter – mixed methods. 2) COVID og påvirkning på svindel og "computer misuse" - utforskende studie.
Farahbod et al. [102]	Cybersikkerhetsindekser og cyberkrim, årlig tap og økonomiske virkninger. Utforsker forholdet mellom cyberangrep og faktorer som kan forutsi virkningen av slike angrep innenfor forsynings-kjededomener.	Bruker ICT Development Index (IDI), Global Cybersecurity Index (GCI), National Cyber Security Index (NCSI), og måler forholdet mellom ulike lands årlige cyberkrim-tap og BNP.
Furnell og Dowling [14]	Gjennomgår data om omfang og virkninger av cyberkriminalitet, inkludert ulike tilnærminger til å definere og måle det.	En gjennomgang og analyse av undersøkelses-bevis brukes for forståelse av omfanget av cyberkriminalitet og effekten på ofre.
Gañán et al. [103]	Økonomisk virkning av cyberkriminalitet.	Rammeverk for systematisk identifisering kort- og langsiktige konsekvenser av cyberkriminalitet for aktører og samfunn.
Graham et al. [32]	Vilje til å rapportere cyberkriminalitet versus annen kriminalitet.	Bruker Amazons MTurk-program for deltakelse i undersøkelser. Ber 534 respondenter vurdere ti kriminelle hendelser og anslå sannsynlighet for rapportering til politiet samt tro på at politiet vil identifisere og arrestere lovbryter.
Hawdon et al. [104]	Hvordan pandemi har påvirket frekvensen av cyberviktimisering. Benytter seg av rutine-aktivitetsteori.	Sammenligner pre- og postpandemiske rater for ofre ved bruk av datasett samlet inn med Dynata (tilfeldig sifferoppringing). 1 109 respondenter pre- og 1 021 post-COVID-19.
Junger et al. [96]	Sammenheng mellom internettbruk og sosioøkonomiske forhold og tre former for cyberkriminalitet: 1) netthandelsvindel, 2) svindel med nettbank og 3) cyberangrep (her DDoS).	Måler hvilken aktivitet og adferd som er typisk for cyberofrene blant de 17 811 respondentene i Europabarometeret.
Kemp et al. [92]	Endringer i omfang av rapportert cyberkriminalitet og svindel under COVID-19-pandemien.	Tidsserieanalyse av historiske data rapportert til Action Fraud i perioden 2017-2020.
Kemp et al. [105]	Faktorer assosiert med virksomheters rapportering av cyberkriminalitet.	Analyserer data fra UK Cyber Security Breaches Survey (CSBS). Utvalg av virksomheter n = 1 519 (2018), 1 566 (2019) og 1 348 (2020).
Khiralla [106]	Statistikk over cyberkriminalitet 2016-2020.	Sammenstilling av statistikk fra ulike kilder.
Lallie et al. [68]	Omfanget av cyberkriminalitet (mer konkret cyberangrep) globalt under COVID-19-pandemien.	Etablere en tidslinje som kartlegger spredningen av angrep under pandemien basert på artikler fra store mediehus som BBC og Reuters, blogg-innlegg, innlegg fra sosiale medier og sikkerhets-firmaer.

Publikasjon	*Hva* måles?	*Metode* for måling
Leukfeldt et al. [107]	En vurdering av konseptualiseringen av finansiell nettkriminalitet som organisert kriminalitet.	Case-studie, systematisk analyse av 40 saker fra ulike land. Data fra 18 politietterforskningsfiler.
Näsi et al. [90]	Cyberviktimisering ift. sosioøkonomiske forhold, tidligere opplevelser av cyberkriminalitet og individers nettaktivitet.	Befolkningsundersøkelse i Finland med 5 455 respondenter, distribuert som del av nasjonal krimundersøkelse.
Paoli et al. [4]	Cyberkriminalitet sin innvirkning på forretnings-virksomhet.	Nettbasert spørreundersøkelse/survey i Belgia.
Riek og Böhme [108]	Kostnaden av forbrukerrettet cyberkriminalitet.	Offerstudie, telefonintervjuer med 1 242 ofre identifisert i en større undersøkelse av tilfeldig utvalg internett-brukere i seks EU-land.
Shan-A-Khuda og Schreuders [42]	Forholdet mellom demografi av ofre for cyber-kriminalitet og karakteristikker ved ofrenes boligområde for fire kategorier cyberkriminalitet: 1) *Harassement/ Unwanted contact*, 2) *Fraud/ Theft/Handling*, 3) *Sexual/Incident*, 4) *Other*	Bruker data fra registrerte cyberkriminalitets-hendelser fra et av Englands største politistyrker fra en treårsperiode. Offerdatasett på 5 270 individer.
Srivastava et al. [28]	Påvirkning av økonomisk kapital og teknologisk kapital på frekvensen av cyberkriminalitet i et land. Presenterer et rammeverk som forklarer frekvensen av cyberkriminalitet i et land.	Analyserer data fra mange ulike kilder fra 124 land.
Van de Weijer et al. [91]	Rapportering av cyberviktimisering - basert på hypotetisk viktimisering.	Utvalg på 595 individer presentert for tre hypotetiske scenarier og bedt om å forestille seg at de selv var utsatt for viktimiseringen. Regresjonsanalyse av respondentenes intensjon om å rapportere mot andre faktorer.
Woods og Walter [109]	Gjennomgang av estimater for ofre for cyber-kriminalitet og cyberrisikosannsynlighet.	Metastudie basert på 48 studier fra akademia, statistiske institutter og cybersikkerhets-leverandører, inkludert offerundersøkelser, sakskontrollstudier og forsikring.

En av de største offerstudiene i utvalget er en amerikansk spørreundersøkelse med 534 respondenter, der vilje til å rapportere eventuelle hendelser er forsøkt målt [32]. Med hensyn til utfordringer ved egen-rapportering av faktiske opplevelser, har forskerne i denne studien valgt å vinkle spørsmålene mot konstruerte hendelser som respondentene ikke nødvendigvis har vært utsatt for. Det er vanskelig å avgjøre om respondentenes svar på hva *de ville ha gjort* i en gitt situasjon samsvarer med virkeligheten for dem som opplever det, men det er i alle tilfelle en måte å sikre et stort utvalg på og samtidig redusere bias fra stigma eller andre følelser som kan oppstå som resultat av å bli utsatt for kriminalitet. Studiens formål er dessuten å måle om ofre for kriminalitet utviser en *forskjell* i rapporteringsvilje knyttet til om hendelsen skjer i det digitale eller fysiske rom. Med måling av forskjellen som utgangspunkt reduserer forskerne en av de kjente svakhetene ved egenrapportering, fordi et samsvar mellom respondentenes egenoppfatning og virkeligheten ikke er utgangspunkt for hva som måles. Undersøkelsen fremla flere sammenlignbare eksempler på digital og ikke-digital kriminalitet for respondentene, og resultatet viser en noe større rapporteringsvilje ved ikke-digitale hendelser og lavere tiltro til politiets håndtering (identifisering og pågripelse av gjerningsperson) for kriminalitet i det digitale rom.

En annen befolkningsundersøkelse av cyberkriminalitet er gjennomført i Finland, med 5 455 respondenter i alderen 15 til 74 år (Näsi et al. [90]). Målet med studien er å undersøke cyberviktimisering sett opp mot variabler som sosioøkonomiske forhold, tidligere opplevelser av cyberkriminalitet (polyviktimisering) og personens aktivitet på internett. Undersøkelsen ble distribuert som del av den finske nasjonale kriminalitets-undersøkelsen i 2018 og kartla gjennom denne ulike typer cyberkriminalitet, som phishing, cybersvindel, identitetstyveri, skadevare, hacking, seksuell og annen trakassering, brudd på personvernrettigheter, ærekrenkelse og trusler på nett. Resultatet viser at skadevare, trakassering, seksuell trakassering, hacking og svindel er de vanligste former for cyberkriminalitet, og at digitale rutiner, eksponering for mulige lovbrytere, sammen med tidligere offeropplevelser, er betydelige risikofaktorer for viktimisering av en rekke

ulike typer kriminalitet på nett. Denne undersøkelsen utviklet altså et eget batteri spørsmål som ble lagt til en eksisterende befolkningsundersøkelse for å få mer ut av denne og sørge for at forskningen gir tidsriktig og nyttig informasjon i tråd med teknologisk utvikling og integrering. På grunn av lignende kontekst som Norge kan denne type undersøkelse være relevant å undersøke nærmere [110].

Breen et al. [98] har gjennomført en nokså omfattende befolkningsundersøkelse i USA knyttet til seks spesifikke typer cyberkriminalitet rettet mot individer knyttet til økonomisk tap. Totalt svarte 11 953 respondenter over 18 år på denne i løpet av juli-september 2020, og utvalget representerte 97% av husholdningene i USA. Noen av respondentene (n=1 002) fikk full undersøkelse, men et større utvalg (n= 10 951) fikk først listen over de seks kriminalitetstypene og ble videresendt til subsett med spørsmål knyttet til de fire mest sjeldne dersom de svarte ja på å ha opplevd minst en av dem. Oppsummert tyder resultatene på at sjansen for å bli utsatt for kredittkort- eller banksvindel var rundt 12,1%, mens bare 1,08% har et reelt økonomisk tap som følge. Sjansen for å bli utsatt for manglende levering av kjøpte varer var rundt 3,2%, mens de andre typene (utpressing, forskuddsgebyr, uteblivelse av betaling, overbetaling) var alle under 0,4%. Av de som faktisk fikk et økonomisk tap lå medianen av dette på $300 eller under (utpressing var ikke tatt med i dette estimatet). Spredt på hele befolkningen taper en gjennomsnittsamerikaner under $7 årlig grunnet disse seks typene cyberkriminalitet. Ifølge FBI *Internet Crime Complaint Center* (IC3) [111] utgjør disse 30% av cyberkriminalitet mot individer, så alle former koster dermed en amerikaner i underkant av $23 i gjennomsnitt. Forfatterne har også kombinert sine data med andre Europeiske undersøkelser, og anslår da at for eksempel sjansen for kredittkort- eller banksvindel ligger på mellom 3,5% og 12,5%, mens sjansen for faktisk å tape penger fra dette er under 1,1%. De andre typene var tilsvarende lave.

Med utgangspunkt i den økende bekymringen for forbrukerrettet cyberkriminalitet, presenterer Riek og Böhme [108] en undersøkelse som eksplisitt spør om cyberkriminalitetsrelaterte tap og kostnader ved beskyttelse. Studien er en offerstudie gjennomført i form av telefonintervjuer med 1 242 ofre identifisert i en større undersøkelse av tilfeldig utvalg internett-brukere i seks EU-land. Ifølge resultatene er det forbrukere i UK som har tapt mest penger til cyberkriminalitet de siste 5 årene før studien, og også pådratt seg det største totale tapet, mens det er forbrukere i Tyskland som bruker mest penger på beskyttelsestiltak. Samlet sett er kostnadene ved beskyttelsestiltak klart større enn tap ved faktiske cyberkriminalitets-hendelser. Forfatterne beskriver selv de vanligste utfordringene med spørreskjemabasert kostnads-estimering. For eksempel er det få berørte og tapene er konsentrerte, noe som medfører at estimatene kan være basert på et lite antall respondenter. De tar høyde for statistiske utfordringer i sitt design, og argumenterer for at funnene fra deres studie gir kunnskapsbasert innsikt som er til nytte for utforming av spørreskjema og dataanalyse i fremtidige målinger av forbrukerrettet cyberkriminalitet.

Abdulai [99] gjennomførte en offerstudie på Saskatschewan University i Canada. Dette var en undersøkelse av innvirkningen tidligere offeropplevelse har på frykten for å bli offer for cyberkriminelle handlinger i fremtiden. Utvalget besto i totalt 462 studenter, og undersøkelsen ble gjennomført som en online spørre-undersøkelse som samlet demografiske data og spurte om respondenten noen gang hadde vært engstelig for å bli offer for kreditt-/debetkortsvindel. Forfatteren brukte binær logistisk regresjon for å forutsi frykt for cyberviktimisering. Studien viste at studenter med tidligere offeropplevelser rapporterte større frykt for å bli offer for cyberkriminelle handlinger enn andre. Sosiodemografiske faktorer og kunnskap om cyber-kriminalitet var derimot ikke signifikante årsaksvariabler. Denne studien har noen klare begrensninger, noe forfatteren selv også påpeker. For det første ble det ikke brukt et tilfeldig utvalg av respondenter, noe som gjør at man må være forsiktig med generalisering av funnene, og det er heller ikke oppgitt en svarprosent. For det andre er studien basert på en student-populasjon, som ikke nødvendigvis er representativ for den generelle befolkningen. Studien kan være til inspirasjon for hvordan man kan måle ulike variablers innvirkning på frykt for cyberviktimisering i Norge.

Akdemir et al. [22] presenterer funn fra en undersøkelse av det britiske politiets utfordringer med håndtering av økonomisk cyberkriminalitet i UK, særlig med fokus på handlinger som skjer over landegrenser. Forfatterne har gjort en tematisk analyse av data fra ti semistrukturerte intervjuer med politibetjenter som jobber i cyberkriminalitetsavdelinger og tre semistrukturerte intervjuer med eksperter som jobber i IT-avdelinger hos lokale myndigheter. Analysen indikerer at økonomisk kriminalitet er et multidimensjonalt og komplekst tema som angår både nasjonale og internasjonale aktører i tillegg til politiet. Manglende internasjonalt samarbeid er fremhevet som den største utfordringen knyttet til teamet. Det anerkjennes at ikke-europeiske land er tilbakeholdne med å dele informasjon om online gjerningspersoner. Videre påpeker en av respondentene at mange ikke forstår forskjellen mellom lovbruddet, trusselen og risikoen, og hevder at 50% av lovbruddene er *cyber-enabled* eller *cyber-dependent* (forklart i seksjon 2.3.1), men at folk i de fleste tilfellene ikke er klar over det. Denne undersøkelsen er ikke basert på et stort utvalg, men som påpekt tidligere i dette kapittelet, kan personer med særskilt erfaring eller ekspertkompetanse utgjøre gode kilder til å forstå et fenomen.

Blant studier som bruker eksisterende data for måling i ny studie, finner vi Anderson et al. [39] som måler den totale samfunnsøkonomiske kostnaden av ulike typer cyberkriminalitet, samt endinger av disse fra 2012 til 2019. Forfatterne jobber etter et "best mulig grunnlag" (*best-efforts basis*) og henter data fra ulike kilder. Det påpekes at måling ikke nødvendigvis er rett fram, da cyberkriminalitet ofte krysser ulike jurisdiksjoner og at tilgjengelige statistikker er fragmenterte. For noen kriminalitetstyper (f.eks. kortsvindel) har man tall kun fra enkeltjurisdiksjoner, mens for andre (f.eks. svindel knyttet til kryptovaluta) har man kun globale tall som skaleres opp eller ned. Den samfunnsøkonomiske kostnaden regnes som summen av direkte tap, inkludert kriminell vinning/fortjeneste (*criminal revenue*), indirekte tap og kostnader knyttet til forebygging. De to sistnevnte er imidlertid vanskelig å attribuere til individuelle kriminalitetstyper. Oppsummering av kostnad og trender for hovedkategorier er oversatt og presentert i Tabell 5 (her benyttes litt ulike geografiske områder).

Tabell 5.Oppsummering av hovedkategorier av cyberkriminalitet, gjengitt fra Anderson et al [39].

Type cyberkriminalitet brukt av forfatterne	Verdi	Endring fra 2012 til 2019
Online kredittkortsvindel (*Online credit card fraud*)	£731.8 mill. (UK)	Svak nedgang i prosent av turnover
Online banksvindel (*Online bank fraud*)	£121.4 mill. (UK)	Økte kostnader, men økt aktivitet
Autorisert push-betalingssvindel (*Authorized push payments*)	£236 mill. (UK)	Ny kategori siden 2012
«In-person» kortsvindel (*In-person card fraud*)	£158 mill. (UK)	Har økt, men kan ha nådd toppen
Løsepengevirus (*Ransomware*)	Godt over $10 mill.	Stor økning
Kriminalitet knyttet til kryptovaluta (*Cryptocrime*)	$2 mrd.	Var ikke et tema i 2012
Annonsesvindel (*Ad fraud*)	Noen få $mrd.	Økning, ingen gode offentlig data
Ulisensierte legemidler eller patentinngrep (*Pharmaceuticals*)	Titalls $mill.	Nedgang
Kupongsvindel (*Coupon fraud*)	$300+ (US)	Ikke diskutert i 2012
«Lojalitetsprogram»-svindel (*Loyalty-program fraud*)	$235 mill.	Ny siden 2012
Svindel knyttet til kjøp av reiser (*Travel fraud*)	$1 mrd.	Ny siden 2012
Forfalsket programvare (*Counterfeit software*)	Noen få $mill.	Synkende trend
Tyveri av materiale med opphavsrettigheter (*Copyright t*heft)	Noen få titalls $mill.	Drastisk nedgang
Falske antivirusprodukter (*Fake antivirus*)	$7.1 mill. (US)	Sunket med 90%
«Teknisk støtte»-svindel (*Tech support scams*)	$39 mill. (US)	Rask økning
Kompromittert e-post (*Compromised email*)	-	Ikke tall fra 2012
Falske firma/virksomheter (*Fake companies*)	Titalls $mill.	Få gode tall
Svindel knyttet til forskuddsgebyrer (*Advance fee fraud*)	Få hundretalls $mill.	Ingen gode estimater
Kompromittert bedrifts-e-post (*Business email compromise*)	-	Ikke tall fra 2012
Telefonsvindel (*Telecoms fraud*)	$7 mrd.	Klar nedgang
Wannacry / NotPetya (*Wannacry / NotPetya*)	$1-2 mrd.	Engangshendelser
Skatte- og velferdssvindel (*Fiscal fraud*)	Mange $mrd.	Ikke inkludert i 2012
Kjærlighetssvindel (*Romance fraud*)	$143 mill. (US)	Flere rapporter i 2019 enn i 2012

Fra denne tabellen er det interessant å se at verdien på skatte- og velferdssvindel er den typen cyber-kriminalitet som koster samfunnet mest, hver borger rundt noen hunder dollar per hode i året. Det er slik at juks i elektroniske skattemeldinger regnes som «*computer crime*», så til sammen blir dette store summer bare basert på data fra Storbritannia og USA. Til sammenligning koster nettbasert kredittkort- og banksvindel hver borger noen titalls dollar i året. Kostnaden for løsepengevirus ser overraskende lav ut, til tross for at dette har en stor aktivitet. Dette skyldes nok at målingene er basert på faktiske innbetalinger som spores gjennom transaksjoner i kryptovaluta, og ikke hva det koster individer og organisasjoner i indirekte tap, for eksempel driftsstans og gjenoppretting av data. Kriminalitet knyttet til kryptovaluta er derimot betydelig av størrelse, hvor de som driver tjenester som oppbevarer eller veksler penger for kunder stikker av med verdiene (*exit scam*).

Anderson et al. [ibid.] syntetiserer også funn fra mange befolkningsundersøkelser fra flere land. Interessante funn fra England og Frankrike tyder det på at rundt halvparten av all vinningskriminalitet (*property crime*) foregår over nett. Flere ulike befolkningsundersøkelser i USA viser derimot at nettbasert vinningskriminalitet har distansert den tradisjonelle varianten. En sammensatt studie i Belgia, med både individuelle offer og organisasjoner, la fram at skadevare (*malware*) genererte flest offer, mens svindel/bedrageri utgjorde de største tapene. Tallene for svindel ligger over typiske akademiske undersøkelser, men godt under det de benevner som skremselspropaganda fra kommersielle sikkerhetsselskaper. Forfatterne slår i hjel offisielle uttalelser om at den totale mengden kriminalitet har gått ned de siste ti årene, og legger fram tall om at selv om fysisk kriminalitet har gått ned, har cyberkriminalitet økt mye mer. Det er derimot en forskjell i typen kostnader som følge av disse endringene. Da man ved fysisk kriminalitet hadde tap knyttet til den direkte tapsverdien til for eksempel en bil eller sykkel, dominerer indirekte kostnader og beskyttelseskostnader innenfor cyberkriminalitet.

I andre studier som måler cyberkriminalitet i Storbritannia brukes ulike typer nasjonale data. En studie gjort av Kemp et al. [105] bruker 2018-, 2019- og 2020-data fra *the UK Cyber Security Breaches Survey (CSBS)* av det britiske *Departementet for digital, kultur, media og sport* for å undersøke faktorer knyttet til virksomheters rapportering av cyberkriminalitetshendelser. CSBS gir en oversikt over cybersikkerhets-lovbrudd [112], og er designet til å samle inn informasjon fra et tilfeldig utvalg av firmaer og veldedige organisasjoner på tvers av regioner, størrelse og sektorer hvert år. Kemp et al. analyserer data basert på virksomheter som har rapportert at de har vært utsatt for minst én hendelse de siste 12 månedene, altså fra 43,9%, 33,6% og 50,4% av utvalget fra henholdsvis 2018, 2019 og 2020. En sammenstilling av dataen viser at den vanligste rapporterte cybersikkerhetshendelsen er mottak av svindel-e-poster eller å bli ledet til svindelrelaterte nettsider (34,5%), at noen utgir seg for å være virksomheten i eposter eller på internett (12,0%) og at datamaskiner blir infisert med virus, spionvare eller skadevare (8,8%). Resultatene fra studien indikerer at typen cyberkriminalitet er relevant for beslutningen om å rapportere, samt at sannsynligheten for å rapportere cyberkriminalitet er større når hendelser har negativ innvirkning og når virksomheten prioriterer cybersikkerhet høyt.

En annen studie gjort av Kemp et al. [92] bruker tidsserieanalyse av cyberkriminalitet og svindeltrender under COVID-19 i Storbritannia, og benytter seg av en rekke nasjonale kilder for å måle dette. De bruker individdata fra 2017 til 2020, samlet inn fra *City of London Police* og *National Fraud Intelligence Bureau* gjennom *UK Action Fraud* – som er det britiske nasjonale rapportsenteret for svindel og cyberkriminalitet. I tillegg bruker de nasjonale data fra *Office for National Statistics* (2020) [113], flydata fra *Civil Aviation Authority* (2020), og kinodata fra *UK Cinema Associasjon* [114], [115]. Resultatene fra denne analysen viser at omfanget av både cyberkriminalitet og svindel har økt, men at endringer i viktimisering ikke var lik på tvers av typer svindel og offer.

Correia et al. [101] bruker også data *UK Action Fraud* (AF), og foretar to studier av data fra et antall politirapporter i Wales for perioden 2014-2020. Den ene studien har fokus på sårbarheter og poly-viktimisering, og den andre på virkningen av svindel og datamisbruk i Wales under Covid-pandemien med søkelys på rapporteringsmønstre og offermedvirkning. Datagrunnlaget for førstnevnte utgjør 17 049 saker i perioden 2014-2016, mens den andre studien omfatter 11 934 saker i en periode i 2020. Forfatterne erkjenner at en betydelig svakhet ved å benytte politirapporter er de store mørketallene for rapportering, som kan forårsake et skjevt eller uriktig bilde. To aspekter ved dette er at offeret selv må erkjenne viktimisering og ha kunnskap om kriminalitet for å rapportere, og at politiet i andre instans må ha tilstrekkelig kunnskap til å vurdere hendelser for at disse registreres som kriminalitet.

Også relatert til COVID-19, ser Hawdon et al. [104] på cyberviktimiseringsrater før og etter pandemien for å finne ut om pandemien endret omfang av cyberkriminalitet som følge av blant annet at folk tilbragte mer tid hjemme. I denne undersøkelsen er viktimiseringen begrenset til å skulle ha funnet sted i løpet av de siste 12 månedene. De bruker to datasett, et fra tiden før pandemien og et fra tiden etter, for så å sammenligne disse. Respondentene her ble spurt om de hadde opplevd syv ulike typer cyberkriminalitet, blant annet tap av penger som følge av svindel, at noen andre har misbrukt deres identitet til å åpne bankkonto, om ukjente transaksjoner i bankkonto, sårende kommentarer på nett og uønsket seksuell oppmerksomhet. Slik konkretisering av spørsmål virker nyttig, da det i alle fall er mulig å identifisere hva folk opplever. Men igjen er respondentenes tolkning sentral; uspesifiserte transaksjoner i kontoutskrift kan ofte være legitime selv om brukeren ikke gjenkjenner dem, og kommentarer som er uønsket og sårende kan også være innenfor loven. Denne undersøkelsen studerer viktimisering, men er ikke forpliktet til å gjøre mål om kriminalitet. Problemet med spørsmål som gir rom for tolkning er heller at denne kan variere stort mellom individer. Spørsmål knyttet til egenbeskyttelse gir derimot mer konkrete mål, da disse spørsmålene går mer direkte på handling, som om en har dekket til kamera eller installert antivirusprogram.

Junger et al. [96] bruker data fra Europabarometeret for å se spesielt på kriminalitet rettet mot netthandel, nettbankbrukere og cyberangrep (som eksempelvis distribuerte tjenestenektangrep mot større aktører), for deretter å måle dette opp mot sosioøkonomiske faktorer og nettvaner. Intervjuene i Europabarometeret ble gjennomført ansikt-til-ansikt hjemme hos intervjupersonene i de enkelte landene, og tilpasset de ulike nasjonale språk. Der CAPI (*Computer Assisted Personal Interview*) var tilgjengelig, ble dette benyttet. Intervjupersonene ble stilt spørsmål om hvor ofte de har erfart eller vært ofre for kriminalitet knyttet til bankbruk, handel på nett eller nedetid på nettsted. Svar ble avgitt i form av dikotome variabler (0=offer, 1=ikke-offer), og er dermed begrenset til å måle det omfanget av kriminalitet som respondentene selv er klar over og husker i intervjusituasjonen. Denne tilnærmingen fordrer at respondentene har kunnskap om de ulike former for kriminalitet og til og med tekniske kunnskaper om hva som kan forårsake nedetid på nettsteder. Dette utgjør en betydelig svakhet i undersøkelsen. Dessuten har ikke undersøkelsen satt tidsramme for rapporteringen, altså når respondentene skal ha opplevd eller ikke opplevd kriminaliteten, og det er derfor ikke mulig å si så mye om omfang som den kunne ha gjort dersom tidsperiode var spesifisert i spørsmålene. Derimot, gir undersøkelsen viktig kunnskap om korrelasjon mellom viktimisering, nettvaner og sosioøkonomiske forhold til tross for at den i større grad vektlegger kartlegging av internettvaner og sosiotekniske faktorer enn ulike former for- eller omfang av nettkriminalitet. Responsraten for Europa-barometeret varierer dessuten mellom landene.

Både Junger et al. [96], Hawdon et al. [104] og Näsi et al. [90] bruker for øvrig rutineaktivitetsteori (RAT) som teoretisk rammeverk, og det kan legge føringer for utviklingen av undersøkelsens design. RAT, utviklet av Cohen og Felson i 1979 [116], er kanskje den vanligste teorien innen viktimiseringsstudier (Miró [117], sitert i Hawdon et al. [104]). Den fremsetter tre premisser for at viktimisering kan skje: motiverte lovbrytere, et passende mål, og fravær av beskyttelse. Rutinemessig aktivitetsteori mener tilbakevendende og høy grad av aktivitet hos individet igjen bidrar til at disse tre premissene oppfylles og dermed påvirker individets risiko

for å rammes. Junger et al. sitt metodeverk ser ut til å ha sterkere fokus på rutineaktivitet for kriminalitet enn cyberdimensjonen i kriminaliteten, noe som viste seg å gi noen svakheter i undersøkelsens funn. Vi kan anbefale at undersøkelser går grundigere inn i cyberteoretiske perspektiv metodologisk, slik at de unngår samme svakhet i undersøkelsesdesign. Junger et al. har en stor og god undersøkelse som dessverre ikke klarer å måle omfang fordi det ikke er tatt tilstrekkelig høyde for kompleksiteten i cyberkriminalitets-konseptet i undersøkelsens metodedesign.

Gañán et al. [103] gir overordnede eksempler på hvordan data kan brukes i evaluering av cyberkriminalitetskostnader, inkludert selvrapporterte data fra forbrukere og organisasjoner, varsler på brudd gitt av organisasjoner til regulatorer eller kunder, forsikringsdata, innsamlede tekniske hendelsesdata, observasjoner fra *honeypots*, *sandboxes*, *spam traps*, det mørke nettet og antivirus-klienter, kriminalrapporter og nyhetsrapporter. Artikkelen gjør ingen forsøk på å måle dette selv, men gir mange eksempler på feil som gjøres i andre undersøkelser. Mange av studiene som estimerer kostnader knyttet til cyberkriminalitet gjør dette ved å summere individuelle kostnader, noe som ofte vil føre til dobbeltelling. Eksempelet som brukes her er når man tar kostnadene knyttet til en hendelse og ekstrapolerer dette til sektoren eller et land, glemmer man at offeret gjerne flytter virksomheten til en konkurrent, som da får økt inntekt. Det er med andre ord en økonomisk overførsel, ikke et rent tap. Artikkelen konkludere med at bare en håndfull studier har gjort seriøse forsøk på å måle kostnadene ved cyberkriminalitet, og selv disse klarer ikke å ta hensyn til ulike forvrengninger i estimatene. Vi anbefaler å følge rådene fra Gañán et al. for enhver omfangsundersøkelse som fokuserer på kortsiktig og langsiktig økonomisk tap for enkeltindivider og samfunn.

3.2 Hvilke kilder vises det til for å si noe om omfanget til cyberkriminalitet?

Svært mange av artiklene i utvalget som uttaler seg om omfang gjør dette basert på data fra andre. Få bruker offisielle datakilder fra politi og rettssystem, men vi har for eksempel sett det er blitt referert til *INTERPOL National Cybercrime Strategy Guidebook* [66]. Mange artikler i utvalget refererer til én eller flere andre typer kilder for å underbygge ulike argumenter knyttet til studien. Her kan kildene deles inn i ulike kategorier som data fra internasjonale organisasjoner, nasjonale organisasjoner, forskning og analysebyrå, sikkerhets-firmaer, og andre kilder som medie- og blogginnlegg. Eksempler fra internasjonale organisasjoner er rapporter og publikasjoner fra FN [54], [118], *World Economic Forum* [119], *International Telecommunication Union* [120], INTERPOL og *Health IT Security* [121]. Disse omhandler ofte kriminalstatistikk eller annen relevant informasjon. Blant refererte europeiske organisasjoner finner vi *Den Europeiske Sentralbanken* [122] og Europol [123].

I England og Wales gjennomfører *Office for National Statistics* en årlig ansikt-til-ansikt befolknings-undersøkelse kjent som *Crime Survey for England and Wales* (CSEW) [124]. Denne omhandler mange typer kriminalitet og har et med et representativt utvalg av 35 000 voksne over 16 år. I noen av rapportene presenteres dataene fra undersøkelsene sammen med rapporteringstall fra Politiet. Den siste utgivelsen av denne rapporten har et eget kapittel som omhandler datamisbruk (*computer misuse*), og dekker i tillegg kriminalitet som ikke er rapportert til politiet. Statistikken viser at til og med juni 2023 var det 850 000 lovbrudd i denne kategorien, med en økning på 33% fra samme tid året før. Denne befolkningsundersøkelsen er referert i flere studier i utvalget [14], [101], og vi har lagt ved spørsmål knyttet til omfang fra denne i vedlegg B.

I Storbritannia brukes også data fra Departementet for digital, kultur, media og sport [14], [105], [112], som gjennomfører *the UK Cybersecurity Breaches Survey (CSBS).* Undersøkelsen kartlegger informasjon om digitale trusler, strategier for cybersikkerhet og digitale karakteristikker, basert på spørreundersøkelser av virksomheter og frivillige organisasjoner, samt et mindre utvalg dybdeintervjuer. Lignende kilder fra samme departement brukes også av Furnell og Downing [14], i tillegg til bruk av data fra det britiske senteret for

Action Fraud fra 2017 og 2018 [124], [101]. I kategorien forskningsinstitutter og analysebyrå er det hovedsakelig én institusjon som er referert til flere ganger knyttet til kostnader for cyberkriminalitet [13], [102], [103] og det er ulike rapporter fra Ponemon Institute [125]. Andre typiske kilder er rapporter fra sikkerhetsselskaper, som Norton, McAfee og Symantec [14], [32], [102], [103].

Omtalt i flere av artiklene fra vår seleksjon [98], [103], [39], [104], [83] er FBI *Internet Crime Complaint Center* (IC3) [111], [126]. Dette er et egenrapporteringssystem for kriminelle handlinger som har skjedd på nett. Her kan man varsle for seg selv, men også andre. FBI samler her inn bakgrunnsinformasjon om offeret, informasjon om transaksjonen, konkret informasjon om hvordan personen ble utsatt for den kriminelle handlingen, og annen relevant informasjon om hendelsen. En studie fra Cordova et al. [24] refererer til FBI og *Computer Security Institute* sin årlige undersøkelse som viser at 60% av angrep ikke oppdages og bare 15% går til politianmeldelse.

I Storbritannia har de et lignende system for egenrapportering, men som i hovedsak dreier seg om svindel, som heter *Action Fraud* (omtalt brukt i [92], [101]). Her kan personer varsle på vegne av seg selv eller andre som har vært offer for nettsvindel. Man begynner med å definere om man er et offer selv, om man rapporterer for andre, for firmaer eller om man bare er vitne til kriminelle hendelser på internett.

Eurobarometer er en annen befolkningsundersøkelse referert til i utvalget vårt [39], [96]. Denne gjennomføres årlig i alle EU-land. I nyere versjoner av denne undersøkelsen er det egne kapitler om digital teknologi og samfunn, der det blant annet er gjort egne undersøkelser på små og mellomstore bedrifter og cyberkriminalitet [127].

US National Crime Victimization Study (NCVS) blir også vist til for omfang, blant annet av Anderson et al. [39], for tall knyttet til identitetstyveri i USA. I 2016 var litt over 10% av amerikanerne rammet av dette, opp fra 7% et par år tidligere. Bare rundt en fjerdedel av disse var klar over at det var blitt lurt. Her må vi bemerke at uautorisert uttak fra bankkontoer utgjorde en betydelig andel, og at betalingssystemene i USA er ganske forskjellige fra Europa og Norge.

Graham et al. [32] viser til en studie fra sikkerhetsselskapet Norton (Symantec) hvor det er oppgitt at 143 millioner amerikanere ble utsatt for cyberkriminalitet i 2017 til en tapsverdi av totalt 19,4 milliarder USD. Samtidig melder FBI IC3, som mottar klager fra ofre for cyberkriminalitet, at 301 580 saker ble rapportert samme år – noe som kan indikere mørketall. Blant de vanligste sakene var manglende betaling eller leveranse (84 079), personvernbrudd (30 904 ofre) og *phishing/vishing/smishing/pharming* (25 344), mens størst økonomisk tap ble registrert ved *business email compromise* (BEC) (675 millioner USD) og *confidence fraud/romance* (211 millioner USD).

Tall og statistikker fra organisasjoner og virksomheter benyttes for å beskrive og predikere trusselbildet. Donalds og Osei-Bryson [128] viser til anslag fra blant annet Ponemon Institute og Accenture, om at cyberkriminalitet kostet organisasjoner i USA 11,7 millioner USD i 2017, en økning på 23% fra året før, og Trend Micro, som estimerte globale tap bare for e-postangrep på over 9 millioner USD i 2018. Reinhart [129] viser til Gallups årlige kriminalitetsstudie, som fant at 23% av befolkningen i USA opplevde cyberkriminalitet i 2018.

Srivastava et al. [28] har blant annet brukt *SANS Institute* som kilde, spesifikt deres *Internet Storm Center* (ICS) [130]. Her har de hentet ut åpne data knyttet til titusenvis av logger fra innbruddsdeteksjonssystemer (*intrusion detection systems*) og brannmurer hos frivillige brukere. Dataene fra 2014 er kombinert med annen informasjon om nasjoners evne til å generere inntekt, teknologisk modenhet og evne til å beskytte

seg mot cyberangrep. Studien her viste at nasjoner med mye teknologi tilgjengelig har en tendens til å være kilde til cyberkriminalitet. Det motsatte gjelder for lavinntektsland.

Utfordringen med *økende omfang* av cyberkriminalitet fremkommer tydelig i mange av publikasjonene fra utvalget. Blant annet Akdemir et al. [22] vektlegger at dette er den raskest voksende av all kriminalitet. Følger vi kildene til tallene videre, finner vi i flere tilfeller at tallene kommer fra nyhetsartikler som igjen baserer seg på tall fra byråer og organisasjoner, og i mindre grad akademiske studier. Dette innebærer at også den fagfellevurderte forskningen gjerne legger vekt på ikke-fagfellevurderte målinger særlig når det kommer til måling av omfang og utbredelse. I noen tilfeller viser artikkelen til nyhetsartikkelens forfatter, altså journalisten, i stedet for byrået som har fremlagt tallene. Dette er ikke nødvendigvis uriktig, og vil avhenge av hvorvidt den fagfellevurderte artikkelen referer en større idé eller tanke, eller kun tallene. I alle tilfelle bidrar det til uklarhet rundt ulike måls opprinnelse og hvordan tall er fremskaffet med hensyn til bruk i videre forskning. De underliggende kildene er blant annet journalistene Summerville [131] (nyhetsartikkel i CNBC), Reinhart [132] (nyhetsartikkel i Gallup) og Graham [133] (nok en nyhetsartikkel fra CNBC). Lallie et al. [68] benytter seg også av ikke-faglige artikler for å kartlegge omfanget av cyberkriminalitet under COVID-19 pandemien. Artikler fra store mediehus som BBC og Reuters, blogginnlegg, innlegg fra sosiale medier og sikkerhetsfirmaer brukes i denne artikkelen for å etablere en tidslinje som kartlegger spredningen av angrep under pandemien. På generell basis anbefaler vi å være forsiktig med å basere måling av omfang basert på nyhetsartikler, da disse kan være tatt ut av kontekst og være grove forenklinger. Fra vårt utvalg gir Anderson et al. [39] et eksempel på dette, hvor deres estimater om nettbasert skatteunndragelse i Storbritannia ble ukritisk skalert opp av journalister til et globalt nivå for cyberkriminalitet. Dette ble da svært misvisende.

3.3 Er omfang omtalt i litteraturen samstemt?

Måten omfang omtales på i litteraturen er svært forskjellig, og er som nevnt basert på varierende kilder. En felles enighet er derimot at fenomenet cyberkriminalitet er raskt voksende i omfang [22], [134]. I omtalen av omfanget brukes det mange ulike mål, premisser og enheter i utvalget. I noen tilfeller fremstilles omfanget som en sammenligning mot noe som har vært målt tidligere, eksempelvis en økning fra forhenværende år eller tidligere måling [128]. Hvilken parameter som brukes for å presentere målingen skifter fra artikkel til artikkel, der noen viser til målinger som omtaler at enkeltindivider er rammet [22], mens andre omtaler det som datamaskiner. Flere av studiene omtaler kostnader [32], [60], der noen også presenterer globale tall [28]. Tidsspennet varierer også, der *WannaCry*-viruset rammet 300 000 maskiner på 24 timer [128], så rapporteres det også om at 23% av befolkningen i USA ble rammet av cyberkriminalitet i løpet av året 2018, eller at en økning med 48% i 2014, tilsvarer 117 339 angrep per dag [83]. I andre sammenhenger omtales også omfang som antall rapporteringer [90] eller underrapporteringer [32].

Fra vårt utvalg gir Gañán et al. [103] eksempler på hvor lite samstemte ulike rapporteringer av omfang kan være. Eksempelet deres er fra 2010, hvor FBI sitt *Internet Crime Complaint Center* (IC3) estimerte økonomisk tap for alle individer i USA til å være på $560 millioner (populasjonen utgjorde da 4,5% av verdens befolkning), mens sikkerhetsselskapet McAfee sitt estimat var på $1 trillion[7] globalt. Her det det altså snakk om mange tierpotenser forskjell når man normaliserer tilfellene i USA opp mot resten av verden. Dersom vi spoler litt fram i tid og ser på senere rapporter som McAfee har gitt ut sammen med *Center for Strategic and International Studies* (CSIS) er det derimot snakk om mer moderate tall. I 2018 var dette tallet $600 billion (på norsk milliarder) (0,8% av global GDP) [135], mens først i 2020 var tallet kommet opp til $1 trillion (1% av global GDP) [136]. Et annet ekstremt eksempel vises av Breen et al. [98], som også bruker tall fra FBI IC3

[7] Merk at det benyttes forskjellige skalaer for store tall. Engelskspråklige land benytter den korte skalaen hvor $1 trillion = $1000 000 000 000 (eller 10^{12}), mens de fleste europeiske land (inkludert Norge) benytter den lange skalaen hvor en billion er 10^{12}, og en trillion er 10^{18}. I dette tilfellet refererer McAfee til den korte skalaen.

hvor 0,15% av alle amerikanere har vært utsatt for cyberkriminalitet, mens sikkerhetsselskapet Norton sier i sin rapport fra 2019 at 30% av alle amerikanere var ofre for cyberkriminalitet det året.

Også fra vårt utvalg er det her verdt å nevne Hawdon et al. [104] sin undersøkelse av cyberkriminalitet i USA under COVID-19. De viser til at blant annet at selv om FBI rapporterte om en firdobling i denne perioden, så stemmer ikke det med deres offerundersøkelse i det hele tatt. Ifølge dem var antall hendelser stabilt, men deres hypotese er at bred omtale i media og mange advarsler fra myndighetene førte til høyere bevissthet i befolkningen og dermed mange flere anmeldelser og rapportering av hendelser.

3.4 Hva regnes som de største utfordringene i litteraturen knyttet til måling av cyberkriminalitet?

Artiklene i utvalget fremlegger flere utfordringer knyttet til måling av cyberkriminalitet. Flere av disse studiene, blant annet Correia et al. [137], Breen et al. [98], Akdemir et al. [22] og Al-Khater [71], peker på at underrapportering er en av de største utfordringene knyttet til måling av omfang. Dette gjelder både i forhold til anmeldelser hos politi og i undersøkelser. Litteraturen prøver også å gi en forklaring på hvorfor kriminelle hendelser i det digitale rom ikke blir rapportert. De Paoli et al. [9] har i sin litteraturstudie skilt på hvorfor individer og organisasjoner ikke gjør det. I forhold til individer har forfatterne identifisert fem hovedgrunner:

1. Man vet ikke at man er et offer.
2. Man ønsker muligens ikke å innrømme at man har blitt gjort til offer.
3. Ofrene er likegyldige, siden mange hendelser har liten innvirkning isolert sett.
4. Manglende kjennskap til rapporteringsmekanismer.
5. Manglende felles tillit til politiets evne til å pågripe cyberkriminelle.

For organisasjoner lister de opp følgende tre hovedgrunner:

1. Mulig skade på omdømmet.
2. Virksomheter tror de har en bedre forståelse av problemene og de mest effektive måtene å håndtere dem på.
3. Ulike mål: Politiet ønsker å bevise at en forbrytelse har funnet sted, mens organisasjoner ønsker å stanse inntrengningen, minimere tapene og unngå negativ publisitet.

Graham et al. [32] viser til forskning som peker på at det er forskjellig praksis for rapportering av tradisjonell kriminalitet og cyberkriminalitet, og mener at dette gjør det mindre sannsynlig at ofrene rapporterer cyberkriminalitet enn tradisjonell kriminalitet. Al-Khater et al. [71] trekker også fram at underrapporteringen av cyberkriminelle hendelser er tilknyttet mangelen på kunnskap eller at det er en del sosiale begrensninger knyttet til rapportering, samt at det er utfordrende å få offisiell statistikk på grunn av kulturen/konseptet til cyberkriminaliteten. Dette samstemmer med Shan-A-Kuda og Schreuders [42], som viser til at noen ofre ikke forstår definisjonen på cyberkriminalitet og dermed ikke vet at de er ofre. Disse forfatterne viser også til Bentaleb et al. [138], som hevder at cyberkriminalitet involverer noen latente kategorier som ikke kan bli målt direkte.

Chandra & Snowe [38] mener at fraværet av en grundig taksonomi for cyberkriminalitet, og at mangelen på klarhet og forståelsen av selve konseptet også gir dårlige forutsetninger for å måle fenomenet. Dette henger også sammen med at mange ofre ikke forstår at de har blitt rammet, som igjen stemmer godt med den første grunnen som De Paoli et al. lister opp. Koops [1] argumenterer med at fremstillingen av cyberkriminelle i populærkulturen, som arketypiske hackere, gir et feilaktig virkelighetsbilde i den generelle befolkningen knyttet til omfang og gjerningsmenn. Dette påvirker nok persepsjonsstudier hos befolkningen, som kanskje tror at cyberangrep vanligvis foregår på spektakulært vis hvor enorme pengebeløp er involvert. Sannheten

er nok en annen, og Wall har tidligere (2013) [139] argumentert for at det meste av finansielle tap som følge av cyberkriminalitet kan karakteriseres som «*de minimis*», som betyr at cyberkriminelle passer på å stjele små summer for å unngå forfølgelse av myndighetene.

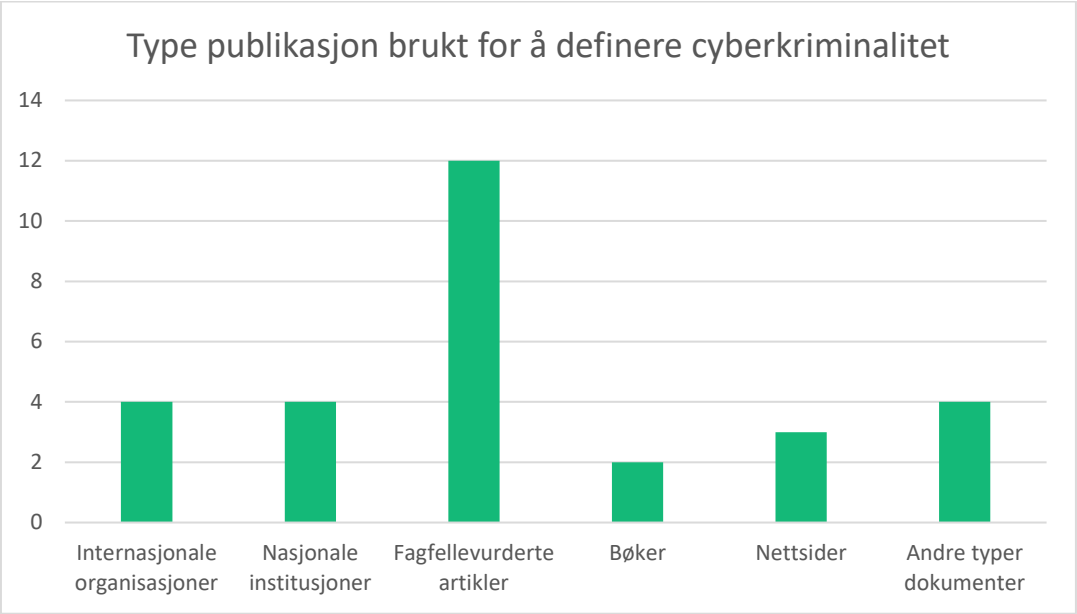
Akdemir et al. [22] peker på ulikheter mellom nasjonal jurisdiksjon og manglende koordinering mellom politiets organer og private regjeringsaktører som viktige utfordringer for måling. Tilsvarende utfordringer knyttes til landegrenser, hvor informanter fra britisk politi sier at ikke-europeiske land er lite villige til å dele informasjon om nettbaserte gjerningspersoner. Spesielt afrikanske land blir nevnt, samt selskaper som opererer fra Luxemburg, Panama og Gibraltar. Cordova et al. [24] trekker også fram det faktum at gjerningspersonene i mange tilfeller oppholder seg geografisk langt unna ofrene som blir utsatt for de kriminelle handlingene. Anderson et al. [39] poengterer også at cyberkriminalitet ofte krysser ulike jurisdiksjoner, men nevner samtidig andre sentrale utfordringer som at statistikker er fragmenterte, lider av både under- og overrapportering, samt at de er avhengige av hvem som samler inn data. Furnell og Dowling [14] peker på at sikkerhetsindustrien, selv med tilgang til mye data, mislykkes med å gi langsiktig innsikt på grunn av lite konsistens i de ulike temaer de undersøker. De Paoli et al. [9] kritiserer målingene som sikkerhetsfirmaer gjennomfører og publiserer med at de ofte er forutinntatte (*biased*), mens Breen et al. [98] hevder de benytter svake metoder, mangler transparens og ikke er til å stole på.

4 Observasjoner om litteraturen

4.1 Hvilken type publikasjoner benyttes for å beskrive cyberkriminalitet?

Ulike typer publikasjoner brukes i beskrivelsen av cyberkriminalitet. I dette avsnittet er det særlig lagt vekt på de ulike publikasjonene brukt av de fagfellevurderte artiklene i utvalget, og hvilke definisjoner de har brukt for cyberkriminalitet. De ulike publikasjonstypene kan deles inn i ulike grupper fra 1) rapporter fra internasjonale organisasjoner, 2) rapporter fra nasjonale institusjoner, 3) fagfellevurderte artikler, 4) bøker, 5) nettsider og 6) en samlekategori med andre typer dokumenter.

Vi har videre undersøkt publikasjonstypene som er grunnlaget for definisjonene brukt i utvalget (se Tabell 1). Den aller mest brukte publikasjonstypen for å definere cyberkriminalitet er fagfellevurderte artikler (11). Det er imidlertid jevnt mellom de andre publikasjonstypene, der bøker er aller minst brukt (2). Bruk av andre typer publikasjoner fordeles jevnt over de andre kategoriene.



Figur 8: Type publikasjon brukt for å definere cyberkriminalitet

Det som kjennetegner flere av artiklene i utvalget, er bruken av flere ulike kildetyper til å beskrive cyberkriminalitet. Ett eksempel er Cordova et al. [24], som benytter seg av både rapporter fra Europa-kommisjonen [37], fagfellevurderte artikler [41] og bøker (*Oxford Dictionary of Law*). Andre forfattere, som Luknar [30], benytter seg av flere kilder fra flere fagfellevurderte artikler, som Gordon and Ford [31], Pradillo [49] og Moitra [29], der førstnevnte er en anerkjent artikkel brukt av flere i vårt utvalg.

I definisjonene brukt fra internasjonale organisasjoner så er rapporter fra EU-kommisjonen [37], Europol [34], FN [20], og Samveldet av uavhengige stater [22] brukt. I nasjonale rapporter henvist til i utvalget, så er definisjonene hentet fra Storbritannia, USA og Sør-Afrika. I nettside-kildene er det typisk oppslagsverk og leksikon som er brukt [18], [54]. Dette gjelder også for én av to brukte bøker [41]. I kategorien som omhandler andre type rapporter og dokumenter, er definisjonene hentet fra blant annets selskaper med virke innenfor cybersikkerhetsdomenet [60], [22].

4.2 I hvilke tidsskrifter og konferanser publiseres de mest siterte artiklene?

I gjennomgangen av artiklene i utvalget som er sitert mest, har vi satt grensen på 20 siteringer. Den aller mest siterte artikkelen er Lallie et al. [68], med 455 siteringer. Dette er en *outlier* i så måte, og derfor er det nødvendig at vi går fram med en bredere tilnærming.

Tabell 6. Oversikt over artiklers siteringer og journaler/konferanser

Forfattere	Tittel	År	Siteringer	Journal/konferanse
Lallie et al. [68]	*Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*	2021	445	*Computers & Security*
Leukfeldt et al. [107]	*Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime*	2017	122	*European Journal on Criminal Policy and Research*
Anderson et al. [39]	*Measuring the changing cost of cybercrime*	2019	93	*The 18th Annual Workshop on the Economics of Information Security*

Forfattere	Tittel	År	Siteringer	Journal/konferanse
Hawdon et al. [104]	*Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment*	2020	91	*American Journal of Criminal Justice*
Donalds og Osei-Bryson [128]	*Toward a cybercrime classification ontology: A knowledge-based approach*	2019	60	*Computers in Human Behavior*
Tsakalidis og Vergidis [83]	*A systematic approach toward description and classification of cybercrime incidents*	2017	60	*IEEE Transactions on Systems, Man, and Cybernetics: Systems*
Kemp et al. [92]	*Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19*	2021	57	*Journal of Contemporary Criminal Justice*
Al-Khater et al. [71]	*Comprehensive review of cybercrime detection techniques*	2021	51	*IEEE Access*
Jhaveri et al. [140]	*Abuse Reporting and the Fight Against Cybercrime*	2017	46	*ACM Computing Surveys*
Broadhead [13]	*The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments*	2018	44	*Computer Law and Security Review*
Paoli et al. [4]	*The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium*	2018	42	*Crime, Law and Social Change*
Hadlington et al. [65]	*A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime*	2021	41	*Policing (Oxford)*
Graham et al. [32]	*Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice*	2020	37	*Policing: An International Journal*
van de Weijer et al. [91]	*Reporting cybercrime victimization: determinants, motives, and previous experiences*	2020	26	*Policing: An International Journal*
Junger et al. [96]	*Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in europe*	2017	24	*2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*
Nouh, Mariam et al. [12]	*Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement*	2019	24	*arXiv preprint arXiv:1902.06961 Computer Science > Human-Computer Interaction*
Riek og Böhme [108]	*The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates†*	2018	24	*Journal of Cybersecurity*
Chandra og Snowe [38]	*A taxonomy of cybercrime: Theory and design*	2020	22	*International Journal of Accounting Information Systems*
Gañán et al. [103]	*Beyond the pretty penny: the Economic Impact of Cybercrime*	2017	21	*Proceedings of the 2017 New Security Paradigms Workshop*
Jeong [89]	*Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues*	2020	21	*IEEE Access*
Farahbod et al. [102]	*Cybersecurity indices and cybercrime annual loss and economic impacts*	2020	20	*Journal of Business and Behavioral Sciences*

Som oversikten viser, er utvalget publisert i et bredt utvalg av ulike tidsskrifter og konferanser. Det meste av de siterte artiklene er fra forskjellige tidsskrifter, mens to artikler er fra tidsskriftet *Policing: An Internasjonal Journal* [32], [134], som hovedsakelig omhandler studier knyttet til ulike deler av politiarbeid. I tillegg er Leukfeldt et al. [107] publisert i lignende tidsskrift, *European Journal on Criminal Policy and Research*. Andre artikler [68], [140] er publisert i rene datasikkerhets-tidsskrifter som *Computers & Security* og *ACM*

Computing Surveys. I tillegg er andre artikler [38], [102] publisert i tverrfaglige tidsskrift som *International Journal of Accounting Information Systems* og *Journal of Business and Behavioral Sciences*.

5 Grå litteratur

I mange tilfeller benytter fagfellevurdert litteratur grå litteratur til kilder for typisk definisjoner eller for å si noe om omfang. Dette har vi allerede gitt en oversikt over i seksjon 3. Som nevnt i seksjon 1.2 identifiserte vi under seleksjonsprosessen 29 kilder som var relevante, men som ikke var fagfellevurdert. Vi har valgt å syntetisere data fra disse også, da flere inneholder definisjoner og tilnærminger til måling av omfang.

Majoriteten av den grå litteraturen fra seleksjonsprosessen, det vil si 20 av 29, var bøker eller bokkapitler. Her benyttes som regel ikke fagfellevurdering i tradisjonell forstand, men gjerne en redaksjonell kvalitetssikring av innhold. Slike kilder som regel ikke er fritt tilgjengelig for forskere fra universitets- og institutt-sektoren, og må derfor kjøpes inn spesifikt. Når slike kilder likevel blir hyppig sitert, kan det derfor være en indikasjon på kvalitet. Et typisk trekk med denne typen litteratur er at den samler og oppsummerer informasjon. Dette kan anses som en type sekundærstudier, selv om det sjelden er beskrevet noen metode for hvordan denne innsamlingen har foregått. Man må derfor anta at forfatterne vet hva de snakker om. I det utvalget vi presenterer her har vi vektlagt godt siterte kilder, men også hvor vi også har sett at forfatterne står bak anerkjente fagfellevurderte artikler i tillegg.

Av norsk grå litteratur er samtlige kilder funnet gjennom Oria (se protokoll Vedlegg A), som indekserer elektronisk og trykt materiale ved Universitetsbiblioteket i Oslo, samt de fleste andre norske fag- og forskningsbibliotek. Dette er i hovedsak bøker, offentlige rapporter og hovedoppgaver.

5.1 Sentrale internasjonale bøker og bokkapitler

I 2020 ble boken *The Palgrave Handbook of International Cybercrime and Cyberdeviance* [141] utgitt, og denne inneholder flere relevante kapitler som vi har analysert. Thomas J. Holt og Adam Bossler har vært redaktører for denne boken, og nettopp disse to har publisert mye litteratur knyttet til cyberkriminalitet de siste 15 årene. Til sammen har boken og delkapitler i overkant av hundre siteringer, som er relativt bra med tanke på at dette er litteratur som ikke er åpen. Denne boken inneholder et eget kapittel, *Defining cybercrime* av Payne [142], som går gjennom historisk utvikling av fenomenet cyberkriminalitet. Her forsterkes mange av våre observasjoner knyttet til fenomenet (se seksjon 2.2), deriblant at det ikke finnes noen universell definisjon og at det kanskje er naivt å tro at man kan få til det. Likevel er det viktig med en felles forståelse av hva cyberkriminalitet er for noe. Et interessant poeng som tas opp her er at definisjoner som stammer fra samfunnsvitenskapelig litteratur og kriminologi ofte er noe forskjellige fra de mer teknologiske. Tabell 7 oppsummerer hvordan litteratur med ståsted i det samfunnsvitenskapelige eller teknologiske skiller seg fra hverandre ut ifra definisjon og konseptualisering av cyberkriminalitet.

Tabell 7. Ulik konseptualisering av cyberkriminalitet

Samfunnsvitenskapelig ståsted	Teknologiske ståsted
Teori tar utgangspunkt i fornærmelsen.	Teori tar utgangspunkt i angrepshandlingen.
Mål om å endre/hindre ulovlig oppførsel til gjerningspersoner.	Brukes til å finne teknologiske løsninger på problemet.
Bruker ofte samfunnsvitenskapelige forskningsmetoder, som spørreundersøkelser, intervjuer, feltstudier, analyse av nettforum og andre metoder hvor data kommer direkte fra personene det forskes på.	Bruker gjerne andre forskningsmetoder, for eksempel modellerings- og simuleringsteknikker, honningkrukker og eksperimenter i laboratorium.
Metoder kan kritiseres for å være for påtrengende.	Metoder kan kritiseres for å være begrenset til enkelte typer angrep.

Et annet interessant poeng i denne teksten er at det forskes og skrives forholdsmessig mindre om cyberkriminalitet enn andre typer kriminalitet. Det virker som om forskere foretrekker konvensjonelle teorier anvendt på tema knyttet til for eksempel narkotika- eller voldskriminalitet. Cyberkriminalitet som tema regnes også som multidisiplinært, og det kan være vanskelig å bryte ned samarbeidsbarrierer mellom forskere med ulik bakgrunn.

Fra et kapittel om den historiske utviklingen av cyberkriminalitet [143] beskrives en semantisk nettverks-analyse av engelskspråklig litteratur knyttet til temaet. Viktigste funn her er at det er to nøkkelord som dominerer - «(computer-related) cybercrime» og «Internet», som igjen korresponderer til definisjonene av cyberkriminalitet som finnes i litteraturen. Dette stemmer overens med de 32 cyberkriminalitets-definisjonene fra utvalget vårt vi har tatt med i Tabell 1, hvor 10 av definisjonene inneholder «Internet» og 21 inneholder «computer».

Også fra denne boken er det verdt å nevne kapitlet om cyberpsykologi av Attrill-Smith og Wesson [144], som definerer cyberkriminalitet i deres kontekst til å være *«an act conducted or enabled through digital technologies that causes either online or offline harm to another person(s), item, or animal.»* Her beskrives flere typologier relatert til cyberkriminalitet, blant annet typer personlighetstrekk hos cyberkriminelle. Forfatterne tar utgangspunkt i Wall sin typologi fra 2001[8] [23], som grovt deler cyberkriminalitet inn i:

- Nettinnbrudd (cybertrespass)
- Nettbedrag og tyveri (cyberdeception and theft)
- Nettpornografi og usømmeligheter (cyberpornography and obscenity)
- Nettvold (cyber-violence)

For hver at typene gir de så eksempler på psykologisk karakteristikk hos gjerningspersoner. Vi ser ikke dette som relevant for våre forskningsspørsmål her, men denne typen kartlegging vil være relevant for å lage målrettede preventive tiltak mot mulige gjerningspersoner i videre arbeid.

Dette kapitlet i boken diskuterer også resultater og utfordringer med å måle enkelte typer cyberkriminalitet, for eksempel hevnpornografi. Dette ble ulovlig i England og Wales i 2015, men har lav anmeldelsesrate. Når det blir anmeldt, blir også disse ofte trukket tilbake av offeret. Det henvises til en undersøkelse fra BBC, hvor 7806 tilfeller ble anmeldt i England og Wales mellom 2015 og 2018, hvor en tredjedel av disse ble trukket av offeret. Videre vises det til en befolkningsundersøkelse i Australia hvor 20% av de spurte hadde var blitt avbildet i seksuelt krenkende bilder/video, hvorav 11% var blitt offentlig delt. En britisk undersøkelse fra 2017 av *Childnet International* fant ut at 12% av tenåringene rapporterte at de var blitt presset til å dele nakenbilder av seg selv. Begrepet «hevnpornografi» betegnes også som problematisk da det ikke alltid er snakk om «hevn» eller hva mange oppfatter som pornografisk materiale. Noen forfattere har foreslått bredere begreper slik som «bildebasert seksualmisbruk», men dette er lite brukt i praksis. Selv med usikkerhet rundt måling konkluderes det med av hevnpornografi er et voksende problem og kan ha svært alvorlige konsekvenser. Som eksempel viser en undersøkelse fra USA utført av *Cyber Civil Rights Initiative* i 2014 at 51% av ofrende har vurdert selvdrap.

Et siste kapitel vi ønsker å trekke fram fra denne boken handler om datasett for analyse av cyberkriminalitet [145], som utfyller kildene vi har sett i utvalget av fagfellevurdert litteratur. Her poengteres det at slike analyser ofte brukes til å finne korrelasjoner mellom for eksempel typer cyberkriminalitet og arbeidsledighet eller demografi. På grunn av store mørketall i rapporterte anmeldelser er det vanlig at kriminologer trekker på data fra offerstudier og befolkningsundersøkelser. De datasettene som trekkes fram er først og fremst tilknyttet USA, og de er gruppert i offisielle data, proprietære data og åpne kildedata. For offisielle data nevnes:

[8] Merk at denne typologien er forskjellige fra taksonomien foreslått av samme forfatter i 2007 [41]. Se seksjon 2.3.2.

- *National Incident-Based Reporting System* (NIBRS): Amerikansk rapporteringssystem for politiet. Inneholder informasjon om type kriminalitet (ikke bare cyber), offer, gjerningsperson, arrestasjoner og relasjon mellom offer og gjerningsperson. Fra dette systemet kan man trekke ut om en datamaskin var brukt til gjennomføring av den kriminelle aktiviteten, men informasjon er først og fremst knyttet til nettsvindel. De fleste andre typer cyberkriminalitet blir ikke registrert.
- FBIs *Internet Crime Complaint Center* (IC3): Egenrapporteringssystem vi har omtalt i seksjon 3.2. Her omtales det som det som det mest fremtredende systemet i USA som kan si noe om omfang av cyberkriminalitet. Likevel, det som er rapportert her utgjør bare en liten fraksjon av antatte tilfeller. Dataene fra IC3 er åpne og kan lastes ned, og brukes derfor mye av forskere for å si noe om trender, gjerne i kombinasjon med andre datasett.
- *National Crime Victimization Survey* (NCVS): Amerikansk offerstudie vi har omtalt i seksjon 3.2 som inneholder spørsmål knyttet til identitetstyveri. Undersøkelsen har et eget supplement for kriminalitet på skoler som samler informasjon om cybermobbing (cyberbullying). Informasjon som kan trekkes ut herfra er blant annet hvordan forbrytelsen ble oppdaget, økonomisk tap, om hendelsen ble anmeldt og preventive tiltak. En klar begrensing i denne undersøkelsen er at den bare tar for seg noen få typer cyberkriminalitet.
- *National Computer Security Survey* (NCSS): Amerikansk undersøkelse rundt cybersikkerhets-hendelser i bedrifter, og som tilsvarer Mørketallsundersøkelsen her i Norge. Denne har ikke blitt gjennomført siden 2005 og det er derfor lite oppdatert informasjon å hente.
- *General Social Survey* (GSS): Dette er en Kanadisk befolkningsundersøkelse som har spørsmål knyttet til om respondentene har vært utsatt for ulike type cyber-dependent og cyber-enabled kriminalitet.
- *Crime Survey for England and Wales*: Britisk befolkningsundersøkelse vi har omtalt i seksjon 3.2. Når det gjelder cyberkriminalitet er hovedfokus på nettsvindel (online fraud).

Proprietære data er data som samles inn av kommersielle og ikke-offentlige organisasjoner. Mange av disse datasettene har kommersiell verdi og er som regel ikke tilgjengelig for forskning, men noen unntak nevnes:

- *Kaspersky Lab* er multinasjonalt sikkerhetsselskap med over 400 millioner brukere (2018). Fra disse brukerne samles det inn data om skadevareinfeksjoner, Web-trusler, nettverksangrep, sårbarheter, søppelpost, infisert epost og *botnet*-aktivitet. Deres aggregerte trusselkart er åpent tilgjengelig og kan brukes til å vise variasjoner mellom ulike land og globale trender.
- *Bitdefender* er et alternativ til Kaspersky Lab, og samler inn data fra 500 millioner brukere (2018). De åpne dataene viser hvor angrep kommer fra og hvilke land som blir angrepet. Merk at mye av denne informasjonen kan være misledende ettersom angrep kan være fordekte.
- *McAfee* viser på samme måte som de over interaktive kart over angrep og søppelpost for ulike land. Dette inkluderer hvor mye skadevare et land mottar, type skadevare, risiko og oppdagelsestid.
- *Trend Micro* tilbyr interaktive kart over lokasjonen til kommando- og kontrolltjenere.
- *Arbor Networks* lager programvare som motvirker distribuerte tjenestenektangrep (DDoS), og som brukes av alle nivå 1 internettleverandører i verden (2018). De har laget et interaktivt kart som viser distribusjon og historisk trend for slike angrep.
- *Project Honey Pot* er et selskap som samler inn IP-adresser til tjenere som sender ut søppelpost. Denne dataen kan brukes til å identifisere hvilke land som sender og mottar mest søppelpost.
- *Zone-H* lar angripere registrere/skryte av vellykkede overtatte Web-sider (*defacement*). Noen av disse dataene er offentlige, mens historiske data må kjøpes fra de som driver tjenesten. Data man kan hente ut er angripers navn og motivasjon (selv-rapportert) og mål. Det er kjente svakheter ved disse dataene, men de kan brukes til å vise trender for misbruk av Web-sider for ulike land. De fleste Web-sider som blir registrert her er knyttet til offentlige institusjoner.
- *Cambridge Cybercrime Centre* tilbyr datasett knyttet til distribuerte tjenestenektangrep, diskusjons-forum og søppelpost. Senteret henter data fra nettverkssensorer fra ulike steder i verden og disse kan brukes til å identifisere hvor angrep kommer fra og mot hvilke land. Forumdata kan brukes til å

identifisere angrepstrender og teknikker, men er begrenset til hva angriperne faktisk deler på disse forumene.

Eksempler på åpne kildedata er det ikke så mange av, og er en svakhet ved dette kapitlet. Blant annet nevnes ikke kjente kilder til *Open Source Intelligence* (OSINT) som gjerne brukes kommersielt og innen forskning. De forfatterne nevner er:

- *Malware Domain List* ligner på Zone-H, bare at her kan hvem som helst rapportere inn skadevare-instanser. Disse dataene har klare begrensninger, men kan gi en viss pekepinn på global distribusjon av skadevare.
- Eksempler på artikler som har brukt Web-forum og sosiale medier til å studere cyberkriminalitet. Som eksempel på funn nevnes at de som eksponerer seg mye på sosiale medier gjerne er mer utsatt for angrep.

Til slutt konkluderer dette kapitlet med at det er behov for pålitelige data for å analysere ulike typer cyber-kriminalitet. Et tiltak for dette kan være å etablere data-konsortium der det offentlige og næringsliv deler sine data med hverandre. Ved å deklassifisere og anonymisere data kan man gjøre bedre forskning rundt cyberkriminalitet og øke forståelsen rundt fenomenet.

En annen bok med fokus på definisjoner av cyberkriminalitet er *Cybercrime, organized crime, and societal responses* [146] fra 2017, hvor det er et dedikert kapittel for *Cybercrime: Definition, Typology, and Criminalization* [147]. Av det som omtales som hoved-definisjoner her trekkes Wall sin klassifisering fra 2007 [41] fram (som vi har omtalt i avsnitt 2.3.2), i tillegg til en annen oppdeling fra Susan Brenner (2007) [148] som vi ikke har registrert brukt andre steder i vårt utvalg. Hun skiller mellom kriminalitet som er definert som cyber, og kriminalitet som har migrert fra den virkelige verden inn i cyberdomenet. Strengt talt skiller dette seg ikke noe nevneverdig fra de to dimensjonene vi har omtalt i seksjon 2.3.1.

Marcum og Huggins står bak kapitlet *Cybercrime* fra boken *Handbook on Crime and Deviance* utgitt i 2019. Dette er en kilde som er godt sitert (over 40 ganger) selv om den ikke er åpent tilgjengelig. Som definisjon på cyberkriminalitet brukes en vi ikke har sett brukt av andre: *«destruction, theft, or unauthorized or illegal use, modification or copy of information, programs, services, equipment or communication network».* Denne er igjen hentet fra en bok om hvitsnippkriminalitet fra 2002 [149] og virker mest orientert rundt «cyber-dependent» kriminalitet. Forfatterne omtaler tre generasjoner av cyberkriminalitet, hvor den først omhandlet bruk av datamaskiner for å få tak i informasjon til å for eksempel lage bomber eller produsere narkotika. Dette virker ikke helt å være i tråd med den definisjonen forfatterne referer til. Andre generasjon cyberkriminalitet handler om misbruk av telefonsystemer for å ringe gratis langdistanse, mens tredje generasjon dreier seg om bruken av bredbåndsmulighetene til Internett for å skalere opp kriminell aktivitet. Videre beskriver forfatterne et ganske stort sett med cyberkriminalitetskategorier uten at det er beskrevet noen metodikk for hvordan de har kommet fram til dette. Hver kategori inneholder en samling av informasjon fra ulike kilder, men det virker som om omfang først og fremst er knyttet til amerikansk målestokk. For eksempel innenfor cybertrakassering vises det til flere kilder fra mellom 2010-2015 som sier at nettbasert trakassering er mindre utbredt enn fysisk trakassering. Avhengig av undersøkelse vises det til at mellom 19% og 45% har opplevd *nettstalking*, og mellom 11% og 13% har opplevd misbruk knyttet til nettdating. En undersøkelse om identitetstyveri fra 2012 rapporterer at 9 millioner mennesker er offer for dette hvert år i USA, men dette gjelder ikke bare nettbasert kriminalitet. Mellom 5% og 35% av unge vokse innrømmer å ha deltatt i «*sexting»* (sende tekst, bilder eller video med seksuelt innhold). Dette er nødvendigvis ikke ulovlig i seg selv når det gjøres med samtykke, men kan bli misbrukt i ettertid. For eksempel er «*sextortion»* tyveri av slikt materiale hvor gjerningspersonen så forsøker utpressing. Her refereres det til en undersøkelse fra *Crimes Against Children Research Center* ved Universitetet i New Hampshire som viste at 60% av ofrene kjente gjerningspersonen, mens 40% traff denne første gang på nett. Nesten halvparten av ofrene var under 18 år.

Roderic Broadhurst er professor emeritus innen kriminologi og leder *Cybercrime Observatory* ved Australian National University. Han har skrevet kapittelet *Cybercrime in Australia* [150] som inngår i *the Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice* fra 2017. I forhold til definisjoner nevnes juridiske definisjoner fra Australia, USA og UK, men disse er forholdvis gamle og begrensede til spesifikke typer kriminalitet, for eksempel *US Computer Fraud and Abuse Act* (CFAA) fra 1986 og *Commonwealth Criminal Code Act* fra 1995. Broadhurst viser også til noen trender og målinger, blant annet til estimater fra 2015 om at det blir lagt ut så mye som 20 000 seksualiserte bilder av barn hver uke og at det under en politioperasjon i Australia i 2013 ble avslørt rundt 1000 kriminelle i løpet av tre måneder. Dette året ble 372 saker knyttet til denne typen misbruk av barn behandlet i den Australske retten. Broadhurst refererer også til data fra *Australian Cybercrime Online Reporting Netwo*rk (ACORN), hvor 39 491 hendelser ble rapportert i 2015, som var det første året systemet var i drift. Uten at det detaljeres nærmere, beskriver Broadhurst at svindel er den typen cyberkriminalitet som blir mest rapportert til politiet. Ifølge en undersøkelse fra *Australian Bureau of Statistics* fra 2016 har rundt halvparten av den Australske befolkningen blitt usatt for minst ett forsøk på økonomisk svindel eller identitetstyveri, hvorav 4% av disse faktisk ble offer. Et siste interessant moment her er at Broadhurst kritiserer sikkerhetsindustrien for bruken av *angrepsbegrepet* («attack») i slike estimater, da det i realiteten er snakk om kriminalitet av typen «lav verdi, høyt volum». Han mener altså at man bør skille på målrettete *angrep* (av typen «høy verdi, lavt volum») og automatiserte *bot*'er som blindt sikter seg inn på tilfeldige offer.

Marion og Twede har laget et omfattende leksikon, *Cybercrime: An encyclopedia of digital crime* [151], som ble publisert i 2020. Her listes i underkant av 250 fenomener knyttet til cyberkriminalitet i alfabetisk rekkefølge med tilhørende referanser fra litteraturen. Som overordnet definisjon av cyberkriminalitet brukes *U.S. Department of Justice* sin[9], som lyder *«any illegal activity for which a computer is used as its primary means of commission, transmission, or storage»*. Det innslaget i dette leksikonet som sier mest om omfang er «costs of cybercrime». Her påpekes det at det er store forskjeller mellom ulike kilder, mellom $400 milliarder og $3 billioner globalt årlig for omtrent samme tidsrom. Slike forskjeller stemmer med avvikene vi har omtalt i seksjon 3.3. Det nyeste tallet det refereres til her kommer fra forsikringsselskapet *Hiscox* sin *Cyber Readiness Report* fra 2017[10], hvor de basert på enn undersøkelse av 3000 selskaper estimerer den globale kostnaden til å ligge på $450 milliarder.

Fra vårt utvalg av fagfellevurdert litteratur er det referanser til boken *INTERPOL National Cybercrime Strategy Guidebook* [66]. Denne ble utgitt i 2021 og gir en interessant oversikt over hvilke offentlige institusjoner som samler inn statistikk over cyberkriminalitet i enkelte land og regioner:

- *Statistics Canada* er ansvarlig for å rapportere natur og omfang for kriminalitet i Canada.
- I Sør-Korea samler det nasjonale politiet data fra sine regionale politiavdelinger via et integrert informasjonssystemet kalt *Korea Information System of Criminal Justice Services* (KICS).
- I Storbritannia publiserer innenriksdepartementet *Home Office Counting Rules* (HOCR), hvor kriminalitet er registrert av politiet og andre.
- I USA analyserer, publiserer og distribuerer Justisdepartementet informasjon om kriminalitet, kriminelle gjerningspersoner, ofre for kriminalitet og driften av rettssystemer.
- *The United Nations Office on Drugs and Crime* (UNODC) produserer og distribuerer statistikk om narkotika, kriminalitet og rettssystemet på internasjonalt nivå.

[9] Denne definisjonen brukes også av mange hundre andre kilder på Internett, men vi har ikke sett noen som angir fra hvilket år og spesifikt hvilken kilde de har brukt. Det er dermed vanskelig å si om denne definisjonen er offisiell.
[10] Vi har undersøkt den siste Hiscox-rapporten fra 2023 [152] som inneholder over 5005 respondenter. Hiscox har her sluttet å operer med globale estimater, men heller med tall fra der hvor respondentene kommer fra (USA, UK, Frankrike, Tyskland, Spania, Belgia, Nederland og Irland).

Sammenlignet med oversiktskapitlet [145] i *Palgrave Handbook of International Cybercrime and Cyberdeviance* omtalt over, er det lite overlapp, så det er grunn til å tro at ingen av dem gir et komplett bilde, og det er først og fremst statistikk fra den vestlige verden som omtales. INTERPOL uttaler også i boken at de har et mål om å aggregere data om cyberkriminalitet og statistikk globalt gjennom en plattform ved navn *Cyber Analytical Platform*. Vi har lett etter mer informasjon om denne plattformen, og antar den har endret navn til INSIGHT. I 2023 virker denne fremdeles å være under utvikling og tidlig testing [153].

Fra boken *Cybercrime in Context* har vi identifisert kapitlet *Text Mining for Cybercrime in Registrations of the Dutch Police* [154], publisert av van der Laan og Tollenaar i 2021. Denne kilden er ikke mye sitert, men det er heller ikke å forvente da den er relativt ny og må kjøpes. Det som er interessant fra denne er at den presenterer en konkret metode for å estimere omfang av cyberkriminalitet fra ustrukturerte fritekstfelt i anmeldelsesregistret i Nederland. Her er utgangspunktet at mange hendelser som burde vært klassifisert som cyberkriminalitet har blitt feilregistrert som tradisjonell kriminalitet, og at denne informasjonen rettes ved hjelp av maskinlæring. Hver anmeldelse blir klassifisert i en eller flere av de 8 typene gjengitt i Tabell 8.

Tabell 8. Klassifisering brukt mot det Nederlandske anmeldelsesregisteret.

Overordnet kategori	Type cyberkriminalitet
Cyber-dependent	Hacking
	Utsending av løsepengevirus (*sending ransomware*)
	Distribuert tjenestenektangrep (*DDoS attack*)
Cyber-enabled	Trusler over nett (*online threat*)
	Personforfølgelse over nett (*online stalking*)
	Injurie over nett (*libel online*)
	Nettbasert identitetstyveri (*online identity theft*)
	Nettbasert bedrageri (*online fraud (selling/purchase)*)

Akkurat disse åtte typene ble valgt ut basert på litteratur og gjennom diskusjon med eksperter på cyber-kriminalitet og politi. Disse typene er regnet som viktig for politiarbeid, samtidig som det er for disse man mangler god oversikt over omfang. Metoden ble prøvd ut på registeret fra 2016, hvor 928 870 fornærmelser var registrert. Mellom 3,38% og 7,70% av disse ble klassifisert som cyberkriminalitet, og verdt å merke var *cyber-dependent* kriminalitet (0,10%-0,62%) langt mindre enn *cyber-enabled* kriminalitet (3,33%-7,41%). Blant *cyber-dependent* var *hacking* det mest vanlige, mens for *cyber-enabled* var det trusler. Sammenlignet med offerstudier i Nederland er det færre fornærmelser knyttet til både cyber-dependent og *cyber-enabled* kriminalitet som blir anmeldt, med unntak av trusler. En svakhet som ble identifisert med metoden er at en enkel anmeldelse kan ofte inneholde flere typer fornærmelser, både fysiske og på nett. Dette kan gjøre automatisk klassifisering vanskeligere.

Fahey sitt kapittel *Developing EU cybercrime and cybersecurity On legal challenges of EU institutionalisation of cyber law-making* [155] fra boken *Routledge Handbook of European Integrations* ble utgitt i 2022. Hun problematiserer prosessen med å få til et felles lovverk i Europa, og peker på konkurrerende definisjoner og taksonomier knyttet til cyberkriminalitet som noen av årsakene. Institusjoner som *EU Cybercrime Centre* (EC3), som er underlagt Europol, får kritikk for å mangle ressurser til å samle in data fra ulike kiler og bistå politi, rettsvesen og privat sektor. Videre får Europarådet kritikk for å ikke ha dekket cyber-terrorisme i Budapestkonvensjonen (selv om dette omtales som en aktivitet på Web-siden deres), at konvensjonen er i overkant bred og at det er overlapp mellom de forskjellige kategoriene av kriminelle handlinger. Hun påpeker også at i Europakommisjonens *EU Security Union Strategy* [156] fra 2020 beskriver et sett med kriminelle aktiviteter som er forskjellige fra Budapestkonvensjonen sine, og at dette har skapt mange spørsmål rundt juridiske definisjoner. Også FN sitt arbeid med en alternativ cybertraktat til Budapest-konvensjonen får kritikk, først og fremst fordi den handler lite om cyberkriminalitet og mer om kontroll av

Internett. Et annet poeng er at det internasjonale miljøet som skal etablere lover beskrives som mer fragmentert enn før, i hovedsak splittet mellom Kina, Russland og vesten.

5.2 Norsk grå litteratur

På 2000-tallet utarbeidet et eget Datakrimutvalg på oppdrag fra Justis- og politidepartementet to sentrale rapporter. Disse finner vi sitert i flere av de norske kildene. Den første, *Lovtiltak mot datakriminalitet, delutredning I* [157], ble utgitt i 2003 og omtalte behovet for lovendringer i Norge for å kunne ratifisere Budapestkonvensjonen. *Delutredning II* [158] ble utgitt i 2007 med et noe annet sammensatt utvalg og hvor mandatet også skulle ta for seg bruken av reservasjonsadgang. Særlig relevant for vårt arbeid har vært det siste utvalgets omtale av begrepet «datakriminalitet» som «både kriminalitet som er rettet mot data og datasystemer, og kriminalitet hvor datautstyr benyttes som verktøy for å begå handlingen». Selv om man her ikke eksplisitt omtaler *nettverk* slik de fleste av definisjonene fra Tabell 1 i vår seksjon 2.2 gjør, er forståelsen ellers temmelig lik de fleste, altså angrep ved hjelp av eller rettet mot datasystemer. Det er verdt å merke at utvalget ikke så noe behov for en rettslig definisjon av uttrykket.

Tidligere sorenskriver Stein Schølberg, som var leder for første instans av Datakrimutvalget, publiserte boken Cyberkriminalitet [159] i 2017[11]. Boken tar for seg den historiske utviklingen av tilknyttede begreper og strafferettsbestemmelser i Norge sett opp imot Budapestkonvensjonen. Forfatteren har selv vært med på å definere begrepet «datakriminalitet» sammen med professor Jon Bing i 1976, og refererer til Straffelovrådets utredningsrapport om *Datakriminalitet* fra 1985 [160] hvor begrepet ble definert som *«kriminalitet hvor utnyttelse av datateknologi har vært vesentlig for overtredelsen».* Her valgte Straffelovrådet å ikke inkludere hærverk på eller tyveri av datautstyr for å begrense omfanget. Schølberg påpeker også at begrepet cyberkriminalitet i de senere år har blitt mer naturlig å bruke fremfor datakriminalitet (tilsvarende utviklingen vi har beskrevet i litteraturen, se seksjon 2).

Inger Marie Sunde har skrevet en noe beslektet bok ved navn *Datakriminalitet: en fremstilling av straffe-rettslige regler om datakriminalitet* [161]. Boken ble utgitt i 2016, mens det er andre opplag som er indeksert for 2019 i Oria. I hennes omtale av datakriminalitet gjøres et skille mellom *handlinger* og *ytringer* i den digitale del av virkeligheten, hvorav handlinger retter seg mot datasystemer, mens ytringer har menneskelig adressat. Samtidig kan også datakriminalitet kombinere ytringer og handlinger, for eksempel ved at en gjerningsperson gjennomfører et datainnbrudd (handling) og så true fornærmede om publisering av private bilder (ytring). Definisjonen av datakriminalitet Sunde lander på er *«en straffbar ytring eller handling som er formidlet eller utført ved bruk av datateknologi»*. Videre poengterer hun at i en juridisk sammenheng må uttrykkenes betydning søkes presisert på grunnlag av supplerende rettskildemateriell. Hun nevner også at Justisdepartementet ikke har ønsket legaldefinisjoner for å unngå at straffebudene blir utdaterte på grunn av teknologiutvikling.

Oslo politidistrikts rapport *Trender i kriminalitet 2018-2021: Digitale og globale utfordringer* [162] er indeksert i Oria som en bok og dermed kommet med i det grå litteraturutvalget. Rapporten ble utgitt i 2018 og har et eget kapittel om IKT-kriminalitet. Som står her, *«det er uklare forestillinger både utenfor og innfor politiet om hva "datakriminalitet" omfatter».* Det refereres til Justis- og beredskapsdepartementets definisjon fra 2015 [163] hvor IKT-kriminalitet er *«lovbrudd mot datasystemer og lovbrudd begått ved hjelp av datautstyr og/eller -nettverk»*, samtidig med at Politidirektoratet ved Kripos har presisert at *«bruken av data må endre lovbruddenes "karakter, omfang og effekt" i forhold til tidligere, før det kan kalles "IKT-kriminalitet"»* [164]. I selve trendrapporten behandles datakriminalitet som en integrert del andre typer kriminalitet da det inngår nesten over alt i en eller annen form. Rapporten har også betraktninger knyttet til omgang. Blant annet at det er få undersøkelser som kan dokumentere det faktiske omfanget, og at i Norge

[11] Andre utgave av denne boken ble utgitt i 2023, men etter vår seleksjonsprosess.

finnes primært omfangstall for dataangrep som rammer bedrifter (i hovedsak *Mørketallsundersøkelsen*). Av internasjonale undersøkelser som ofte benyttes, nevnes kriminalitetsundersøkelsen i England og Wales (som vi har omtalt i seksjon 3.2 og 5.1), hvor det i 2016/2017 ble estimert at rundt halvparten av alle lovbrudd var knyttet til bedrageri- og datakriminalitet. Samtidig sier rapporten at omfangstallene her ikke kan oversettes direkte til norske forhold på grunn av ulik bruk av datautstyr og -nettverk. Ellers nevnes en generell trend om at tradisjonell vinningskriminalitet avtar, og nye typer økonomisk kriminalitet vokser fram i forbindelse med generell digitalisering og mindre bruk av kontanter.

Det er tre relativt ferske masteroppgaver indeksert av Oria som er med i dette utvalget da de har et norsk perspektiv på våre forskningsspørsmål, og spesielt i forhold til definisjoner av cyberkriminalitetsbegrepet. Tar vi dem kronologisk nevner vi først Enstad sin masteroppgave *Internettkriminalitet og jurisdiksjon* [165] fra 2018. Hun benytter en oversatt definisjon av datakriminalitet fra Howard [166], som lyder *«all form for kriminalitet der hvor data eller nettverk benyttes som mål, middel eller arena for å skaffe seg uberettiget tilgang, uberettiget vinning (økonomisk og ikke-økonomisk), eller å utføre skade»,* og refererer også til Straffelovrådets fortolkning fra 1985 [160]. Videre definerer hun Internettkriminalitet til å være en underkategori av datakriminalitet, hvor *«den straffbare handlingen skjer på Internett, eller lovbryteren benytter Internett som et verktøy for å begå den straffbare handlingen».* Oppgaven omhandler videre viktigheten med harmonisering av straffelovgivning, spesielt med tanke på Budapestkonvensjonen, for å løse spørsmål rundt jurisdiksjon ettersom datakriminalitet blir behandlet som en grenseløs form for kriminalitet. Hun taler også for et felles internasjonalt regelverk for å bedre kunne gjennomføre straffeforfølgning.

Nerlien har skrevet masteroppgaven *Politiet i møte med cyberkriminalitet* fra 2018. Hun presenterer ulike definisjoner av cyberkriminalitet, men trekker fram Wall sin *transformeringstest* [41] som en god metode for å si hva som hører inn under begrepet og ikke. Dette er en tommelfingerregel hvor man fjerner nettverksteknologi fra ligningen, og dersom det da ikke blir igjen noe lovbrudd kan man kalle det cyberkriminalitet. Hun beskriver også cyberkriminalitet som noe som er umulig å kvantifisere på grunn av sin grenseløshet og store mulighet for anonymitet, med henvisning til Jewkes og Jar [167] og Politidirektoratet [168]. Videre har hun intervjuet ni av politiets cyberkriminalitetsspesialister, hvor det kom fram at det var mangel på generell og spesialistkunnskap i politietaten, og at dette gjør at det private markedet har tatt over oppgaver som egentlig skulle tilhørt politiet.

Lorentzen sin masteroppgave *Cyberkriminalitet mot næringslivet* [169] fra 2021 har et hovedfokus på løsepengevirusangrep, men tar også for seg det generelle problemet med underrapportering påpekt i Mørketallsundersøkelsen og refererer til litteraturen for å finne årsaken til dette. En forklaring kommer fra Wall [170], som hevder at usikkerheten rundt cyberkriminalitetsbegrepet gjør at mange tenker at årsaken til sikkerhetsbrudd er utilstrekkelig sikkerhet fremfor kriminelle aktører. Lorentzen beskrives også sin egen erfaring med hvor vanskelig det er å finne informanter fra næringslivet som vil fortelle om sikkerhetsbrudd. I forhold til terminologi ble hun oppfordret til å legge bort begrepet cyberkriminalitet, da dette *«distanserer handlingen fra å være en oppgave for politiet, til å være et ansvarsområde tilegnet IT-avdelingene».* Anbefalingen var å heller bruke mer spesifikke begrep, i hennes tilfelle «vinningskriminalitet gjennom det digitale rom».

6 Konklusjoner og anbefalinger

6.1 Definisjoner og begreper

Vi kan ikke anbefale en enkelt definisjon av cyberkriminalitet fremfor noen andre. Vi støtter Phillips et al. sitt argument om at det er for mange begreper som prøver å beskrive det samme fenomenet, samt at det er et altfor bredt spekter av kriminalitet som faller inn under cyberkriminalitet. Samtidig kan man i mange tilfeller bare fjerne prefikset «cyber» og behandle handlingene som tradisjonell kriminalitet. Vår anbefaling er derfor

å bruke mer detaljerte kategorier eller klassifiseringer når man skal forstå og operasjonalisere cyberkriminalitet, for eksempel når man skal beskrive, gjøre måling av omfang, etterforske, analysere eller presentere for andre.

Dessverre finnes det ikke noen komplett taksonomi eller et rådende klassifiseringsrammeverk for cyber-kriminalitet. Det overordnede skillet mellom «*cyber-enabled*» og «*cyber-dependent*» er helt klart det som dominerer, men heller ikke her er situasjonen svart-hvitt. Et dataangrep inneholder som regel flere faser, og et enkelt angrep kan gå ut over både mennesker og eiendom, ødelegge dataintegritet og eksponere hemmeligheter, være motivert av økonomisk vinning og hevn, for å nevne noen eksempler. Det blir fort for enkelt å bare dele cyberkriminalitet i to kategorier. Man trenger i praksis en klassifisering som klarer å skille mellom de mange måtene å begå forbrytelser med og mot teknologi, og samtidig er forståelig for dem som skal bruke den. Budapest-konvensjonen er den klassifiseringen som er mest anerkjent internasjonalt i forhold til lovbrudd, og selv om den er kritisert for ikke å ta tilstrekkelig høyde for nye fenomener, pågår arbeid med oppdateringer som skal fange nye trender. I en operasjonell sammenheng vil det nok også være nyttig å tenke på flere karakteristika når man beskriver cyberkriminalitet, slik som hendelse, gjerningsperson, offer, motivasjon og skadeomfang (se eksempler hos Tsakalidis et al. [83] og Somer [36]). Phillips et al. [8] sin klassifisering favner mange av de tidligere klassifiseringene og virker gjennomarbeidet, men den er relativt fersk (2022) og det er derfor vanskelig å si hvor anvendelig den er i praksis. Likevel er det nettopp anvendelse som gjør at begreper får praktisk innpass, og en norsk tilnærming med for eksempel bruk av Budapest-konvensjonen for å beskrive lovbrudd, i kombinasjon med en oversatt taksonomi basert på Phillips et al. for å beskrive handling, vil kunne gi svar om anvendbarhet. Fordelen med en taksonomi er at man kan velge hvilket nivå av hierarkiet man legger seg på, og samtidig ha muligheten til å abstrahere oppover for statistiske formål.

Denne kunnskapsoversikten gir en oversikt over hvilke definisjoner og begreper som er sentrale i fagfelle-vurdert litteratur utgitt de siste fem årene. Likevel er det viktig å påpeke at fagfellevurdert litteratur bare står for deler av det store bildet. Annen litteratur, massemedia, populærkultur (film og TV-serier), sosiale media og andre kanaler bidrar til en gjensidig påvirkning om hvilke begreper vi benytter og hvordan vi forstår dem. Denne utviklingen går raskere enn hva lovtekst klarer å holde følge med, og det er derfor viktig å ha en oppdatert tolkning og forståelse av de ulike typene cyberkriminalitet.

Den store fordelen med systematiske litteraturstudier som dette er at de enkelt kan repeteres med jevne mellomrom for å fange opp ny informasjon og endringer. I den vedlagte protokollen til dette studiet har vi beskrevet nøyaktig hvilke søkestrenger som er brukt opp mot de ulike indekseringsdatabasene og sørget for full sporbarhet til resultatene. Så lenge selve funksjonaliteten til disse databasene ikke endrer seg, kreves det ikke mye arbeid å gjenta søkene om for eksempel to eller tre år. En oppdatering av kunnskapsoversikten trenger dermed bare å se på differansen mellom eksisterende syntetisering og ny litteratur.

6.1.1 Nye begreper og definisjoner

Som påpekt av referansegruppen er det enkelte begreper, spesielt aktuelle det siste året, som ikke inngår i denne kunnskapsoversiken. Dette er riktig da vår stoppdato for artikkelinnsamling var midten av februar 2023. Og selvfølgelig stoppet ikke verden opp da. For eksempel ble språkmodellen GPT-4 lansert 14. mars 2023, og skapte mye furore i media knyttet til cyberkriminelles potensielle bruk av *generativ kunstig intelligens*, noe også Kripos tegnet bilde av i sin temarapport fra Juli 2023 [171]. Denne typen bruk av store språkmodeller var ikke nytt da heller, men den økte støtten for flere symboler gjorde at kapasitet og effekt utgjorde et nytt fenomen som lettere kunne brukes til kriminelle handlinger.

Fagfellevurdert litteratur har en utgivelsessyklus som kan være tidkrevende. Tar vi igjen eksempelet med GPT-4, betyr det at de tidligste vitenskapelige eksperimentene med denne modellen ble gjennomført og

sendt til publisering i april-mai. Prosessen med fagfellevurdering, som skal sikre kvalitet og metodisk riktighet tar gjerne 4-5 måneder. Videre kan selve publiseringsprosessen og indeksering også ta flere uker. Derfor er det først rundt november 2023 vi kan se fagfellevurdert litteratur som omhandler GPT-4. For å generalisere, det tar gjerne et halvt år fra et fenomen oppstår til man har tilgjengelig fagfellevurdert litteratur som omhandler det (og ofte lengre tid).

I praksis får man heldigvis gjerne tilgang på resultater før de har blitt offisielt publisert gjennom fortrykk eller foredrag, og vi har her lyst til å nevne begreper som vi ser for oss vil komme ytterst i Type III cyberkriminalitet, altså fenomener som er per i dag teknisk krevende eller umodent, men som over tid kan bevege seg til å bli mer tilgjengelig for cyberkriminelle:

- «*DeepCrime*» er et begrep vi har observert brukt på nylige cybersikkerhetskonferanser knyttet til ondsinnede angrep mot eller påvirkning av maskinlæringsalgoritmer. Dette er mer spesifikt enn «*malicious attacks against AI*» / «ondsinnede angrep mot KI», og vi tror flere slike mer spesifikke begreper knyttet til cyberkriminalitet vil dukke opp ettersom sårbarheter i KI avdekkes.
- «Kriminalitet begått med generativ kunstig intelligens» er begrepet Kripos benytter i sin temarapport [171], og er et eksempel hvor KI benyttes som verktøy[12] for kriminelle. Men generativ KI er mer en verktøykasse som inneholder et bredt spekter av teknikker[13] som kan misbrukes. Det er også her grunn til å tro at vi får mer spesifikke begreper, for eksempel avhengig av om man genererer støtende tekst, falske bilder, misvisende lyd, ondsinnet kildekode eller bryter personvernet eller åndsverk. Mer generelt hører dette inn under «ondsinnet bruk av KI»/ «*malicious/adverse use of AI*».
- «*Quantum computing crime*» er knyttet til teoretisk misbruk av kvantedatamaskiner for å enklere kunne knekke krypteringsnøkler og stjele informasjon. Dette foregår mye forskning på kvante-datamaskiner og fenomenet omtales i diverse trusselrapporter (for eksempel fra PST [172] og NSM [173]), men vi har ikke observert dette i vårt utvalg av fagfellevurdert litteratur knyttet til cyberkriminalitet. Dette vil likevel være naturlig å plassere under «*using advanced technology*» om vi skal bruke Phillips et al. sin taksonomi.
- «*Biological computing crime*» kan sees på som en alternativ måte å knekke koder på, hvor levende celler utvikles til å gjøre ekstremt raske beregninger. Her er teknologien knapt i krybbestadiet, men det økende antall publikasjoner om biologiske datamaskiner i 2023 hinter om et nytt fenomen som er i anmarsj og som sikkert kan misbrukes.

6.2 Måling av omfang overført til Norge

Litteraturen gir klare råd om at det er veldig vanskelig å måle cyberkriminalitet på overordnet nivå, siden begrepet er så løst definert. Man vil også få misvisende tall og trender siden underlagsdataene vil være mangelfulle og skeivfordelte. Derimot bør måling gjøres i forhold til mer spesifikke typer eller grupperinger av cyberkriminalitet, slik vi har redegjort for i denne kunnskapsoversikten. Det er også anbefalinger om å bruke ulike målemetoder og kilder for ulik type cyberkriminalitet, igjen fordi underlagsmaterialet er fragmentert, manglende og skeivfordelt. Eksempelvis er befolkningsundersøkelser eller offerstudier for typer cyberkriminalitet som ofte ikke blir anmeldt, blitt benyttet i USA, Storbritannia, Belgia, Frankrike, Finland, Nederland og Australia etter 2015. Spesielt får *Crime Survey for England and Wales* mye positiv omtale i vår litteratur. Denne er ment til å fange opp omfang av kriminalitet som ikke blir rapportert til eller registrert av politiet, samtidig som den får fram endringer mellom tradisjonell kriminalitet og nye og frem-

[12] Generativ KI er ikke et ondsinnet verktøy i seg selv, men kan misbrukes. Forsiden på denne rapporten er for eksempel laget ved hjelp av en type generativ KI betegnet som «stable infusion».

[13] For eksempel «Recurrent Neural Networks» (RNNs), som kan brukes til ulovlig overvåkning, eller Generative Adversarial Networks (GANs), som kan brukes til å rekonstruere sensitive opplysninger om individer.

voksende typer. Vi har gjengitt et utdrag av kategorier fra denne undersøkelsen i vedlegg B, og tror disse kan være overførbare til Norge.

Det er vanskelig å fastslå at omfanget som beskrives i litteraturen kan si noe direkte om norske forhold. Likevel er det naturlig å anta at den økende trenden av cyberkriminalitet som man ser i litteraturen også gjenspeiler situasjonen i Norge. Mange av artiklene i utvalget vårt referer til rapporter fra sikkerhetsselskaper for å si noe om omfang. For eksempel går rapportene fra McAfee og CSIS mye igjen. Målemetoden de har brukt er ikke veldig godt beskrevet, men de har samlet åpent tilgjengelige data om kostnader fra noen titalls land rundt om i verden og kombinert dette med intervjuer hos stort sett vestlige selskaper og myndigheter. De har så laget en kalkyle hvor kostnadene fra cyberangrep i forskjellige regioner er estimert til å være en prosentandel av GDP. I den seneste rapporten fra 2020 var dette estimatet på litt over 1% av global GDP, som utgjør rundt $ 1 trillion (norsk: billion) på verdensbasis. Om vi anvender samme prosentestimat på norsk bruttonasjonalprodukt i 2020[14] får vi rundt 34 milliarder kroner for Norge. Dette er ikke tall vi har veldig mye lit til da selve metoden er dårlig dokumentert, tar ikke særlig høyde for lokale variasjoner og baserer seg på åpne data av svært variabel kvalitet. I tillegg bruker McAfee en definisjon av cyberkriminalitet som er begrenset til at kriminelle får tilgang til et offers datamaskin eller nettverk. Det vi heller kan ta med oss fra de forskjellige utgavene av denne rapporten er at dette prosenttallet har steget betydelig, henholdsvis 0,62% i 2014, 0,8% i 2018 og 1% i 2020.

Dersom vi velger å anta at Norge har lignende nivå av teknologi og sosiale forhold som England og Frankrike kan vi anta at omtrent halvparten av all vinningskriminalitet gjøres over nett. Ved å ta utgangspunkt i anmeldt fysisk vinningskriminalitet (som gjerne blir anmeldt), kan man kanskje anta at den digitale motparten er like stor. Likevel blir slike anslag veldig usikre, spesielt med tanke på at dette forholdstallet er i endring.

Den amerikanske befolkningsundersøkelsen omtalt av Breen et al. [98] viste at kostnadene cyberkriminalitet påfører gjennomsnittsamerikaneren ligger på rundt $23 i året. Dersom vi omregner dette basert på *Purchasing Power Parities*, som tar hensyn til både prisnivå og kjøpekraft i hvert enkelt land, kan det tilsvare et tap rundt 350 NOK årlig for en gjennomsnittsnordmann (tall basert på 2022 fra FN [174]). Igjen, dette blir veldig spekulativt da det er store forskjeller mellom USA og Norge, og derfor ingen god målestokk.

Forskere som Broadhead [13] påpeker at selv om selve omfanget er vanskelig å måle (jf. 3.4), kan man si noe om endringen basert på tilgjengelige datakilder. Spesielt trekkes fram måling av kostnader knyttet til 1) kriminell inntekt, 2) direktetap, 3) indirekte tap, 4) beskyttelseskostnad og 5) kostnader for samfunnet. Vi anbefaler derfor å følge Broadhead [13] og Anderson et al. [72] sin tilnærming med å fokusere på endringer og trender av ulik type cyberkriminalitet, heller enn å prøve å måle totalomfang. Dette reduserer feilkilder og vil ha en større nytteverdi med hensyn til hvor tiltak bør iverksettes. Det vil kreve gjentagende målinger over tid og fordre en godt beskrevet metodikk som er uavhengig av spesifikke institusjoner. Vi fikk også tilbakemelding fra referansegruppen om at denne typen oversikt er interessant, fordi endringer sier noe om hvor problemet er voksende og om motvirkende tiltak har effekt.

Som allerede nevnt, utvikler INTERPOL plattformen INSIGHT for å hente inn data om cyberkriminalitet. Skal Norge bidra til denne vil det være naturlig å forholde seg til hva INTERPOL ønsker. *INTERPOL National Cybercrime Strategy Guidebook* [66] inkluderer en mal for å måle cyberkriminalitet, og lister her følgende eksempler på figurer og trender som bør rapporteres knyttet til en nasjons statistikk på cyberkriminalitet:

- Antallet «cyber-dependent» angrep etter type, f.eks. løsepengevirusangrep i en gitt periode.
- Antallet «cyber-enabled» kriminalitet rapportert i en gitt periode.

[14] Ifølge Statistisk Sentralbyrå var BNP i Norge på 3 413 milliarder kroner i 2020.

- Hovedtyper av cyberkriminalitet (tjenestenekt, vansiring av Web-sider, løsepengevirus, *phishing*, overgrepsmateriale, trakassering på nett, osv.).
- Økning i ulike typer cyberkriminalitet, prosentvis og faktiske tall over en gitt periode, f.eks. år-for-år.

Blant internasjonale retningslinjer, finner vi *Guide for Criminal Justice Statistics on Cybercrime and Electronic Evidence* [175], som beskriver en plan for sammenstilling av strafferettsstatistikk med viktige steg for datainnsamling, analyse og samarbeid mellom flere interessenter. Det skilles her mellom praksis for datainnsamling hos politiet, rettsmyndighetene og andre aktører (som CERT/CSIRT og cybersikkerhets-industrien). Det vil være naturlig å basere et system for måling av omfang i Norge på denne veilederen.

På et mer generelt nivå ser vi for oss at følgende steg er sentrale for en undersøkelse knyttet til omfang i Norge:

1. Identifisere hvilke typer cyberkriminalitet det er interessant å kunne måle.
2. Identifisere målemetoder og alternative datakilder knyttet til valgte typer cyberkriminalitet. Hvilke eksisterende norske undersøkelser kan utvides?
3. Gjennomføre en eller flere typer målinger som prioriteres på gitt tidspunkt.
4. Dataanalyse av måling(er). Hvordan unngå duplikater når flere kilder sammenstilles?
5. Kommunisere resultater til ulike målgrupper.
6. Planlegge gjentagelse.

Disse stegene har blitt presentert for aktører i referansegruppen med positiv tilbakemelding. Et mer detaljert undersøkelsesdesign vil måtte utvikles i samarbeid mellom flere aktører og dette krever god dialog. Et konkret innspill fra referansegruppen var å fortsette med lignende tverrfaglige møteplasser fremover også, da cyberkriminalitet er et problem som må forstås og adressers i fellesskap. Ulike aktører fra både privat og offentlig sektor sitter allerede med en god del data, og det er lite hensiktsmessig å gjøre dobbeltarbeid. Samtidig må eierskap og insentiver for å dele data bli avklart.

6.2.1 Eksisterende undersøkelser som måler omfang av cyberkriminalitet i Norge

Det finnes en rekke undersøkelser som på ulike måter måler omfang av cyberkriminalitet i Norge. For å kartlegge hvilke typer cyberkriminalitet som dekkes av de mest sentrale undersøkelsene, er det gjort en kartlegging av disse mot henholdsvis Budapestkonvensjonen [16] og klassifiseringen fra Phillips et al. [8]. Dette innebærer at de enkelte spørsmålene i hver undersøkelse er vurdert for relevans mot de ulike kategoriene. Tabell 9 gir en oversikt over denne kartleggingen. Mer detaljerte beskrivelser av de enkelte undersøkelsene og hvilke temaer som dekkes finnes i vedlegg B.

Tabell 9. Gjennomgang av Norske undersøkelser mot hhv. Budapestkonvensjonen og klassifiseringen i Phillips et al.

Undersøkelse	Klassifisering i *Budapestkonvensjonen*	Klassifisering i *Phillips et al.*
Mørketallsundersøkelsen	2 Ulovlig tilgang 4 Inngrep i dataens integritet 5 Inngrep i driften av et datasystem 6 Misbruk av innretninger og tilgangsdata 8 Datarelatert bedrageri	Illegal access (hacking/cracking) Illegal data acquisition (data espionage) Data interference System Interference Misuse of Device Extortion/Ransomware Computer-related fraud Phishing Cyberfraud

Undersøkelse	Klassifisering i *Budapestkonvensjonen*	Klassifisering i *Phillips et al.*
Kriminalitets- og sikkerhetsundersøkelsen Norge (KRISINO)	5 Inngrep i driften av et datasystem 8 Datarelatert bedrageri	System interference Extortion/Ransomware Computer-related fraud Trademarks and related offenses Phishing
Nasjonal omfangsundersøkelse av økonomisk kriminalitet rettet mot virksomheter og kommuner	2 Ulovlig tilgang 5 Inngrep i driften av et datasystem 8 Datarelatert bedrageri	Illegal access (hacking/cracking) System interference Extortion/Ransomware Computer-related fraud Phishing
Bedrageri mot næringslivet	2 Ulovlig tilgang 6 Misbruk av innretninger og tilgangsdata 8 Datarelatert bedrageri	Illegal access (hacking/cracking) Misuse of device Computer-related fraud Identity theft Phishing
Nasjonal trygghetsundersøkelse	8 Datarelatert bedrageri	Computer-related fraud Identity theft Harassment Image based abuse Sextortion
Politiets innbyggerundersøkelse	8 Datarelatert bedrageri	Computer-related fraud Identity theft Harassment Extortion (e.g., Romance fraud) Image based abuse

Sammenstillingen over er basert på spørsmål fra *siste års utgave* av de ulike undersøkelsene. Det kan derfor være tilfeller av at undersøkelser fra tidligere år dekker kategorier som ikke fremgår her. Dette gjelder blant annet *Politiets innbyggerundersøkelse*. Undersøkelsene i tabellen dekker spørsmål som relaterer seg til de ulike artiklene i Budapestkonvensjonen og kategoriene i Phillips et al. på ulike måter og i ulikt omfang. Eksempelvis inkluderer Mørketallsundersøkelsen ett spørsmål om hvorvidt virksomheten har vært utsatt for bedrageri, mens KRISINO inkluderer flere spørsmål om ulike typer for svindel/bedrageri. Det er også enkeltspørsmål som kan kobles opp mot flere av kategoriene. Et eksempel finner vi i KRISINO, som spør om bedriftens merkevare/logo har blitt misbrukt i falske annonser/kampanjer på nett, SMS eller i epost. Spørsmålet relateres til *Computer-related fraud*, men også til *Trademarks and related offenses* og *Phishing*.

Oppsummert viser sammenstillingen at det under Budapestkonvensjonens kategori A (Straffbare handlinger som rammer datasystemers og dataenes fortrolige karakter, integritet og tilgjengelighet) kun er artikkel 3 (Ulovlig oppfanging av data) som ikke direkte omfattes av disse undersøkelsene. For kategori B (Straffbare handlinger knyttet til datamaskiner) inkluderer samtlige av undersøkelsene spørsmål relatert til artikkel 8 (Datarelatert bedrageri), men det er derimot ingen spørsmål knyttet til datarelatert falsk (artikkel 7). Verken kategori C (Straffbare handlinger knyttet til innhold), kategori D (Straffbare handlinger knyttet til krenkelser av opphavsrett og nærstående rettigheter) eller kategori E (Kriminalisering av rasistiske og fremmed-fiendtlige handlinger begått i et datasystem) er direkte omfattet av undersøkelsene.

Videre viser gjennomgangen at undersøkelsene samlet sett inkluderer mange spørsmål knyttet til Phillips et al. sin underkategori *Against individuals and organisations* (under *1. Attacks against data and systems*). *Illegal interception* og *Heist* er de eneste eksemplene i denne underkategorien som ikke er omfattet. Det er likevel verdt å merke at kategorien kun dekkes av undersøkelsene som retter seg mot virksomheter, næringsliv og kommuner, og ikke av de to undersøkelsene som er rettet mot individer. Underkategorien *Against States and Nations* dekkes ikke av undersøkelsene. For *2. Attacks against property or theft* ser vi at

undersøkelsene ikke omfatter spørsmål knyttet til *Computer-related forgery*, *Copyright infringement*, *Digital piracy* og *Spam*. Både *Harassment* og *Extortion (e.g., Roance Fraud)* under *3. Interpersonal Violence* dekkes av spørsmål i undersøkelsene rettet mot individer. Under *4. Sexual Violence* er det derimot kun *Image based abuse* og *sextortion* som omfattes. Undersøkelsene inkluderer ingen spørsmål relatert til de øvrige kategoriene i klassifiseringen til Phillips et al.: *5. Violence Against Groups*, *6. Violence (General)*, *7. Incidental Technology Use*, *8A. Using Advanced Technology* og *8B. Using false Information*. Dersom man løfter blikket til de mer overordnede kategoriene i Phillips et al. sin klassifisering, viser gjennomgangen at undersøkelsene i stor grad dekker spørsmål som omhandler *I Crimes against the machine* og *II Crimes using the machine*. Deler av *III Crimes in the machine* dekkes, mens verken *IV Cyber assisted, V Cross-category: Organised Crime, Deep Web Markets, Illegal Virtual Marketplaces and Cybercrime-as-a-Service* eller *VI Cross category: Information and behavioural Manipulation* omfattes av disse undersøkelsene.

7 Kilder

[1] B.-J. Koops, 'The Internet and its Opportunities for Cybercrime'. Rochester, NY, Dec. 01, 2010. doi: 10.2139/ssrn.1738223.

[2] Riksrevisjonen, 'Riksrevisjonens undersøkelse av politiets innsats mot kriminalitet ved bruk av IKT: Dokument 3:5'. 2021. [Online]. Available: https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-politiets-innsats-mot-kriminalitet-ved-bruk-av-ikt

[3] UN, 'UNODC Comprehensive Study on Cybercrime', United Nations Office on Drugs and Crime (UNODC), Feb. 2013. Accessed: Nov. 06, 2023. [Online]. Available: https://www.icnl.org/post/report/unodc-comprehensive-study-on-cybercrime

[4] L. Paoli, J. Visschers, and C. Verstraete, 'The impact of cybercrime on businesses: a novel conceptual framework and its application to Belgium', *Crime Law Soc. Change*, vol. 70, no. 4, pp. 397–420, Nov. 2018, doi: 10.1007/s10611-018-9774-y.

[5] Justiskomiteen, 'Innst. O. nr. 66'. Lovdata, 2005. [Online]. Available: https://lovdata.no/static/INNST/inno-200405-066.pdf

[6] B. L. Andreassen, 'Vil ha slutt på bruken av ordet «barneporno»'. Accessed: Nov. 20, 2023. [Online]. Available: https://www.advokatbladet.no/vil-ha-slutt-pa-bruken-av-ordet-barneporno/112843

[7] E. Bergskaug, 'Kripos vil ha slutt på bruken av begrepet «barneporno»', Vårt Land. Accessed: Nov. 20, 2023. [Online]. Available: https://www.vl.no/nyheter/2021/02/24/kripos-vil-ha-slutt-pa-bruken-av-begrepet-barneporno/

[8] K. Phillips, J. C. Davidson, R. R. Farr, C. Burkhardt, S. Caneppele, and M. P. Aiken, 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies', *Forensic Sci.*, vol. 2, no. 2, pp. 379–398, Apr. 2022, doi: 10.3390/forensicsci2020028.

[9] S. De Paoli *et al.*, 'A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists', *Polic. J. Policy Pract.*, vol. 15, no. 2, pp. 1429–1445, 2021.

[10] M. McGuire, 'It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime', in *The Human Factor of Cybercrime*, Routledge, 2019.

[11] P. H. Meland, 'Storyless cyber security: Modelling threats with economic incentives', NTNU, 2021. Accessed: Nov. 04, 2023. [Online]. Available: https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2825312

[12] M. Nouh, J. R. Nurse, H. Webb, and M. Goldsmith, 'Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement', *ArXiv Prepr. ArXiv190206961*, 2019.

[13] S. Broadhead, 'The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments', *Comput. Law Secur. Rev.*, vol. 34, no. 6, pp. 1180–1196, Dec. 2018, doi: 10.1016/j.clsr.2018.08.005.

[14] S. Furnell and S. Dowling, 'Cyber crime: a portrait of the landscape', *J. Criminol. Res. Policy Pract.*, vol. 5, no. 1, pp. 13–26, Jan. 2019, doi: 10.1108/JCRPP-07-2018-0021.

[15] S. Lazarus, M. Button, and R. Kapend, 'Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types', *Howard J. Crime Justice*, vol. 61, no. 3, pp. 381–398, 2022, doi: 10.1111/hojo.12485.

[16] COE, 'Convention on Cybercrime', ETS no. 85, 2001. [Online]. Available: https://rm.coe.int/1680081561

[17] M. Sackson, 'Computer ethics: are students concerned?', 1996, Accessed: Oct. 10, 2023. [Online]. Available: https://digitalcommons.pace.edu/cgi/viewcontent.cgi?article=1030&context=tech

[18] U. V. Awhefeada and O. O. Bernice, 'Appraising the Laws Governing the Control of Cybercrime in Nigeria', *J. Law Crim. Justice*, vol. 8, no. 1, pp. 30–49, 2020.

[19] UN, 'Crimes related to computer networks :: background paper for the Workshop on Crimes related to the Computer Network', UN, Vienna, Feb. 2000. Accessed: Oct. 05, 2023. [Online]. Available: https://digitallibrary.un.org/record/432653

[20] V. Babanina, I. Tkachenko, O. Matiushenko, and M. Krutevych, 'Cybercrime: History of formation, current state and ways of counteraction', *Amazon. Investiga*, vol. 10, no. 38, pp. 113–122, 2021.

[21] B. D. Loader and D. Thomas, *Cybercrime: Law enforcement, security and surveillance in the information age*. Routledge, 2000.

[22] N. Akdemir, B. Sungur, and B. Başaranel, 'Examining the Challenges of Policing Economic Cybercrime in the UK', *Güven. Bilim. Derg.*, no. International Security Congress Special Issue, pp. 113–134, 2020.

[23] D. S. Wall, *Crime and the Internet*. Routledge, 2001. Accessed: Oct. 20, 2023. [Online]. Available: https://www.routledge.com/Crime-and-the-Internet/Wall/p/book/9780415244299
[24] J. G. L. Cordova, P. F. C. Álvarez, F. de J. E. Ferrandiz, and J. C. Pérez-Bravo, 'Law versus Cybercrime', *Glob. Jurist*, vol. 18, no. 1, Apr. 2018, doi: 10.1515/gj-2017-0024.
[25] P. Pati, 'CYBER CRIME'. Accessed: Oct. 11, 2023. [Online]. Available: https://www.naavi.org/pati/pati_cybercrimes_dec03.htm
[26] O. Goni, 'Cyber crime and its classification', *Int J Electron. Eng. Appl.*, vol. 10, no. 1, 2022.
[27] D. Heimans, 'Cybercrime-the EU response', 2004. Accessed: Oct. 11, 2023. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/1514379/
[28] S. K. Srivastava, S. Das, G. J. Udo, and K. Bagchi, 'Determinants of Cybercrime Originating within a nation: A cross-country study', *J. Glob. Inf. Technol. Manag.*, vol. 23, no. 2, pp. 112–137, 2020.
[29] S. D. Moitra, 'Developing policies for cybercrime: Some empirical issues', *Eur J Crime Crim Crim Just*, vol. 13, p. 435, 2005.
[30] I. M. Luknar, 'Cybercrime-Emerging Issue', *Arch. Reiss Days*, vol. 10, 2020.
[31] S. Gordon and R. Ford, 'On the definition and classification of cybercrime', *J. Comput. Virol.*, vol. 2, no. 1, pp. 13–20, Aug. 2006, doi: 10.1007/s11416-006-0015-z.
[32] A. Graham, T. C. Kulig, and F. T. Cullen, 'Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice', *Policing*, vol. 43, no. 1, pp. 1–16, 2020, doi: 10.1108/PIJPSM-07-2019-0115.
[33] G. Conway and L. Hadlington, 'How Do Undergraduate Students Construct Their View of Cybercrime? Exploring Definitions of Cybercrime, Perceptions of Online Risk and Victimization', *Polic. Oxf.*, vol. 15, no. 1, pp. 119–129, 2021, doi: 10.1093/police/pay098.
[34] V. Ratten, 'The effect of cybercrime on open innovation policies in technology firms', *Inf. Technol. People*, vol. 32, no. 5, pp. 1301–1317, Jan. 2019, doi: 10.1108/ITP-03-2018-0119.
[35] S. W. Brenner, 'Cybercrime, cyberterrorism and cyberwarfare', *Rev. Int. Droit Pénal*, vol. 77, no. 3, pp. 453–471, 2006.
[36] T. Somer, 'Taxonomies of cybercrime: An overview and proposal to be used in mapping cyber criminal journeys', presented at the European Conference on Information Warfare and Security, ECCWS, 2019, pp. 475–483.
[37] EU, 'Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime {SEC(2007) 641} {SEC(2007) 642} /* COM/2007/0267 final */'. 2007. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52007DC0267
[38] A. Chandra and M. J. Snowe, 'A taxonomy of cybercrime: Theory and design', *Int. J. Account. Inf. Syst.*, vol. 38, p. 100467, Sep. 2020, doi: 10.1016/j.accinf.2020.100467.
[39] R. Anderson *et al.*, 'Measuring the Changing Cost of Cybercrime', *18th Annu. Workshop Econ. Inf. Secur.*, 2019, doi: https://doi.org/10.17863/CAM.41598.
[40] C. Wilson, *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress*, vol. 29. Congressional Research Service Washington, DC, 2008. Accessed: Oct. 10, 2023. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA477642
[41] D. S. Wall, 'Cybercrime: The transformation of technology in the networked age'. Cambridge: Polity Press, 2007.
[42] M. Shan-A-Khuda and Z. C. Schreuders, 'Understanding cybercrime victimisation: Modelling the local area variations in routinely collected cybercrime police data using latent class analysis', *Int. J. Cyber Criminol.*, vol. 13, no. 2, pp. 493–510, 2019, doi: 10.5281/zenodo.3708924.
[43] N. Kshetri, 'Positive externality, increasing returns, and the rise in cybercrimes', *Commun. ACM*, vol. 52, no. 12, pp. 141–144, Desember 2009, doi: 10.1145/1610252.1610288.
[44] N. Kshetri, 'The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures', in *The Global Cybercrime Industry*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 1–34. doi: 10.1007/978-3-642-11522-6_1.
[45] EC-Council, 'Investigation Procedures and Response'. Cengage Learning, 2010.
[46] B. Amro, 'Cybercrime as a Matter of the Art in Palestine and its Effect on Individuals', Sep. 2018, Accessed: Feb. 16, 2023. [Online]. Available: http://dspace.hebron.edu:80/xmlui/handle/123456789/47
[47] D. Halder and K. Jaishankar, *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations: Laws, Rights and Regulations*. Igi Global, 2011. Accessed: Oct. 11, 2023. [Online]. Available: https://www.academia.edu/download/87786799/CYBER_WOMEN_VICTIMIZATION_BOOK.pdf
[48] M. M. Azad, K. N. Mazid, and S. S. Sharmin, 'Cyber crime problem areas, legal areas and the cyber crime law', *Int. J. New Technol. Res.*, vol. 3, no. 5, pp. 1–6, 2017.
[49] J. C. O. Pradillo, 'Fighting against cybercrime in Europe: the admissibility of remote searches in Spain', *Eur J Crime Crim Crim Just*, vol. 19, p. 363, 2011.
[50] ISO/IEC, 'ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity'. 2012. [Online]. Available: https://www.iso.org/standard/44375.html
[51] SA, *Electronic Communications and Transactions Amendment Bill*. [Online]. Available: https://cybercrime.org.za/docs/ECT_Amendment_Bill_2012.pdf

[52] V. A. Nomokonov and T. L. Tropina, 'Kiberprestupnost'kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat] Kriminologiya: vchera, segodnya, zavtra [Criminology: yesterday, today, tomorrow]'. 2012.
[53] K. Almazkyzy and Y. N. Esteusizov, 'The essence and content of cybercrime in modern times', *J. Adv. Res. Law Econ.*, vol. 9, no. 3 (33), pp. 834–841, 2018.
[54] S. Malby, R. Mace, A. Holterhof, C. Brown, S. Kascherus, and E. Ignatuschtschenko, 'Comprehensive study on cybercrime', *U. N. Off. Drugs Crime Tech Rep*, 2013.
[55] F. Gerry and C. Moore, 'A Slippery and Inconsistent Slope: How Cambodia's Draft Cybercrime Law Exposed the Dangerous Drift Away from International Human Rights Standards'. Rochester, NY, Sep. 01, 2015. Accessed: Oct. 13, 2023. [Online]. Available: https://papers.ssrn.com/abstract=2664766
[56] D. K. O. Mendoza, 'The vulnerability of cyberspace-the cyber crime', *J. Forensic Sci. Crim. Investig.*, vol. 2, no. 1, pp. 1–8, 2017.
[57] B. Akhgar *et al.*, 'Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism', in *Combatting Cybercrime and Cyberterrorism*, B. Akhgar and B. Brewster, Eds., in Advanced Sciences and Technologies for Security Applications. , Cham: Springer International Publishing, 2016, pp. 295–321. doi: 10.1007/978-3-319-38930-1_16.
[58] E. F. G. Ajayi, 'Challenges to enforcement of cyber-crimes laws and policy', *J. Internet Inf. Syst.*, vol. 6, no. 1, pp. 1–12, 2016.
[59] K. H. Mohammed, Y. D. Mohammed, and A. A. Solanke, 'Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria', *Int. J. Cybersecurity Intell. Cybercrime*, vol. 2, no. 1, pp. 56–63, 2019.
[60] Symantec, '11 ways to help protect yourself against cybercrime'. Accessed: Oct. 06, 2023. [Online]. Available: https://us.norton.com/blog/how-to/how-to-recognize-and-protect-yourself-from-cybercrime
[61] EC3, 'Internet Organised Crime Threat Assessment'. Obtenido de EUROPOL: https://www. europol. europa. eu/iocta/2017/index. html, 2017. [Online]. Available: https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf
[62] AICPA, 'How CPAs can protect themselves and their clients. February. Top Cybercrimes White Paper.' 2017. [Online]. Available: https://us.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/resources/privacy/cybersecurity/downloadabledocuments/top-5-cybercrimes.pdf
[63] 'Cybercrime | Definition, Statistics, & Examples | Britannica'. Accessed: Oct. 10, 2023. [Online]. Available: https://www.britannica.com/topic/cybercrime
[64] 'cybercrime - Quick search results | Oxford English Dictionary'. Accessed: Oct. 11, 2023. [Online]. Available: https://www.oed.com/search/dictionary/?scope=Entries&q=cybercrime
[65] L. Hadlington, K. Lumsden, A. Black, and F. Ferra, 'A Qualitative Exploration of Police Officers' Experiences, Challenges, and Perceptions of Cybercrime', *Polic. J. Policy Pract.*, vol. 15, no. 1, pp. 34–43, Mar. 2021, doi: 10.1093/police/pay090.
[66] INTERPOL, 'National Cybercrime Strategy Guidebook'. 2021. [Online]. Available: https://cybilportal.org/publications/national-cybercrime-strategy-guidebook/
[67] Kripos, 'Cyberkriminalitet 2023', Apr. 2023. [Online]. Available: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/cyberkriminalitet-2023.pdf
[68] H. S. Lallie *et al.*, 'Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic', *Comput. Secur.*, vol. 105, p. 102248, Jun. 2021, doi: 10.1016/j.cose.2021.102248.
[69] CPS, 'Cybercrime - prosecution guidance | The Crown Prosecution Service'. Accessed: Oct. 06, 2023. [Online]. Available: https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance
[70] S. Gordon and R. Ford, 'Cyberterrorism?', *Comput. Secur.*, vol. 21, no. 7, pp. 636–647, 2002.
[71] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, 'Comprehensive Review of Cybercrime Detection Techniques', *IEEE Access*, vol. 8, pp. 137293–137311, 2020, doi: 10.1109/ACCESS.2020.3011259.
[72] R. Anderson *et al.*, 'Measuring the Cost of Cybercrime', in *The Economics of Information Security and Privacy*, R. Böhme, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 265–300. doi: 10.1007/978-3-642-39498-0_12.
[73] D. S. Wall and A. Pattavina, 'The internet as a conduit for criminals (pp, 77-98)', *Inf. Technol. Crim. Justice Syst. Thousand Oaks CA Sage*, 2005.
[74] R. Sarre, L. Y.-C. Lau, and L. Y. C. Chang, 'Responding to cybercrime: current trends', *Police Pract. Res.*, vol. 19, no. 6, pp. 515–518, Nov. 2018, doi: 10.1080/15614263.2018.1507888.
[75] S. Ibrahim, 'Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals', *Int. J. Law Crime Justice*, vol. 47, pp. 44–57, 2016.
[76] S. Lazarus, 'Just married: the synergy between feminist criminology and the Tripartite Cybercrime Framework', *Int. Soc. Sci. J.*, vol. 69, no. 231, pp. 15–33, 2019.
[77] S. Ghernaouti-Helie, *Cyber power: Crime, conflict and security in cyberspace*. Crc Press, 2013. Accessed: Nov. 05, 2023. [Online]. Available: https://books.google.com/books?hl=en&lr=&id=eYJFAQAAQBAJ&oi=fnd&pg=PP1&dq=Cyberpower:+Crime,+Conflict+and+Security+in+Cyberspace&ots=_AdR1th-ru&sig=BvvbW4JOwesRUcU74NehJGkPDbc

[78] J. Hakmeh and A. Peters, 'A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet', Council on Foreign Relations. Accessed: Oct. 11, 2023. [Online]. Available: https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet

[79] COE, 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems', ETS No. 189, 2003. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

[80] Lovdata, 'Konvensjon om datakriminalitet - ETS nr. 185 - Lovdata'. Accessed: Jan. 03, 2024. [Online]. Available: https://lovdata.no/dokument/TRAKTAT/traktat/2001-11-23-1

[81] Lovdata, 'Tilleggsprotokoll som gjelder kriminalisering av rasistiske og fremmedfiendtlige handlinger begått i et datasystem til Konvensjon om datakriminalitet - ETS nr. 189 - Lovdata'. Accessed: Jan. 03, 2024. [Online]. Available: https://lovdata.no/dokument/TRAKTAT/traktat/2003-01-28-192?q=datakrim

[82] J. Clough, 'The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World', *Crim. Law Forum*, vol. 23, no. 4, pp. 363–391, Dec. 2012, doi: 10.1007/s10609-012-9183-3.

[83] G. Tsakalidis and K. Vergidis, 'A Systematic Approach Toward Description and Classification of Cybercrime Incidents', *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 49, no. 4, pp. 710–729, Apr. 2019, doi: 10.1109/TSMC.2017.2700495.

[84] G. Tsakalidis, K. Vergidis, S. Petridou, and M. Vlachopoulou, 'A cybercrime incident architecture with adaptive response policy', *Comput. Secur.*, vol. 83, pp. 22–37, 2019.

[85] EU, 'Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA', OJ L 218, 2013. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

[86] EDPD, 'Statement 02/2021 on new draft provisions of the second additional protocol to the Council of Europe Convention on Cybercrime (Budapest Convention) | European Data Protection Board'. Accessed: Nov. 05, 2023. [Online]. Available: https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-022021-new-draft-provisions-second-additional_en

[87] T. Sõmer, 'Modelling Financially Motivated Cyber Crime', Tallin Univesrity of Technology, 2022. Accessed: Jan. 03, 2024. [Online]. Available: https://digikogu.taltech.ee/en/Download/7b78abe7-8a51-4cbb-9720-03f04746e13a/ModellingFinanciallyMotivatedCyberCrime.pdf

[88] IWGT, 'Terminology guidelines for the protection of children from sexual exploitation and sexual abuse', Ecpat International, 2016. [Online]. Available: https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf

[89] D. Jeong, 'Artificial Intelligence Security Threat, Crime, and Forensics: Taxonomy and Open Issues', *IEEE Access*, vol. 8, pp. 184560–184574, 2020, doi: 10.1109/ACCESS.2020.3029280.

[90] M. Näsi, P. Danielsson, and M. Kaakinen, 'Cybercrime Victimisation and Polyvictimisation in Finland—Prevalence and Risk Factors', *Eur. J. Crim. Policy Res.*, 2021, doi: 10.1007/s10610-021-09497-0.

[91] S. van de Weijer, R. Leukfeldt, and S. Van der Zee, 'Reporting cybercrime victimization: determinants, motives, and previous experiences', *Policing*, vol. 43, no. 1, pp. 17–34, 2020, doi: 10.1108/PIJPSM-07-2019-0122.

[92] S. Kemp, D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño, 'Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19', *J. Contemp. Crim. Justice*, vol. 37, no. 4, pp. 480–501, 2021, doi: 10.1177/10439862211027986.

[93] C. Barclay, 'Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica', *Commonw. Law Bull.*, vol. 43, no. 1, pp. 77–107, 2017.

[94] A. Nukusheva, R. Zhamiyeva, V. Shestak, and D. Rustembekova, 'Formation of a legislative framework in the field of combating cybercrime and strategic directions of its development', *Secur. J.*, vol. 35, no. 3, pp. 893–912, 2022.

[95] I. M. Sunde, 'Datakrimretten i «fugleperspektiv»', *Tidsskr. Strafferett*, vol. 19, no. 2, pp. 129–147, Jun. 2019, doi: 10.18261/issn.0809-9537-2019-02-02.

[96] M. Junger, L. Montoya, P. Hartel, and M. Heydari, 'Towards the normalization of cybercrime victimization: A routine activities analysis of cybercrime in europe', in *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, Jun. 2017, pp. 1–8. doi: 10.1109/CyberSA.2017.8073391.

[97] T. K. Yerjanov, Z. M. Baimagambetova, A. M. Seralieva, Z. Zhailau, and Z. T. Sairambaeva, 'Legal issues related to combating cybercrime: Experience of the Republic of Kazakhstan', *J. Adv. Res. Law Econ.*, vol. 8, no. 7 (29), pp. 2286–2301, 2017.

[98] C. Breen, C. Herley, and E. M. Redmiles, 'A Large-Scale Measurement of Cybercrime Against Individuals', in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, in CHI '22. New York, NY, USA: Association for Computing Machinery, Apr. 2022, pp. 1–41. doi: 10.1145/3491102.3517613.

[99] M. A. Abdulai, 'Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud', *Int. J. Cyber Criminol.*, vol. 14, no. 1, pp. 157–174, 2020, doi: 10.5281/zenodo.3749468.

[100] Ardiansyah, M. Rafi, and P. Amri, 'The Importance of Strengthening Legal Concepts in Overcoming Cybercrime During the Covid-19 Pandemic in Indonesia', in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Ed., in Lecture Notes in Computer Science. Cham: Springer International Publishing, 2022, pp. 469–479. doi: 10.1007/978-3-031-05563-8_29.

[101] S. G. Correia, 'Patterns of online repeat victimisation and implications for crime prevention', in *2020 APWG Symposium on Electronic Crime Research (eCrime)*, Nov. 2020, pp. 1–11. doi: 10.1109/eCrime51433.2020.9493258.

[102] K. Farahbod, C. Shayo, and J. Varzandeh, 'Cybersecurity indices and cybercrime annual loss and economic impacts', *J. Bus. Behav. Sci.*, vol. 32, no. 1, pp. 63–71, 2020.
[103] C. H. Gañán, M. Ciere, and M. van Eeten, 'Beyond the pretty penny: the Economic Impact of Cybercrime', in *Proceedings of the 2017 New Security Paradigms Workshop*, in NSPW 2017. New York, NY, USA: Association for Computing Machinery, Oktober 2017, pp. 35–45. doi: 10.1145/3171533.3171535.
[104] J. Hawdon, K. Parti, and T. E. Dearden, 'Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment', *Am. J. Crim. Justice*, vol. 45, no. 4, pp. 546–562, 2020, doi: 10.1007/s12103-020-09534-4.
[105] S. Kemp, D. Buil-Gil, F. Miró-Llinares, and N. Lord, 'When do businesses report cybercrime? Findings from a UK study', *Criminol. Crim. Justice*, 2021, doi: 10.1177/17488958211062359.
[106] F. A. M. Khiralla, 'Statistics of cybercrime from 2016 to the first half of 2020', *Int J Comput Sci Netw*, vol. 9, no. 5, pp. 252–261, 2020.
[107] E. R. Leukfeldt, A. Lavorgna, and E. R. Kleemans, 'Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime', *Eur. J. Crim. Policy Res.*, vol. 23, no. 3, pp. 287–300, Sep. 2017, doi: 10.1007/s10610-016-9332-z.
[108] M. Riek and R. Böhme, 'The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates', *J. Cybersecurity*, vol. 4, no. 1, p. tyy004, 2018.
[109] D. W. Woods and L. Walter, 'Reviewing Estimates of Cybercrime Victimisation and Cyber Risk Likelihood', presented at the Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2022, 2022, pp. 150–162. doi: 10.1109/EuroSPW55150.2022.00021.
[110] 'Use of information and communications technology - Statistics Finland'. Accessed: Nov. 13, 2023. [Online]. Available: https://stat.fi/en/surveys/stvk
[111] 'Internet Crime Complaint Center(IC3) | Home Page'. Accessed: Oct. 25, 2023. [Online]. Available: https://www.ic3.gov/
[112] I. Mori, 'Cyber Security Breaches Survey 2020: Statistical Release'.
[113] 'Nature of fraud and computer misuse in England and Wales - Office for National Statistics'. Accessed: Oct. 25, 2023. [Online]. Available: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019
[114] Mariette, 'UK cinema admissions and box office - Monthly admissions', UK Cinema Association. Accessed: Oct. 25, 2023. [Online]. Available: https://www.cinemauk.org.uk/the-industry/facts-and-figures/uk-cinema-admissions-and-box-office/monthly-admissions/
[115] Mariette, 'Latest UK cinema statistics - Monthly admissions', UK Cinema Association. Accessed: Oct. 25, 2023. [Online]. Available: https://www.cinemauk.org.uk/the-industry/facts-and-figures/latest-uk-cinema-statistics/monthly-admissions/
[116] L. E. Cohen and M. Felson, 'Social change and crime rate trends: A routine activity approach', *Am. Sociol. Rev.*, pp. 588–608, 1979.
[117] F. Miró, 'Routine Activity Theory', in *The Encyclopedia of Theoretical Criminology*, 1st ed., J. M. Miller, Ed., Wiley, 2014, pp. 1–7. doi: 10.1002/9781118517390.wbetc198.
[118] Nations Unies, Ed., *United Nations e-government survey 2014: e-government for the future we want*. in ST/ESA/PAD, no. 188. New York: United Nations, 2014.
[119] World Economic Forum, 'COVID-19 Risk Outlook. A Preliminary Mapping and Its Implications.', 2020. [Online]. Available: https://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf
[120] ITU and M. Minges, 'Global Cybersecurity Index 2017', 2017. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
[121] J. Davis, 'COVID-19 Impact on Ransomware, Threats, Healthcare Cybersecurity', HealthITSecurity. Accessed: Nov. 21, 2023. [Online]. Available: https://healthitsecurity.com/news/covid-19-impact-on-ransomware-threats-healthcare-cybersecurity
[122] E. C. Bank, 'Fifth report on card fraud, September 2018', European Central Bank. Accessed: Oct. 25, 2023. [Online]. Available: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport201809.en.html
[123] 'European Cybercrime Centre - EC3', Europol. Accessed: Oct. 25, 2023. [Online]. Available: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[124] 'Crime in England and Wales - Office for National Statistics'. Accessed: Oct. 25, 2023. [Online]. Available: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2017
[125] Ponemon, 'Ponemon Institute', Ponemon Institute. Accessed: Jan. 21, 2024. [Online]. Available: https://www.ponemon.org/
[126] 'FBI Releases the IC3 2017 Internet Crime Report and Calls for Increased Public Awareness — FBI'. Accessed: Oct. 25, 2023. [Online]. Available: https://www.fbi.gov/news/press-releases/fbi-releases-the-ic3-2017-internet-crime-report-and-calls-for-increased-public-awareness
[127] 'SMEs and Cybercrime - mai 2022 - - Eurobarometer survey'. Accessed: Nov. 16, 2023. [Online]. Available: https://europa.eu/eurobarometer/surveys/detail/2280

[128] C. Donalds and K.-M. Osei-Bryson, 'Toward a cybercrime classification ontology: A knowledge-based approach', *Comput. Hum. Behav.*, vol. 92, pp. 403–418, Mar. 2019, doi: 10.1016/j.chb.2018.11.039.
[129] J. Hawdon, 'Cybercrime: Victimization, Perpetration, and Techniques', *Am. J. Crim. Justice*, vol. 46, no. 6, pp. 837–842, 2021, doi: 10.1007/s12103-021-09652-7.
[130] '2014 Security Predictions | SANS Institute'. Accessed: Oct. 25, 2023. [Online]. Available: https://www.sans.org/webcasts/2014-security-predictions-97067/
[131] A. Summerville, 'Protect against the fastest-growing crime: cyber attacks', CNBC. Accessed: Nov. 21, 2023. [Online]. Available: https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html
[132] R. Reinhart, 'One in Four Americans Have Experienced Cybercrime', Gallup.com. Accessed: Nov. 21, 2023. [Online]. Available: https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx
[133] L. Graham, 'Cybercrime costs the global economy $450 billion: CEO', CNBC. Accessed: Nov. 21, 2023. [Online]. Available: https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html
[134] S. G. A. Van De Weijer and E. R. Leukfeldt, 'Big Five Personality Traits of Cybercrime Victims', *Cyberpsychology Behav. Soc. Netw.*, vol. 20, no. 7, pp. 407–412, 2017, doi: 10.1089/cyber.2017.0028.
[135] J. A. Lewis, 'Economic Impact of Cybercrime', Feb. 2018. Accessed: Jan. 05, 2024. [Online]. Available: https://www.csis.org/analysis/economic-impact-cybercrime
[136] McAfee, 'New McAfee Report Estimates Global Cybercrime Losses to Exceed $1 TrillionPress Release', McAfee. Accessed: Jan. 08, 2024. [Online]. Available: https://www.mcafee.com/de-ch/consumer-corporate/newsroom/press-releases/press-release.html
[137] S. G. Correia, 'Making the most of cybercrime and fraud crime report data: a case study of UK Action Fraud', *Int. J. Popul. Data Sci.*, vol. 7, no. 1, 2022, doi: 10.23889/ijpds.v7i1.1721.
[138] Y. Bentaleb, A. Abarda, H. Mharzi, and S. El Hajji, 'Probabilistic approach to estimate the risk of being a cybercrime victim', *Appl. Math. Sci.*, vol. 9, no. 125, pp. 6233–6240, 2015.
[139] D. S. Wall, 'Policing Identity Crimes', *Polic. Soc. Int. J. Res. Policy*, vol. 23, no. 4, pp. 437–460, Nov. 2013.
[140] M. H. Jhaveri, O. Cetin, C. Gañán, T. Moore, and M. V. Eeten, 'Abuse Reporting and the Fight Against Cybercrime', *ACM Comput. Surv.*, vol. 49, no. 4, p. 68:1-68:27, Jan. 2017, doi: 10.1145/3003147.
[141] T. J. Holt and A. M. Bossler, *The palgrave handbook of international cybercrime and cyberdeviance*. Springer, 2020.
[142] B. K. Payne, 'Defining Cybercrime', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds., Cham: Springer International Publishing, 2020, pp. 3–25. doi: 10.1007/978-3-319-78440-3_1.
[143] K.-S. Choi, C. S. Lee, and E. R. Louderback, 'Historical Evolutions of Cybercrime: From Computer Crime to Cybercrime', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, T. J. Holt and A. M. Bossler, Eds., Cham: Springer International Publishing, 2020, pp. 27–43. doi: 10.1007/978-3-319-78440-3_2.
[144] A. Attrill-Smith and C. Wesson, 'The psychology of cybercrime', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp. 653–678. doi: 10.1007/978-3-319-78440-3_25.
[145] C. J. Howell and G. W. Burruss, 'Datasets for analysis of cybercrime', in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020, pp. 207–219. doi: 10.1007/978-3-319-78440-3_15.
[146] E. C. Viano, 'Cybercrime, organized crime, and societal responses', *Int Approaches Basel*, p. 1103, 2017.
[147] E. C. Viano, 'Cybercrime: Definition, Typology, and Criminalization', in *Cybercrime, Organized Crime, and Societal Responses: International Approaches*, E. C. Viano, Ed., Cham: Springer International Publishing, 2017, pp. 3–22. doi: 10.1007/978-3-319-44501-4_1.
[148] S. W. Brenner, 'Cybercrime: Re-thinking crime control strategies', in *Crime Online*, Willan, 2007, pp. 12–28. Accessed: Dec. 19, 2023. [Online]. Available: https://www.ojp.gov/ncjrs/virtual-library/abstracts/cybercrime-re-thinking-crime-control-strategies-crime-online-p-12
[149] S. M. Rosoff, H. N. Pontell, and R. Tillman, *Profit without honor: White-collar crime and the looting of America*, 2nd ed. Prentice Hall Upper Saddle River, NJ, 2002.
[150] R. Broadhurst, 'Cybercrime in Australia', in *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*, A. Deckert and R. Sarre, Eds., Cham: Springer International Publishing, 2017, pp. 221–235. doi: 10.1007/978-3-319-55747-2_15.
[151] N. E. Marion and J. Twede, *Cybercrime: An Encyclopedia of Digital Crime*. ABC-CLIO, 2020.
[152] Hiscox, 'Hiscox Cyber Readiness Report 2023 | Hiscox Group'. Accessed: Jan. 05, 2024. [Online]. Available: https://www.hiscoxgroup.com/cyber-readiness
[153] INTERPOL, 'INSIGHT'. Accessed: Nov. 21, 2023. [Online]. Available: https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis2/INSIGHT
[154] A. M. van der Laan and N. Tollenaar, 'Text Mining for Cybercrime in Registrations of the Dutch Police', in *Cybercrime in Context: The human factor in victimization, offending, and policing*, M. Weulen Kranenbarg and R. Leukfeldt, Eds., in Crime and Justice in Digital Society. , Cham: Springer International Publishing, 2021, pp. 327–350. doi: 10.1007/978-3-030-60527-8_18.
[155] E. Fahey, 'Developing EU cybercrime and cybersecurity: On legal challenges of EU institutionalisation of cyber law-making1', in *The Routledge Handbook of European Integrations*, 2022, pp. 270–284. doi: 10.4324/9780429262081-20.

[156] EU, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy', COM(2020) 605 final, Jul. 2020. Accessed: Jan. 04, 2024. [Online]. Available: https://www.coe-civ.eu/kh/communication-from-the-commission-on-the-eu-security-union-strategy-1

[157] S. Schjølberg *et al.*, 'Lovtiltak mot datakriminalitet, Delutredning I', NOU, Nov. 2003. [Online]. Available: https://www.regjeringen.no/contentassets/9842026befcd4bff8d3993292e23f3e3/no/pdfs/nou200320030027000dddpdfs.pdf

[158] K. Rønning *et al.*, 'Lovtiltak mot datakriminalitet, Delutredning II', NOU, Feb. 2007. [Online]. Available: https://lovdata.no/static/NOU/nou-2007-02.pdf

[159] S. Schjølberg, *Cyberkriminalitet*. Oslo: Universitetsforl., 2017.

[160] J. Andenæs *et al.*, 'Datakriminalitet', Straffelovrådet, NOU 1985:31, May 1985. [Online]. Available: https://www.regjeringen.no/globalassets/upload/kilde/odn/tmp/2002/0034/ddd/pdfv/154594-nou1985-31.pdf

[161] I. M. Sunde, *Datakriminalitet : en fremstilling av strafferettslige regler om datakriminalitet*. Bergen: Fagbokforlaget, 2019.

[162] M. Sætre, C. Hofseth, and B. L. Kjenn, *Trender i kriminalitet 2018-2021 : digitale og glokale [i.e. globale] utfordringer*. Oslo: Oslo politidistrikt, 2018.

[163] Justis- og beredskapsdepartementet, 'Justis- og beredskapsdepartementets strategi for å bekjempe IKT-kriminalitet', Regjeringen.no. Accessed: Jan. 09, 2024. [Online]. Available: https://www.regjeringen.no/no/dokumenter/justis--og-beredskapsdepartementets-strategi-for-a-bekjempe-ikt-kriminalitet/id2413705/

[164] Kripos, 'Trusler og utfordringer innen IKT-kriminalitet (2017)', Politidirektoratet, 2017. [Online]. Available: https://www.politiet.no/globalassets/dokumenter-strategier-og-horinger/pod/ikt_krim_pod.pdf

[165] L. H. Enstad, 'Internettkriminalitet og jurisdiksjon – en sammenlikning mellom norsk straffelovs jurisdiksjon, andre lands straffelovers og internasjonale konvensjoners jurisdiksjon', The University of Bergen, 2018.

[166] J. D. Howard, *An analysis of security incidents on the internet 1989-1995*. Carnegie Mellon University, 1997. Accessed: Jan. 09, 2024. [Online]. Available: https://search.proquest.com/openview/26b4425b41777ee9b6cac10b78da998a/1?pq-origsite=gscholar&cbl=18750&diss=y

[167] Y. Jewkes and M. Yar, *Handbook of Internet crime*, 1st ed. Routledge, 2010.

[168] Politidirektoratet, 'Datakrimstrategien', May 2015. [Online]. Available: https://www.regjeringen.no/contentassets/4d2ba37bf2ae4cc9ac39afdf20a2f41b/datakrimstrategi_2015.pdf

[169] V. Ø. Lorentzen, 'Cyberkriminalitet mot næringslivet: en studie av løsepengevirusangrep mot norske virksomheter', 2021.

[170] D. S. Wall, 'Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime', *Int. Rev. Law Comput. Technol.*, vol. 22, no. 1–2, pp. 45–63, Jul. 2008, doi: 10.1080/13600860801924907.

[171] Kripos, 'Generativ kunstig intelligens og cyberkriminalitet', Jul. 2023. [Online]. Available: https://www.politiet.no/globalassets/tall-og-fakta/datakriminalitet/etterretningsrapport-generativ-kunstig-intelligens-kripos.pdf

[172] PST, 'Nasjonal trusselvurdering 2023', 2023. [Online]. Available: https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2023/

[173] NSM, 'Risiko 2023', Feb. 2023. [Online]. Available: https://nsm.no/aktuelt/risiko-2023-uforutsigbare-tider-krever-hoyere-beredskap

[174] FN, 'BNP per innbygger i PPP-dollar'. Accessed: Jan. 19, 2024. [Online]. Available: https://fn.no/Statistikk/bnp-per-innbygger-i-ppp?country=42686&country2=42264

[175] INTERPOL/GLACY+, 'Guide for criminal justice statistics on cybercrime and electronic evidence'. 2020. [Online]. Available: https://rm.coe.int/3148-3-1-12-guide-for-criminal-justice-statistics-on-cybercrime-and-ee/1680a0250a