Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

Bjørnar Husby

Resiliens og cyberkriminalitet

En kvalitativ masteroppgave om håndteringen av cyberangrepet mot Norsk Hydro

Masteroppgave i sosiologi
Veileder: Petter Grytten Almklov
Mai 2023

NTNU
Kunnskap for en bedre verden

Bjørnar Husby

Resiliens og cyberkriminalitet

En kvalitativ masteroppgave om håndteringen av cyberangrepet mot Norsk Hydro

Masteroppgave i sosiologi
Veileder: Petter Grytten Almklov
Mai 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for samfunns- og utdanningsvitenskap
Institutt for sosiologi og statsvitenskap

NTNU
Kunnskap for en bedre verden

Sammendrag

Før Russlands invasjon av Ukraina meldte PST at cyberangrep utgjør den viktigste trusselen mot norske interesser. En måned etter rapporterte PST at vi kunne forvente en økning nettverksoperasjoner fremover. Digitalisering har gjort verden mer sammenkoblet, men det menes likevel at befolkningen har forholdsvis lite kunnskap om digitale trusler. Med etableringen og utviklingen av internett har cyberkriminalitet som fenomen vokst parallelt. Som et resultat av de endrede sårbarhetsflatene har *resiliens* vokst frem som en ny sikkerhetstenkning i virksomhetene og hvordan de håndterer avvikssituasjoner. I forhold til andre tilnærminger tar begrepet for seg hvordan man forbereder seg *før* situasjonen, responderer *under* situasjonen, og hvordan man lærer *etter* situasjonen.

Utgangspunktet ligger i problemstillingen: *hvilke ikke-tekniske faktorer bidrar til cyberresiliens i Hydro*? Avhandlingen har som formål å skape innsikt i hvordan Norsk Hydro opprettholdte tilnærmede normaltilstander i drift under cyberangrepet i 2019 med fokus på ikke-tekniske faktorer – herunder menneskelige, sosiale og organisatoriske dimensjoner av resiliens. For å besvare problemstillingen har oppgaven tatt utgangspunkt i et datamateriale på ti kvalitative intervjuer foretatt i ett av Hydro-verkene i landet. For å holde et fokus på hvordan informantene selv erfarte cyberangrepet har oppgaven tatt utgangspunkt i fenomenologi, eksplorativt design og abduktiv metode.

Analysen struktureres etter tidsperioden før, under og etter cyberangrepet, og i analysen identifiseres fem ikke-tekniske faktorer som gjorde seg gjeldende før, under og etter angrepet som diskusjonen struktureres etter. (1) *Evnen til å antesipere* ble sentral før angrepet i form av bevisstgjøring og grunnkompetansen alle ansatte besitter. (2) *Avvikserfaring og improvisasjon* ble sentral under angrepet i form av at responsgrunnlaget befant seg i ansattes egne erfaringer fra andre avvikssituasjoner og prosedyrer. (3) *Desentralisering og organisatorisk struktur* ble sentral både før og under angrepet siden strukturene var på plass lenge før angrepet fant sted, men også for at operatørene selv har myndighet over rutinemessige oppgaver. (4) *Åpenhet* ble sentral under og etter angrepet, både for hvordan konsernet håndterte angrepet utad og hvordan det ble håndtert lokalt. (5) *Læring- og kunnskapsformidling* er sentral etter angrepet og viser til bevisstgjøringen som har skjedd i etterkant. Avslutningsvis diskuterer jeg to problemer som kommer frem i intervjuene. Den ene er et såkalt «paradoksalt læringsutbytte» der man må ha krisesituasjoner for å oppnå læringsutbytte. Den andre er avveiningen mellom funksjonalitet og sikkerhet, og vanskeligheter med å kombinere sikkerhetsarbeid sammen med ordinært arbeid.

Abstract

Before Russia's invasion of Ukraine, the Norwegian Police Security Service reported that cyber-attacks are the most important threats against Norwegian interests. A month later they reported that we could expect an increase in network operations going forward. Digitization has made the world interconnected, but the awareness about digital threats within the Norwegian populace is low. With the development and the rapid growth of the internet, cybercrime as a new form of crime as grown similarly. As a result of the changing vulnerabilities, *resilience* has emerged as a nuanced way of studying security and safety in businesses and how they handle insecurities, crisis, and disturbances. Contrasting other ways of studying risk, resilience takes an aim at looking at disturbances *before* the situation, *during* the situation, and *after* the situation.

The point of departure lies in the question: *which non-technical factors contribute to cyber-resilience in Hydro*? The dissertation aims at creating an understanding of how the Norwegian aluminum plant Norsk Hydro maintained near-normal working conditions during the 2019 cyber-attack, by focusing on non-technical factors – meaning human, social and organizational dimensions of resilience. The work builds on data generated through ten qualitative interviews in one of the Hydro firms in Norway, and builds on phenomenology, explorative design and abductive methods.

The analysis is structured after the time-period before, during and after the cyber-attack, and five non-technical factors are identified for which the discussion is structured after. (1) *The ability to anticipate* was important before the attack in the form of awareness-building and basic training all employees must go through. (2) *Crisis experience and improvisation* was essential during the attack as the response tactic played on employees' previous experiences with crisis and procedures. (3) *Decentralization and organizational structure* were found to be important both before and during the attack as these structures were in place long before the attack, but also because employees at the sharp end have authority over daily routine tasks. (4) *Transparency* was a key factor during and after the attack, both for how the company publicly handled the attack, but also locally. (5) *Learning and knowledge* distribution are important after the attack, mostly for their role in awareness-building after the fact. Furthermore, I discuss two arising problems from the data. One entailing *paradoxical learning*, where learning is only achieved through crisis. The other discussing the balance between functionality and security and finding the right balance between security work and routine tasks.

Forord

Høsten 2021 begynte jeg på masterstudiet i sosiologi ved NTNU og var umåtelig spent på hvordan de to neste årene kom til å gå. Etter flere metodeemner og fordypningsemner, og flere valgmuligheter for hva jeg kunne skrive om i masteroppgaven, sitter jeg i dag med en mastergrad i sosiologi. Jeg har mange jeg må takke for å ha kommet så langt.

Aller først må jeg rette en stor takk til kontaktpersoner som viste stor interesse for oppgaven og for at dere satte meg i kontakt og arrangerte intervjuer for meg. Stor takk til alle informanter som stilte til intervju ved verket. Takk for at dere bidro med refleksjoner på 45 minutter om cyberangrepet og hvordan dere håndterte det. Jeg er absolutt ikke foruten den informasjonen dere ga meg i intervjuene, og takk for at dere gjorde masteroppgaveskrivingen til det morsomste prosjektet jeg har jobbet med.

Stor takk til veileder Petter Almklov som ga meg gode ideer, løsninger og tilbakemeldinger for hvordan jeg best kunne håndtere tematikken, og alle veiledningstimene siden september 2022 frem til den siste veiledningstimen 26. mai 2023.

Stor takk til mamma, pappa og brødrene mine som har forsikret meg om at det alltid «ordner seg til slutt» og for at dere alltid stiller opp.

Til slutt vil jeg også takke Aleksander, Andreas og Magnus for de uhorvelige mengdene og timene Smash Bros vi har spilt de siste to årene, og ikke minst for alle formelle og ganske så uformelle fagsamtaler over flere kanner «bønnejus».

Fem år som sosiologistudent på NTNU er herved avsluttet og jeg går nå over til nye eventyr.

Bjørnar Husby
Trondheim
Mai 2023

Innholdsfortegnelse

Liste over tabeller

Liste over figurer

1. Introduksjon

> Det skal koste å utfordre Norge. Velger andre land å gå mot norske virksomheter, skal vi sørge for at de brenner betydelige ressurser, og de skal vite at vi oppdager dem. I tiden fremover skal vi fokusere på tre hovedområder. Vi skal videreutvikle robuste mekanismer, som forhindrer og stopper sikkerhetstruende investeringer, uten å stå i veien for næringsutvikling. Vi skal dele all informasjon vi kan til dere, trussel og sikkerhetsrapporter, veiledere, tekniske angrepsindikatorer, varsler og analyser. Og i retur så må dere omsette dette til motstandskraft i din virksomhet. Jeg forventer at dere varsler oss om hendelser og sårbarheter tilbake. Vi skal også fortsette å styrke vår evne til å forsvare Norge i cyberspace for å unngå trøbbel. Det skal være trygt for næringslivet, den enkelte og nasjonen [...] og det skal koste å utfordre Norge (NSM, 2022a, 13:56).

24. februar 2022 invaderte Russland Ukraina til sjøs, på land og i luften. Bakgrunnen var at president Putin anerkjente territoriene Donbas og Luhansk som uavhengige regioner, og som et resultat av invasjonen ble det stilt spørsmål om hva dette ville si for verdensfreden. Tidligere var Russland én av de viktigste eksportørene av gass i Europa, men på grunn av det geopolitiske skiftet som skjedde da Russland invaderte Ukraina, måtte de europeiske landene se etter andre løsninger. I det samme året ble det rapportert at Norge eksporterte seks ganger så mye gass til Europa som tilsvarende måned i 2021. Før invasjonen, og som tidligere år, meldte Politiets Sikkerhetstjeneste (PST) at cyberangrep fortsatt utgjorde den viktigste trusselen mot norske interesser (2022a, s. 7). I løpet av mars 2022 rapporterte dermed PST at vi kunne forvente en signifikant økning nettverksoperasjoner fremover som et følge av invasjonen (2022b). Norge er et av de mest digitaliserte landene i verden. Dette kommer som et følge av individers og organisasjoners bruk av «tingenes internett» (IoT), men også de norske virksomhetenes plassering i digital infrastruktur og avhengighet til teknologi. Digitalisering har gjort verden mer sammenkoblet og i enkelte tilfeller lettere – gjerne i form av enklere kommunikasjonsflater mellom individer, så vel som økt effektivitet og produktivitet i de norske bedriftene. Introduksjonen har samtidig introdusert nye problemstillinger og nye sårbarheter. Til tross for at samfunnet er gjennomdigitalisert, blir det ment at befolkningen har forholdsvis lite kunnskap om de digitale truslene (Kripos, 2023, s. 6).

Med etableringen og utviklingen av internett har *cyberkriminalitet* som fenomen vokst parallelt. Cyberkriminalitet er et samlebegrep for flere typer kriminelle handlinger, men som ofte deles i to. *Cyber-dependent* (kriminalitet mot datasystemer) begås fullstendig på internett

– gjerne i form av *hacking*, *tjenestenektangrep* og *virus*. *Cyber-enabled* (kriminalitet støttet av datasystemer) minner om tradisjonell kriminalitet der handlingen kan utøves med *hjelp* av verktøy koblet til nett – som *bedrageri*, *tyveri* og *hvitvasking* (Kripos, 2023, s. 10). Her er førstnevnte interessant fordi det illustrerer et endret risikolandskap, og introduserer nye kriminalitetsformer som av ulik grad rettes mot det norske næringslivet. I den årlige rapporten *Nasjonalt digitalt risikobilde* av Nasjonal Sikkerhetsmyndighet (NSM) blir det beskrevet hvilke metoder som er vanlige når kriminalitet begås på internett, og hvilke samfunnsområder som rammes spesielt. Frem mot 2022 har NSM oppdaget en økende andel ondsinnet aktivitet mot norske virksomheter. Av de rapporterte tilfellene som NSM har registrert er det teknologibedrifter, forskning og offentlig forvaltning som rammes hardest av cyberoperasjoner (NSM, 2022b, s. 15). Som det kommer frem er cyberkriminalitet et økende problem i dagens samfunn, og man kan forvente at problemet vokser parallelt med den teknologiske utviklingen. Spørsmålet man kan stille seg til slutt er hvordan norske virksomheter skal håndtere dette på best mulig måte. I denne avhandlingen ser jeg hvordan en fabrikk i Norsk Hydro håndterte cyberangrepet som skjedde i 2019 med bakgrunn i *resiliens*. Resiliens har etablert seg fra å være en teori i økologien som forklarer hvordan miljøer klarer å ivareta en tilnærmet normaltilstand i avvikssituasjoner (Holling, 1973), til å være en relevant teori som belyser hvordan man forbereder og opprettholder normaltilstander både før, under og etter avvikssituasjoner i sosiotekniske systemer (Hollnagel, 2013). I dag benytter man også *cyberresiliens* for de systemene som tilpasser seg og opprettholder en tilnærmet normaltilstand før, under og etter en cyberhendelse. Når man snakker om cyberresiliens snakker man også om *ikke-tekniske faktorer*. Dette betegnes som *menneskelige*, *sosiale* og *organisatoriske* dimensjoner av cyberresiliens, som kan komme til syne gjennom motivasjon, læring, kunnskapsdeling og organisasjonsstruktur (Flin, O'Connor & Crichton, 2008).

1.2 Problemformulering

Avhandlingen har som formål å finne ut av hvordan Hydro opprettholdte tilnærmede normaltilstander i drift under cyberangrepet i 2019 med fokus på ikke-tekniske faktorer. Utgangspunktet ligger i én problemstilling og følgende tre forskningsspørsmål:

Hvilke ikke-tekniske faktorer bidrar til cyberresiliens i Hydro?

a. Hvordan ble cyberangrepet håndtert?
b. Hva er gjort av tiltak etter cyberangrepet?
c. Hvor avhengige er de ansatte av teknologi?

1.3 Strukturering

Førstkommende kapittel er et bakgrunnskapittel med hensikt om å være en guide i cyberkriminalitetsfeltet, med fokus på redegjørelse av begreper, avklaring av terminologi og differensiering av de ulike kriminelle aktivitetene som kan begås på internett. Kapitlet har også som hensikt å se på tilstanden i Norge og hvilke ansvarsområder de offentlige etatene har.

I kapittel 3 presenteres teori. Hovedfokuset ligger på resiliens, men også cyberresiliens som den naturlige varianten av resiliensbegrepet når fokuset ligger på cyberkriminalitet mot virksomheter. Siden formålet er å se på ikke-tekniske faktorer, herunder *menneskelige*, *sosiale* og *organisatoriske* dimensjoner av resiliens, går jeg innom teori og tidligere forskning senere.

Deretter går fokuset over til det rent metodiske i oppgaven i kapittel 4. Metodekapitlet vil naturlig nok presentere oppgavens metode og datatilfang, og innledningsvis går jeg igjennom avhandlingens case og hvor fokuset ligger. Deretter redegjør jeg forskningsdesign og intervju som metode for datagenerering. Senere i kapitlet går jeg også igjennom min egen posisjon som forsker, og hvilke negative og positive påvirkninger dette kan ha for det rent metodiske og analytiske senere. Deretter går jeg igjennom rekrutterings- og utvalgsprosessen, og hvordan jeg knyttet kontakt med virksomheten. Etter det gir jeg en presentasjon av analyseprosessen og hvordan jeg gikk frem med å bearbeide intervjudataen, i form av transkriberingsprosess og koding. Kvalitetskriterier gjennomgås deretter, og her har jeg et fokus på *validitet*, *reliabilitet* og *overførbarhet*. Avslutningsvis trekkes frem etiske problemstillinger.

I analysekapitlet presenteres funnene fra intervjudataene. Allerede her benyttes noe av teorien fra teorikapitlet, men hensikten ligger likevel ikke i å begynne diskusjonen av problemstillingen og forskningsspørsmålene her. Siden jeg i stor grad har tatt utgangspunkt i abduktiv metode ligger hensikten heller i å forankre funnene mer overordnet i teori, gi forslag til hvordan egen empiri passer inn i tidligere forskning og teori, og at teorien samtidig får et større spillerom i løpet av kapitlet. Siden resiliens i dag har et overordnet fokus på det dynamiske aspektet, er kapitlet formet ut fra *før*, *under* og *etter* cyberangrepet.

Diskusjonskapitlet i etterkant av analysen tar utgangspunkt i å samle det rent teoretiske, tidligere forskning og funnene fra analysen for å besvare problemstillingen jeg presenterte tidligere. Fra funnene i analysen finner jeg fem ikke-tekniske faktorer som gjorde seg gjeldende under cyberangrepet: (1) evnen til å antesipere; (2) avvikserfaring og improvisasjon; (3) desentralisering og organisasjonsstruktur; (4) åpenhet; og (5) læring og kunnskapsformidling. I det siste kapitlet konkluderer jeg oppgaven med en kort oppsummering av viktige funn og en ren besvarelse av både problemstilling og forskningsspørsmål. Kapitlet peker avslutningsvis på videre forskning som kan gjøre seg gjeldende, og som jeg ikke hadde som hensikt å se på.

2. Bakgrunn

Norge er et av de mest digitaliserte landene i verden, både når det gjelder på individnivået så vel som organisasjonsnivået, men med økt bruk av digitale verktøy øker sårbarhetene parallelt. Et bredt spekter av kriminelle utnytter den stadig skiftende sårbarhetsflaten i Norge, og bruker teknologi målrettet for å forsterke slagkraften sin og for å anskaffe verdier (Kripos, 2023, s. 13). I følgende kapittel gjennomgår jeg cyberkriminalitet som begrep og fenomen. Cyberkriminalitet er et omfattende begrep, som også illustrert ved at det ikke finnes et konkret begrep på fenomenet. Cyberkriminalitet er dog ikke et homogent fenomen, og den kriminelle handlingen bør ses i forhold til *hvordan* handlingen ble utøvd. I løpet av kapitlet fokuserer jeg på løsepengevirus som en type vinningskriminalitet som utøves på nett. Siden cyberkriminalitet ikke er et homogent fenomen, ser kapitlet også på typologier av cyberkriminelle for å presisere og konkretisere hvilke kriminelle som kan finnes i cyberspace. Det har skjedd flere cyberangrep i Norge, men i kapitlet presenteres to aktuelle hendelser – Helse Sør-Øst og Østre Toten Kommune. Etter det ser jeg hvordan cybersikkerhet er bygd opp i Norge. Dette for å se hvor ansvaret ligger, så vel som å presisere hvilke sentrale bidragsytere som finnes i landet. Nest siste kapittel ser på forskjeller og likheter mellom cyberkriminalitet og «tradisjonell» kriminalitet. Avslutningsvis redegjør jeg for det «digitale risikosamfunnet» og betydningen dette har for kritisk infrastruktur, så vel som å trekke frem et eksempel der St. Olavs Hospital opplevde to bortfall av IKT-tjenester i 2006 og 2009.

2.1 Cyberkriminalitet

I 1992 publiserte Ulrich Beck boka *Risk society: towards a new modernity*, der han problematiserer forholdet mellom formuesfordeling og risikofordeling i dagens samfunn. Før i tiden kunne risiko kjennes fysisk gjennom smak-, lukt-, syn-, hørsel- og følesans, som han eksemplifiserer med seilerne som falt ned i Themsen. Seilerne druknet ikke, men kvaltes av å puste inn den giftige luften av ekstrem forsøpling og resulterte i at en god del av risikokonseptet før i tiden kom av dårlig hygienisk teknologi (1992a, s. 21). I dagens samfunn mener Beck (1992a; 1992b) at risiko unnslipper fysisk oppfatning – som giftstoffer i matvarer (Beck, 1992a, s. 21).[1] Ut fra denne forståelsen påpeker han også at en stor del av de risikoene som befinner seg i dagens samfunn etableres som et resultat av industriell overproduksjon, og differensierer

[1] Et nytt eksempel på dette er blant annet funn av mikroplast i norsk luft og drikkevann (miljødirektoratet, 2023) og i morsmelk blant mødre i Roma, Italia (Ragusa et al., 2022).

seg fra tidligere trusler gjennom dens globale trussel og de moderne årsakene som ligger til grunn for dem (Beck, 1992a, s. 21).

Norge er et av de mest digitaliserte landene i verden, og denne utviklingen omfatter både individer og de norske virksomhetene. Utviklingen har gjort at teknologien har blitt et av de kritiske og viktigste infrastrukturene i landet, og det digitale rom betegnes ofte som «cyberspace». Selve betegnelsen «cyberkriminalitet» brukes i de internasjonale anbefalingene som gis, men det finnes derimot ingen internasjonal enighet om hva som defineres som «cyberkriminalitet» siden definisjonen er overlatt til hvert enkelt land (Schjølberg, 2017, s. 17). Parallelt til den internasjonale utviklingen brukes også begrepene «cybersikkerhet» og «cyberkriminalitet» i Norge, og de fleste land tar utgangspunkt i Europarådets konvensjon om cyberkrim fra 2001. Konvensjonen definerer bare en minimumsliste over hva som bør inkluderes, og frarøver ikke hvert enkelt land å inkludere utvidelser ut over disse artiklene. Traktaten inneholder fem typer lovbrudd på det nasjonale nivået, og den første er «lovbrudd mot konfidensialiteten, integriteten og tilgjengeligheten av data og systemer» (Council of Europe, 2001, s. 3). Innenfor slike lovbrudd innebærer dette *ulovlig tilgang*, *ulovlig avlytting*, *forstyrrelse av data*,*forstyrrelse av system*, og *enhetsmisbruk*. Den andre typen er «datarelaterte lovbrudd» (Council of Europe, 2001, s. 5). Dette innebærer *datamaskinrelaterte forfalskninger* og *datamaskinrelatert bedrageri*. Den tredje typen er «innholdsrelaterte lovbrudd» (Council of Europe, 2001, s. 5). Dette innebærer *pornografiske fremstillinger og pornografiske materiale av mindreårige*. Den fjerde og siste er «lovbrudd som relaterer seg til brudd på opphavsretten og andre relaterte retter» (Council of Europe, 2001, s. 6).

Ut fra denne traktaten innbefatter cyberkriminalitet mye og omfatter blant annet innbrudd på datamaskiner, uberettiget tilgang til data, identitetskrenkelser, krenkelse av retten til privat kommunikasjon, fare for driftshindring, anslag mot infrastruktur, skadeverk, elektronisk dokumentforfalskning, databedrageri og seksuelt overgrep mot barn (Schjølberg, 2017, s. 18). Straffelovrådet i NOU 1985:31 påpeker på sin side at datakriminalitet kan deles i to. På den ene siden har vi de formene for kriminell aktivitet der en datamaskin, eller datautstyr, er selve målet for den kriminelle handlingen. På den andre siden ha vi også de aktivitetene der datamaskinen eller datautstyret er det sentrale hjelpemiddelet for å utøve disse handlingene.

Cyberkriminalitet har forandret sikkerhetslandskapet og farges av dens globale omfang. I sin definisjonsavklaring argumenterer Beck (2006, s. 333-334) for at global risiko er karakterisert av tre egenskaper. (1) Risiko er *de-lokalisert* – årsaker og konsekvenser er ikke lenger forbundet med ett geografisk punkt, ett tidspunkt eller ett rom. De er i prinsippet allestedsværende. (2) Risiko er *ukalkulerbar* – i prinsippet er konsekvensene ukalkulerbare i

det at man heller snakker om «hypotetisk risiko», som bugner i det man *ikke* vet. (3) Risiko kjennetegnes av *manglende kompensasjon* – og er i dag erstattet med å lage *forholdsregler gjennom forebygging*. Cyberkriminalitet er et stort begrep og det trengs en begrepsavgrensning når jeg senere går over til det rent analytiske i avhandlingen. I denne oppgaven er det spesielt løsepengevirus som cyberkriminalitet som gjør seg gjeldende.

2.2 Løsepengevirus som vinningskriminalitet

I Europarådets traktat om cyberkrim er de lovbruddene som omhandler konfidensialitet, integritet og tilgjengelighet av data og systemer interessant, ettersom at vi da beveger oss i en retning av innbrudd i datasystem, fare for driftshindring og anslag mot infrastruktur. I straffeloven § 204 defineres *innbrudd i datasystem* som når en beskyttelse brytes og når en uberettiget fremgangsmåte skaffer seg tilgang til et datasystem eller deler av det (Straffeloven, 2005, § 204). I straffeloven § 206 defineres *fare for driftshindring* som når man uberettiget overfører, skader, sletter, forringer, endrer, tilføyer eller fjerner informasjon som resulterer i fare for avbrudd eller vesentlig hindring av driften av et datasystem (Straffeloven, 2005, § 206). I straffeloven § 192 defineres *anslag mot infrastrukturen* som når det ytes omfattende forstyrrelse i den offentlige forvaltning eller i samfunnslivet for øvrig ved å ødelegge, skade eller sette ut av virksomhet: a) en informasjonssamling, eller b) et anlegg for energiforsyning, kringkasting, elektronisk kommunikasjon eller samferdsel.

Det som forbinder de tre paragrafene fra straffeloven er at uberettiget tilgang til et datasystem kan i verste fall føre til at informasjonen som eventuelt overføres, forringes eller skades kan sette en bedrift ut av virksomhet. Overordnet sett er det dette vinningskriminalitet går ut på. Vinningskriminalitet er når gjerningspersonene søker etter å oppnå profitt – oftest i form av pengegevinster – når de begår kriminelle handlinger. Ifølge R. T. Naylor (2003) kan vinningskriminalitet deles i tre respektive underkategorier: plyndring- og utnyttelseslovbrudd; markedsbaserte lovbrudd; og kommersielle lovbrudd (Naylor, 2003, s. 84-88). Mest interessant er det førstnevnte vinningslovbrudd. I plyndringslovbrudd forekommer ufrivillige transaksjoner og overføringer, der virkemiddelet ofte er bruken av vold, trusler og løsepengekrav. I slike lovbrudd er også offeret lett identifiserbart, enten dette måtte dreie seg om individer, organisasjoner eller virksomheter. På lignende måte er også tapet relativt lett å identifisere, der eksempelvis virksomheten kan vise til spesifikke eiendommer som ble tapt under handlingen (Naylor, 2003, s. 84).

I et cyberkrimperspektiv foregår også vinningskriminalitet i cyberspace, med noe mer nyanserte virkemidler. I de fleste tilfeller brukes datavirus ved plyndringslovbrudd på internett, og i likhet med Naylors (2003) definisjon ovenfor, brukes såkalte «ransomware»-programmer som et utpressingsmiddel for å anskaffe penger fra offeret. Dette kan gjøres ved at datasystemet blir utilgjengelig, ofte som et resultat av at informasjon, filer og data krypteres av gjerningspersonene. For at man i ettertid av angrepet skal få tilgang til disse filene, blir offeret pålagt et løsepengekrav av gjerningspersonene, og ofte må kravet betales i den digitale valutaen «Bitcoin» (Schjølberg, 2017, s. 87).

2.3 Typologier av cyberkriminelle

Tidligere har cyberkriminalitet ofte blitt forbundet med stereotypiske illustrasjoner. På den ene siden har cyberkriminalitet ofte blitt assosiert med den «ensomme ulven» som utfører cyberoperasjoner i kjelleren til aktørens foresatte. På den andre siden sidestilles cyberkriminalitet med konvensjonelle kriminelle handlinger, en feiltolkning mener Broadhurst, Grabonsky, Alazab & Chonz (2014, s. 1) siden fenomenet er i konstant utvikling og kriminalitet begås fullstendig på internett. Artikkelen til Broadhurst et al. (2014) tar et dykk i de variasjonene man finner i organisert vinningskriminalitet i cyberspace. Selv om en stor del av organisert cyberkrim utøves av profesjonelle og dyktige teknikere, har vi også å gjøre med de terrestriske og konvensjonelle krimgruppene som har begynt å samle digital teknologi (Broadhurst et al., 2014, s. 1; Kripos, 2023, s. 10). Nasjoner, akademikere, rettshåndhevelsesbyråer og organisasjoner som spesialiserer seg på cybersikkerhet spekulerer at konvensjonelt organiserte grupper i økende grad involverer seg i digital kriminalitet. Empirien viser blant annet at kriminelle i høyere grad involverer seg i løse nettverk enn formelle organisasjoner. Samtidig viser empirien at cyberkriminelle geografisk sett posisjonerer seg nært hverandre, og at angrep utføres på den andre siden av kloden. På verdensbasis kaller man slike geografiske posisjoneringer for «hot spots». Øst-Europa og den tidligere Sovjet Unionen betraktes som hot spots i dag (Broadhurst et al., 2014, s. 3). Cyberkriminelle er en paraplybetegnelse for de gruppene og nettverkene man finner. McGuire (2012) og Broadhurst et al. (2014) typifiserer tre typer cyberkriminelle, med tilsvarende seks undergrupper.

Type I er de individene og gruppene som for det meste begår handlingene sine i cyberspace, og gruppene kan deles i «swarms» og «hubs» - som for det meste er virtuelle grupper der tillit avhenger av det ryktet man har fra tidligere kriminelle handlinger. Swarms deler i flere tilfeller de samme trekkene som typiske nettverk og beskrives som løse

organisasjoner med et felles mål, uten at organisasjonen har en utnevnt lederposisjon. Aksjonene tar utgangspunkt i såkalt «hacktivisme» - aksjoner som bærer preg av hatkriminalitet og politisk motstand. Gruppen Anonymous kan beskrives som en swarm. Hubs vil på lik linje som en swarm for det meste befinne seg i cyberspace, men til forskjell inngår hubs i en klarere organisatorisk struktur med spesifikke kommandolinjer. Til forskjell fra swarms kan aktørene i hubs inngå i tyngre kriminalitet, eksempelvis piratkopiering, phishing-angrep, botnets og seksuelle krenkelser (Broadhurst et al., 2014, s. 5-6).

Type II er hybride og kombinerer handlinger på nett med konvensjonell terrestrisk kriminalitet. Innenfor denne typen har vi også to undergrupper: «gruppehybrider» og «utvidede hybrider». Førstnevnte kan i stor grad sammenlignes med hubs fra type I, men til forskjell foregår de kriminelle handlingene på tvers av cyberspace og det fysiske rom. Sistnevnte er nokså lik førstnevnte, men de utvidede hybridene er mindre sentralisert enn gruppehybridene, samtidig som at de bevarer en viss koordinasjon for at handlingen i seg selv skal være suksessfull (Broadhurst et al., 2014, s. 6).

I *Type III* blir handlingene for det meste utøvd i det fysiske rom, men aktørene benytter seg av digital teknologi for å muliggjøre handlingene sine. Denne typifiseringen kan videre tilegnes to undergrupper: «hierarkier» og «aggregater». Hierarkiene er de typiske og tradisjonelle kriminelle gruppene, men som har muligheten til å eksportere en god del av handlingene sine til cyberspace – som utpressing og hacking. Aggregatene er løst organiserte, midlertidige og uten et spesifikt formål. I de fleste av tilfellene vil aggregatene benytte seg av digital teknologi som en improvisert løsning for å gjennomføre en handling, og bruken av teknologi er sjeldent eneste verktøy i handlingen (Broadhurst et al., 2014, s. 7).

2.4 Cyberangrep i Norge

I NSMs «nasjonalt digitalt risikobilde» av 2022 forklarer de at cyberangrep er hverdagskost (NSM, 2022b), og som det ble forklart tidligere er teknologibedrifter, forskning og offentlig forvaltning sentrale mål i landet. I det følgende presenterer jeg to instanser der et cyberangrep ble rettet mot to forskjellige mål: Helse Sør-Øst og Østre Toten kommune. Angrepene har til felles at ansatte måtte gå fra teknologisk til manuell arbeidsutførelse da angrepene fant sted, og kritiske samfunnsfunksjoner i stor grad avhenger av teknologi i arbeidshverdagen.

Helse Sør-Øst 2017-2018

Tidlig i romjula 2017 fikk en aktør tilgang til datasystemet til helseforetaket Helse Sør-Øst. Ifølge Forsvarets forskningsinstitutt ble tilgangen oppnådd ved at en sårbar applikasjon ble kjørt på en tjener forvaltet av Sykehuspartner, men som driftes av det lokale helsepersonellet (Bruvoll, Thuv & Enemo, 2020, s. 29). Tilgangen gjorde at aktøren kunne kompromittere infrastrukturen ytterligere, og sårbarhetene i systemet ble deretter utnyttet. Det var ikke før 8. januar i 2018 at Sykehuspartner ble varslet av HelseCERT – det nasjonale cybersikkerhetssenteret for helse- og omsorgssektoren – og 9. januar gikk de i rød beredskap. Et tilsvarende angrep, av de samme aktørene, ble gjort mot Helse Vest i den samme perioden. Helse Vest IKT deaktiverte i første omgang en site2site VPN-tunnel som et følge av uklare konsekvenser rundt bruken av en slik tjener. I etterkant medførte dette problemer med utveksling av pasientinformasjon (Bruvoll et al., 2020, s. 29). Etter en vurdering av Sykehuspartner og Helse Vest IKT ble forbindelsen gjenopprettet. Av andre tiltak tok Sykehuspartner ned kompromitterte tjenere den 9. januar, men i løpet av kvelden ble det kjent at aktørene hadde fått større tilgang til infrastrukturen enn det de hadde antatt. Den første nedstengningen av tjenerne var dermed ikke nok til å fjerne aktøren (Bruvoll et al., 2020, s. 29). 13. januar hadde aktørene gått enda dypere enn de foregående dagene, og de hadde nå fått tilgang til SIKT – den regionale infrastrukturplattformen. 17. januar overleverte Helse Sør-Øst en tiltaksliste til Helsedirektoratet som innebar økt årvåkenhet, oversikt over nettverkskomponenter, kartlegge brukere med tjenstlig behov, forberedelse på at kritiske systemer kunne gå ned, og forberedelse på konsekvensene av slike tiltak (Bruvoll et al., 2020, s. 31). De fortløpende konsekvensene av de tiltakene som ble iverksatt var svakere muligheter for pasientkommunikasjon, forskningseffektivitet og kontakt mellom sykehus og ambulanse. På grunn av manglende bevis og opplysninger henla PST saken 29. november 2018.

Østre Toten kommune 2021

Natt til lørdag 9. januar 2021 ble Østre Toten kommune utsatt for et løsepengevirus, noe som førte til at systemer i 240 virksomheter ble utilgjengelige. På grunn av COVID19-pandemien hadde kommunen allerede iverksatt et kriseteam, men et nytt team ble iverksatt for å håndtere det digitale viruset (Østby & Kowalski, 2022, s. 4). 10. Januar meldte Østre Totens ordfører til NRK at sensitiv pasientinformasjon kunne risikere å komme på avveie, som en konsekvens av angrepet (Solbakken, 2021). Under angrepet hadde aktørene tatt seg bak en brannmur, slettet sikkerhetskopier og kryptert alle data. Som et følge hadde 1300 kommunalt ansatte mistet tilgang til datasystemet. I helse- og omsorgssektoren, NAV og barnevernstjenesten i kommunen

måtte alt arbeid heretter utføres manuelt. Brannvarslingssystemet ved et omsorgshjem ble også satt ut av spill. Den 30. mars rapporterte NRK at personsensitive data hadde havnet på «det mørke nettet», noe hackerne selv hadde opplyst om, og den 31. mars ble det kjent at opplysninger fra voksenopplæringen i kommunen hadde kommet på avveie. (Trøen, Vogt & Kessel, 2021). Dataangrepet i kommunen er i dag det mest omfattende angrepet mot en norsk kommune noensinne, og angrepet kostet kommunen over 30 millioner kroner (Mo, 2021).

2.5 Cyber- og informasjonssikkerhet i Norge

Ofte brukes både *cybersikkerhet* og *informasjonssikkerhet* om hverandre, men det finnes forskjeller mellom begrepene. På den ene siden dreier cybersikkerhet seg om å beskytte cyberspace, det som fungerer i cyberspace, og de eiendelene som kan nås i cyberspace, som også innebærer bevarelsen av konfidensialitet, integritet og tilgjengelighet (CIA-triaden) (Solms & Niekerk, 2013, s. 101). På den andre siden dreier informasjonssikkerhet seg også om bevaringen av CIA-triaden, men Whitman og Mattord (2009, sitert i Solms & Niekerk, 2013, s. 98) mener at definisjonen bør inkludere *accuracy* (nøyaktighet), *authenticity* (autentisitet), *utility* (nytte) og *possession* (besittelse) siden informasjonssikkerhet er i stadig endring.

I Norge har Justis- og beredskapsdepartementet et samordningsansvar for den digitale sikkerheten for den sivile siden av samfunnet. Et samordningsansvar innebærer at departementet utvikler og følger opp nasjonale strategier, identifiserer sektorovergripende spørsmål og bidrar til at ansvaret blir plassert og oppgaver blir håndtert på en god måte (Regjeringen, 2021). Underlagt Justis- og beredskapsdepartementet finnes Nasjonal Sikkerhetsmyndighet (NSM), et direktorat som har ansvar for forebyggende nasjonal sikring. Forsvarsdepartementet har også instruksjonsmyndighet over NSM der direktoratet håndterer saker i ansvarsområdet deres (NSM, u.å.a). Innenfor NSM finnes fire fagavdelinger; nasjonalt cybersikkerhetssenter (NCSC), avdeling for beskyttelse av grunnleggende nasjonale funksjoner, avdeling for kontroll, og avdeling for forsvar mot avanserte digitale trusler. NCSC håndterer dataangrepene som rettes mot Norge, og gir råd for hvordan de norske virksomhetene kan beskytte seg mot digitale sårbarheter (NSM, u.å.b). NCSC (tidligere under akronymet NorCERT) er den operative delen av NSM, som er en del av forsvarssektoren og underordnet forsvarsdepartementet, og fungerer som den digitale innbruddsalarmen for AS Norge (Thomstad, 2017, s. 51). NCSC kan i den grad ses som en del av det norske totalforsvaret, selv om tjenesten brukes i det daglige og ikke bare under kriser (Thomstad, 2017, s. 51).

Nasjonalt cyberkrimsenter (NC3), innenfor Kripos og underlagt politidirektoratet, er det nasjonale senteret for forebygging, avdekking og bekjempelse av kriminalitet i det digitale rom (Politiet, u.å.a). Senteret ble offisielt åpnet 25. januar 2019, og etter planen skal senteret være et nasjonalt kunnskaps- og kompetansesenter innenfor teknologirelaterte politioppgaver innen utgangen av 2022. En av hovedoppgavene til NC3 er å være en sentral bidragsyter for å øke tryggheten blant norske innbyggere og virksomheter, som bekjempelse av cyberkriminalitet fra etterretning, metodeutvikling, forebygging, etterforskning, sikring av digitale spor samt patruljering på nett (Politiet, u.å.a).

I Norge finnes det ingen organisasjon som har det overordnede ansvaret for cybersikkerhet, og med samordningsansvaret til Justis- og beredskapsdepartementet innebærer dette at departementet tilrettelegger for at virksomhetene kan beskytte seg *selv* mot uønskede digitale hendelser. For de norske virksomhetene vil også dette innebære at sikkerheten blir privatisert. I rapporten *Nasjonal strategi for digital sikkerhet* blir det sagt at:

> Å ivareta digital sikkerhet er først og fremst et virksomhetsansvar. Virksomhetsledere er ansvarlig for å foreta risikovurderinger, og på bakgrunn av dette gjennomføre tilstrekkelige tiltak. Myndighetene skal legge til rette for at virksomheter kan beskytte seg mot uønskede digitale hendelser, både for å ivareta egen sikkerhet og for å øke samfunnets samlede robusthet. Et godt forebyggende arbeid med digital sikkerhet, og en systematisk tilnærming til håndtering av risiko, vil redusere muligheten for at uønskede digitale hendelser får konsekvenser for egen og andres virksomhet, for den enkelte privatperson og for samfunnet i stort (Regjeringen, 2019, s. 13).

Sitatet viser at virksomhetene er ansvarlige for å håndtere cyberhendelser i stor grad selv, men at myndighetene skal legge til rette for at de skal kunne gjøre dette. Ifølge Beck (1992a) sirkulerer et refleksivt samfunn rundt industrirevolusjonens økte fokus på individualisering. I løpet av industrirevolusjonen destabiliserte velferdssamfunnet de tradisjonelle levemåtene, og arbeidsmarkedssamfunnet – som i og for seg var beskyttet av velferdssamfunnet – løste opp klassesamfunnets fundamenter og kjernefamilien (Beck, 1992a, s. 153). Med økt individualisering betyr dette at individene «løslates» fra de tradisjonelle, tilegnede rollene. Avrundingen av post-historien førte til et gradvis tap av de tidligere tenke-, leve- og arbeidsmåtene – som tidligere var sterkt forbundet med familien, giftemål, og manns- og kvinneroller. Med andre ord vil dette si at individet selv kunne råde over seg selv, og han forklarer hvordan angst og usikkerhet var noe individet selv måtte håndtere i det nye samfunnet

(Beck, 1992a, s. 153). En god del av denne tematikken kommer også frem i Michel Foucaults (1978; 2002) teori om «biomakt» og «governmentality». Blant annet forteller Foucault hvordan det nye samfunnet åpner opp for at individet har mulighet til å regjere seg selv, noe han mener er begynnelsen av biomaktparadigmet (1978, s. 140). Han sier at befolkningen i seg selv måtte være det ultimate sluttmålet, og ikke styringen, for at befolkningens levekår og helse kunne bedres (Foucault, 2002, s. 63-64). Som et svar til denne økte individualiseringen etablerte befolkningen selv utdanningsinstitusjoner, kurs, terapi og politiske institusjoner for å håndtere de individuelle problemene som måtte dukke opp (Beck, 1992a, s. 153). Refleksiv modernitet betyr dermed at kulturell oppfatning ikke lenger er koblet til myndigheter og vitenskap, og utfordringer blir i dag et større ansvar for individer og enkelte virksomheter. I et samfunn der teknologiutviklingen skjer raskt, skaper også dette nye risikoer og usikkerheter. En refleksiv modernitet innebærer at man systematisk håndterer og vurderer risiko ut fra moderniteten i seg selv, men de blir samtidig politisk refleksive ved farens globale omfang (Beck, 1992a, s. 21).

Wu, Ren, Zhang, Fan & Fu (2018) forklarer hvordan introduksjonen av digital produksjon benytter seg av «Industrial Internet of Things» (IIoT) for å øke produktivitet, samt gjøre produksjonen mer kostnadseffektiv. Innenfor et produksjonssystem finner man både informasjons- (IT) og operasjonsteknologiske (OT) systemer. IT-systemene bruker datamaskinene for å lagre, motta, sende og behandle produksjonsrelaterte data. OT-systemene bruker maskin- og programvare for å kontrollere selve produksjonsutstyret (Wu et al., 2018, s. 5). En typisk konsekvens av tilgangsangrep gjennom hacking er tap av konfidensielle data, der de som utøver angrepet får uautorisert tilgang til sensitive data og system. Beskyttelse mot potensielle farer handler i stor grad om risikobesluttsomhet, som betyr at man erkjenner risikonivået til et produksjonssystem, men det handler likeledes om at man innehar et visst kunnskapsnivå i det produksjonssystemet man håndterer (Wu et al., 2018, s. 10).

Når en enhet er koblet til et større nettverk, kan dette utgjøre en sikkerhetsrisiko, og når samfunnet og næringslivet digitaliseres er behovet større for generisk og spesialisert IKT-kompetanse. De siste årene har etterspørselen for IKT-spesialister innen sikkerhet økt markant (Mark, Edelhard, Næss & Røsdal, 2019, s. 177), men likevel viser data fra Eurostat (2023) at omtrent 5,5% av alle norske fulltidsansatte innehar spesialisert IKT-kompetanse. Av disse har ca. 70% utdannet seg som IKT-spesialist på universitetet eller en annen form for høyere utdanning (Eurostat, 2023). Samtidig hadde 50% av norske virksomheter problemer med å ansette IKT-spesialister i bedriften (Eurostat, 2021). I Nasjonal strategi for digital sikkerhet er derimot dette en prioritet:

> Kompetanse og kunnskap om trusler, sårbarheter og effektive tiltak er en forutsetning for å kunne beskytte verdier mot uønskede digitale hendelser. Dette forutsetter at alle – både privatpersoner, virksomheter og myndigheter, har tilgang til informasjon om digitale sikkerhetsutfordringer og mottiltak. Spesialisering i digital sikkerhet som kreves for å ivareta vårt nasjonale sikkerhetsbehov skal gis særlig prioritet (Regjeringen, 2019, s. 17).

Mark et al. (2019) tar for seg gapet mellom den drastiske teknologiutviklingen og det generelle IKT-kompetansenivået her til lands. Mark et al. (2019, s. 181) viser til et økende gap mellom tilgang og behov, og at gapet kommer til å øke frem mot 2030. Selvfølgelig kan gapet minimeres dersom IKT-sikkerhet får avtagende fokus i næringene, men at fokuset øker i et utdanningspolitisk perspektiv. På en lignende måte kan gapet minimeres ved at flere studenter søker seg til studieområder som spesialiserer seg innenfor IKT (Mark et al., 2019, s. 182-183). Likevel predikerer de at gapet økes frem mot 2030 på grunn av den økte digitaliseringen og den komplekse utviklingen av cyberkriminalitet som fenomen (Mark et al., 2019, s. 183).

2.6 Terrestrisk kriminalitet vs. virtuell kriminalitet

Cyberkriminalitet og vinningskriminalitet på internett kan i grove trekk sammenlignes med andre «tradisjonelle» former for kriminalitet. Når kriminalitet på internett i stor grad betegnes som «cyberkriminalitet», kan den fysiske motparten betegnes som «terrestrisk kriminalitet». På politiets nettsider betegnes organisert kriminalitet som når kriminalitet begås i grupper eller nettverk, men denne formen for kriminalitet skjer ofte på tvers av politidistrikter og landegrenser (Politiet, u.å.b). I Norge og ute i Europa ser politiet at samarbeidet mellom kriminelle ofte foregår i faste organisasjoner, som omtales som løst sammensatte nettverk. Flere av nettverkene er multikriminelle, der aktørene begår flere typer lovbrudd. I en mer konkret definisjon av begrepet betegner politiet organisert kriminalitet som «et samarbeid mellom tre eller flere personer som har som hovedformål å begå en handling som kan straffes med fengsel i minst 3 år, eller som går ut på at en ikke ubetydelig del av aktivitetene består i å begå slike handlinger» (Politiet, u.å.b).

2.7 Det digitale risikosamfunnet og kritisk infrastruktur

Introduksjonen av ny teknologi har ført med seg en lang rekke av nye problemer og problemstillinger, og man vil kunne argumentere for at cyberkriminalitet er en bivirkning av dagens modernisering. Beck forteller som en forlengelse av det refleksive samfunnet at når de

teknologiske valgmulighetene etableres og utvikles, øker dens ukalkulerbare konsekvenser parallelt (1992a, s. 22). På en lignende måte er cyberkriminalitet en bivirkning av moderniseringen, på den måten at fenomenets eksistens og oppstandelse i sin helhet kommer av ikke-kunnskap og usikkerhet (Eskola, 2012, s. 123). Et sentralt argument i Eskolas (2012) artikkel er i stedet for at vi befinner oss i et såkalt risikosamfunn, beveger vi oss heller inn i «nettverkssamfunnet» - en selvekspanderende sirkel der kunnskapsbasert informasjonsteknologi forsterker og akselerer produksjonen av kunnskap og informasjon.

I Norge inngår utførelsen av arbeid og produksjon i interaksjon med høyavansert teknologi i de fleste virksomheter. Som Wu et al. (2018) forteller skal introduksjonen av IT- og OT-systemer forsøke å øke produktivitet og effektivitet innenfor en gitt virksomhet, men som en konsekvens vil dette også si at produksjonslinjene utsettes for en større sårbarhet i cyberspace. Også her kan Becks karakteristikk av det globale risikosamfunnet anvendes. Som tidligere nevnt kan det globale risikosamfunnet kjennetegnes av de tre egenskapene de-lokalisering, ukalkulerbarhet og manglende kompensasjon (Beck, 2006, s. 333-334). I de aller fleste tilfeller vil et cyberangrep – eksempelvis et løsepengevirus – bli utført av en eller flere aktører fra ett sted i verden, mens målet ligger på den andre siden. Et angrep på én virksomhet kan i verstefall også bety at angrepet setter IT- og OT-systemene i en annen virksomhet enn målet ute av spill. Dette følger de-lokaliseringsprinsippet til Beck (2006) om at risiko er allestedsværende, men også dens ukalkulerbarhet. Dagens risikoer og dens katastrofer varer lengre enn tidligere, og prediksjoner om hvilke skader som følger av angrepet kan i mindre grad forutses. Dette avhenger av hvor langt inn i infrastrukturen aktørene kommer, hvilke filer de får tilgang til og hvor sårbar virksomheten er i det digitale rom.

Fra samfunnsperspektivet er IKT en viktigere del av det hverdagslivet enn hva det tidligere har vært. I NOU 2015:13 presiseres det at flere samfunnskritiske virksomheter blir avhengige av digitale verdikjeder som går på tvers av land og sektorer, som elektronisk kommunikasjonsinfrastruktur (EKOM-infrastruktur). I samme stund har også kriminaliteten utviklet seg i lignende retning som de digitale verdikjedene, og en god del av kriminaliteten som foregår i dag har i økende grad digitale elementer i seg. Kritisk infrastruktur kan omfatte mye; eksempelvis mat, agrikultur og nødhjelp, men også elektrisitet, luftfart og internett (Egan, 2007, s. 5). En infrastruktur er betegnet som kritisk når: det gir rutinefunksjoner som er nødvendig for funksjonen og opprettholdelsen av et system; når det ikke finnes lettvinte og raske løsninger dersom systemet er nede; plutselige dysfunksjoner innenfor disse elementene kan forårsake skade; de er tilknyttet større, gjensidige og integrerte systemer (Egan, 2007, s. 5). I forlengelsen av dette benytter Almklov, Antonsen, Størkersen og Roe (2018, s. 2) seg av

«infrastrukturering» som et relasjonelt fenomen ved menneskets, organisasjonenes og de tekniske systemenes relasjon. Det argumenteres for at infrastrukturering er selve fundamentet for industrisamfunnets eksistens, blant annet for at dette har tillat både effektivisering og økt produktivitet innenfor virksomhetene, men også en kraftig livsstilsendring sett fra samfunnsperspektivet (Egan, 2007, s. 5). Sammenkoblingen av systemene har likevel vært til hodebry for beslutningstakere. Når et kritisk system er koblet med et annet blir de kritiske elementene fra det ene også et kritisk element for de andre. Til gjengjeld skaper også dette nye sårbarheter gjennom «kritiske eksternaliteter» - feilen fra ett element har en negativ påvirkning på et annet (Egan, 2007, s. 7). Både ikke-intenderte feil og hacking har relativt like konsekvenser. Tidligere gikk jeg gjennom to cyberangrep i Norge og hvilke tekniske konsekvenser dette hadde for de virksomhetene som ble berørt. Lignende konsekvenser kan også ses i bortfall av IKT-tjenester som *ikke* kommer som et resultat av cyberkriminalitet, men som heller er resultatet av sammenkoblingen av verdikjeder. I Norge kan dette illustreres med følgende case.

St. Olavs Hospital opplevde i 2006 og 2009 to alvorlige bortfall av sykehusets IKT-tjenester. I 2006 falt IKT-nettet bort i den delen av sykehuset som omfatter laboratoriesenteret, kvinne- og barn-avdeling, nevrosenteret og pasienthotellet (Almklov, Antonsen & Fenstad, 2010, s. 6). Dette resulterte i at alle nettverksbaserte funksjoner var utilgjengelige, som innebar e-post, telefonkommunikasjon, journalsystemer, bildediagnostikk og laboratoriesystemer. I etterkant ble det meldt om en rekke potensielt alvorlige konsekvenser for pasientene: manglende kontakt med de vakthavende legene, porttelefoner som var ute av funksjon, og manglende tilgang til arkivsystemene i blodbanken (Almklov et al., 2010, s. 6). I 2009 skjedde det på nytt en lignende hendelse ved St. Olavs, og denne gang var det problemer knyttet til IP-telefonien (Almklov et al., 2010, s. 7). I denne hendelsen ble det derimot ikke rapportert om instanser som potensielt kunne vært alvorlig for pasientene. Den utløsende årsaken for begge hendelsene var enten feil i nettverkskomponenten eller programvareoppdatering utført av en internasjonal leverandør.

Cyberkriminalitet er et komplekst felt med flere mulige innfallsvinkler, og spørsmålet til slutt er hvordan norske virksomheter skal håndtere problematikken. Når virksomhetene i større grad digitaliserer seg, eskalerer også sårbarhetsflatene. Når virksomhetene også i større grad ekspanderer verdikjedene sine, er ikke risiko lengre forbundet med én plass. Risikohåndtering kan være en sentral vinkling, men i denne avhandlingen er det spesielt en teoretisk vinkling jeg vil konsentrere meg om.

3. Teori

I følgende kapittel tar jeg for meg det rent teoretiske i oppgaven. «Resiliens» brukes her som det overordnede rammeverket videre og redegjøres i kapittel 3.1. Teorien har blitt konseptualisert og operasjonalisert over flere forskningsdisipliner, som økologi, psykologi, sosiologi og statsvitenskap, men utgangspunktet ligger her i Erik Hollnagels (2013) definisjon av begrepet. «Resilience engineering» er også viktig i dette ettersom at dette tar for seg resiliensaspektet til bygde systemer og miljøer. For å vinkle teorien i retningen av avhandlingens tematikk definerer jeg begrepet «cyberresiliens» og tidligere forskning på området senere. Siden oppgaven har som mål å avdekke ikke-tekniske faktorer som kan bidra til organisatorisk cyberresiliens, ser jeg mot slutten av kapitlet på organisatoriske og menneskelige faktorer, og skaper et overblikk over det som til nå er forsket på. Her retter jeg blikket spesielt mot mennesket som løsning på krisesituasjoner i sosiotekniske systemer.

3.1 Resiliens

Holling (1973) definerte begrepet «resiliens» som måten et økosystem klarer å absorbere en rekke endringsmekanismer for å fortsette og eksistere. Samtidig peker han på hvordan systemet klarer å opprettholde en viss grad av stabilitet i etterkant av disse situasjonene. Tidlig på 70-tallet ble resiliens ofte brukt som en sentral terminologi i psykologiske stressmestringsundersøkelser blant barn. Under disse undersøkelsene ble begrepet definert som måten man håndterer traumatiske hendelser og bruker traume som starten på noe nytt (Tisseron, 2007, sitert i Hollnagel, 2013, s. 1). Ved århundreskiftet ble likevel begrepet brukt blant sikkerhetsspesialister som en alternativ fremgangsmåte for å forklare hvordan noe eller noen håndterer sikkerhet, ulykke og risiko. Spesialistene ble nå i større grad opptatt av den dynamiske komponenten bak begrepet. Når jeg referer til resiliens som begrep defineres dette som *evnen til å foreta funksjonsendringer før, under og/eller etter en avvikssituasjon, for å klare og opprettholde en viss grad av operasjonsevne under forventede og uforventede situasjoner* (Hollnagel, Paries, Woods & Wreathall, 2011, sitert i Hollnagel, 2013, s. 2).

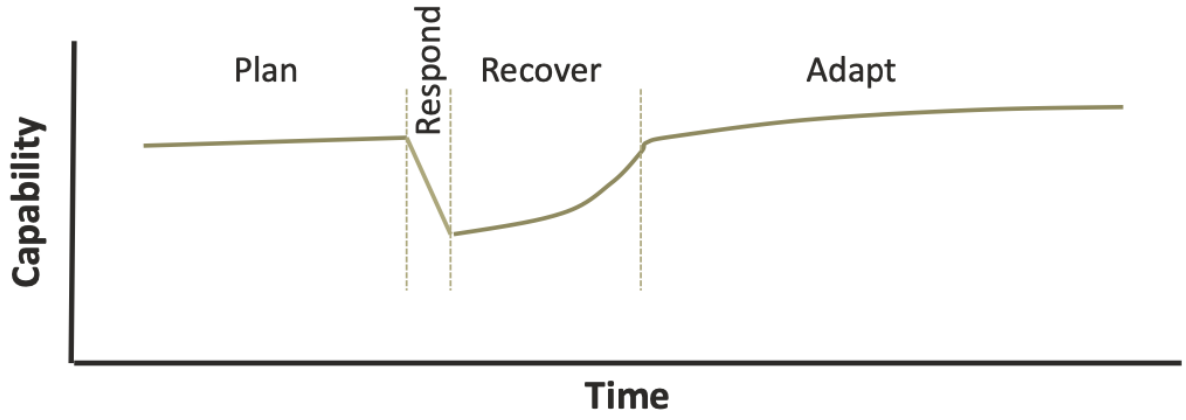
Erik Hollnagel (2013) utforsker dette videre ut fra «built environment», som han mener bør betraktes som et «system» dersom man tar utgangspunkt i hvor resilient et miljø er. Ettersom at resiliens er assosiert med dynamikken av systemet, er man i mye større grad er opptatt av hva det *gjør* enn hva det *er* (Hollnagel, 2013, s. 4). Samtidig klarer de bygde systemene «å handle» nettopp siden de er sosiotekniske systemer – en interaksjon mellom mennesket, teknologien og miljøet. Sagt på en annen måte krever systemene en viss grad av

selvbevissthet og intelligens for at det i det hele tatt kan betraktes som et resilient system. Til tross for at *kunstig intelligens* (KI) det siste året virkelig har gjort sin inntreden på verdensbasis – i form av *ChatGPT*, *OpenAI* og *GPT-4* – har den likevel ikke utviklet seg nok til å kunne gjøre teknologien helautonom. Teknologien krever fortsatt at den i mer eller mindre grad opereres og styres av et menneske.

Hva kan likevel betraktes som en «resilient organisasjon»? Ofte bruker man «High Reliability Organization» (HRO) for å betegne de organisasjonene som under ulike vilkår klarer å opprettholde operasjonskapabilitetene sine under et vidt spekter av situasjoner (Boin & van Eeten, 2013, s. 432).[2] Boin og van Eeten (2013, s. 433) finner at disse organisasjonene har fem viktige trekk: (1) høy gjennomgående teknisk kompetanse i organisasjonen; (2) en særskilt bevissthet om ulike hendelser som bør unngås; (3) et sett av utviklede prosedyrer som har som formål å unngå katastrofale hendelser (se også Suchman, 1985; Johansen, Almklov & Mohammad, 2016); (4) formelle rollestrukturer, ansvarsområder og rapporteringsforhold som under krisesituasjoner kan transformeres til desentraliserte og team-baserte ordninger; og (5) en kultur av reliabilitet som distribuerer verdiene rundt forsiktighet, prosedyrerespekt, oppmerksomhet og individuelt ansvar. Samtlige av disse trekkene er interessante, men i forhold til egen casestudie er trekk fire særlig interessant. Boin og van Eeten (2013) finner at NASA skapte interdisiplinære teams, med høy grad av autonomi, for å få skape teknologien som skulle frakte et mannskap til månen og tilbake. Fleksibiliteten i teamene var best demonstrert under flere nesten-ulykker. Tilslutningen til prosedyrer gjorde at ingeniørene kunne finne feil og hva som måtte bedres, men det var likevel kapasiteten til å improvisere og gå bort fra prosedyrene som reddet mannskapet (Boin & van Eeten, 2013, s. 439). Som Hydro (2014) forteller har de, kontrastert til referansebedriftene, fokusert på de myke sidene ved produksjonsmiljøet ved innføringen av lean-prinsipper (se kapittel 4.1). Mens andre har hatt et ensidig fokus på rasjonalisering og logistikk, har Hydro også inkorporert det organisasjonsmessige aspektet ved teamarbeid og synlig ledelse (Hydro, 2014). I dette ligger det at hver enkelt operatør blir involvert i beslutningsprosessene. Hydro (2014) finner at ansatte rapporterer større forståelse for rollene sine og ser oppgavene sine i en større sammenheng. Bungum, Forseth og Kvande (2016, s. 19) forklarer at samarbeidsforsøkene i 1961, der også Norsk Hydro var et av de fire feltforsøkene, til at bedriftsdemokrati, medbestemmelse, medvirkning og selvstyre ble sentrale begreper i det norske arbeidslivet. I lys av Boin og van Eeten (2013) kan dette ses i forhold til

[2] I dag er det debatter om hvorvidt resilience engineering kan betraktes som en HRO (jf. Haavik, Antonsen, Rosness & Hale, 2019). I denne oppgaven tar jeg utgangspunkt i Boin og van Eetens (2013) argumentasjon som mener dette.

at den tekniske kompetansen ligger ute blant operatørene med en viss grad av autonomisk selvstyre, selv om Bungum et al. (2016) forklarer at samarbeidsforsøkene ikke nødvendigvis førte til mer handlefrihet og autonomi. Ut fra Boin og van Eeten (2013), de fire resiliensdimensjonene og tabell 1 nedenfor beskriver, bør dette være tilrettelagt fra organisasjonssiden for at autonomi og fleksibilitet i det hele tatt kan utøves.



Figur 1. Stadier av resiliens (Roege et al., 2017, s. 386)

Illustrert i figur 1 tar resiliens utgangspunkt i fire dimensjoner: *antesipere*, *respondere*, *monitorere* og *lære* (Patriarca, Bergström, Gravio & Costantino, 2018, s. 90). Å antesipere dreier seg om å vite hva man kan forvente, men også forutse utvikling over tid – som potensielle forstyrrelser eller endrede driftsforhold (Hollnagel, 2015, s. 4). Å forutse sammenfaller med proaktiv resiliens – eller det Boin & van Eeten (2013) kaller «precursor resilence» – der man i forkant av hendelser fokuserer på endring og tilpasning (Stavland & Bruvoll, 2019, s. 12). Det motsatte er reaktivitet, der fokuset ligger i å gjenopprette systemer og funksjonsfeil i etterkant av hendelsen (Stavland & Bruvoll, 2019, s. 12).

Å respondere dreier seg om å vite hva man skal gjøre, eller vet hvordan man skal respondere på vanlige og uvanlige endringer og muligheter, ved å aktivere forberedte handlinger eller justere gjeldende funksjonsmåter (Hollnagel, 2015, s. 3). Sagt på en annen måte handler dette om hvordan man responderer på en forstyrrelse for å tilpasse seg etter de uønskede hendelsene (Stavland & Bruvoll, 2019, s. 17).

Monitorering dreier seg om å vite hva man leter etter, eller at man har en forståelse over hva som kan være en forstyrrende faktor, både positive og negative, for systemytelsen. Samtidig skal monitoreringen kunne dekke systemets egen ytelse så vel som de endringene som skjer i miljøet systemet befinner seg i (Hollnagel, 2015, s. 3). Med andre ord dreier dette seg om å overvåke situasjoner og eventuelle hendelser som kan oppstå (Stavland & Bruvoll, 2019, s. 12).

Den siste dimensjonen er læring. Å lære er evnen til å vite hva som har skjedd eller at man evner å lære fra erfaring – spesielt viktig er at man klarer å lære fra de rette erfaringene (Hollnagel, 2015, s. 4). Læring er sentralt i forberedelsen av eventuelle hendelser. Stavland og Bruvoll (2019, s. 14) argumenterer for at virksomhetene ikke bare skal «sprette tilbake», men at de skal «sprette tilbake bedre» eller «sprette fremover». I dette ligger det at systemet ikke skal sprette tilbake til det som var utgangspunktet før hendelsen skjedde, men at en hendelse vil kreve endring. Sagt med andre ord skal en hendelse skape en ny normaltilstand som er mer resilient enn tidligere (Stavland & Bruvoll, 2019, s. 14).

Dimensjonene er gjensidig avhengig av hverandre. Hollnagel (2015) forklarer at system som ikke evner å respondere i utgangspunktet er dødsdømt. Med mindre systemet er fullstendig statisk bør responsen også endre seg over tid, noe man gjør ved å lære (Hollnagel, 2015, s. 4). Å respondere avhenger også av å monitorere, og et system uten overvåkning vil alltid befinne seg i en høy beredskapstilstand, noe som er umulig sett fra et økonomisk- og produksjonsrelatert ståsted. Det forutsettes også at respondering og monitorering endres ut fra erfaring, noe som igjen kommer fra læring, der man har et fokus på det som både fungerte bra og endre det som fungerte mindre godt (Hollnagel, 2015, s. 4). Resiliens forsøker å legge vekt på det dynamiske i krisehåndtering, og mye av det som til nå er skrevet om innenfor resiliens legger grunnlaget for teorien som et sikkerhetsperspektiv i virksomheter.

3.1.1 Resilience engineering

Resilience engineering (RE) har som formål å undersøke hvordan sosiotekniske systemer håndterer forandringer i ulik grad, og har sine røtter i den tidligere tanken om at robusthet og feilsikre konstruksjoner kan gi falsk trygghet, og at sårbarheter kun gjør seg gjeldende under krisesituasjoner (Yu et al., 2020, s. 1511). RE tar heller sikte i å la usikkerheten bli en del av regnestykket, og er et nytt paradigme i sikkerhetsstyring med fokus på den komplekse balansegangen mellom produktivitet og sikkerhet (Patriarca et al., 2018, s. 79). RE bruker feil i komplekse systemer, så vel som organisatoriske risikobidragsytere og faktorer som påvirker menneskelig ytelse for å etablere verktøy som kan håndtere risiko proaktivt (Patriarca et al., 2018, s. 79). Samtidig bygger RE på tanken om at et system fungerer som et resultat av at folk, både i en individuell og kollektiv kontekst, klarer å tilpasse seg ut fra en rekke arbeidsforhold. De klarer å identifisere og overkomme feil, de gjenkjenner krav og justerer arbeidet sitt fortløpende, og som et følge tolker de og anvender prosedyrer som matcher forskjellige arbeidsbetingelser (Hollnagel, 2013, s. 6).

Yu et al. (2020, s. 1527 - 1530) peker på åtte prinsipper som kan forbedre eller øke resiliens sett fra RE-perspektivet: (1) *Systemkonteksten har noe å si* - en infrastruktur og dens organisasjon i isolasjon kan ikke reflektere resiliens i full grad ettersom at dette også er en del av sosiale, økologiske og teknologiske kontekster; (2) *fostre sosial kapital* – innebærer immaterielle og gruppebaserte eiendeler som tillit, deltagelse, samarbeid over sosiale nettverk så vel som formelle og uformelle institusjonelle ordninger; (3) *opprettholde mangfold* – responsmangfold og et funksjonelt mangfold, som både eksisterer i fysiske komponenter så vel som sosial kapital, har mye å si på grunn av deres komplementære effekter; (4) *håndtere tilkoblingen* – tilkobling gir mulighet før kunnskaps- og ressursdeling, så vel som samarbeidende interaksjon mellom sosiale noder; (5) *oppmuntre lære-ved-å-gjøre* – læring forbedrer resiliens i dens sentrale rolle ved beslutningstaking under usikkerhet; (6) *omfavne polysentrisk kontroll* – der hver enhet er koblet horisontalt med andre enheter for å jobbe sammen på et felles problem, eller interagere vertikalt med enhetene i det hierarkiske styringssystemet; (7) *løse tilpasningsproblemet* – gjelder hvor godt strukturen av et sosialt samarbeidsnettverk sammenfaller med strukturen av det bygde systemet; og (8) *håndtere kompleksitet* – gjelder et skifte i aktørenes underliggende mentale modeller som anerkjenner det komplekse adaptive systemet til det infrastruktur-avhengige systemet som overvåkes. Sosiotekniske system innebærer et samarbeid mellom mennesket og teknologien, og siden det meste av teknologien som brukes i dag ikke er helautonome krever de fortsatt en viss grad av menneskelig styring. Med andre ord spiller menneskelige faktorer en viktig del i resiliensbegrepet, og spesielt viktig blir dette når cyberkriminalitet også blir en del av regnestykket.

3.1.2 Cyberresiliens

Som en del av utviklingen til selve resiliensbegrepet, så vel som utviklingen av samfunnet generelt, kan vi i dag snakke om *cyberresiliens*. Som presisert tidligere gjør samfunnet i sin helhet seg mer teknologiavhengig, og en stor del av de aktivitetene som gjennomføres på samfunnsbasis utføres i tråd med teknologiske systemer. Som resiliens ovenfor er også cyberresiliens forsøkt definert av flere forskere innen tematikken. Björck, Henkel, Stirna og Zdravkovic (2015, s. 312) mener at cyberresiliens refererer til *at man gjentatte ganger har evnen til å levere de intenderte utkommene til tross for ugunstige cyberhendelser*. Ifølge Linkov og Kott (2019, s. 2) bør derimot selve cyberresiliensbegrepet vurderes i kontekst av komplekse systemer som ikke bare består av fysiske- og informasjonsdomener, men også kognitive og sosiale domener. Når Linkov og Kott referer til cyberresiliens snakker de om *systemets evne til*

å forberede seg, absorbere, gjenopprette og tilpasse seg etter uønskede etterfølger som et resultat av en cyberhendelse (2019, s. 2). Med både Björck et al. (2015) og Linkov og Kotts (2019) definisjoner satt opp mot hverandre, er det kun sistnevnte definisjon som tar det dynamiske aspektet ved resiliens i betraktning. I tråd med Hollnagels (2013) definisjon av resiliens, samtidig som at jeg har en interesse om å undersøke et systems respons før, under og etter en hendelse (Roege et al., 2017, s. 388), går jeg videre med denne definisjon av cyberresiliens: *et systems evne til å absorbere, gjenopprette og tilpasse seg før, under og etter uønskede hendelser som kommer av en cyberhendelse*.

Til tross for at det overordnede målet for både cybersikkerhet og cyberresiliens er å verne en organisasjon mot cybertrusler i cyberspace, finnes det forskjeller mellom begrepene og metodene. På den ene siden er cybersikkerhet en policy, strategi og et program som har som formål å verne om informasjon og gjøre datatilgang vanskeligere (Bagheri, Ridley & Williams, 2023, s. 3). Med andre ord går cybersikkerhet i retningen av å beskytte cyberspace, det som fungerer i cyberspace, og de eiendelene som kan nås i cyberspace (Solms & Niekerk, 2013, s. 101). På den andre siden handler derimot cyberresiliens om det å forberede seg, komme seg og gjenopprette systemer etter en cyberhendelse (Roege et al., 2017, s. 386). Selv om formålet med begge er å skape en eller annen form for beskyttelse mot cyberkriminalitet, ligger forskjellen i det dynamiske aspektet ved cyberresiliens der man foretar en vurdering før, under og etter en hendelse.

En cyberresilient organisasjon krever ifølge Hult og Sivanesan (2013, s. 113) fokus på lederskap, folk og prosesser, samtidig som at man har en gjennomgående organisasjonskultur preget av trusselforståelser og læring gjennom feil. Effektiv cyberresiliens kjennetegnes også av sikkerhetskultur, og at de ansatte selv har muligheten til å se på viktigheten av sikkerhetsarbeidet sitt og det de har å bidra med i dette arbeidet (Hult & Sivanesan, 2013, s. 114). Som et følge av dette kan cyberresiliens ses på som et interdisiplinært samarbeid mellom de ulike avdelingene og rollene i en virksomhet (Antunes, Palma-Oliveira & Linkov, 2017), og kontrastert til cybersikkerhetsbegrepet, er det en fordel at sikkerhetsarbeid i cyberspace ikke bare er forbundet med IT-arbeid. En cyberresilient organisasjon bør derfor fordele sikkerhetsarbeidet og inkorporeres som en del av overordnede organisasjonskulturen, og på den måten kan samtlige jobbe ut fra delte verdier og incentiver (Hult & Sivanesan, 2013, s. 114). Ut fra det Hult og Sivanesan (2013) og Antunes et al. (2017) mener, bygger flere av disse aspektene på ikke-tekniske faktorer.

3.2 Ikke-tekniske faktorer

I boka *Safety at the sharp end: a guide to non-technical skills* definerer Flin et al. (2008, s. 1) ikke-tekniske ferdigheter som sosiale, kognitive og personlige ressursferdigheter som utfyller de tekniske ferdighetene, og som bidrar til sikker og effektiv arbeidsutførelse. De anser *situasjonsbevissthet*, *beslutningstaking*, *kommunikasjon*, *teamarbeid*, *lederskap*, *stresshåndtering* og *utmattelsestakling* som grunnleggende ferdigheter i høyrisikoorganisasjoner (Flin et al., 2008, s. 1). De argumenterer også for at ferdighetene påvirkes av de forholdene de jobber i og andres atferd, spesielt de i lederposisjon (Flin et al., 2008, s. 2). Til tross for at man ofte snakker om menneskelige feil som et uunngåelig fenomen, er det likevel mennesket som evner å drifte et uforutsigbart teknisk system (Flin et al., 2008). Inspirert av Flin et al. (2008) definerer jeg «ikke-tekniske faktorer» som «menneskelige, sosiale og organisatoriske dimensjoner av resiliens som utfyller tekniske ferdigheter».

I likhet med Flin et al. (2008) har Per Morten Schiefloe (2017) etablert modellen for mennesker, teknologi og organisasjon (MTO-modellen). Fremover er det ikke selve modellen som anvendes i analysen senere, og brukes heller som en kontekstualisering over hvilke faktorer som kan være resiliensytende. Relevant er forholdet mellom mennesket og organisasjon, og hva dette har å si på bruk og håndtering av teknologi. M-faktoren er *menneskefaktoren* og man snakker herunder om sikkerhetskritisk atferd, eller en type atferd som har direkte eller indirekte konsekvenser for en aktivitet (Schiefloe, 2017, s. 285). I slike instanser krever likevel situasjonen en dypere analyse av situasjonen, og man retter blikket mot O-faktoren som ligger på det administrative nivået og ser på den organisatoriske kvaliteten i sin helhet. Det vil si at man utforsker hvordan handlinger utføres gjennom en virksomhets beslutningslinjer, og hvorvidt organisasjonen driver opplæring av nye systemer, risikovurderinger, kommunikasjonssvikt og svakheter i sikkerhetskulturen (Schiefloe, 2017, s. 284-285). T-faktoren dreier seg om de teknologiske kvalitetene virksomheten eller organisasjonen opererer med. Før teknologi kan anvendes må den i seg selv være pålitelig, men teknologien skal også gi tilstrekkelig sikkerhet for de som benytter den (Schiefloe, 2017, s. 283).

Steen, Haakonsen og Patriarca (2022) anvender begrepet «samhandling» for å fremkalle relevante trekk ved resiliensbegrepet, og utforsker hvordan oljeplattformen West Phoenix i Nordsjøen håndterte et COVID19-utbrudd sommeren 2020. I artikkelen ser de på nyansene rundt resiliensbegrepet gjennom fire semistrukturerte dybdeintervjuer. Forfatterne finner at å håndtere en kompleks nødssituasjon med høy grad av usikkerhet krever en proaktiv, åpen og transparent fremgangsmåte med felles beslutningstagninger, og at felles beslutninger forsterker

felles rolleforståelse og ansvarsområder. Til syvende og sist forsterker dette samhandlingskapasiteten (Steen et al., 2022, 267).

Broekema, van Kleef og Steen (2017) undersøker hvordan det nederlandske mattilsynet responderte på fire veterinærkriser, med fokus på det som bidrar til organisatorisk læring. I materialet finner de seks relevante trekk: (1) Organisatorisk læring ble i stor grad påvirket av den daværende *politisk-økonomiske konteksten*, i form av budsjettkutt og politisk press; (2) organisatorisk læring påvirkes av *sosial-emosjonell forståelse* – eksemplifisert av bønder som tydde til vold under munn- og klovsyken i 2001, som et følge av uenigheter av de tiltakene det nederlandske mattilsynet innførte; (3) organisatorisk læring påvirkes av den overordnede *organisasjonskulturen*, der interkollegiale forhold bidrar til informasjons- og kunnskapsdeling innad i organisasjonen som bidrar til økt gjensidig tillit; (4) organisatorisk læring påvirkes av *organisatorisk struktur*, der det kommer frem at reorganiseringer og mannskapserstatninger påvirker læring i negativ retning; (5) organisatorisk læring påvirkes av *trinnene i krisehåndteringen*; og (6) organisatorisk læring påvirkes av *organisatorisk glemsel*, som betyr at kriseekspertise og erfaringer fra tidligere kriser gradvis fases ut som et følge av at ansatte slutter eller pensjoneres (Broekema et al., 2017, s. 333 - 336).

Tidligere forskning på cyberresiliens har hatt et overordnet fokus på de tekniske faktorene for hvordan en bedrift klarer å være resiliente i cyberspace, og et minimalt fokus vies til de ikke-tekniske faktorene. Av ikke-tekniske faktorer viser Bagheri et al. (2023) blant annet hvordan forskjellige IT- og virksomhetsledere betrakter cyberresiliens. Vasudevan, Piazza og Carr (2022) ser på kvalitative faktorer, for å se hvilken grad disse faktorene påvirker cyberresiliens. Dupont (2019) finner fra finansinstitusjoner fem organisatoriske dimensjoner av resiliens – dynamikk, nettverk, innøving, adaptivitet og bestridelser. Både Aakre (2020) og Antunes et al. (2017) ser på risikokommunikasjon og intern- og ekstern åpenhet under krisesituasjoner. Til tross for at disse artiklene tar for seg relevante ikke-tekniske faktorer, refererer de dog lite til de ikke-tekniske faktorene som befinner seg og utøves lengre ned i organisasjonen, og en god del av litteraturen har et overordnet fokus på virksomhets- og bedriftsledere. Jeg sier derimot ikke at lederskap ikke er en relevant faktor for hvordan krisesituasjoner håndteres, og argumenterer heller for det motsatte. Heldal og Antonsen (2014) ser for eksempel på hvordan kontekstuelle faktorer – som organisasjonsstruktur, styringsfilosofi, forandringshistorikk og samfunn – påvirker ledelse av operative team i en norsk høyrisikoorganisasjon. De finner at faktorene interagerer og forsterker hverandre i hvordan teamlederne styrer det operative teamet, og har mye å si for hvordan operatørene bedømmer gode lederegenskaper (Heldal & Antonsen, 2014, s. 396). Weick (1993) beskriver

også viktigheten av et godt lederskap ut fra det manglende rollesystemet og ledelsesstrukturen i Mann Gulch katastrofen. Brannmannskapet besto av formannen Wagner Dodge, skogvokteren Jim Harrison, syv skogbruksstudenter og 12 tidligere militært personell. Til overraskelse for alle antente Dodge en gressflekk foran seg, ba mannskapet om å fjerne alt av verktøy og legge seg ned ved det brente gresset. I stedet løp mannskapet til den nærmeste fjellryggen, siden Dodge var den eneste som visste at brannen ikke ville berøre dette området (Weick, 1993, s. 629). Hendelsen resulterte i 13 døde personer. I artikkelen identifiserer han fire dimensjoner som transformerer sårbarhet til resiliens: (1) *improvisering og bricolage*; (2) *virtuelle rollesystemer*; (3) *visdomsholdninger*; og (4) *respektable interaksjoner* (Engen, Kruke, Lindøe, Olsen, Olsen & Pettersen, 2016, s. 318; Weick, 1993, s. 638 - 643).

3.2.1 Menneskelige faktorer og organisatorisk resiliens

Human factors (menneskelige faktorer) kan på en og samme tid anses som en vitenskapelig disiplin og profesjon ifølge Kongsvik, Albrechtsen, Antonsen, Herrera, Hovden & Schiefloe (2018). Som vitenskap har menneskelige faktorer som formål å se på relasjonen mellom mennesket og operasjonaliseringen av teknologien man omgir seg med. Som profesjon forsøker man dermed å benytte seg av denne kunnskapen – gjerne i form av økt produktivitet i virksomheten (Kongsvik et al., 2018, s. 192). I noen sammenhenger blir det fortalt at 80-90% av alle ulykker skyldes menneskelige faktorer, og ofte er det disse faktorene som ses i sammenheng med feil som enkeltpersoner kan ha gjort.

Når man snakker om ikke-tekniske faktorer som resiliensytende elementer, snakker man i flertallet av tilfellene også om menneskelige faktorer. Til tross for at tekniske komponenter er en viktig dimensjon i det overordnede resiliensnivået i en organisasjon, er det likevel sluttbrukeren som opererer dem. I likhet med at en god del av sikkerhetsarbeidet i en virksomhet dreier seg om sikker drift av dens teknologi, dreier cybersikkerhet seg om forholdet mellom mennesket og teknologien. På samme måte som Hollnagel (2013), argumenterer Schultz (2005) for at teknologi er designet på en måte som gjør mennesket i stand til å drifte den, selv om teknologien er designet for autonom drift. Teknologidrift krever med andre ord en forståelse av menneskelig atferd, og organisasjonsklimaet spiller en sentral rolle for å holde ansatte oppdaterte på sikkerhet og sikkerhetstiltak i cyberspace (Schultz, 2005; Triplett, 2022, s. 473). Til tross for at en virksomhets kjerneaktivitet kan forstyrres som et følge av cyberangrep, viser likevel beredskapsorganisasjonene lite bevisstgjøringsarbeid rundt de mulige konsekvensene av dem (Giacomello & Pescaroli, 2019, s. 257). For å bedre dette mener Giacomello og Pescaroli (2019) på den ene siden at trening og læring av ansatte, og kunnskaps- og

informasjonsformidling kan bedre dette, i form av scenariobygging og én definisjon av «akseptabel risiko». På den andre siden mener de også at et fellestrekk i omtrent alle cyberangrep er sluttbrukerne som ikke tar sikkerhet på høyeste alvor, ofte som et følge av at fokuset ligger på daglige arbeidsoppgaver, men også for at det er vanskelig å se gevinsten av og holde seg oppdatert på cybertrusler dersom fordelene ikke er umiddelbare (Giacomello & Pescaroli, 2019, s. 258).

Den samme problematikken peker også Eirik Albrechtsen (2006) på. I en kvalitativ studie i en norsk bank og et norsk IT-selskap forsøker han å gi kunnskap om databrukernes erfaringer med IT-sikkerhet og deres individuelle sikkerhetsrolle i det daglige arbeidet. I IT-selskapet baserer sikkerhetsarbeidet seg på dokumenterte regler og retningslinjer, mens i banken baserer den seg i all hovedsak på en sikkerhetshåndbok (Albrechtsen, 2006, s. 279). I begge virksomhetene ble det trukket frem at bevisstheten rundt informasjonssikkerhet var utilstrekkelig, blant annet gjennom at:

> [...] informantene gjennomførte en lav andel handlinger som var rettet mot informasjonssikkerhet; at informantene ikke hadde kjennskap til eventuelle faremomenter; at informantene ikke hadde kjennskap til mulige konsekvenser av eventuelle sikkerhetsbrudd; at informantene ikke kunne se problemer eller forbedringspotensial i sine egne arbeidsforhold; og at informantene ikke kunne se verdien av deres egen rolle i informasjonssikkerhet i et holistisk sikkerhetsarbeid for virksomheten (Albrechtsen, 2006, s. 280, egen oversettelse)

Informantene sier imidlertid i Albrechtsens (2006) studie at de er motiverte for å gjøre et sikkerhetsarbeid, men at problemet ligger i at de ikke vet hvordan. Informantene forklarer dette gjennom tre aspekter: (1) for lite kommunikasjon med profesjonelle innen informasjonssikkerhet; (2) at informasjonssikkerhet tilskrives som en teknologisk disiplin og bør som en konsekvens behandles av profesjonelle på sikkerhetsnivået; og (3) for lite tid til å jobbe med sikkerhetsarbeid sammen med det daglige arbeidet (Albrechtsen, 2006, s. 281). Siste poeng baserer seg på en konflikt mellom *funksjonalitet* og *sikkerhet*, der de fleste informantene ikke finner den rette balansen mellom disse, enten for at informasjonssikkerhet ikke er informantens jobb eller for at overdrevne sikkerhetstiltak tar for mye tid (Albrechtsen, 2006, s. 281). En løsning, og et gjentagende mønster i dataen, er at organisasjonsnivået involverer arbeiderne i sikkerhetsarbeidet i større grad enn før. Informantene argumenterer blant annet for mer sikkerhetsorientert problemløsing, ha flere muligheter for å reflektere over egen situasjon

og egen bruk av informasjonsteknologi, og til sist møte sikkerhetsprofesjonelle ansikt til ansikt slik at de blir mer synlige på bedriftsnivået (Albrechtsen, 2006, s. 283-284). Nyansering av sikkerhetsarbeid er noe Arias-Vargas, Sanchis og Poler (2022) ser på gjennom «spillifisering» av kurs. Ved spillifisering kan ansatte testes, trenes og drive kunnskapsoppnåelse. Albrechtsen (2006) finner dog at dette kan være problematisk dersom spillet i seg selv blir viktigere enn læringsformålene. Det overordnede målet bør derfor bli å motivere og legge til rette for at ansatte faktisk har mulighet og evne til å lære av de rette hendelsene, siden læring ikke kan skje før også evne til å antesipere, respondere og monitorere er på plass (Hollnagel, 2013; 2015; Stavland & Bruvoll, 2019; Patriarca et al., 2018).

	Motivasjon	**Mulighet**	**Evne**
Antesipere	Villig til å se etter forstyrrelser, nye krav, nye muligheter og/eller endrede driftsprosesser.	Inneha ressurser som tillater en å se etter utvikling i fremtiden.	Vite hva man kan forvente.
Monitorere	Villig til å overvåke det som kan alvorlig påvirke systemytelse på kort sikt, både positivt og negativt.	Inneha ressurser som kan overvåke systemytelse og hva som skjer i miljøet rundt.	Vite hva man skal se etter.
Respondere	Villig til å respondere på vanlige og uvanlige endringer og forstyrrelser.	Inneha ressurser som hjelper deg å foreta handlinger.	Vite hva man skal gjøre.
Lære	Villig til å lære fra erfaring.	Inneha ressurser som tillater deg å lære fra de rette erfaringene.	Vite hva som har skjedd.

Tabell 1. Rammeverk for resiliensytende atferd (Van der Kleij & Leukfeldt, 2019, s. 23).

Van der Kleij og Leukfeldt (2020) mener at disse aspektene også kan anvendes i konteksten av cyberresiliens, men at dette bør dreies i en retning av menneskelig atferd. De foreslår *motivasjon*, *mulighet* og *evne* som tre essensielle forhold illustrert i tabell 1 ovenfor. Organisatorisk cyberresiliens avhenger av de ansattes motivasjon, mulighet og evne til å utføre

de fire resiliensfunksjonene (Van der Kleij & Leukfeldt, 2019, s. 20). Motivasjon dirigerer atferd, som vanlige prosesser, emosjonell respons og analytisk beslutningstaking. Mulighet er de aspektene som ligger utenfor de ansatte, som gjør resiliensytelse mulig – eksempelvis organisasjonskultur. Evne tilsier individets psykologiske og fysiske kapasitet til å engasjere seg i aktuelle aktiviteter, som inkluderer nødvendig kunnskap og ferdigheter på området (Van der Kleij & Leukfeldt, 2019, s. 21). Til tross for at teknologiske komponenter er essensielle for den overordnede organisatoriske resiliensytelsen, argumenterer jeg for at en like viktig del befinner seg ved hver enkelt ansatt. I de fleste tilfellene blir menneskets evne løsningen på problemet.

3.2.2 Mennesket som løsning

Van der Kleij og Leukfeldt (2020) mener at organisasjonskulturen i seg selv har ansvar for at ansatte har mulighet, motivasjon og evne til å utøve resiliensytende atferd. Tidligere har man fra det tradisjonelle sikkerhetskonseptet *Safety-I* definert sikkerhet ut fra at så få ting som mulig går galt. I resiliensforstand er Safety-I betraktet som en reaktiv respons på kriser, og mennesket anses her som en byrde og et problem som bør fikses. Det har derimot blitt argumentert for at forståelsen er lite anvendbar i komplekse sosiotekniske systemer, og Ham (2021, s. 11) mener at Saftey-I kun kan anvendes i systemer som bare består av tekniske komponenter. I den forstand har RE og *Safety-II* gjort seg spesielt relevante. Her vies et større fokus på det som går bra. I motsetning til Safety-I, er proaktivitet viktig i Safety-II, og man forutser endringer og etableringer kontinuerlig. Også kontrastert til den foregående sikkerhetsforståelsen er mennesket i denne forstanden sett på som en viktig ressurs for den overordnede fleksibiliteten og resiliensytelsen i en organisasjon (Hollnagel, Wears og Braithwaite, 2015)

Til tross for at 80-90% av de beregnede ulykkene kan forårsakes av menneskelige feil, er likevel mennesket et viktig element i avvergelsen og forhindringen av potensielle faremomenter. I de fleste områder er mennesket proaktive, problemløsende og uerstattelige dersom en fare oppstår (Kongsvik et al., 2018, s. 200), og i et organisasjonssosiologisk perspektiv brukes ofte begrepet *barrierestyring* i slike situasjoner. Barrierestyring er oftest anvendt i petroleumsindustrien. Etter en rekke hendelser med store ulykkespotensial – som konstruksjonshendelsen på Alexander L. Kielland i 1980, hydrokarbonlekkasjen på Piper Alpha i 1988, og en ukontrollert utblåsning på Snorre A i 2004 – skal barrierene tidlig oppdage feil, fare- og ulykkessituasjoner, redusere mulighetene for at disse utvikler seg og begrense skader og ulemper (petroleumstilsynet, 2017, s. 3). Sagt med andre ord skal barriereelementene forsøke å avlede og begrense «energi på avveie» (Kongsvik et al., 2018, s. 200).

Dette krever derimot at alle ansatte har samme situasjonsforståelse, samtidig som at det krever en organisasjon som selv fostrer en sikkerhetskultur, som en reliabilitetskultur Boin og van Eeten (2013) kjennetegner som en viktig faktor i en HRO. Relatert til differansen mellom Safety-I og Safety-II skiller Dynes (1993, s. 183) mellom to konseptuelle modeller for krisehåndtering. På den ene siden tar «militærmodellen» sikte i å fjerne kaos ut fra kommando og kontroll, og med andre ord et sentralisert håndteringsgrunnlag. Her menes det at militært organiserte enheter klarer å håndtere kaos, og at sivilt organisert enheter ikke evner dette (Dynes, 1993, s. 183). På den andre siden betrakter «problemløsningsmodellen» sosial kontinuitet, koordinering og samarbeid som viktige faktorer for krisehåndtering, og mener at en stor del av løsningen befinner seg ute i befolkningen, noe som tilsier en desentralisert håndtering (Dynes, 1993, s. 183). I forlengelsen av dette ser Woods (2011, s. 4) på antesipasjon som en viktig forutsetning for resiliens, der han blant annet mener at et resilient system evner å navigere gjensidige avhengigheter på tvers av roller, strukturer, aktiviteter og nivåer, men også at et slikt system klarer å foreta perspektivskifter og kontrastere diverse perspektiver som går utenfor den nominelle systemposisjonen.

3.3 Resiliens vs risiko

Som i bakgrunnskapittelet tidligere ble Ulrich Becks (1992a; 1992b; 2016) risikoteori mye brukt for å beskrive cyberkriminalitet som fenomen. Forholdet mellom resiliens og risiko er omdiskutert. Det finnes flere likheter mellom dem, men de besitter samtidig ulikheter som gjør det mulig at de kan utfylle hverandre (Stavland & Bruvoll, 2019, s. 37). Av ulikheter har risikohåndtering på den ene siden som formål å redusere potensielle skadevirkninger knyttet til kilder man allerede er kjent med, mens man med resiliens på den andre siden evner å opprettholde tidskritiske funksjoner samtidig som at en kritisk situasjon pågår (Stavland & Bruvoll, 2019, s. 14). Risikohåndtering handler også om hvordan man styrker et system i et gitt tidsrom, mens resiliens dreier seg om en langvarig prosess for å beskytte systemfunksjonaliteter mot øvrig skade (Stavland & Bruvoll, 2019, s. 14). Av likheter mener Linkov, Trump og Fox-Lent (2016, s. 3) at både risiko og resiliens: (1) ønsker å unngå negative konsekvenser som et følge av uønskede situasjoner; og (2) undersøker systemsvakheter og identifiserer handlinger som kan bidra til å redusere dem. De mener også at «risiko» er det operative begrepet for dem begge, og det overordnede målet er å redusere eventuelle skader fra krisesituasjonene.

4. Metode

I følgende kapittel presenterer jeg først en beskrivelse av casen, og deretter den metodiske bakgrunnen for datagenereringsgrunnlaget og analysen senere. Deretter presenterer jeg forskningsdesign og intervju som metode, og eventuelle implikasjoner metoden kan ha for innsamling av data. Deretter undersøker jeg hvilke implikasjoner min rolle som forsker kan ha for innsamlingen av data, men også hvordan dette analyseres i ettertid. Deretter presenterer jeg selve utvalgsprosessen og hvordan jeg gikk frem med å rekruttere informanter for avhandlingen. Etter det presenterer jeg hvordan dataen ble behandlet i ettertid av innsamlingen, der jeg diskuterer transkribering og koding som bearbeidingsprosess. Kvalitetskriterier som validitet og reliabilitet gjennomgås deretter. Avslutningsvis vender jeg blikket mot etiske betraktninger for studiet og datainnsamlingen.

4.1 Casebeskrivelse

Det empiriske grunnlaget har bakgrunn i cyberangrepet som ble utløst i Norsk Hydro i 2019. Løsepengeviruset ble først utløst og oppdaget i en av fabrikkene i USA, men påvirket hele den globale organisasjonen senere. Med hjelp av manuelle prosedyrer foregikk driften og produksjonen av aluminium som normalt til tross for viruset som befant seg på konsernets nett. I etterkant av angrepet ble kostnadene av angrepet estimert til godt over 800 millioner kroner (Hydro, 2020; Stolt-Nielsen & Lysberg, 2021). Hydro ble senere tildelt en pris for hvordan angrepet ble håndtert offentlig – åpen og hyppig kommunikasjon (Hydro, 2019). Hydro er den første private virksomheten som ble tildelt Åpenhetsprisen. Juryen argumenterte for at deres åpenhet senere ville ha stor samfunnsmessig betydning og bidrar til å øke bevissthet og kunnskap om cyberangrep, og hvilke konsekvenser cyberangrep har for andre bedrifter (Hydro, 2019).

I lokalsamfunnet er Hydro en hjørnesteinsbedrift, og er viktig for sysselsettingen og jobbmulighetene for fremtidige ingeniører og yrkesfagelever. Per dags dato har den ene fabrikken jeg undersøkte i underkant av 700 ansatte, fordelt på ulike underavdelinger med deres respektive områdeledere, fagledere, handlingsansvarlige og operatører. I tillegg ansetter fabrikken godt over 100 ferievikarer i året, og om sommeren består en god del av arbeidskraften av studenter og øvrige unge voksne hjemme på ferie. Med andre ord har fabrikken alt fra lærlinger i 18-årsalderen til godt erfarne arbeidere ved pensjonsalder.

Verket har produksjonskapasitet på hele 400 000 tonn elektrolysemetall, støperikapasitet på 500 000 tonn, og produserer 80 000 tonn anoder hvert år. Fabrikken er det

man kan kalle en høyrisikoorganisasjon, der aktiviteter gjennomføres blant kritiske og farlige miljø, og sjansen for store ulykker er stor (Heldal & Antonsen, 2014), for eksempel fra høyspenning, varme og eventuelle eksplosjoner dersom vann kommer i kontakt med flytende metall. For å minimere sjansen for at slike situasjoner oppstår finnes det et antall teknologiske sikringssystemer, samt standardiserte arbeidsprosedyrer – «Standard Operating Procedures» (SOP) – for at arbeidet ikke skal gjøre materielle eller menneskelige skader. Dette inngår som en del av Aluminium Metal Production System (AMPS), et produksjonssystem som tar sikte i å inkludere ansatte i større grad, og baserer seg på fem prinsipper: (1) standardiserte arbeidsprosesser; (2) definerte kunde- og leverandørforhold; (3) optimalisert flyt; (4) dedikerte team; og (5) synlig ledelse (Hydro, 2014). Tanken bak AMPS er stabil produksjon av aluminium gjennom lik jobbutførelse og kontinuerlig forbedringsarbeid. Som et resultat av AMPS kan arbeidsutførelsen oppleves som lite kompleks ut fra de standardiserte arbeidsprosessene, selv om risiko er en faktor.

4.2 Forskningsdesign og metode

Som kjent innledningsvis er jeg opptatt av å se på ikke-tekniske faktorer for cyberresiliens ved Norsk Hydro. Før jeg begynte med datainnsamlingen tok jeg utgangspunkt i en åpen problemstilling der jeg ville utforske hvordan cyberangrepet hadde bidratt til endring av bedriftssikkerhet i etterkant, og formet intervjuguiden noe ut fra dette. Siden feltet er nokså nytt i sosiologien var jeg likevel forberedt på å måtte endre problemstillingen ut fra det som kom opp i løpet av intervjuene, noe som i etterkant også ble faktum. På den måten tar avhandlingen utgangspunkt i et eksplorativt design. Målet å skape innsikt ut fra informantenes egne refleksjoner rundt tematikken, og den vitenskapelige posisjoneringen går derfor mot fenomenologien. Satt på spissen har fenomenologien som overordnet mål å finne ut av hvordan en person forstår et gitt fenomen ut fra det dem selv erfarer, oppfatter og opplever (Sohlberg & Sohlberg, 2020, s. 87). Med andre ord er det viktigste i denne sammenhengen å sette lys på essensen i datamaterialet og det informantene forteller. I kontekst av tematikken er jeg interessert i å finne ut av hvordan cyberangrepet ble håndtert ut fra informantenes egne fortellinger. I utformingen av avhandlingen var det tidlig klart at kvalitative intervjuer var den mest gjeldende metoden for å få frem hvordan informantene snakker om tematikken, hvilke erfaringer de besitter, hvordan cyberangrepet ble håndtert og ikke minst siden hendelsen skjedde i 2019. Ergo er jeg interessert i å finne ut av informantenes egne holdninger for å besvare problemstillingen og forskningsspørsmålene jeg har formulert.

Forskningsstrategien kommer som et følge av den fenomenologiske posisjoneringen og det eksplorative designet. Helt siden skriveprosessen begynte tidlig forrige semester har jeg tatt utgangspunkt i en abduktiv strategi. Abduksjon tar utgangspunkt i en dialog mellom empiri og teori, men også en åpenhet rundt hvilken teori som er best egnet til å belyse den empirien man har for hånden (Mathiesen & Volckmar-Eeg, 2022, s. 11). Et overordnet mål i abduksjon er at empirien dermed bidrar til teoriutviklingen. Med andre ord kombinerer abduktive metoder både *induksjon* og *deduksjon*. Den induktive delen går i at man jobber empirinært og at teoriutviklingen dannes fra bunnen av, også kalt «grounded theory». Den deduktive delen tar derimot sikte i å forklare enkelthendelser fra en generell regel, og baserer forskningsstrategien på hypotesetesting (Tjora, 2018, s. 18). I forkant av intervjuene leste jeg meg opp på tematikken – herunder resiliens, risiko og tidligere forskning innenfor cyberkriminalitet – for å se etter mulige sammenhenger mellom disse, men også for å se etter sentral tematikk som kunne gjøre seg gjeldende når intervjuene ble foretatt senere. For eksempel er det argumentert i tidligere forskning innen cyberresiliens at fokuset bør ligge på hele hendelsesforløpet til en cyberhendelse (jf. Dupont, 2019) for å se hvor resilient en organisasjon faktisk er både før, under og etter hendelsen, noe jeg selv tok utgangspunkt i da intervjuene ble foretatt og i strukturingen av analysen senere. Likevel ville jeg ikke låse empirien som ble generert i etterkant til den teorien jeg hadde lest meg opp på, og jeg ville at refleksjonene informantene selv kom med skulle få en større plass i selve analysearbeidet. Jeg ville åpne opp for at intervjudataene går inn på teori jeg selv ikke hadde vært innom på forkant, selv om teorien jeg brukte før intervjuene utgjorde den teoretiske basisen for intervjuguiden (jf. vedlegg 3).

4.2.1 Intervju som metode for datagenerering

I en intervjusituasjon har forskeren som mål å samle kunnskap fra én eller flere informanter, hvor man deretter forsøker å trekke konklusjoner og mønster fra utsagnene som kommer opp i løpet av intervjuet (Hammersley, 2017, s. 173). I samfunnsvitenskapen finnes det flere intervjumetoder, men i denne avhandlingen benytter jeg meg av én. Som nevnt har man i fenomenologien et overordnet mål at analysen tar utgangspunkt i informantens egne erfaringer og refleksjoner av et fenomen, noe de *semistrukturerte (dybde)intervjuene* har som formål å ta tak i (Kvale, 1997, sitert i Tjora, 2018, s. 114). Semistrukturerte intervju brukes for å få frem meninger og erfaringer innenfor et avgrenset felt. I et semistrukturert intervju forsøker man så langt det er mulig å skape en fri samtale mellom forsker og informant, men at samtalen i mer eller mindre grad tar utgangspunkt i noen spesifiserte tema innenfor den overordnede tematikken i avhandlingen. Som et følge formulerer man åpne spørsmål for at informanten har

mulighet til å avgi en dypere refleksjon over de spørsmålene som stilles i intervjusituasjonen, men på den måten kan informanten også gå inn på tema som jeg ikke har tenkt på i forkant av intervjuet (Brinkmann & Kvale, 2019).

Sett i forhold til andre metoder i sosiologien, som den kvalitative metoden *observasjon* eller bearbeidingen av kvantitative data, ble kvalitative intervju den mest gjeldende metoden for min del. Cyberkriminalitet er et komplekst felt i konstant utvikling, men som har særdeles lite tidligere forskning i norsk sosiologi. I avhandlingen er jeg interessert i å se på de ikke-tekniske faktorene som bidro til cyberresiliens i en virksomhet ved å ta utgangspunkt i hendelsesforløpet av et cyberangrep fra 2019. Like viktig er hvordan resiliens opprettholdes i etterkant av angrepet. På den måten er jeg interessert i å undersøke noe som ikke er observerbart siden hendelsen allerede har skjedd, men man kan også snakke om ikke-observerbarhet når man snakker om ikke-tekniske faktorer som dimensjoner av cyberresiliens. Selve datagenereringsgrunnlaget bugner derfor i refleksjoner av noe som allerede har skjedd, som eventuelt kan være problematisk i analysen senere.

Intervju er i enkelte instanser utilstrekkelig dersom målet er å gi konkrete beskrivelser av det som foregår i samfunnet, og fokuset ligger heller her i å undersøke informantens egen subjektivitet (Atkinson, 2015, s. 92). I en avhandling som tar sikte i å undersøke et fenomen som skjedde for noen år siden, er det også en rekke andre momenter som bør tas i betraktning. For det første kan de svarene informantene oppgir i løpet av intervjusituasjonen farges av dårlig hukommelse og ufullstendig kunnskap om tematikken (Walford, 2007, sitert i Roulston, 2010, s. 203). Det kan hende at informantene ikke husker det fullstendige hendelsesforløpet da cyberangrepet skjedde for fire år siden. For det andre er cyber- og informasjonssikkerhet ofte konfidensiell av natur, og det kan tenkes at informantene rett og slett ikke kan snakke om diverse tema jeg har pekt meg ut. For å løse dette har jeg ikke formulert spørsmål der man kan forvente å få oppgitt informasjon som kan regnes som konfidensiell. Likevel var det spesielt førstnevnte problematikk som ble relevant i løpet av de ti intervjuene jeg foretok, og spesielt var hukommelsen en viktig faktor for hvordan informantene svarte på spørsmålene som rettet seg mot tiden *før* og til dels *under* cyberangrepet.

4.3 Forskerrollen

Hydro er en aluminiumsprodusent jeg har kjennskap til i form av et ferievikariat siden 2018, og denne kjennskapen kan virke avskrekkende for informantene på flere måter. Under intervjusituasjonen er det et overordnet mål å skape trygghet og et gjensidig tillitsforhold

mellom forskeren og den/de som forskes på. Når jeg som forsker går inn i et område for å undersøke et spesifikt tema er jeg avhengig av at informanten faktisk strekker til og reflekterer over sine erfaringer. Det kunne også virke avskrekkende fordi intervjusituasjonen foregikk i et miljø informanten har kjennskap til – på arbeidsplassen – da betydningen av sted kan ha en stor betydning for hvordan man responderer på intervjuspørsmål (Tjora, 2018, s. 122). Resultatet av dette kan føre til at informantene avgir lange svar som til syvende og sist forbedrer intervjuets kvalitet (Roulston, 2010, s. 202). Likevel må også balansen mellom forsker og vikar diskuteres. For det første går jeg inn i en virksomhet jeg er godt kjent med. Naturligvis kan dette bidra til at analysearbeidet generelt i større grad tolkes ut fra det informantene faktisk mente, nettopp siden opplæringen jeg har også er en del av den samme grunnkompetansen informantene selv innehar. For det andre kan likevel mine forkunnskaper, både fra min tid som ferievikar og forsker på feltet, bidra til at analysearbeidet dreies i en bestemt retning. Derfor er det enda viktigere at informantenes refleksjoner får enda større plass i analysekapitlet senere. Noen vil likevel argumentere for at det er umulig å gå inn i et felt uten noen form for forkunnskap, siden en total forkastelse av teoretiske innsikter i utgangspunktet innebærer at man ikke kan tolke noe som helst (Masi, 2001, sitert i Kusenbach, 2003, s. 457). I løpet av intervjuene avga nesten samtlige av informantene lange svar på spørsmålene jeg stilte og jeg la opp til at de kunne reflektere fritt over spørsmålene som ble stilt. Samtidig gjorde min erfaring med Hydro det enklere å få innpass i virksomheten da jeg knyttet første kontakt på tampen av fjoråret. For det tredje besitter jeg også en del informasjon som et følge av intervjuene. Å være en insider kan også være en trussel, alt ettersom hvilken informasjon jeg har fått oppgitt og hvordan informasjonen behandles. Mye av den samme tematikken blir også nevnt i kapittel 4.7.1 om personvern.

4.4 Utvalgsprosess og rekruttering

Som nevnt i det forrige kapitlet er Norsk Hydro en virksomhet jeg selv har erfaring med. Som et grunnlag av dette hadde jeg flere muligheter for å starte førstekontakt. I begynnelsen av november 2022 tok jeg kontakt med en bekjent som jobber der, og omtrent én uke senere fikk jeg beskjed om at han hadde videreført idéen og formålet med avhandlingen videre til HR-avdelingen. HR ville ta ballen videre derfra for å se om noen ansatte ville være behjelpelige med et dybdeintervju på 45 minutter. Til tross for at min kjennskap til Hydro gjorde det enkelt å oppnå førstekontakt, fungerer min kjennskap til fabrikken, den bekjente og HR-avdelingen som døråpnere for å få tilgang til mulige informanter i virksomheten (Tjora, 2018, s. 130). For

selve utvalget hadde jeg to utvalgskriterier: over 18 år og ansatt ved virksomheten under cyberangrepet. Siden cyberangrepet var noe som berørte samtlige av fabrikkene i konsernet globalt sett, var det ikke nødvendig at informanten jobbet ved den fabrikken jeg selv har erfaring med. Jeg hadde likevel et ønske om at intervjuene inneholdt en viss grad av lokalkunnskap, som resulterte i at jeg tok kontakt med kun én av konsernets fabrikker. For å få en viss variasjon i intervjuene, og for å øke sjansen for at intervjuene inneholdt en grad av motstridende og ny informasjon, hadde jeg et ønske om at informantene i mer eller mindre grad hadde varierende stillinger og arbeidsoppgaver i fabrikken. Utvalgsprosessen er med andre ord strategisk ettersom at jeg er ute etter å forske på et fenomen som informantene selv har erfaring med (Tjora, 2018, s. 130). Tabell 2 viser en liste over informanter, med anonymiserte navn, som ble intervjuet. Til høyre i tabellen vises også hvilket nett informantene jobber mot i løpet av en arbeidsdag, der «>» viser hvilket nett de jobber mest på dersom de jobber på begge. Samtlige av informantene i utvalget har varierende stillinger og ansvarsområder i fabrikken.

Informant	**Arbeidsområde**
«Ivar»	Kontornett
«Ulrik»	Kontornett > Prosessnett
«Johanne»	Kontornett
«Ole»	Prosessnett
«Birgitte»	Kontornett
«Ingrid»	Kontornett
«Magnus»	Prosessnett
«Kari»	Kontornett
«Atle»	Prosessnett > Kontornett
«Karl»	Prosessnett

Tabell 2. Informanter.

I forkant av studien stile jeg meg noen spørsmål for hvor mange informanter jeg faktisk trengte, men omfanget ville naturligvis avhenge av tematikk, problemstilling, tid og hva jeg faktisk hadde et ønske å finne ut av. Kvale (1996) mener samtidig at datainnsamling skal kunne fortsettes helt til «teoretisk metning» finner sted, og at all datainnsamling etter det ikke avdekker nye funn. Datainnsamlingen vil kun bekrefte og samsvare med det som allerede er sagt i en eller annen grad. Etter en diskusjon med veileder ble det bestemt at utvalget skulle bestå av ti informanter. I likhet med Kvales (1996) argumentasjon kunne jeg etter de ti

intervjuene se en viss grad av teoretisk metning, og jeg argumenterer for at all datainnsamling ut over dette kun hadde bekreftet det som allerede hadde blitt funnet.

4.5 Bearbeiding av intervjudata og analyse

Etter at samtlige intervjuer hadde blitt foretatt var det på tide å begynne med bearbeiding av empirien jeg hadde samlet inn, og naturlignok begynne selve analysearbeidet. Her er det to områder jeg vil trekke frem som essensielle deler av analysearbeidet. Til tross for at både *transkriberingen* og *kodingen* skjedde i etterkant av intervjuene, var analysearbeidet et kontinuerlig arbeid, delvis som et følge av at jeg allerede i løpet av intervjuene gjorde meg opp tanker om hvilke teoretiske perspektiver som kunne passe inn i informantenes refleksjoner.

4.5.1 Transkribering

Å transkribere betyr å endre form, som i dette tilfellet innebærer å gå fra lyd til tekst. Transkriberingens første krav er naturligvis at man har et intervju som i en eller annen grad ble tatt opp (Brinkmann & Kvale, 2019). For å gjøre transkriberingsjobben i etterkant enklere, og ikke minst for at informantens egne refleksjoner skal gjengis så nøyaktig som mulig, ble hvert av de ti intervjuene ble tatt opp med lyd. Lydopptak ble foretrukket her for at fokuset skulle ligge på tematikken og intervjudynamikken (Brinkmann & Kvale, 2019), og siden jeg foretok fysiske intervju ville det ut fra oppgavens tematikk være lite hensiktsmessig å benytte meg av videoopptak i samme slengen.

De ti intervjuene ble foretatt over tre dager i februar 2023. Som en konsekvens av at intervjuene befant seg så tett på hverandre valgte jeg å begynne selve transkriberingsjobben dagen etter at jeg hadde foretatt det siste intervjuet, men også for at informantene ikke skulle bli distrahert av at jeg skrev samtidig som at de svarte på intervjuspørsmålene. Siden intervjuene i gjennomsnitt varte i 40-45 minutter gikk transkriberingen relativt fort. For å likevel kunne transkribere så nøyaktig som mulig, samtidig som å opprettholde en viss grad av effektivitet, ble lydopptakets lengde fordoblet. Det vil si at dersom et opptak hadde en lengde på 45 minutter, ville den fordoblede versjonen ha en lengde på 90 minutter. På den måten kunne jeg transkribere fortløpende uten å måtte gå tilbake i opptaket dersom det var noe jeg ikke fikk med meg. I transkriberingen og analysen har jeg tatt med muntlige preg som «...», «ehh» og «ehm» for å illustrere at dette betyr pause eller at informanten tenker seg om før han/hun svarer, men også for å gi en så rett fremstilling av sitatene som mulig i analysen. For min del utgjorde transkriberingsjobben den første delen av selve analysearbeidet. Allerede her kunne jeg se en

viss grad av sammenheng mellom intervjuene og den gjennomgående tematikken over samtlige intervjuer, som til syvende og sist gjorde kodejobben enklere.

4.5.2 Koding

Koding innebærer at et tekstsegment forbindes med en eller flere kodeord eller setninger, med formålet om at man lett kan identifisere det som ble sagt ut fra denne koden (Brinkmann & Kvale, 2019). Kodene kan basere seg på konseptdrevne eller empirinære koder. Konseptdrevne koder er koder etablert i forkant av forskeren, gjerne hentet fra eksisterende litteratur om tematikken. På den andre siden vil empirinære koder si at forskeren ikke starter med koder i forkant, men at kodene etableres ved analysering av primærdataen (Brinkmann & Kvale, 2019).

Kodearbeidet ble foretatt i det kvalitative analyseverktøyet Nvivo 20. For min del ble kodingen den andre delen av analysearbeidet og skjedde så fort jeg ble ferdig med transkriberingen. I bearbeidingen av egen intervjudata ble kodearbeidet fordelt på to deler, og den første delen dreide seg om å få en generell oversikt over de 450 kodene jeg etablerte fra den transkriberte intervjudataen, koder som var både konseptdrevne og empirinære. En stor del av denne perioden gikk i å dele de mest relevante kodene inn i overordnede kategorier som tar form av hendelsesforløpet til cyberangrepet – før, under og etter – og koder som går innenfor øvrig refleksjon. Den andre delen gikk i å etablere mer tema-rettede kategorier for hver tidsperiode, og hvilken tematikk som ble nevnt i intervjuene. Etter denne jobben endte jeg opp med 12 kategorier som oppsummerer hovedlinjene i empirien, i tillegg til syv kodegrupper under øvrig refleksjon. Store deler av analysekapittelet tar utgangspunkt i tabell 3, men siden flere av kodegruppene samsvarer med hverandre er underkapitlene noe bearbeidet.

	Hendelsesforløpet			
	Før	**Under**	**Etter**	**Refleksjoner**
Koder	Basisopplæring Bevisstgjøring	Ansvarsfordeling Åpenhet Belastning Informasjonsflyt Manuell drift Møtevirksomhet Oppbemanning	Bevisstgjøring Tiltaksintensivering Læring	Ansvarsområde Cyberdefinisjon Risikoforståelse Sårbarhet Sikkerhetsarbeid Teknologiavhengig Tillit

Tabell 3. Koder.

4.6 Kvalitetskriterier

I det nest siste kapitlet diskuterer jeg sentrale kvalitetskriterier opp mot tematikken og eventuelle implikasjoner rundt egen posisjon og det feltet jeg har forsket på. I kvalitative metoder er det spesielt to kriterier som bør diskuteres. Hvorvidt det er mulig å oppnå total *validitet*, *reliabilitet* og *overførbarhet* er ikke hensikten med dette kapitlet. Kapitlet har heller som hensikt å informere om valg som er gjort enn en ren konstatering.

4.6.1 Validitet

Validitet, også kjent som *gyldighet*, dreier seg om de svarene vi får oppgitt faktisk er svar på det vi er ute etter. En avhandlings validitet vil samtidig dreie seg om funnene samsvarer med forskerens og informantens ståsted (Creswell & Creswell, 2018, s. 199). Validitet kan styrkes ved at man tydeliggjør de valgene man tar – enten dette måtte være valg av teori og hvordan den anvendes, men også valg av metode og hvordan den brukes. Dette innebærer at man lar leseren selv være kritisk til forskningsopplegget, og hvorvidt den er anvendbar i egen forskning (Tjora, 2018, s. 234). Som nevnt tidligere gikk jeg i begynnelsen av forskningsperioden bredt ut i teorien, som også resulterte i en åpen problemstilling, for å etablere en grunnleggende innsikt i feltet. Dette ble også gjort for at empirien i seg selv kunne bestemme hvilken teori som ble mest hensiktsmessig for å belyse tematikken i etterkant. Herunder argumenterer jeg for at teorien er godt egnet for å belyse både problemstilling og tema. En annen ting som er verdt å nevne er at datamaterialet mitt kun består av ett utvalg fra én virksomhet, og hvorvidt resultatene fra denne avhandlingen kan overføres til en annen kontekst bør leseren selv vurdere. Man kan naturligvis argumentere for at intervjudataen kan suppleres med observasjon i tillegg for å se hvordan ting er i praksis (jf. Atkinson, 2015). Som et følge av fenomenologien og en case som skjedde for fire år siden mener jeg likevel at intervjuene har nok fruktbarhet i analysen. Her har jeg tatt utgangspunkt i å skape gyldighet ved å forklare hvordan jeg har gått frem i feltet, valgt teori og metode, og ikke minst mitt eget ståsted, for at leseren selv kan gjøre en vurdering om hvor anvendbart funnene er i en annen kontekst.

4.6.2 Reliabilitet

Reliabilitet, også kjent som *pålitelighet*, dreier seg om å dokumentere stegene i forskningsprosessen så godt som mulig, slik at andre i ettertid kan følge prosessen (Creswell & Creswell, 2018, s. 201). Med andre ord vil dette si om resultatene i avhandlingen kan legge til

grunn for at andre kan reprodusere de samme eller tilsvarende resultater i eget forskningsopplegg. Avhandlingens reliabilitet kan styrkes ved at man reflekterer over det som er til felles mellom forskeren og informantene, forutinntattheter og kunnskap om tematikken i forkant av intervjuene (Tjora, 2018, s. 235-236). Som det har blitt diskutert tidligere kan forkunnskap peile datagenereringen i én spesifikk retning, men også hvordan man velger å analysere funnene i etterkant. Som jeg har nevnt en rekke ganger har jeg god kjennskap til Hydro som bedrift, noe som kan være et sentralt element i hvordan jeg har analysert. Min interesse for cyberkriminalitet kan også peile teorien i en spesifikk retning. Tematikken jeg har valgt kan likevel gjøre det krevende å produsere de samme eller tilnærmede resultater ettersom at cyberkriminalitet som fenomen endrer seg mye for hvert år.

4.6.3 Overførbarhet

Når man snakker om overførbarhet og generalisering snakker man om ofte om de tre formene *naturalistisk*, *moderat* og *konseptuell* generalisering (Tjora, 2018). Valg av form forutsetter hva formålene med forskningen er, men rent overordnet er generalisering argumentet om at et fenomen i et spesifikt tid-og-rom også skjer en annen plass eller tidspunkt (Payne & Williams, 2005, s. 296). Hensikten med naturalistisk generalisering er å redegjøre godt nok for de valgene som er tatt for at leseren selv kan bedømme om funnene har gyldighet i egen forskning (Tjora, 2018, s. 239). I moderat generalisering beskriver forskeren selv hvilke situasjoner resultatene er gyldige (Tjora, 2018, s. 239). Foretar man konseptuell generalisering etablerer man konsepter eller teorier som kan overføres i andre casestudier enn det som er studert (Tjora, 2018, s. 239). Målet i kvalitativ forskning er likevel én form for overførbarhet. Som det til en viss grad kommer frem i kapittel 4.6.1 mener jeg at det er mest hensiktsmessig at leseren selv bedømmer om funnene har gyldighet i en annen case. Siden forskningen tar utgangspunkt i ti intervjuer og en organisasjonskontekst som ikke nødvendigvis er tilfelle i andre norske virksomheter, vil ikke dette åpne opp for at funnene automatisk kan overføres i andre kontekster. Jeg går heller ut fra antagelsen om at funnene *kan* være gjeldende i lignende settinger.

4.7 Etikk

Før et forskningsprosjekt kan begynne er det en rekke etiske betraktninger som bør etterstrebes for at forskningen ikke kommer til skade for de involverte. Etiske betraktninger kan være spørsmål om hvordan personvernet ivaretas og beskyttes, og hvor godt beskrevet prosjektet er for informantene i forkant av intervjuene. 19. oktober 2022 godkjente Personverntjenester

(Sikt) prosjektet og de vurderte at databehandlingen er lovlig dersom behandlingen følger det som står beskrevet i meldeskjemaet (jf. Vedlegg 1).

4.7.1 Personvern

I løpet av hele forskningsopplegget har det vært viktig å opprettholde og ivareta informantenes personvern etter etiske retningslinjer. Før jeg begynte med selve datainnsamlingen ble prosjektets formål, intervju og informasjonsskriv vurdert av Sikt, og opplegget måtte godkjennes før innsamlingen kunne starte. Anonymisering er et av de viktigste tiltakene man kan gjøre for å sikre informantenes personvern. Etter at samtlige intervjuer ble foretatt ble alle personidentifiserende kjennetegn erstattet med en koblingsnøkkel som lå fysisk adskilt fra øvrige data, og etter at jeg hadde fullført transkriberingsjobben ble alle lydopptak slettet forløpende. For ordens skyld fikk også samtlige informanter tildelt et tilfeldig dekknavn som ikke har noen tilknytning til personidentifiserbare data. Navnene ble kun opprettet for å enklere kunne følge gangen i analysen enn hva det hadde vært ved bruk av flersifrede koder. For å anonymisere ytterligere slik at informantene ikke kjenner seg igjen i analysen, også som et følge av en ujevn kjønnsbalanse i utvalget, er noen av informantene tilfeldig kjønnsvridd.

4.7.2 Informert samtykke

I vedlegg 2 kan man se informasjonsskrivet jeg sendte ut før intervjuene ble foretatt. Informasjonsskrivet har som formål å informere aktuelle kandidater om studiets formål, hvem som har tilgang til materialet, konsekvenser for deltakelse, og hvilke rettigheter kandidatene har i løpet av hele forskningsperioden. Informasjonsskrivet har også kontaktinformasjonen til meg, min veileder og NTNUs personvernombud dersom informantene hadde behov innsyn i hvordan datamaterialet ble brukt. Det informerte samtykket ble gitt etter at informantene hadde lest igjennom informasjonsskrivet, og intervjuet ble ikke startet før informantene hadde gitt et skriftlig samtykke med underskrift. Signerte samtykkeskriv ble deretter oppbevart i en perm som kun jeg har tilgang til, og fysisk adskilt fra lydopptak og transkriberinger.

5. Analyse

I kommende kapitler presenterer jeg og analyserer de fortellingene som kom frem i løpet av intervjuene. Datamaterialet består av ti intervjuer fra informanter med forskjellige stillinger og ansvarsområder i den virksomheten jeg har foretatt intervjuene i. Aller først presenterer jeg hendelsesforløpet til angrepet i kapittel 5.1 uten noen særlig teoretisk tilknytning for å få frem hvordan virusangrepet ble lagt merke til og hvordan de ansatte responderte på hendelsen. I påfølgende kapitler går jeg dypere inn i informantenes refleksjoner og tanker for hvordan cyberangrepet ble håndtert. Analysen er i all hovedsak styrt empirisk, men i form av den abduktive tilnærmingen spiller teori og tidligere forskning en rolle i noen grad.

5.1 Cyberangrepet

> Ivar: [...] før angrepet var det gjort noen kartlegginger med hensyn til ... det var året før ... 2018 ... både her lokalt og ellers andre plasser i konsernet ... der det ble initiert kartlegginger for hvordan tilstanden var, da, med Accenture tror jeg ... eller et annet eksternt konsulentselskap. Der kom det en rapport med anbefalinger og tiltak. Så den rapporten kom vel på januar og februar det samme året, men vi hadde jo ikke kommet i gang med det før angrepet kom [...]

I 2019 ble Norsk Hydro angrepet av et omfattende løsepengevirus, men allerede på tampen av året før var et norsk konsulentselskap på besøk for å avdekke eventuelle svakheter i systemene deres. Informanten Ivar forteller at rapporten konsernet fikk inneholdte en rekke anbefalinger og tiltak konsernet kunne gjøre for å forsterke eventuelle svake ledd, både sentralt og lokalt ute i fabrikkene. Rapporten ble overlevert tidlig på nyåret, men konsernet rakk likevel ikke å iverksette tiltakene før et cyberangrep ble utløst. Angrepet skjedde tidlig morgen norsk tid, og informanten Ole ble oppringt av sin nærmeste leder:

> Ole: Jeg husker jeg våknet ... før jeg ... før vekkerklokka ringte, for da ringte sjefen min den gangen og sa at han var litt usikker, men sa det var cyberangrep og sa at vi hadde blitt angrepet. Så var vi litt sånn ... på det tidspunktet visste ingen 100% hva som hadde skjedd ... var det øvelse eller var det reelt ... jeg var jo drittrøtt og han hadde sikkert akkurat våknet, men vi konkluderte begge to om å dra på jobb med en gang.

Bjørnar: Mhm.

Ole: Så det vare bare opp og ut i bilen og komme seg på jobb. Da vi kom dit skjønte vi at ... det er ikke øvelse og det er reelt. Da var det jo trøbbel ute i produksjonsavdelingen i forhold til ... det som jeg husker spesielt godt var at vi har noen instrumenter som analyserer metallprøvene ... kjemisk analyse ... der var det ... husker ikke om skjermen var blå, men der var det rett og slett en beskjed om at dersom vi rører noe her så låser de PCen og de skal ha penger. Det var den eneste ... vi hadde to slike PCer. Det var heldigvis kun de to PCene de hadde kommet lengst med som de klarte å låse og der det hadde kommet krav om betaling, og dersom vi gjorde noe så slettet de alle filene og låste PCen.

Ole visste ikke om det var øvelse eller en reell hendelse da han ble oppringt av sin leder, men fant raskt ut at det var en realitet da han ankom jobben tidlig den morgenen. For de fleste informantene ble det derimot gitt beskjed i portvakten eller da de hadde ankommet kontoret den morgenen. En av dem var informanten Atle. Han fikk beskjed tidlig om morgenen at den lokale datavakten hadde lagt merke til uregelmessig aktivitet på systemet.

Atle: [...] jeg fikk jo beskjed tidlig på morgenen da jeg kom på jobb. Det var jo lokal datavakt som da hadde merket at det var noen ulumskheter som foregikk. I løpet av natten så hadde de også koblet ut WAN-linken vår ut fra det store internett, da, slik at det ikke skulle spre seg mer. Det som jeg var opptatt av var om det her var noe som en orm som reiste rundt på innsiden, og da ville det jo ikke hjelpe å trekke ut noe som helst. Så det som møtte meg ... da jeg kom på jobb var det litt kaos da. Det første jeg fikk melding om er vel spectroanalysen, for den ville ikke starte opp. Så det var det første vi fikk se av det da.

I begynnelsen var også Atle usikker på hva som hadde skjedd i løpet av natten, og trodde det hele skyldtes datafeil:

Atle: [...] det som skjedde da var at vi trodde jo først at det kanskje var en feil på en PC da, så vi var nede og hentet den PCen ...

Bjørnar: Åja!

> Atle: Så det som skjedde da var at ... i en PC har du noen remedier som sier hvordan den skal bootes opp, den filen var tydeligvis ødelagt da, for det sa PCen også da vi prøvde å boote den «den her filen kan ikke bootes på» ... vi er nysgjerrige av natur da, så det vi gjorde var å ta en PC ... en lik PC ... kopierte bootfilen og la den inn på den ødelagte PCen ... så da startet den, men det som var ganske artig å se ... da vi gikk inn i katalogen begynte den å kryptere den etterhvert som vi var der. Først da begynte vi å skjønne hvilket omfang det her var. Da visste vi kanskje et par ting ... jeg visste at det var en mekanisme på PCen som begynte å kryptere, noe startet på den av en eller annen grunn, og når den fikk gjort jobben sin så krypterte den alt som var ... og det var ikke mulig å få det tilbake uten backup.

Det var likevel ikke før de begynte med feilsøking de skjønte at et løsepengevirus hadde blitt utløst på kontornettet, og som en respons måtte fabrikken iverksette strakstiltak for at viruset ikke skulle spre seg lengre ut i systemet. Siden nesten alle former for internett- og systemtilgang behøver strømtilførsel, er det enkleste og viktigste tiltaket en enkeltperson kan gjøre i slike hendelser å fjerne støpselet fra stikkontakten:

> Johanne: Alt ble jo slått av. Det var liksom det første og viktigste. Det var liksom ... «OFF». Det var rett av med bryteren. Tror alle telefonene ringte konstant på alle avdelingene. Det var ikke så masse forklaring. Det vare bare å nappe ut alt av strømtilførsel og ... få det av. Ehm ... så vidt jeg husker og fikk fortalt at det skulle plugges ut og ikke igjen før du fikk beskjed. Haha. Så noe mer ... du bare visste at de jobbet mot deg og at det var cyberangrep og snakk om et pressmiddel som de krevde at Hydro betalte.

Som Johanne, og øvrige informanter forklarer, var fjerning av strømtilførsel det viktigste strakstiltaket man kunne gjøre selv, men som en konsekvens måtte arbeidsutførelsen bestå av alternative arbeidsmetoder.

> Kari: [...] så vi klødde oss litt i hodet der da. Hahaha. Ehm, ja, så det kom meldinger som på en måte ikke var godt beskrevet ... «hvordan løse det» da, i praksis. Så skrudde de av Wifi-nettet en periode, så måtte vi finne alternative måter og jobbe på da.

På en eller annen måte måtte de ansatte uansett få tilgang til prosedyrene som befant seg på nettet, og måtte finne en løsning som gjorde internettilgang mulig uten at dette gjorde ytterligere

skader på selve kontornettet. Som informanten Kari og andre informanter forklarer var løsningen i lomma og konsernet sendte ut en melding om at det gikk fint å komme seg på nettet så lenge et mobilt hot-spot ble brukt, som vil si at man kobler seg på nett med mobilnettet.

> Kari: Husker ikke om vi måtte koble oss opp til nettet i veggen, eller om vi bare kunne bruke Wifi ... Jo! Vi måtte koble oss opp på mobil-wifi! For da var det ... «hvordan lære seg å koble opp via mobil-wifi» var det som var løsningen, siden de skrudde av nettet, men mobilen var sikker. Så det ble en slik variant en stund.

Samtidig som at viruset hadde gjort sin inntreden måtte konsernet finne ut av hvordan dette skulle behandles utad. I denne casen valgte konsernet å gå ut offentlig.

> Karl: Gikk ut og var veldig åpne. Slik jeg forsto det fra mitt ståsted involverte de de riktige myndighetene raskt, og var tidlig ute med å si at det her sannsynligvis var en ransomware-sak, og sa at det ikke var aktuelt. Var heller villige til å ta den støyten.
>
> *
>
> Atle: De var ganske tidlig ute med det, og de hadde ingen intensjoner om å betale de løsepengene for å få tilbake filene. Det er jo et ganske sterkt signal å gi, da, og et viktig signal! [...] det må jeg si ... Sjefen som også gikk ut i media og fortalte om det her da. Han gjorde en god figur. Veldig god figur.

Høsten 2021 deltok Kripos på en internasjonal etterforskning mot organiserte digitale kriminelle i Ukraina. Som et følge av etterforskningen ble det i flere norske aviser (NTB, 2022) meldt den 16. september 2022 at konsernets krypteringsnøkler ble funnet, som betyr at filene som ble låst under angrepet nå kunne låses opp igjen.

5.2 Før angrepet

Som hendelsesforløpet viser var Hydro kjent med at cyberkriminalitet som fenomen fantes før de senere ble angrepet i 2019, gjerne i form av den rapporten fabrikkene fikk tildelt etter at Accenture hadde vært på besøk. Intervjuene viser også at det på andre områder hadde skjedd et bevisstgjøringsarbeid i forkant av angrepet, men at selve basisopplæringen alle ansatte må igjennom ble særlig relevant for hvordan angrepet i sin helhet ble håndtert på operatørnivå.

5.2.1 Bevisstgjøring

Informantene oppgir at konsernet var godt kjent med og bevisst over en del cybertrusler som løsepengevirusangrep. Før angrepet fant sted oppgir nesten samtlige informanter at det i forkant av angrepet hadde blitt gitt noe kursing på området i varierende grad. Alle informantene erkjente at cyberangrep var noe som kunne skje, og bekrefter at konsernet var godt bevisst på trusselen. Flere av informantene rapporterer derimot at kursingen og selve bevisstgjøringsjobben av de ansatte i forkant var spesielt lav. Informanten Ivar forteller at det var kun noen forenklede versjoner av den opplæringen som blir gitt i dag. Til tross for at andelen av kurs var forholdsvis lav i forkant, hadde de likevel ikke mulighet til å gjøre noe i egen regi, og at kursingen ble gitt fra sentralt hold:

> Ivar: Det var vel noen forenklede versjoner av det som er i dag ... av cyber awareness og sånt ... kampanjer. Jeg husker nesten ikke selv. Det var fire år siden. Men det var ... det var nok ikke noe spesielt det egentlig. Oss lokalt fulgte det som kom ovenfra egentlig. Vi oppfant ikke noe selv, og hadde ikke kapasitet til å begynne og forske og sette oss inn i det.

Ivar er dog ikke alene om tanken at kursingen før 2019 var mye mer forenklet enn hva som finnes av e-læringskurs i dag, og Karl mener samtidig at virksomheten var bevisste på at et cyberangrep kunne skje:

> Karl: Mener at vi kun var bevisst på det i forkant. Ehm, mener og husker ... små kurs gjennom One som går på enkle ting som phishing, bevisstgjøring rundt det at vi kan være hjelpemiddel dersom folk ønsker inn. Vi er jo fullt ... vi var ikke naive i forhold til det, men var vi bevisst nok? Sannsynligvis ikke.

Som informanten Karl forklarer var ikke konsernet naive rundt tematikken. I forkant av angrepet viser dette til en viss grad av proaktivitet blant de ansatte, men spesielt fra konsernet som var godt kjent med problematikken. Til tross for at bevisstgjøringen i forkant av angrepet var forholdsvis lav, var det flere av informantene som pekte på basisopplæringen sin som en viktig del av håndteringen av det.

5.2.2 Basisopplæring

En fellesnevner i flere av intervjuene er at kursingen og opplæringen i forkant var nokså lav i forhold til hva nivået har vært i etterkant av angrepet. Til tross for dette sikter flertallet av informantene i en eller annen grad til basisopplæringen de får som en del av konsernets «Standard Operating Procedures» (SOP). «SOPene» gir de ansatte klare og spesifiserte retningslinjer og instrukser for hvordan en arbeidsoppgave skal utføres, og ikke minst hvordan disse skal utføres for at arbeidet ikke kommer til skade for seg selv, andre eller materiell. En informant trekker eksempelvis frem bedriftsprosedyrene som styrende dokumenter som befinner seg på flere ulike områder i bedriften, og forteller blant annet hvordan man skal forholde seg til teknologi og bruk av internett i det daglige:

> Ivar: [...] vi følger jo det de ... «corporate procedures» som gjelder innenfor konsernet da.
>
> Bjørnar: Men er det da spesifikt internt fra virksomheten eller ...
>
> Ivar: Ja, det er jo globale prosedyrer som ligger på konsernnivå, ikke sant ... styrende dokumenter innen virksomheten. Både innenfor IT og andre områder, da. Det er jo et sett med sånne governance-dokumenter ... og det er blant annet innen IT, som er styringsdokumenter, som hver enkelt fabrikk og enhet må forholde seg til da, etter beste nevne, ikke sant. Så det er jo det som fantes da.

Ulrik forteller også at:

> Ulrik: Tror til dels så hadde de noen rutiner rundt det, men de var ikke så veldig gode, tror jeg. Men for vår del var det ... vi håndterte det ganske greit med den kjennskapen og de rutinene med ... ja ... kjennskapen vi hadde til rutinene våre. Det med APICS ... det styrer alle operasjoner som vi gjør, men det er ... vi håndterte det ganske greit.

Som Ivar og Ulrik forteller var det kun bedriftsprosedyrer og rutiner som var på plass før angrepet. En spesifikk prosedyre flere av informantene trekker frem er for eksempel bruken av eksterne «stikker» (minnepinne) og at det under ingen omstendigheter er lov til å bruke ekstern minnepinne på noen av fabrikkens datamaskiner. Dette som et følge av at ansatte og besøkende i bedriften kan benytte seg av en minnepinne som infiseres av virus, men likedan kan et virus inne på minnepinnen få tilgang til datamaskinen. Innenfor cybersikkerhetslandskapet snakker

man her om å minimere innsidetrusselen, enten denne trusselen dreier seg om direkte eller indirekte handlinger. Å ha etablerte prosedyrer viser til den tredje faktoren for hva som kan kalles en HRO (Boin & van Eeten, 2013). Det finnes likevel ikke spesifikke prosedyrer for hva man skal gjøre under et cyberangrep, og i intervjuene får man inntrykk av at en god del av håndteringen før og under angrepet baserte seg på de erfaringene og rutinene man har fra andre avvikssituasjoner som har skjedd tidligere. Disse erfaringene, som det påpekes fra en av informantene, gjør at de ansatte er tilpasningsdyktige:

> Karl: En ting vi er gode på er nødprosedyrer. Vi har vel ikke en direkte nødprosedyre på cybersikkerhet som er på vårt nivå, men ligger vel et annet sted som kommer frem den dagen det skal skje. Vi er generelt gode på prosedyreverk, gode på nødprosedyrer som også er tilgjengelige for alle ... alle er inne og leser, alle kvitterer på at vi har lest og til en viss grad forstått ... det er elementer i de prosedyrene ... om det ikke er den ... ikke har en spesifikk prosedyre for den spesifikke hendelsen, ligger det flere prosedyrer vi enkelt kan adoptere i de fleste avvik.

Karl forteller her om bruken av nødprosedyrer og at det ikke finnes, ut fra det han vet, en spesifikk prosedyre for cyberangrep dersom en slik hendelse skulle skje. Selv om informanten her ikke kunne sikte til en spesifikk prosedyre for cyberangrep, har likevel fabrikken en rekke nødprosedyrer som kan adopteres inn i andre avvikssituasjoner. I resilienslitteraturen snakker man ofte om evnen til å tilpasse seg når noe uforutsett har skjedd, og de avvikssituasjonene Karl beskriver her er en type resiliens der etablerte rutiner og prosedyrer er mangelfulle, men at man «låner» rutiner fra andre prosedyrer (Engen et al., 2016, s. 153). Dette kan peke på en type *improvisasjon* og *bricolage*, der man handler ut fra det man har på hånden (Harper, 1987, sitert i Engen et al., 2016, s. 318; Weick, 1993). I situasjoner der man har manglende kunnskap, peker også Bruner (1983, sitert i Engen et al., 2016) på *kreativitet* som en viktig faktor, som handler om en nytenkning der man bruker det man allerede vet.

5.2.3 Oppsummering

Som både hendelsesforløpet i kapittel 5.1 og mer spesifikt perioden før angrepet i kapittel 5.2 til 5.2.2 viser, hadde Hydro fått besøk av et konsulentselskap som skulle avdekke eventuelle mangler og svake ledd, med hensikt om å være mer forut dersom det skulle skje noe. Likevel satte de ikke i gang tiltakene før et angrep skjedde noen måneder etter. Tiden før angrepet var likevel preget av noe bevisstgjøring blant informantene – noe forenklet enn det som finnes av

kursing og kampanjer i dag. Flere av informantene peker på basisopplæringen og rutineverket som et sentral håndteringsverktøy, til tross for at det ikke finnes noen spesifikke prosedyrer på cyberhendelser. Fra tiden før angrepet gir dette den ikke-tekniske faktoren «evnen til å antesipere». Til tross for at opplæring og bevisstgjøringen var noe lavt krever likevel antesipering kjennskap til andre avvikssituasjoner og evnen til å lære fra de rette erfaringene (som illustrert i tabell 1), som også relaterer seg til de faktorene som gjorde seg gjeldende under angrepet.

5.3 Under angrepet

Tiden før angrepet var preget av noe kursing og bevisstgjøring. Informantene pekte også på basisopplæringen som en essensiell dimensjon for hvordan cyberangrepet i ettertid ble håndtert. Selv om det ikke finnes noen nødprosedyre for cyberangrep, er det flere av nødprosedyrene som kan adopteres inn i avvikssituasjoner med manglende kunnskap. Følgende tidsperiode i forhold til hendelsesforløpet dreier seg i stor grad om hvordan cyberangrepet ble håndtert, og hvordan informantene reflekterte over denne håndteringen. I følgende kapittel er det fire sentrale temaer som kommer frem i løpet av intervjuene: *høy grad av manuelt arbeid*; *«det er bare en forenkling av arbeidsdagen»*; *drift innenfor egne rammer*; og *desentralisert kompetanse og åpenhet*

5.3.1 Høy grad av manuelt arbeid

I Hydro-konsernet sirkulerer en rekke arbeidsoppgaver med høyavansert teknologi, både på prosess- og kontornivå. Nesten samtlige av de informantene som deltok i intervju var samstemte om at arbeidsdagen krevde en viss grad av tilpasning som et følge av angrepet, men naturligvis varierende ut fra hvilken stilling hver enkelt informant har. En av de som derimot forteller at han ble lite berørt av angrepet var informanten Magnus:

> Magnus: Eh ... hadde vel ikke noe stort forhold til det sånt sett, da. Det var jo ... altså ... prosessnettet gikk jo som normalt det, og det som kanskje ... det var jo det private [kontornettet] vi ikke kom oss inn på. Det var der problemet ... men er jo ikke så avhengig av det i min jobb i forhold til lederne. Så det påvirket ikke min dag ... sånt sett. Var egentlig ikke ... prosessnettet var ikke berørt.

Magnus forteller at arbeidet i liten grad ble berørt av cyberangrepet og at arbeidsdagen stort sett retter seg mot prosessnettet, som var adskilt fra øvrige nettverk. For fleste andre informanter ble derimot teknologien satt på vent under angrepet, og graden av manuelt arbeid ble større.

> Ulrik: Husker at det var ... vi hadde jo i drift i elektrolysen en rekke møtevirksomheter der vi punktvis satt opp hva vi måtte gjøre for å håndtere det her da ... manuelt og at vi erstatter APICS med manuelle rutiner. Oppretter da noen regneark og en del av den kommunikasjonen som før gikk gjennom nettverket måtte vi ha manuelt. Men jeg husker da ikke ... nei skal ikke påstå alt som skjedde i detalj den dagen. Hehehe. Men som sagt så husker jeg at vi fikk strukturert den manuelle håndteringen. Det var vel det vi holdt på med den dagen.

Som det blir fortalt dreide de første timene og den første dagen seg om å erstatte APICS, produksjonssystemet i Hydro, med manuelle rutiner. Systemet styrer produksjonsprosessene og dekker mer generelt datainnsamling, overvåking og kvalitetskontroll i elektrolysen, støperiet og produksjonen av anoder. Med andre ord kan APICS gi føringer for hvilke elektrolyseovner som skal ha et anodebytte, samt gi et bilde over ovner som «blusser».[3] Som en av informantene nevner senere er det ikke bare å slå av strømbryteren ved avvik, og de manuelle rutinene dreide seg i all hovedsak om å gjøre de arbeidsplanene som før gikk automatisk på produksjonssystemet manuelle, samt holde produksjonen av metall i gang til tross for krisesituasjonen. For flere av informantene betydde det manuelle arbeidet å gå «back to basic» og at man regner på «gammelmåten». Minst like viktig var jobben med å finne personen(e) som kunne gjøre gammelmåten.

> Kari: Fokuset var hva vi måtte ha for å opprettholde driften her og nå, papirblokker slik at vi fikk regne på gammelmåten, og ikke minst finne den personen som faktisk kan det, da. Komme på hvordan vi gjorde det før, så det var mere slike diskusjoner, for vi visste jo ikke om det var ... om vi var uten lenge eller om det var kort.

Som det ble nevnt tidligere er improvisasjon, det man har for hånden og det man allerede vet en viktig faktor for hvordan en krisesituasjon kan håndteres etter beste evne. I denne situasjonen ble papirblokker og regning på gammelmåten en slik improvisasjon, men denne

[3] Når ovnen får for lite tilførsel av aluminiumoksid.

improvisasjonen er samtidig en erfaring de fleste ansatte fortsatt besitter. Når driften blir mer manuell er tilpasningsdyktighet også en viktig egenskap å ha, noe informanten Johanne mener ble en viktig faktor for hvordan cyberangrepet ble håndtert:

> Johanne: [...] Så etter noen uker ble det ... du tilpasser deg, da. Det er ikke noe nytt. Vi har driftet anlegget uten noe særlig teknologi før. Det var penn og papir og enkle systemer som overvåker. Det var litt sånn back to basic, da. Ganske mange av oss som jobber her har jobbet her i ganske mange år. For 23 år siden var det jo kommet ... det var jo ikke noe særlig til internett, og teknologien hadde jo ikke kommet så langt som i dag. Det var MYE mer manuelt. Nå er det jo masse mer sårbart i forholdt til alt.

Johanne legger også til at:

> [...] vi hadde en viss oversikt, men det var mye som var litt ... det er mange arbeidsoppgaver du vet sånn circa hvor langt du skal jobbe før du avslutter og før det neste skiftet kommer og avløser deg. Så det gikk litt på den de første dagene. Men vi har mange fantastisk gode ingeniører og fagledere som satte opp et system ganske fort. Vi fikk ganske grei kontroll på arbeidsdagen etter hvert.

Å ha tillit til at andre besitter kunnskap om hvordan driften var tidligere er en viktig forutsetning for å holde produksjonen i live under krisesituasjoner, og minst like viktig er samarbeidet mellom de ansatte når man må finne de personene som kan «gammelmåten». Som det ble nevnt tidligere forteller APICS hvor mange elektrolyseovner som skal «trekkes»[4] i løpet av en arbeidsdag, men de ansatte vet likevel hvor langt man jobber før det neste skiftet kommer. Steen et al. (2021) anvender begrepet «samhandling» i en casestudie av et COVID19-utbrudd på oljeplattformen West Phoenix i Nordsjøen. De ser på samhandling som en viktig faktor i den overordnede kriseresponsen på plattformen, og finner at responsprosessen i sin helhet baserte seg på et interdisiplinært samarbeid da det ble kjent at en ansatt hadde testet positivt for viruset. Siden det involverte personellet kjente hverandre fra før gjennom felles treningsaktivitet, finner de likeledes at kommunikasjonsflyten mellom dem ble forsterket (Steen et al., 2021, s. 265). Felles treningsaktivitet er viktig her fordi dette kan bety at samtlige av de ansatte befinner seg på samme bølgelengde for å muliggjøre samarbeid.

[4] Anodebytte på elektrolyseovnene.

For å kunne utføre manuelle arbeidsrutiner betyr dette at man bør besitte en rekke erfaringer rundt driftskompetanse som går utenfor bruken av teknologiske verktøy. Til tross for en bortgang av teknologi kan erfaringene, og de rutinene man er kjent med fra tidligere, gjøre slik at driften kan holdes i gang selv under kritiske tilstander – selve grunnlaget i resiliensargumentasjonen. Selv om dette er en god egenskap å ha under diverse situasjoner, mener uansett en av informantene at dette også bør være fokus fremover for å sikre at nyansatte også får en bredere driftskompetanse, slik at driftskompetansen ikke bare ligger i bruken og håndteringen av teknologi:

> Karl: Er ganske redd for at vi har en utvikling da, på godt og vondt, der de nye arbeidstakerne som er ansatt de siste 5-6-7-8 årene kun er vant til drift med hjelp av tekniske hjelpemiddel, så ... når da ... jeg tror generasjonen min er den siste generasjonen med den typen driftskompetanse, som vi da prøver å lære opp ... nå hører jeg faktisk ut som gammelkarene på skiftet da jeg selv begynte ... hahaha ...
>
> Bjørnar: Hahaha.
>
> Karl: ... men det der trenger du virkelig, ikke sant. Sier ikke at det var bedre før, for det var det slettes ikke, men ... ehm, vi klarer ikke å optimalisere driften, men vi klare å holde den gående dersom det er tekniske duppeditter som detter ut. Det blir mye i blinde, men da må vi legge inn de gamle parameterne som vi da har relativt grei kunnskap om.

Å ha kjennskap til de manuelle rutinene gjør at produksjonen av aluminium kan fortsette selv under avvikssituasjoner og bortfall av teknologi. Det siste sitatet viser til en lignende «organisatorisk glemsel» Broekema et al. (2017) peker på. Karl forteller at han tror hans generasjon er den siste med den typen driftskompetanse, som forsøker å lære opp de nyansatte. Problematikken ligger i hva som skjer når denne generasjonen senere pensjoneres og driftskompetansen pensjoneres med dem. Den manuelle driftskompetansen er viktig siden dette åpner opp for at fabrikken fortsatt har mulighet til å drifte anlegget, til tross for at teknologiske verktøy har falt bort. I resiliensteorien er dette sentralt siden man er avhengig av å kunne tilpasse seg under hendelsen også (Hollnagel, 2013). Et spørsmål jeg tidlig var interessert i å få undersøkt var hvor belastende den økte manuelle driften var på informantene, og hvilke konsekvenser som ble betydningsfulle ved bortgangen av teknologi under angrepet.

5.3.2 «Det er bare en forenkling av arbeidsdagen»

I kapittel 5.3.1 trakk jeg frem et sitat fra intervjuet sammen med informanten Johanne som fortalte hvordan hverdagen gikk «back to basic» da arbeidsdagen i høyere grad gikk fra automatisk til manuell drift. Ovenfor forteller hun hvordan de fleste av de ansatte som fortsatt jobber der i dag har vært ansatt i flere år. Et spørsmål jeg stilte meg tidlig var hvor belastende cyberangrepet var på informantene i forhold til hvilken stilling de hadde da cyberangrepet ble utløst, og hva bortfall av teknologi ville si for arbeidsutførelse. Som et følge av at cyberangrepet for det meste berørte kontornettet, er svarene informantene oppgir naturligvis delt i to alt etter nettet informantene jobber mot. En av de som for det meste jobber på kontornettet er informanten Birgitte som uttrykte at følgene av cyberangrepet til en viss grad var belastende. I begynnelsen kjente hun ikke noe særlig til angrepet og måten hun jobbet på, men at belastningen gradvis bygde seg opp som et følge av at alle skulle ha arbeidsordrene skrevet ut på papir:

> Birgitte: Til å begynne med var det ikke det [stress]. Det var jo svart skjerm, og de la jo ut hele skiten. Så kom det en VPN-klient som de lagde til meg for å kunne logge på og ta ut arbeidsordre. Så det ... monterte ... gikk inn på et stort møterom med to printere da som jeg innlosjerte meg inn i ... og satte der med noen hjelpere som matet printerne med papir og ... det gikk så hardt de første ukene at vi tok livet av den ene printeren ... en dyr laserprinter. Da var det slik at alt ble skrevet ut på papir ... back to basic og da måtte de ha alt på papir og noterte på det og utførte og alt sånt. Så skal vi punche det inn på dataen etterpå da. Det gikk døgnet rundt de første 14 dagene altså.
>
> Bjørnar: Ja, det høres ganske stress ut!
>
> Birgitte: Ja, er tross alt 60 mann som skal ha arbeidsordre så er det mange om dagen.

For Birgitte var det likevel ikke selve angrepet som gjorde at belastningen ble større, men viser heller til arbeidsmengden som utgjorde den største påkjenningen. Sagt med andre ord kunne manuelt arbeid medføre mer arbeid enn tidligere. Den samme problematikken peker også informanten Ole på som trekker frem kritikaliteten rundt at de ikke fikk analysert planlagte metallprøver til oppgitte tider i APICS, og som opplevde at kommunikasjonen i og utenfor fabrikken ble vanskeligere som et følge av angrepet.

> Ole: Det er ganske kritisk for oss i drift da, for analyse må vi ha og de metallprøvene våre. Så det var helt låst. Så var det jo da en beskjed om å nappe ut alle ... alt av PCer fra internetten, sant ... ta ut, koble ut, WiFien var vel deaktivert tror jeg? Det tror jeg de koblet ut sentralt ... dataavdelingen shuttet ned alle connections mellom avdelingene og ... så de isolerte hver avdeling. Først ble fabrikkene isolert og isolert avdeling, så nappet vi ut alt og satt der egentlig uten noe kontakt med noen. Og da har vi plutselig ikke programmene vi trenger for å kalkulere, analysere, legere ovnene, så det ble jo stillstans på hele greia i en periode.

For både Birgitte og Ole ble det opplevd tilnærmet lik belastning i form av økende stress da angrepet skjedde. For de ble dette enten et resultat av at arbeidsordrene ikke lengre var tilgjengelig automatisk på nettet, eller for at dataen som kom inn fra produksjonssiden nå måtte behandles manuelt. Fellesnevneren blir dermed at arbeidsutførelsen ikke lengre foregikk på APICS. For andre var derimot ikke dette tilfelle, og jevnt over mente de fleste at arbeidshverdagen var tilnærmet det de var vant med fra før, eller at arbeidsdagen under angrepet ble mye roligere enn det de først hadde antatt:

> Bjørnar: Opplevde du noe kaos og stress, eller følte du at dere hadde kontroll?
>
> Ingrid: Faen meg det motsatte av stress! Hahaha.
>
> Bjørnar: Haha, såpass ja!
>
> Ingrid: Ble veldig rolig. Følte ikke det var noe kaos ... med oss der vi satt. Vi var veldig heldige sånt sett. Jeg har jo mye jeg kan gjøre der jeg ikke trenger data.

Allerede her kan man se at en god del av kritikaliteten avhenger av det ansvarsområdet man har og hadde under angrepet. En god del av det som til nå er sagt i dette kapitlet sammenfaller godt med hvordan informantene reflekterer over egen bruk og hvor avhengige de selv mener de er av den teknologien som brukes i driften. For de som for det meste jobber på prosessnettet, og som har de fleste av arbeidsoppgavene sine i driften, rapporterte flertallet lite avhengighet til teknologien som brukes i drift. Informantene forteller at det ikke er så lenge siden penn og papir ble brukt som et arbeidsverktøy i det daglige, og flere av disse informantene er fortsatt ansatte i dag. Til tross for at Hydro investerer stort i nye teknologi er det interessant at en god del av

informantene likevel beholder gamle arbeidsprosesser, et stort fortrinn ved teknologisk bortgang eller andre avvikssituasjoner. En av de som melder at hun ikke er noe særlig avhengig av teknologien er Johanne som forteller at teknologien kun er et verktøy som gjør arbeidet forenklet, og at man ikke trenger å gå så langt tilbake i tid før penn og papir ble brukt:

> Bjørnar: Vil du da si at du er avhengig av teknologien da for å gjennomføre arbeidsoppgavene dine i løpet av en arbeidsdag?
>
> Johanne: Nei.
>
> Bjørnar: Ånei? Hvorfor det?
>
> Johanne: Jeg er ikke det. Det er bare en forenkling av arbeidsdagen. Det er ikke så mange år tilbake at man brukte penn og papir på medarbeidersamtalene og satte det i perm. Nå er det bare digitalisert. Skrev forhånd alle arbeidslistene kanskje ... ja. Timeføringene husker jeg ikke hvordan var. Det var sikkert ... eh ja, vet ikke. For vi har jo vært igjennom det å ikke ha dataen oppe å gå.

Johanne mener at teknologien kun er en forenkling av arbeidsdagen og mye av den kunnskapen om hvordan driften var før sitter hun fortsatt igjen med. Dette er noe også Karl trekker frem som en sentral del for hvordan driften foregår når teknologien er borte, og mener at tilnærmet alt som kan gjøres med teknologien også kan gjøres manuelt. Ifølge han ligger dette som en del av grunnkompetansen han har tilegnet seg gjennom årene som ansatt i Hydro, men at han også har erfaring fra de fleste avvikssituasjonene man kan komme borti:

> Karl: Nå har jeg vært her såpass lenge at jeg kan utføre alle de jobbene vi gjør i dag manuelt.
>
> Bjørnar: Mhm.
>
> Karl: Det har sammenheng med at jeg har vært her såpass lenge, har vært innom de fleste avvikssituasjonene, og har den grunnkompetansen på drifting.

En av de som gjør det meste av arbeidet sitt på kontornettet, men som tilsynelatende rapporterer at hun ikke er spesielt avhengig av teknologien i det daglige, er Kari. Med bakgrunn i hennes stilling ser hun det som positivt å være uten PC dersom konsekvensen av det er å være mer ute i produksjonen:

> Kari: I tillegg til å ha ansvar for datasystemene, har vi jo ikke noe backup ... det er jo online ... så det ... der har vi ingen backup, sånn manuelt nei. Så for å få tilgang ... det er jo på data, men ellers med min rolle, med businessystemet, det er mye om hvordan vi jobber i hverdagen, så jeg kan ... da er du på en måte ute og snakker og går WOC [Walk-Observe-Communicate], deltar i møter og ... kanskje veilede der da, så om jeg mister PCen en uke hadde det vært en drøm! Hadde fått så mye utetid, og hadde jo ikke vært arbeidsløs for den del. Da hadde det vært utetid, se ting i praksis og ... ja.

Fellesnevneren mellom Johanne, Karl og Kari er at de ikke blir arbeidsløse ved en eventuell teknologisk bortgang. Bortgangen åpner snarere opp muligheten for at man kan benytte seg av grunnkompetansen i drift og mer tid til å gjøre seg synlig ute i produksjonshallene. Det mest påfallende med dette er likevel at informantene generelt sett rapporterer liten grad av teknologiavhengighet og at de gamle arbeidsprosessene fortsatt beholdes i dag. Almklov et al. (2018) ser på sårbarhet som baksiden av vellykkede teknologiske systemer ut fra infrastruktureringsbegrepet. De forteller at bruken av GPS og GPS-satellitter stadig flyter inn i nye domener, men å vite hvilke systemer som avhenger av teknologien kun gjør seg til syne ved bortfall (som et resultat av jamming eller solstorm) (Almklov et al., 2018, s. 2). Til tross for at cyberangrepet ga et bilde over egen sårbarhet i Hydro, ble likevel sårbarheten besvart med teknisk grunnkompetanse i drift. Funnet speiler også et annet funn i datamaterialet som dreier seg om hvordan informantene «bare fikk holde på».

5.3.3 Drift innenfor egne rammer

Hittil har empirien vist at angrepet resulterte i høyere grad av manuelt arbeid og at det ikke er noe problem å holde driften i live i krisesituasjoner så lenge man besitter kompetansen for det. Da angrepet gjorde sin inntreden på kontorsystemet til Hydro rapporterer flertallet av informantene at de ikke fikk noe ansvar ut over det å holde driften i gang. Informanten Birgitte påpeker at dette var noe ledelsen selv la opp til og at de «bare fikk holde på». Informanten Ivar forteller også at det var lite hjelp fra sentralt hold og at eventuelle problemer var noe de selv måtte ordne opp i lokalt. Den samme informanten påpeker samtidig at det er vanskelig å be om

kortsiktig hjelp for noe de har lokalt ansvar over. Ansvaret faller dermed på de ansatte selv og løsningen på hvordan cyberangrepet skulle løses ble håndtert lokalt. Informanten Karl forteller blant annet at handlingsansvarlige på skiftene kunne selv komme med tips, løsninger og eventuelle forslag for hvordan angrepet kunne håndteres:

> Karl: Vi som hadde litt utvidet ansvar på skiftet satte oss ned og fikk en viss orientering på situasjonen, og fikk muligheter til å komme med innspill for hvordan vi kan løse det, hva gjør vi nå, vi har en drift som er nødt til å gå ... det er ikke bare å stenge og avvente situasjonen ... ehm, vi kan ikke slå av bryteren, for da er vi ferdige. Det er jo ... til en viss grad driftskritisk det som skjer, og ingen av oss visste hva vi gikk til, men så du famler litt i blinde, men så er det en del grunnprinsipper i drift, da, for aluminium har vi jo produsert i 130 år, og den kjemiske formelen er den samme i dag som for 130 år siden. Vi vet det går å holde det i live så lenge vi har strøm, men det ... det krever en annen tankegang. Vi sørger for å holde anlegget i drift innenfor de rammene vi har, men så hadde ikke vi noen rolle utenfor det.

Produksjonen av aluminium er tidskritisk, og avhengig av å gå kontinuerlig, og det å slå av strømbryteren kan ofte føre til flere problemer ut over det problemet de forsøker å løse. Som det ble fortalt tidligere skal anodeskift skje etter oppgitte tider, og anodene kan ikke være i elektrolyseovnen lengre enn 26-30 dager før de må skiftes. Samtidig bestiller støperiet en viss mengde metall i løpet av et skift, noe «tapperne»[5] har ansvar å frakte fra elektrolysen til støperiet. For at produksjonen skal kunne fortsette uten at dette skaper noen øvrige skader på nettet, finnes det noen prinsipper som kan sikre driften så lenge det finnes noen form for strømforsyning. Dette krever likevel at de ansatte besitter en grunnkompetanse som går ut over teknologibruk, som evnen til å beherske manuelle prosedyrer. Det at lederne legger opp til at de ansatte «fikk holde på» viser til en type autonomi, men det viser også til en annen relevant faktor i håndteringen av angrepet som relaterer seg til de ansattes kompetanse.

5.3.4 Desentralisert kompetanse og åpenhet

Som det kommer frem av funnene i de foregående kapitlene hvilte en god del av håndteringen av cyberangrepet på den kompetansen de ansatte har, spesielt når det kommer til at arbeidsdagen i mye større grad ble manuell, sammenlagt med en drift som foregår innenfor

[5] Ansatte som tapper flytende metall i elektrolysen og frakter dette til støperiet – +/- 4000 kg per tur.

egne arbeidsrammer. En av informantene mener at det desentraliserte ansvarsområdet som finnes i Hydro-konsernet var det viktigste suksesskriteriet for hvorfor det gikk såpass bra i etterkant, nettopp siden kompetansen befinner seg blant de ansatte.

> Karl: Men at vi er sårbare fordi at det er mange folk. Og det ... alle har tilgang ... og den ... vårt største fortrinn er jo vår største sårbarhet. Fortrinnet er det vi har er ekstremt desentralisert, det er på operatørnivå, men det er også der sårbarheten ligger.

For Karl er det desentraliserte ansvaret det største fortrinnet, men også der den største sårbarhet befinner seg. Sårbarheten kommer til syne gjennom at det er mange ansatte som har tilgang til datasystemene, men at denne tilgangen til syvende og sist også skaper det største fortrinnet. Han eksemplifiserer dette med en hendelse ved den relativt nyopprettede fabrikken Qatulum i Qatar som opplevde strømbrudd:

> Karl: Skjønner at måten vi driver på i Norge i forhold til åpenhet og at det er transparent det vi driver med, så lenge ikke bedriftshemmeligheter og teknologisk hemmelighet kommer frem, for det er vi gode til å skjule. Så er det et suksesskriterie at vi har den [norske] modellen for det også medfører at den enkelte ansatte besitter en kompetanse som gjør oss til noe mer enn roboter, ikke sant? Når vi er i en avvikssituasjon, er vi i større stand til å løse problem. Et konkret eksempel er strømutfall. Vi hadde det ... i det anlegget i Qatar hadde de strømutfall på tre timer ... tok åtte måneder og fire-fem milliarder å få det opp igjen ... sant ... tilsvarende strømutfall her ... tre-fire måneder etterpå ... vi mistet to ovner ... vesentlig ... den eneste forskjellen mellom de to er kompetansen nedover i organisasjonen.

Sitatet viser tilnærmet like avvikssituasjoner, med to forskjellige organisasjonsstrukturer. Når informanten forteller at kompetansen er spredt ut i organisasjonen, kan dette minne om Dynes' (1993) «problemløsningsmodell» som tar utgangspunkt i kontinuitet, koordinering og samarbeid. Modellen tar utgangspunkt i at befolkning og lokalsamfunn besitter ressurser som er viktige i en akutt krisesituasjon og bidrar selv i håndteringen av den (Dynes, 1993, s. 183). På lignende måte kan dette ses i lys av hva som kjennetegner en HRO, og hvordan rollestrukturen under krisesituasjoner kan desentraliseres og team-baseres (Boin & van Eeten, 2013). Empirien viser imidlertid at organisasjonsstrukturen var til stede lenge før angrepet skjedde, siden mye av driften baserer seg på de ansattes roller og kompetanser og krevde lite

tilpasning da angrepet skjedde. Dette kan også illustreres med hvordan operatørsenteret[6] i elektrolysen er bygd opp. I stedet for at lederne befinner seg i et eget avsidesliggende administrasjonsbygg, har flere av lederne kontor i hjertet av bedriften. Et annet eksempel er også terminologien man bruker for å beskrive teamoppbyggingen. Et team kalles «tog» for å tydeliggjøre at ansvaret for å utføre rutinemessige arbeidsoppgaver ligger på de handlingsansvarlige og deres respektive operatører. Spesielt viktig blir dette når lederne oftest jobber dagtid fra mandag til fredag, og operatørene jobber på nattestid og flere 12-timer helgeskift, både formiddag og natt, i løpet av en skiftsyklus.

Under angrepet måtte konsernet også velge hvordan de skulle håndtere cyberangrepet utad – om de skulle holde kortene tett til brystet, eller om de skulle legge alle kortene på bordet. Konsernet valgte sistnevnte. Samtlige av informantene var enten positive eller meget positive for det valget som ble gjort, og mener at dette kunne statuere et eksempel og være til inspirasjon for andre bedrifter som eventuelt blir offer for diverse cyberangrep i fremtiden. Informanten Atle forteller for eksempel at konsernsjefen gjorde en god figur av å gå ut offentlig med det som hadde skjedd i løpet av natten:

> Atle: [...] så fikk vi jo litt informasjon om hvordan de ... sentralt ... ville gå ut med det for eksempel. De var ganske tidlig ute med det, og de hadde ingen intensjoner om å betale de løsepengene for å få tilbake filene. Det er jo et ganske sterkt signal å gi, da, og et viktig signal!

Å være åpen om at man har blitt angrepet av et løsepengevirus, og andre former for cyberkriminalitet, er ikke hverdagskost ifølge mørketallsundersøkelsen (NSR, 2022) fra fjoråret. I rapporten kommer det frem at kun 6% av virksomhetene som ble rammet av en eller annen cyberhendelse offentliggjorde situasjonen, og at den største andelen gikk i å involvere selskapets ledelse (NSR, 2022, s. 25). Til tross for at konsernet kunne velge å holde angrepet hemmelig, mener en annen informant at han som ansatt ikke hadde satt pris på om hendelsen hadde blitt hysjet ned.

5.3.5 Oppsummering

Under angrepet melder samtlige av informantene at manuelt arbeid ble en sentral del av arbeidshverdagen og ukene fremover. Til tross for at Hydro er sterkt digitalisert og anvender

[6] Kontorbygget til elektrolysen.

teknologi i det daglige arbeidet, viser likevel empirien at gamle arbeidsprosesser beholdes. Som spesielt nevnt av to av informantene kommer dette som et resultat av grunnkompetansen fra tiden aluminiumsproduksjonen var betydelig mer manuell. Håndteringen under angrepet hvilte i stor grad på den grunnkompetansen de ansatte besitter, men dessuten på ansattes kompetanse gjennom desentraliserte ansvarsområder. Informantene rapporterer også stor grad av positivitet rundt den offentlige håndteringen konsernet gjorde. I resiliensteorien snakker man om evnen til å tilpasse seg for å sikre at driften kan fortsette til tross for kritiske situasjoner, som illustreres i form av at driftskompetanse strekker seg lengre enn bruk av teknologi, og at teknologien til å begynne med kun forenkler arbeidsrutinene. Fra tiden under angrepet finner jeg tre ikke-tekniske faktorer: «avvikserfaring og improvisasjon», «desentralisering og organisasjonsstruktur» og «åpenhet». I resiliensforstand er også hva som skjer *etter* en hendelse like viktig som det som skjer før og under. For å være resilient etter avvikssituasjoner krever dette at man lærer fra de rette erfaringene.

5.4 Etter angrepet

Som nevnt i kapittel 5.2 var tiden før cyberangrepet preget av lite kursing, men informantene mener likevel at konsernet var bevisst på faren. Før angrepet gikk mye av strategien på de ansattes forkunnskaper og prosedyrestyring, og en del av håndteringsstrategien gikk i å adoptere nødprosedyrer inn i andre avvikssituasjoner. Funn fra intervjuene viser at nesten samtlige informanter rapporterer et større fokus på kursing og bevisstgjøringsarbeid i tiden etter angrepet og frem til i dag, og mener at konsernet tar tematikken på alvor. Mørketallsundersøkelsen fra 2022 viser at kun 18% av de norske virksomhetene som ble rammet av et cyberangrep hadde investert i opplæringsprogram for de ansatte, mens 52% av virksomhetene hadde gjort rutine- eller policyendringer etter at angrepet fant sted. I dette kapitlet trekker jeg frem bevisstgjøringsarbeidet som har skjedd og blir gjort i etterkant av angrepet.

5.4.1 Bevisstgjøringsarbeid i etterkant

Bevisstgjøringsarbeidet har, som det kommer frem i omtrent samtlige intervjuer, hatt en stigende trend siden angrepet fant sted frem til i dag. Informanten Birgitte presiserer for eksempel hvordan kursingen og bevisstgjøringsarbeidet kun ble tema etter angrepet, men at dette er noe hun forstår siden det er noe annet å erfare baksiden av et slikt angrep. Nesten samtlige informanter peker på en type «spillifisering» av bevisstgjøringsarbeidet som har foregått i ettertid av angrepet. Spillifisering vil her si bruken av spillmekanismer i ikke-spill

kontekster med et mål om å øke engasjement og motivasjon. Spillifisering kan være effektivt dersom målet er å minske informasjon som kommer på avveie, og lærer sluttbrukeren å håndtere mistenkelig aktivitet så vel som økt sikkerhetsbevissthet (Arias-Vargas et al., 2023). Ansatte får tilsendt en «falsk» e-post fra noen høyere opp i organisasjonsstrukturen, som skal rapporteres i «hoxhunt»-knappen. En annen type spillifisering som foregår skjer gjennom selve kursingen. Kursene legges opp til at man leser og svarer på noen spørsmål med svaralternativ etterpå. Svarer man feil får man «virus», men svarer man riktig får man noen stjerner i margen. Med både kursing og rapportering av mistenksomme e-poster har de ansatte mulighet for å lære samtidig som at de anvender denne kunnskapen. Flere av informantene mener at denne kursingen i ettertid har vært positiv og at de er interessert i å lære mer om feltet.

> Johanne: Det kom jo først ... først kom det noen kurs etter det her [angrepet]. Som jeg husker. Det var mange år siden, og nå det siste året har det vært masse om sikkerhet på arbeidsplass ... hva er trygt ... masse begreper jeg ikke visste hva var. Når du tar de e-læringskursene så sitter du og leser så må du svare ... så svarer du feil ... du må lese opp og opp igjen. Det er tungt stoff så du blir mye mer bevisst.

Ole forteller også at:

> Ole: [...] Hydro har jo hatt meget, som jeg synes er bra etter den hendelsen som var, så er det jo masse informasjon og kampanjer rundt det med cyber ... altså ... jevnt og trutt innom for å svare på spørsmål og caser og oppgaver for å gjøre ... bevisstgjøre seg da. Så fikk vi også den nye knappen inne i mailboksen som heter «hoxhunt» ... som en skal trykke på når det kommer noe som er helt ... som en tviler på er slik som det skal være. Det har de også utsatt oss for. Vi får en mail nå og da med litt tvilsomt innhold for å se om vi fanger de opp. Det er alltid litt trening på det. Det er jo bra.

Som både Johanne og Ole påpeker bidrar kursene med å opprettholde en viss grad av bevissthet rundt tematikken, og ser på det som bra å få en kontinuerlig påminnelse i form av e-læringskurs. Informanten Ulrik mener også at kursingen og testingen de ansatte settes ut for bidrar til å få en kontinuerlig påminnelse, men at denne påminnelsen også bidrar til at det snakkes om i organisasjonen dersom noen hadde blitt testet:

> Ulrik: Det er en kontinuerlig påminnelse. Det snakkes jo om og tror folk er ganske opptatt av det. De blir jo testet, og da vil det bli snakket om. Hørte jo at det var en gang tilbake at det var en som klarte å gå i fella, og ... og gjort noe han ikke skulle gjøre. Hørte at de [ledelsen] var ganske irritert over det. Så ... det skaper litt oppmerksomhet og bevissthet for hvordan det håndteres og hvordan man håndterer e-poster.

På både godt og vondt bidrar kursingen og de falske e-postene til at det snakkes om i organisasjonen dersom noen ble forsøkt «angrepet». Broekema et al. (2017, s. 329) mener at uformelle kommunikasjonsflater under kaos og stress bidra til tilstrekkelig kunnskapsformidling. For andre har derimot mengden av informasjon og bevisstgjøringsarbeid i etterkant av cyberangrepet vært i det meste laget og ser på mengden som «overkill»:

> Kari: Ja, vi merker det jo på de e-læringskursene. De er hyppigere og omfattende enn før ... nå var det jo en master class-sak som skulle komme der jeg skulle skjønne at jeg skulle rapportere den i «hox» [hunt], knappen øverst oppe på e-posten. Har jo ikke tid til det! Sletter det bare, blokkerer, rapporterer og kaster. Gjør det på min måte, orker ikke å spille i tillegg. Gjorde det noen gang og fikk noen stjerner, men det er liksom ... tenker ... tror det er en stor forskjell på en arbeidshverdag i Oslo på hovedkontoret, enn hva vi gjør her ute i drift. Ære være til hun som ble premiert med master class-ett eller annet ... hun hadde det sikkert gøy på jobb, hahaha. For det gikk jo over flere måneder det der, at det skulle poppe opp og rapporteres ... læring i kanten der da, men ... jeg bare sletter og blokkerer og kaster ut alt jeg ikke kjenner til. Hahahaha. Bort med det, så er det ute av vegen og det tar ett sekund, og at man skal lære av det i tillegg, da. Du ser jo at den der informasjonen og opplæringen er godt ment og hyppigere i ettertid, men det siste var overkill! Det var for mye informasjon.

Informanten Kari påpeker at opplæringen og den bevisstgjøringen etter kurset er godt ment, men hun opplever likevel at det har vært for mye informasjon den siste tiden. Kari strever samtidig med å finne tid til kursene i løpet av en arbeidsdag, og gjør det heller på hennes egen måte og sletter e-postene fortløpende. Dette minner om den samme problematikken Albrechtsen (2006) peker på da han forsket på et IT-selskap og en bank, og hva informantene i disse firmaene mente om IT-sikkerhetsarbeid. Han peker på balansen mellom *funksjonalitet* og *sikkerhet*, der sikkerhetsarbeid tar såpass mye tid at det er krevende å kombinere dette med det

ordinære arbeidet. Kari ser likevel på sikkerhetsarbeid som viktig og ønsker å bidra, men for at utbyttet likevel skal ha noe verdi mener hun at kursingen må tilpasses:

> Kari: Eh, svarer du feil så får du «virus» da, det er noen scenarioer i den læringen, og forklaringer. Men ... nivået på språket i det her er helt fjernt, så kunne ha halvert tiden på det og forklart det på norsk ... hahaha ... så hadde vi fått med oss mye mer, da. Det er jo gitt tydelig tilbakemelding på den siste som ble sendt, for det var rett og slett skrekkelig. Tror det var ... var jo ikke bare en modul, var jo flere!
>
> *
>
> Kari: [...] må tenke litt over hvem målgruppen er da i forhold til det vi skal gjøre og hva de trenger i hverdagen ... ikke for mye og ikke for lite ... men akkurat slik at vi får god struktur for forbedringsarbeidet.

Kari mener at kursingen og opplæring bør nyanseres ut fra den tiltenkte målgruppen, og spesielt viktig er dette dersom konsernet mener alle ansatte bør ha eierskap over eget sikkerhetsarbeid. En annen beskriver derimot kursene som svært «basic», og forventet også at det skulle komme mer enn det som til nå har kommet. Han mener likevel at det kan gjøres mye mer i bevisstgjøringen og sikkerhetsarbeidet i etterkant, og han mener spesielt at fokuset på sikkerhetsarbeid blant de ansatte som befinner seg lengre ned og på operatørnivå i organisasjonen har vært spesielt lav:

> Karl: Ehm ... har det kunne gjort mer i ettertid, har de gjort alt de kan i forhold til opplysning, opplæring og bevisstgjøring ... så føler jeg ikke i min rolle at det har blitt overøst av cybersikkerhet, det gjør jeg ikke.

Og forteller videre at:

> Karl: [...] om du tar det ned på operatørnivå, som de fleste som jobber her er på, så er hverdagen i prinsippet likens som det var før cyberangrepet kom, men at det ligger i bakhodet på oss ... men, det ligger ikke i bakhodet på alle som har begynt etter 2019, og det er mange.

Datamaterialet viser en generell enighet om at kursene i etterkant har vært lærerike og at kursene skaper mer bevissthet om tematikken, og samtlige ser viktigheten av hva dette arbeidet

innebærer. Dette kan tyde på en type reliabilitetskultur (Boin & van Eeten, 2013), der ansatte er klar over det individuelle ansvaret for sikkerhet. Materialet viser dog en uenighet om hvor belastende kursingen er. På den ene siden finnes problemet om balansen mellom funksjonalitet og sikkerhet og at kursing bør bli nyansert ut fra den tiltenkte målgruppen, men på den andre siden oppleves likevel kursingen som mindre og mer forenklet enn det som ble forventet. Ingen av informantene rapporterer dog om en mer aktiv involvering av de ansatte der de faktisk får prøvd hvordan det er å jobbe når teknologien faller ut eller ved simulerte øvelser. Informanten Atle nevner for eksempel at teknologien kun var halvveis borte under angrepet, og at det også bør gjennomføres simulasjonstester der teknologien er «borte borte».

5.4.2 Oppsummering

I etterkant av cyberangrepet og frem til i dag innebærer sikkerhetsarbeidet i all hovedsak om kursing og bevisstgjøring gjennom e-læringsmoduler på intranettet. Overordnet sett er de fleste informantene positive til vektleggingen og fokuset som har vært på bevisstgjøringen i etterkant av angrepet, men kan i enkelte instanser bli problematisk å gjennomføre kursingen i løpet av en arbeidsdag. Andre forteller samtidig at bevissthetsnivået er det samme i dag som det var før angrepet skjedde, og mener at bevisstgjøringsarbeidet bør vektlegges i større grad blant operatørene. Rent overordnet viser funnene fra analysen en preventiv tilnærming til læring, og læringen viser i mindre grad hvorfor og hvordan håndteringen gikk bra. Dette gir den ikke-tekniske faktoren «læring- og kunnskapsformidling»

6. Diskusjon

"There are only two types of companies:
those that have been hacked and those that will be hacked."
– Robert Mueller (tidligere FBI-dierktør)

Frem til nå har avhandlingen sett nærmere på cyberkriminalitet som fenomen og resiliens som teoretisk innfallsvinkel. I dette kapitlet diskuteres det rent empiriske fra kapittel 5 opp mot det rent teoretiske i kapittel 3. 19. mars 2019 ble et løsepengevirus utløst på Hydros globale systemer, men likevel klarte Hydro å opprettholde en tilnærmet normaltilstand til tross for angrepet. I følgende kapittel identifiserer og diskuterer jeg fem ikke-tekniske faktorer som ble gjeldende i håndteringen av cyberangrepet i 2019: *evnen til å antesipere*, *avvikserfaring og improvisasjon*, *desentralisering og organisatorisk struktur*, *åpenhet*, og *læring og kunnskapsformidling*. Avslutningsvis diskuterer jeg hvorvidt tiltakene som gis i dag gjør Hydro mer eller mindre forberedt i eventuelt andre cyberhendelser og krisesituasjoner.

6.1 Evnen til å antesipere

"There is no terror in the bang, only in the anticipation of it."
– Alfred Hitchcock (filmregissør)

Tidligere ble resiliens brukt som et begrep for å se hvordan økologiske miljøer klarte å absorbere en rekke endringsmekanismer for å ivareta en viss grad av normalsituasjon, men også for å kunne eksistere i ettertid (Holling, 1973). I dag betraktes resiliens mer som en dynamisk sikkerhetsstyring når noe forutsett eller uforutsett har skjedd (Hollnagel, 2013). Forskjellen mellom tilnærmingene til Holling (1973) og Hollnagel (2013) er det dynamiske aspektet, der man i større grad enn før også implementerer tiden før, under og etter for å identifisere resiliente systemer.

I forkant av angrepet ble et konsulentfirma innleid for å påpeke sårbarheter og presenterte forslag for hvilke tiltak som bør iverksettes for å sikre eventuelle sårbare ledd. Konsernet rakk likevel ikke å iverksette tiltakene før et cyberangrep skjedde. Som det også kommer frem i empirien forteller nesten samtlige av informantene at det ble gjort noe bevisstgjøring rundt cyberkriminalitet, og mulige måter utenforstående kan komme seg inn i systemet på. I løpet av intervjuene kom det også frem at det ble gitt noe forenklet kursing på tematikken i tiden før angrepet. Informanten Karl forteller blant annet at konsernet ikke var naive på tematikken. Dette peker på en viss grad av antesipasjon der systemer, virksomheter og ansatte handler proaktivt, og handler i nåtid for å være mest beredt i fremtid (Woods, 2011).

Ifølge Woods (2011) dreier evnen til å antesipere seg i retningen av å identifisere nye kontrollstrategier, så vel som navigasjonen av gjensidig avhengighet av roller, aktiviteter og nivåer. Å være forberedt tegner samtidig et bilde av at sikkerhet prioriteres. Organisatorisk struktur er noe jeg kommer tilbake til nedenfor som deler av andre ikke-tekniske faktorer, men bør likevel nevnes til en viss grad her. Organisatoriske strukturer og den interne kulturen spiller en rolle i hvor forberedte ansatte er (jf. tabell 1) (Van der Kleij & Leukfeldt, 2019). For å inneha evnen til å antesipere må organisasjonen åpne opp muligheten for at dette kan skje. Dette påpeker også Broekema et al. (2017). De forteller at ansatte bør dele forståelsen om at læring er en lur investering, og samtidig påpeker de at selve strukturen har mye å si for hvordan dette kan skje (Broekema et al., 2017, s. 329). Nå er det dog ikke læringen som står i fokus her, noe jeg kommer tilbake til nedenfor, men heller sikkerhetskulturen. Sikkerhetskultur, som i enkelte tilfeller også går i retningen av kultur for pålitelighet (Boin & van Eeten, 2013, s. 433), handler ofte om bevissthetskultur der man forventer avvikssituasjoner i stedet for at dette ikke skal være et overraskelsesmoment senere.

Likevel bør en diskusjon om forberedelsene var gode nok i forkant. Informanten Ivar forteller for eksempel at mye av den kursingen som ble gitt i forkant kun var forenklede versjoner av det som finnes i dag. Informanten Karl forteller blant annet at konsernet kun var bevisste på truslene. En annen forteller samtidig at det kun ble tema i etterkant av hendelsen. Sikkerhetsarbeid har tidligere, både innenfor flere vitenskaper og som gjennomføring i organisasjoner tatt utgangspunkt i etterpåklokskap, og som en konsekvens blir tiltak iverksatt på bakgrunn av avvikssituasjoner som allerede har skjedd (Stavland & Bruvoll, 2019, s. 18). På den måten baserer tiltakene seg på en forutsetning om at en avvikssituasjon som allerede har skjedd også er lik i fremtiden. Til tross for at informantene til en viss grad var bevisste på at et cyberangrep kunne skje, tyder likevel funnene i empirien på at et bevisstgjøringsarbeidet ned i organisasjonen var lav i forkant av angrepet, og at en god del av responstaktikken befant seg hos de ansatte siden evnen til å antesipere korresponderer med evnen til å respondere i sosiotekniske systemer (Hollnagel, 2013). I denne sammenhengen dreier evnen til å antesipere seg i retning av lite naivitet rundt tematikken, men det peker samtidig på forholdet mellom å forutse cyberangrep og å forutse situasjoner der man generelt må drive uten IT-systemer. I så måte går dette mot selve håndteringsgrunnlaget på operatørnivå som hvilte på operatørenes egne avvikserfaringer, og kunnskap om prosedyrer som kan anvendes i andre situasjoner gjennom improvisasjon.

6.2 Avvikserfaring og improvisasjon

> "Experience is the most brutal of teachers, but you learn, my God, do you learn."
>
> – C. S. Lewis (forfatter)

Som vist i analysen ovenfor siktet flertallet av informantene på basisopplæring og grunnkompetanse da de snakket om tiden før angrepet. Som kjent fra tidligere har Hydro implementert produksjonssystemet AMPS i den overordnede driften, et system som involverer ansatte gjennom standardiserte arbeidsprosesser, definerte kunde- og leverandørforhold, optimalisert flyt, dedikerte team; og synlig ledelse (Hydro, 2014). De standardiserte arbeidsprosedyrene gjør at samtlige av de ansatte jobber ut fra de samme grunnprinsippene, samtidig som at dette opprettholder en viss grad av effektivisering, og ikke minst for å redusere materielle og menneskelige skader. I tiden før angrepet var det kjent at det ble gjort noe bevisstgjøring innenfor cyberkriminalitet, men flere av informantene siktet likevel til grunnkompetansen og bruk av prosedyrer. Ifølge Boin og van Eeten (2013) er etablerte prosedyrer den tredje faktoren for hva som kjennetegner en HRO, men det sammenfaller også med det femte punktet om reliabilitetskultur og respekt for prosedyrer. Til tross for dette var det ingen av informantene som kjente til eller kunne sikte til etablerte prosedyrer dersom et cyberangrep skulle skje.

Én viktig forutsetning for å være resilient er evnen til å tilpasse seg når et avvik har skjedd (Hollnagel, 2013; Roege et al., 2017). Weick (1993, s. 633) snakker om følelsen av å ha opplevd noe før gjennom uttrykket «déjà vu», og kjennskap til andre situasjoner kan åpne muligheten for beslutninger i andre kriser. Til sammen kan dette danne grunnlaget for improvisasjon i krisesituasjoner. Improvisasjon er ifølge Engen et al. (2016, s. 316) en form for spontan intuisjon, der forhåndsbestemte planer brukes for å løse et problem. Til tross for at prosedyrene ikke gir fullstendig støtte i krisehåndtering, er det summen av alt som gjør improvisering mulig (Engen et al. 2016, s. 316). Empirien viser at en viss grad av tilpasning måtte skje da Hydro-konsernet hadde blitt angrepet av et løsepengevirus, men at tilpasningsdyktigheten ligger i erfaringene ansatte har fra andre avvikssituasjoner og de rutinene de er kjent med. Én av informantene forteller at organisasjonen er god på nødprosedyrer som et resultat av hvor lenge han har vært ansatt, men han forteller også at prosedyrer fra andre avvikssituasjoner kan adopteres inn i andre avvik dersom det ikke foreligger noen spesifikk prosedyre for det. Dette minner samtidig om det Weick (1993) forklarer som bricolage. Bricolage handler om å skape orden ut fra det man har i umiddelbar nærhet, men for at en slik type improvisasjon kan utføres kreves det at alle er på samme bølgelengde (Boin & van Eeten, 2013). Som vist tabell 1 krever dette også at man innehar

ressurser som man kan respondere med (Van der Kleij & Leukfeldt, 2019). SOPene i Hydro åpner opp for at dette kan skje gjennom standardiserte arbeidsprosesser, men at man også har evnen til å operere driften ut over bruk av teknologiske verktøy.

For å sikre at produksjonen av aluminium kunne fortsette ble graden av manuelt arbeid større som et følge av angrepet, og regning på papirblokker erstattet det automatiske produksjonssystemet APICS. Et interessant funn i empirien er graden av teknologiavhengighet informantene rapporterer, og at de fleste oppgir at det meste som gjøres med teknologi kan utføres manuelt, enten som et følge av ansettelseslengde eller som en del av grunnkompetansen. Dagens sosiotekniske systemer krever fortsatt en viss grad av menneskelig interaksjon og menneskelige faktorer for å betraktes som resiliente (Hollnagel, 2013), og ut fra empirien er løsningen en bricolage-lignende improvisering med utgangspunkt i avvikserfaringer. Sagt på en annen måte, og med utgangspunkt i Suchman (1985) og Johansen et al. (2016), går improviseringen i retning av improvisering *med* prosedyrer. Til tross for at prosedyrene gir detaljerte arbeidsbeskrivelser for hvordan man utfører en jobb, er det sjeldent man forutser konsekvensene av en avvikssituasjon. Improviseringen krever derfor en inngående forståelse om etablerte protokoller og prosedyrer (Johansen et al., 2016, s. 334).

Til tross for at erfaringer fra andre kontekster ble en relevant faktor for hvordan angrepet ble håndtert i 2019, må det likevel diskuteres hvor gjeldende dette er i fremtiden siden resiliensteorien også diskuterer hvordan systemer tilpasser seg *etter* avvikssituasjoner. I dag har teknologiutviklingen kommet såpass langt at den har som evne å monitorere og i enkelte tilfeller respondere, men mye av den teknologien som brukes klarer uansett ikke å lære og antesipere av seg selv (Hollnagel, 2013). Med andre ord krever teknologien fortsatt en viss grad av menneskelig innblanding, eller en viss grad av barrierestyring dersom noe går galt. Én av informantene problematiserer dette i noe grad, og mener at hans generasjon er den siste generasjonen med et kompetansenivå som tilsvarer drift ut over bruk av teknologi. I RE går man ut fra antagelsen om at systemer og miljøer fungerer fordi folk innehar en tilpasningsdyktighet som gjør dem bedre rustet til å håndtere forskjellige scenarioer (Hollnagel, 2013). Én informant påpeker viktigheten av nedgangstider fordi dette bidrar til læring og forbedring, men til tross for at mye av den tilpasningsdyktigheten under cyberangrepet kom fra ansatte med lang fartstid i Hydro, er det ikke nødvendigvis sannheten blant personer som ble ansatt etter angrepet. En tilnærmet problematikk trekkes frem av Broekema et al. (2017). De forteller at folk med ekspertise, kunnskap og erfaring kreves for å i det hele tatt kunne drive opplæring, men mye av problematikken tiltrår når erfaringene pensjoneres sammen med de ansatte. Det skal dog sies at mye av forbedringsarbeidet og opplæringen har blitt tatt på alvor i

etterkant av angrepet og frem til i dag, og én av informantene mener at dette bør tas på alvor dersom sluttmålet er å modernisere fabrikken ytterligere. Med bakgrunn i resiliens og RE er likevel problematikken relevant å trekke frem, og ikke minst ta tak i, dersom fabrikken befinner seg i en situasjon der teknologien blir fullstendig borte som et følge av cyberangrep eller andre tilnærmede hendelser. Sagt på en annen måte, for å kunne gjøre improviserte handlinger i krisesituasjoner, bør man ha inngående kunnskap over det verktøyet som benyttes for å få orden på en uoversiktlig situasjon (Weick, 1993). I forlengelsen av dette er læring og kunnskapsformidling en viktig ikke-teknisk faktor jeg kommer tilbake til nedenfor, både som en del av responsen på cyberangrepet i ettertid, men også hvor avveiningene bør går for at de ansatte får eierskap over sitt eget sikkerhetsarbeid. Mye av den tematikken som hittil er diskutert sammenfaller godt med kompetansedelegeringen ute i organisasjonen og hvilket ansvar man har i nedgangstider. Til tross for at mye av håndteringen befant seg i avvikserfaringer og improvisering med prosedyrer, kan mye av svaret også ligge i strukturer som var på plass lenge før angrepet skjedde.

6.3 Desentralisering og organisatorisk struktur

> "Every company has two organizational structures: the formal one is written on the charts; the other is the everyday relationship of the men and women in the organization."
>
> – Harold Geneen (forretningsmann)

Dynes (1993) skiller mellom to planleggingsmodeller for beredskapsrespons. På et globalt nivå har man tidligere tatt utgangspunkt i den såkalte «militærmodellen». Modellen tar utgangspunkt i at katastrofer skaper kaos, og at kaos kun håndteres gjennom kommando og kontroll. Med andre ord påstår modellen at den sivile siden av samfunnet ikke er godt nok egnet til å håndtere kriser, og at militær organisering er den eneste måten man kan håndtere det effektivt. På den andre siden peker han også på «problemløsningsmodellen» som en kontrastert versjon av den forrige. Modellen har basis i sosial kontinuitet, koordinering og samarbeid, og Dynes (1993) argumenterer for at den er mer effektiv siden den tar utgangspunkt i forskning på organisert atferd under kriseperioder. Det viktigste med denne modellen er at løsningen og ressursene befinner seg ute blant befolkningen, og i stedet for å gå ut fra et vertikalt perspektiv på organisering tar man heller utgangspunkt i sosiale mekanismer (Dynes, 1993, s. 183). Den fjerde faktoren i en HRO er også muligheten for at formelle strukturer og ansvarsområder kan transformeres til desentraliserte og teambaserte organer i krisesituasjoner, noe som krever høy teknisk kompetanse blant ansatte (Boin & van Eeten, 2013). Til tross for at det ikke nevnes

eksplisitt tar også Steen et al. (2021) for seg en tilnærmet problemløsningsmodell da de så hvordan oljeplattformen West Phoenix håndterte et COVID19-utbrudd. De finner at felles øvelser, etablert av de sentrale institusjonene, forsterker rolleforståelser og ansvarsområder i responsstrukturen, som til syvende og sist bedrer samhandlingskapasitetene.

Fra før har empirien vist at mye av håndteringen av angrepet baserte seg på de ansattes egne erfaringer fra tidligere avvikssituasjoner. Som et følge har datamaterialet vist at en viss grad av improvisasjon skjedde som et resultat av at det ikke foreligger noen spesifikke prosedyrer på håndteringen av cyberangrep. Empirien viser også at informantene ikke hadde noe ansvar ut over det å holde driften i gang da angrepet først inntraff, men ansatte med et utvidet ansvar kunne likevel komme med innspill for hvordan dette kunne håndteres. I empirien kommer det også frem at terskelen er høy for å be om kortsiktig hjelp utenfra for det de selv har ansvar for lokalt, og eventuelle avvik må håndteres av dem selv. Dette kom til uttrykk i et av intervjuene der det ble det sagt at lederne selv la opp til at de ansatte bare kunne «holde på» der de hadde ansvar. Én av informantene peker samtidig på den organisatoriske strukturingen som et av de viktigste suksesskriteriene for hvorfor det gikk tilsynelatende bra med håndteringen av cyberangrepet. Dette eksemplifiseres med to tilnærmet like strømutfall fra ett av verkene her i Norge og Qatulum fabrikken i Qatar. Der blir det påpekt at en stor forskjell mellom de to tilfellene er kompetansen som befinner seg i og ute i organisasjonen. Med andre ord skjedde en del av håndteringsgrunnlaget ut fra en organisering som var på plass lenge før angrepet, noe som krevde lite tilpasning da avvikssituasjon gjorde seg gjeldende.

En HRO kjennetegnes av muligheten til å desentralisere kompetanse og ansvarsområder ut i forskjellige organer under krisesituasjoner (Boin & van Eeten, 2013). Funn fra mitt datamateriale peker på et lignende element i hvordan angrepet ble håndtert, men funnene tilsier likevel at dette var strukturer som allerede var på plass lenge før angrepet skjedde. Desentraliseringen kommer som et følge av at kompetansen og kunnskap om drift befinner seg blant de ansatte, og som et resultat gjør dem til «noe mer enn roboter», som en av informantene forklarer. Å støtte seg på en struktur som allerede er der kan øke resiliens av flere grunner. For det første, og som forklart tidligere, krever dette mindre tilpasning når det først skjer noe. Som Boin og van Eeten (2013) nevner har HRO-orientert litteratur tatt for seg viktigheten av organisasjonstilpasning under krisesituasjoner, noe jeg mener kan være problematisk. Broekema et al. (2017) finner at restrukturering har en negativ innflytelse på læring siden ansatte må tilpasse seg etter nye roller og ansvarsområder. For det andre kan dette bidra til å forsterke og klargjøre ansvarsområdene fra de samme grunnverdiene. Hult og Sivanesan (2013) mener man burde gå vekk fra silomentaliteten der cybersikkerhet er en ekspertfunksjon, og at

man heller burde ta sikte på å inkorporere cybersikkerhet i hver enhet, avdeling, prosedyre og praksis for å bygge et fundament samtlige ansatte jobber etter. Som et resultat kan dette bidra til felles rolleforståelse og ansvar i andre funksjoner, gitt at alle har vært gjennom et felles trenings- og øvingsopplegg (Steen et al., 2021). For det tredje fremmer dette proaktivitet, og kan ses i Qatar-eksemplet som har blitt nevnt tidligere med fokus på organisasjonskultur. Et resilient system er ikke bare et aktivt og responderende system (Hollnagel, 2013). Å være proaktiv er evnen til å forutse noe før det skjer for å være mest beredt i avvikssituasjoner. Dette krever på sin side en reliabilitetskultur som evner å forutse det uforutsette, men dette krever at alle handler fra de samme grunnverdiene. Som det ble fortalt i intervjuene ble resultatet av et strømutfall i Qatar-fabrikken med flere måneders gjenoppbygning og tap av flere milliarder kroner, mens et tilsvarende strømutfall i Norge endte med bortgang av tre elektrolyseovner. Som informanten Karl påpeker er forskjellen hvordan myndighet er delegert ute i organisasjonen. I Norge er alt arbeidsliv forankret i den norske modellen – et trepartssamarbeid mellom det organiserte arbeidslivet, offentlige velferdsordninger og økonomisk politikk. Samarbeidsforsøkene bidro til at bedriftsdemokrati, medbestemmelse, medvirkning og selvstyre ble en del av det norske arbeidslivet, der produktet av arbeid er mennesker (Bungum et al., 2016, s. 19). Den norske modellen er også forbundet med en annen tematikk som gjorde seg gjeldende i empirien. I den norske modellen er tillit et tema med mye forskning, blant annet for at det generelle tillitsnivået i Norge har bidratt til store økonomiske fordeler og gjør arbeidslivet mer effektivt. Dessuten åpner tillit opp for åpenhet for investering i næringslivet. Samtidig kan tillit bidra til åpenhet i hvordan krisesituasjoner håndteres – både internt i organisasjonen og i det offentlige.

6.4 Åpenhet

"Never let them see you bleed."

– James Bond

Av tidligere litteratur snakkes det særdeles lite om åpenhet, noe som også kan gjenspeiles i lav offentlig rapportering av cyberhendelser både nasjonalt og internasjonalt. I mørketallsundersøkelsen (NSR, 2022) blir det rapportert at kun 6% av norske virksomheter involvert i en cyberhendelse offentliggjorde tilfellet. Til tross for at NSR ikke går i dybden av hvorfor dette er tilfelle, kan det være en rekke årsaker rundt dette. Roar Thon (2020), fagdirektør i NSM, trekker frem en uttalelse av svensk politi som mener at de svenske virksomhetene ikke anmelder forholdene for at det er dårlig PR for varemerket, noe som også er overførbart i en

norsk kontekst. Han mener også at dataangrep har feilaktig blitt assosieres med dårlig datasikkerhet. Viktigst av alt mener han at krisekommunikasjon har mer å si for omdømmet enn at en virksomhet er rammet av et cyberangrep (Thon, 2020). Aakre (2020) mener at økt åpenhet kan avverge angrep, som på sikt gjør cyberkriminalitet en lite lønnsom forretningsmodell. Hun mener også at en viktig årsak for lite offentlig rapportering er at virksomheten kan fremstå som et enkelt mål eller at det svekker tilliten i aksjemarkedet (Aakre, 2020, s. 23).

Da krypteringen av servere og datamaskiner begynte på nettet til Hydro, var de raskt ute med pressekonferanse, anmeldelse og informasjon til media (Aakre, 2020, s. 23), noe samtlige av informantene i utvalget mitt var svært positive til. Informanten Atle mener at å gå ut offentlig med hele situasjonen er et sterkt og viktig signal å gi. Han mener at dette kan statuere et eksempel både for offentligheten, men også de kriminelle aktørene ved å vise ingen interesse for å betale løsepengekravet. Karl hadde samtidig ikke satt pris på om det ble håndtert på en annen måte, og hadde likt det lite dersom hendelsen hadde vært hysjet ned. Det er dog ikke bare den offentlige håndteringen av cyberangrepet som kommer frem som et aspekt av åpenhet i virksomheten. Én av informantene trekker frem at det er lov til å gjøre feil og at man ikke blir straffet dersom man har gjort en feilvurdering. Ut fra dette mener jeg at åpenhet, både av intern og ekstern form, kan forsterke cyberresiliens på tre måter.

For det første vil ekstern åpenhet kunne bidra til at sentrale og relevante institusjoner involveres raskt i responsstrategien, spesielt sentralt blir responsen under angrepet. Samtidig blir det like viktig for hvordan man forbereder seg etter angrepet. Hydros åpenhet var derimot ikke kun til hjelp for Hydro, og det ble i ettertid bevist at åpenheten var til hjelp for andre virksomheter i landet. Bevismaterialet var ikke kun relevant for etterforskningen av angrepet, men bevismaterialet gjorde det mulig å spore opp lignende angrep med samme virus. Som et resultat ble virksomhetene, både i inn- og utland, varslet tidlig og fremtidige angrep ble avverget (Klevstrand, 2019, sitert i Aakre, 2020, s. 23).

For det andre kan ekstern åpenhet bidra til å gjøre det ukjente kjent. Aakre (2020) mener at når en myndighetsaktør deler informasjon om et pågående angrep, eller et tidligere angrep, gjør man det kjente kjent for en virksomhet. Når det derimot deles informasjon fra både myndighetsaktørene og virksomhetene, vil kjent kunnskap øke på bekostning av det ukjente (Aakre, 2020, s. 25). I likhet med det foregående punktet vil informasjonsdeling til gjengjeld kunne åpne opp for en sterkere antesipasjonsevne. Likeledes dreier dette seg om å etablere respons fra læring av hendelser bak i tid, fokus på monitorering, og ikke minst utgjør dette

basisen for en langvarig proaktivitet for at et system kan opprettholdes i krisesituasjoner (Hollnagel, 2013).

For det tredje vil både ekstern og intern åpenhet kunne resultere i tillit. På den interne siden kan åpenhet være tillitsskapende rundt det interkollegiale. Broekema et al. (2017) argumenterer for at man i et tillitspreget miljø kan diskutere krisesituasjoner åpent, både vertikalt og horisontalt og i formelle og uformelle settinger. Antunes et al. (2017, s. 479) argumenterer også for at virksomheter bør monitorere arbeidernes psykososiale status ettersom at krisesituasjonen kan endre risikoforståelser, sikkerhetsatferd og atferd mot andre arbeidere, som kan resultere i endret risikokommunikasjon senere. På den eksterne siden kan åpenhet skape et tillitsforhold mellom én virksomhet og sentrale myndighetsaktører, men mye av dette vil kunne oppstå som et følge av den sårbarhetsgraden de fleste virksomhetene befinner seg i. De færreste virksomhetene i landet er selvforsynte, og de fleste virksomheter befinner seg i et gjensidig avhengighetsforhold med andre – gjerne på et globalt nivå – som kan resultere i cybersårbarhet og konsekvenser lengre ute i verdikjeden (Aakre, 2020, s. 23). Åpenhet er et tema som i seg selv trenger mer akademisk forskning og hvordan dette kan være en resiliensytende faktor i norske virksomheter. Åpenhet åpner imidlertid opp for en ny ikke-teknisk faktor som ble noe berørt i dette underkapitlet. Åpenhet vil kunne resultere i tillit dersom en organisasjonskultur åpner opp for det. Tillit, og spesielt interkollegial tillit, vil samtidig kunne åpne opp for hvordan man lærer av kriser og hvordan man formidler kunnskap ute i organisasjonen.

6.5 Læring og kunnskapsformidling

"If you can't explain it simply, you don't understand it well enough."

– Albert Einstein

Mørketallsundersøkelsen fra 2022 viser at den mest utbredte følgen av en cyberhendelse er endringer i policy og rutiner, og av alle virksomhetene som ble offer for en cyberhendelse i 2022 endret 52% av dem rutinene sine i etterkant. Rapporten viser samtidig at kun 22% av virksomhetene investerte i opplæringsprogram for de ansatte, men viser at av de minste virksomhetene – med 5 eller flere ansatte – var det 52% som hadde innført tiltak for å øke sikkerhetsbevissthet blant de ansatte, der 38% består av e-læringskurs (NSR; 2022). En virksomhets ansatte er i flertallet av tilfellene sistelinjeforsvaret mot trusler i cyberspace, og en resilient organisasjon bør investere i et forbedringsarbeid for å øke sikkerhetskulturen blant

personalet, og ikke minst for at de kan holde seg oppdaterte på taktikk, teknikk og prosedyrer (Hult & Sivanesan, 2013).

Empirien viser mye av de samme funnene som rapporten fra NSR (2022). Tiden etter cyberangrepet har vært preget av en rekke e-læringsmoduler, kursing og testing på intranettet. Overordnet er det en gjennomgående tråd blant informantene at kursingen ses på som positivt og de skjønner godt hvorfor det blir fokusert på. Kursingen fungerer for de fleste av informantene som en kontinuerlig påminnelse om hvor sårbare man kan være, og ikke minst hvor lett det kan være for utenforstående å komme seg inn i systemene dersom de virkelig vil. Et annet funn er at samtlige av informantene vil bidra i sikkerhetsarbeidet. Dette kan trekkes i retning mot en sterk sikkerhetskultur i fabrikken (Boin & van Eeten, 2013; Hult & Sivanesan, 2013). En sterk sikkerhetskultur kjennetegnes av tillit og forsiktighet, men også respekt for at prosedyrer og det individuelle ansvaret for at sikkerhet bearbeides og promoteres som et felles sluttmål (Boin & van Eeten, 2013). Å lære av en hendelse innebærer også at man lærer de riktige tingene fra de rette erfaringene, både suksesskriterier og det som kunne bli gjort annerledes (Hollnagel, 2013). Som nevnt tidligere gir nedgangstider muligheter for forbedringsarbeidet ved verket, men også intensivering av tiltak som enten ikke ble gjort i forkant av angrepet eller sårbarheter som ble synlige under angrepet. Overordnet virker læringen og kursingen i ettertid som en investering i de ansatte og konsernet ser på viktigheten av en holistisk tilnærming til sikkerhetsarbeid, og ikke minst kan dette bidra til å skape et bilde av at sikkerhetsarbeid tas på alvor. Til tross for at mesteparten av kunnskapen befinner seg i IT-avdelingen, kan det likevel komme gode poenger utenfra som én av informantene forklarer. En gjensidig kollegial tillit er noe Broekema et al. (2017) trekker frem som en sentral faktor for hvorfor og hvordan man skaper læring i krisesituasjoner, men også for at resiliens kan opprettholdes til tross for at man befinner seg i et avvik. Tillit gjør at krisesituasjoner kan diskuteres åpent, både i den horisontale og den vertikale strukturen. Likeledes argumenteres det at høy motivasjon blant ansatte styrker behovet for å bidra i form av sikkerhetsarbeid og gjennomføring av kurs, noe også mine informanter gir uttrykk for.

Funnene fra empirien viser dog en dikotomi mellom mengden av kurs og hvor belastende bevisstgjøringsarbeidet har vært i etterkant av angrepet, noe som kan resultere i svekket resiliens dersom målet er å bruke de ansattes potensiale i sikkerhetsarbeidet. På den ene siden blir det nevnt i intervjuene at mengden kurs og e-læringsmoduler har vært stor, og at det er vanskelig å kombinere dette med ordinært arbeid. Samtidig blir det sagt at språket som brukes i kursene gjør det vanskelig å forstå hva målsettingen med modulene er. Problematikken peker i samme retning som det Albrechtsen (2006) pekte på i balansegangen mellom funksjonalitet,

sikkerhet og effektivitet. Dette peker også på en ujevn balansegang mellom motivasjon og mulighet for å lære (Van der Kleij & Leukfeldt, 2019). Til tross for at informantene ser viktigheten av å bidra, er det likevel problematisk å veksle mellom økt mengde sikkerhetsarbeid samtidig som at en viss grad av effektivitet opprettholdes (Albrechtsen, 2006). I ytterste instans kan dette resultere i svakere sikkerhetsytelse, i form av at kunnskapsnivået er mye lavere enn det det skulle ha vært, men også lavere motivasjon for å bidra i sikkerhetsarbeidet dersom formålet ikke er klart nok. Som nevnt er språket som blir brukt en sentral faktor for hvordan det tilsynelatende er vanskelig å balansere mellom sikkerhetsarbeid og funksjonalitet, og at det ifølge informanten Kari kreves en nyansering ut fra den tiltenkte målgruppen.

På den andre siden, og i kontrast med den foregående siden, blir det likevel nevnt at mengden kurs og bevisstgjøring har vært lav i etterkant av angrepet, spesielt blant de på operatørnivå. Informanten Karl mener at nivået i dag kan minne om det samme bevissthetsnivået før angrepet skjedde for disse ansatte, og spesielt de som ble ansatt etter angrepet. Albrechtsen (2006) trekker også frem at kun én av hans ni informanter i IT-selskapet mente at sikkerhetskampanjene hadde positiv effekt på sikkerhetsytelse, som kunne være et resultat av at kursene er lest og like lett glemt, men også at innholdet ikke tar for seg noe mer enn det de ansatte allerede vet. Dette punktet blir også relevant for en gjenværende tematikk som kom frem i intervjuene, og hvordan læring har foregått etter angrepet.

Til slutt nevner samtlige av informantene at det har vært lite eller ingen fysisk involvering av operatører og ansatte lengre oppe i strukturen med fokus på hvordan man håndterer cyberangrep. På en lignende måte rapporteres det heller ikke om sikkerhetsarbeid som rettes inn mot hvordan man håndterer systemet dersom det blir fullstendig slått ut. Ifølge Hult og Sivanesan (2017) kjennetegnes effektiv cyberresiliens av samarbeid, kunnskapsdeling og krysstrening, noe Steen et al. (2021) også trekker frem som sentrale elementer for hvordan man lærer under og etter avvikssituasjoner. Fysiske cyberaktiviteter og øvelser, i tillegg til e-læringsmoduler, har som mål å teste den overordnede effektiviteten i forsvaret mot cyberangrep, men det åpner også opp for trygghet og innsikt i cybersikkerhetsprosesser og kommunikasjonsstrukturer (Hult & Sivanesan, 2017). Samtidig vil jeg også argumentere for at dette kan bidra til å nyansere sikkerhetsarbeidet ut fra de ansattes ansvarsområder, et problem som ble trukket frem ovenfor. For det første kan dette bidra til at de ansatte lærer ved å gjøre, i stedet for at all læring skjer på basis av lesing av e-moduler. For det andre kan dette bidra til å skape et bilde av et felles siktemål og et felles gode, der alle jobber med de samme forutsetningene. Som et resultat kan dette bidra til å validere strategier som faktisk fungerer, men også rette et fokus mot det som fungerer mindre godt (Hult & Sivanesan, 2017).

6.6 Er Hydro forberedt?

"Preparation through education is less costly than learning through tragedy."

- Max Mayfield (meteorolog)

Foreløpig har jeg satt lys på fem ikke-tekniske faktorer som jeg mener er sentrale for cyberresiliens både før, under og etter cyberangrepet som skjedde i 2019. Evnen til å antesipere gjorde seg gjeldende før angrepet, og mye av antesiperingen gjorde seg relevant i tiden før ved lite naivitet på tematikken, og forholdet mellom å forutse cyberangrep og situasjoner der man generelt må drive uten IT-systemer. Avvikserfaring og improvisasjon ble en relevant faktor under angrepet, og faktoren ble en sentral del i hvordan selve angrepet ble håndtert internt i sin helhet. I denne konteksten tar improvisasjonen form av avvikserfaring som et følge av manglende prosedyrer på cyberhendelser, men samtidig improvisering med eksisterende prosedyrer. Desentralisering og organisatorisk struktur ble også en sentral faktor. Teorier innenfor HRO har tidligere tatt utgangspunkt i virksomheter som evner å desentralisere seg under krisesituasjoner, men jeg finner likevel at dette var strukturer som var der fra før av. Til syvende og sist argumenterer jeg for at dette krever mindre tilpasning når en krisesituasjon først har skjedd. Åpenhet er også en annen ikke-teknisk faktor som gjorde seg gjeldende, spesielt hvordan angrepet ble håndtert internt og eksternt. Åpenhet kan bidra til rask involvering av sentrale myndighetsaktører, gjøre det ukjente kjent, og øke det overordnede tillitsnivået. Den siste faktoren er læring og kunnskapsformidling. Overordnet sett viser empirien en generell positivitet til kursingen som har skjedd i ettertid og viser at de ansatte er villig til å gjøre en sikkerhetsytende innsats. Likevel viser empirien et skille mellom for mye og for lite kursing.

Det gjenværende spørsmålet er hvor forberedt Hydro er og hvor forberedt det er mulig å være. Som kjent fra kapittel 2 er cyberkriminalitet et særdeles flytende begrep, noe som også kommer frem i mangelen på én konkret definisjon av det. I denne avhandlingen har jeg tatt utgangspunkt i løsepengevirus i det digitale rom, og gått i retningen av en definisjon som betegner dette som vinningskriminalitet mot datasystemer (Kripos, 2023). Det finnes også flere forskjellige typologier av kriminelle aktører i cyberspace, alt avhengig av hvilke handlinger som utføres og hensikten bak (McGuire, 2012; Broadhurst et al., 2014). På samme måte er organisatorisk resiliens dynamisk i det at risikohåndtering tar utgangspunkt i hele hendelsesforløpet, men dette innebærer også at responsen formes av krisen i seg selv. Som et resultat hadde det vært en feilslutning å basere alle tiltak som innføres i ettertid på én enkelthendelse. Det er dog ikke noe i veien med å ta utgangspunkt i tidligere kriser, og

nedgangstider er et viktig element i det videre læringsutbyttet. Å lære av krisetider er også noe som forventes av det offentlige (Broekema et al., 2017). Krisesituasjoner er derimot komplekse fenomener. Krisesituasjoner er noe som i de fleste tilfeller skjer uforventet, og som Norsk Hydro er sosiotekniske systemer ofte sammenkoblet som gjør det vanskelig å skape et oversiktlig sårbarhetsbilde og potensielle årsaker (Aakre, 2020; Broekema et al., 2017). Et punkt det kan være verdt for Hydro å diskutere er om de befinner seg i et såkalt «paradoksalt læringsutbytte», der den eneste muligheten man har for å utnytte kursingen er om man havner i krisesituasjoner. Én løsning på dette kan være å involvere de ansatte i langt større grad enn det som ble oppgitt i intervjuene, og la organisatorisk trening også bli en del av sikkerhetskulturen. Et kjennetegn med en cyberresilient organisasjon er den overordnede effektiviteten rundt håndteringen av eventuelle angrep i cyberspace (Hult & Sivanesan, 2013). Noe viktigere kan organisatorisk trening være for de som ble ansatt i etterkant av angrepet og frem til i dag. Som det kommer frem i empirien ble det argumentert for at den generelle bevisstheten på operatørnivå er den samme som tiden før angrepet, og at det kom mye mindre kurs enn hva som ble forventet. For å bevare det generelle resiliensnivået er det viktig at samtlige av arbeiderne holder seg oppdaterte, og ikke minst at alle ansatte jobber ut fra de samme grunnprinsippene. I intervjuene finner jeg en generell positivitet til mer fysisk trening og øvelsesscenarioer der de ansatte har mulighet til å anvende det de har lest i e-læringsmodulene. Det kan dog argumenteres for at de falske e-postene som sendes ut, der de ansatte testes på årvåkenhet for mistenkelig e-post, er en form for øvingsscenario. På den ene siden har de ansatte her mulighet til å opprettholde en viss bevissthet for hvordan cyberangrep vanligvis utløses. På den andre siden bør det også kjøres øvelser for når produksjonssystemet faktisk er borte. Til tross for at cyberangrepet i 2019 kan utgjøre en god læringsbasis fremover, bør det likevel tas i betraktning at cyberangrep sjeldent er like, og metodene kriminelle aktører benytter seg av utvikler seg i takt med den digitale utviklingen. Som Albrechtsen (2006) finner er direkte involvering av ansatte en mer effektiv fremgangsmåte for å ivareta det generelle sikkerhetsnivået og bevisstheten rundt tematikken, enn rene bevissthetskampanjer og moduler.

Et annet problem dukker også opp i empirien og innbefatter problemet med funksjonalitet og sikkerhet. Til tross for at det på den ene siden blir forklart at mengden kurs har vært uforventet lite i ettertiden av angrepet, blir det på den andre siden forklart at mengden har vært for mye for noen andre. Samtidig blir det påpekt av flere at språket som benyttes i kursene ofte bærer preg av at cyberhendelser fortsatt er en IT-funksjon. Som et følge, og som én av informantene påpeker, bør det skje en nyansering og spesifisering over hvem den tiltenkte målgruppen er. Albrechtsen (2006) mener at økt sikkerhetsarbeid i enkelte tilfeller går utover

arbeidsfunksjon og effektivitet. En mulig konsekvens av for mye kursing og bruken av et uforståelig språk kan i ytterste tilfelle virke mot sin hensikt, i den grad at målet blir å komme seg igjennom det enn å faktisk oppnå læring. I forhold til språket som brukes er det også viktig å nevne at risikooppfatning kan tolkes ulikt over avdelingene, alt ut fra hvilke arbeidsoppgaver de ansatte har. Dette ble spesielt et tilfelle da jeg spurte informantene om hva de legger i risikobegrepet og hvordan de definerer det. Noen ser på den ene siden på risiko som noe forbundet med arbeid og at prosedyrer følges i sin helhet for å minimere avvik i mest mulig grad. På den andre siden går andre i retningen av å definere dette som sikring av infrastruktur og datanett. Nå er ikke hensikten med denne avhandlingen å avdekke hvordan informantene tolker risiko, men i forhold til cyberresiliens kan dette være relevant i kursoppbygningen fremover. Til tross for at IT-avdelingen «sitter med den store nøkkelen», som informanten Ingrid uttrykker det, er det fortsatt opp til hver enkelt ansatt å bidra i sikkerhetsarbeidet. Det bør samtidig nevnes at det ser ut til at det er gjort noen tiltak for å bedre dette, blant annet ved å gi beskjed til ledelse og konsern om at det blir for mye, som informanten Kari ga uttrykk for. Det er også mye som ikke ble nevnt i intervjuene, og sjansen er stor for at Hydro allerede har tatt problematikken til etterretning. Som et følge av at intervjuene gir et inntrykk for en god sikkerhetskultur, virker de tilsynelatende forberedt på eventuelle krisesituasjoner og nedgangstider. Ved å ta tak i punktene kan likevel resiliensnivået forsterkes.

7. Konklusjon

Norge er et av de mest digitaliserte landene i verden, både på individnivået så vel som organisasjonsnivået. Med økt bruk av digitale verktøy kan sårbarhetene øke parallelt. Cyberkriminalitet er en kompleks kriminell atferd, noe som kommer som et følge av at risiko ikke lengre er forbundet med én geografisk lokasjon. Cyberkriminalitet gjør også strafferammene uklare dersom handlingen er gjort i et helt annet land med et annet rettssystem. I denne oppgaven har jeg tatt utgangspunkt i resiliensteori for å se hvordan én norsk virksomhet håndterte et cyberangrep. Med bruk av kvalitative semistrukturerte intervjuer har jeg tatt utgangspunkt i problemstillingen *hvilke ikke-tekniske faktorer bidrar til cyberresiliens i Hydro?*

Analysen viser at spesielt fem ikke-tekniske faktorer gjorde seg gjeldende før, under og etter angrepet. Den første er evnen til å antesipere, noe som spesielt gjorde seg gjeldende i tiden før angrepet. Evnen til å antesipere kommer som et følge av kursing og basisopplæring, og spesielt sistnevnte ble relevant for den neste faktoren. Den andre er avvikserfaring og improvisasjon som ble relevant under angrepet. Som et følge av at det ikke foreligger prosedyrer på cyberhendelser ifølge informantene, måtte angrepet håndteres ut fra det som var tilgjengelig for dem – spesielt andre relevante prosedyrer og de erfaringene de besitter fra andre avvikssituasjoner. Den tredje faktoren er desentralisering og organisatorisk struktur. Angrepet krevde minimale tilpasninger av organisasjonsstruktur, og håndteringen baserte seg på en desentralisering som allerede var på plass lenge før angrepet. Derfor vil jeg også argumentere for at faktoren er relevant både før og under angrepet. De to siste faktorene gjorde seg gjeldende etter angrepet, der fjerde er åpenhet og femte er læring- og kunnskapsformidling. Hydros åpenhet gjorde at sentrale myndighetsaktører kunne aktiviseres allerede fra begynnelsen av, men åpenhet kan også bidra til at læring skjer mellom virksomheter. Læring er også en viktig del i det overordnede resiliensnivået, og består av kursing og e-læring etter cyberangrepet.

Oppgaven har også tatt utgangspunkt i forskningsspørsmålene: hvordan ble cyberangrepet håndtert? Hva er gjort av tiltak etter cyberangrepet? Hvor avhengige er de ansatte av teknologi? Angrepet ble håndtert med stor grad av forkunnskaper om drift uten teknologi, der de ansatte med lang fartstid ble en viktig faktor i dette. I etterkant av angrepet har kursing og e-læringsmoduler vært sentrale tiltak for å bevisstgjøre de ansatte. Empirien viser også at de fleste ansatte er generelt lite avhengig av teknologi for å få gjort arbeidsoppgavene sine, noe som også blir et resultat av de ansatte med driftskompetanse som går utenfor bruk og drift av teknologi. Avslutningsvis har jeg også pekt på en rekke tiltak som muligens kan gjøre Hydro mer resilient i forhold til cyberangrep, men som også kan anvendes i generele situasjoner der man må drive uten IT-systemer. Jeg mener at ansatte bør involveres i langt større grad enn det

som ble rapportert i analysen. Jeg mener også at det bør gjøres avveininger i forhold til mengde av kursing, og at det bør stilles spørsmål til hvor mye kursing som faktisk kreves. For å bevare et visst resiliensnivå er det også viktig at nye operatører blir bevisstgjort på digital sårbarhet, men også at de blir oppdatert på digitale trusler og drift uten IT.

Som den tidligere FBI-direktøren Robert Mueller en gang sa finnes det kun to typer virksomheter: de som har blitt utsatt for hacking, og de som kommer til å bli hacket. Det kreves mer forskning på cyberkriminalitet og digital sårbarhet generelt, og jeg håper avhandlingen kan åpne opp for at den norske sosiologien også retter fokuset på kriminalitetsformen. Hvert av de ikke-tekniske faktorene kan være egne forskningsopplegg i seg selv. For eksempel kan man undersøke hvorvidt og hvordan desentraliserte organisasjonsstrukturer fremmer cyberresiliens i norske virksomheter. Man kan også undersøke hvordan andre virksomheter bruker egne erfaringer for å holde tritt med den digitale utviklingen. Bare siden pandemien har bruken av digitale verktøy blitt mer relevant for hvert år, og bare i løpet av det året som ble brukt til å skrive avhandlingen har det skjedd mye i cyberspace. KI, i form av ChatGPT, har i det siste vært et hett tema innenfor akademia, men også hva dette har å si for generelle sikkerhetsnivå i virksomheter. Siden avhandlingen ikke hadde som hensikt å problematisere KI, kan også dette være en vinkling i andre forskningsopplegg og utviklingen av kriminalitetsformer.

Bibliografi

Aakre, S. (2020). Hvilket trusselbilde står norske virksomheter overfor, og hvordan kan åpenhet bidra til å forstå cyberrisiko? *Magma – Tidsskrift for økonomi og ledelse*, 23(2), 37 – 45. https://nordopen.nord.no/nord-xmlui/handle/11250/2677253

Albrechtsen, E. (2006). A qualitative study of users' view on information security. *Computers & Security*, 26(4), 276-289. https://doi.org/10.1016/j.cose.2006.11.004

Almklov, P. G., Antonsen, S. & Fenstad, J. (2010). *IKT, nye grensesnitt og nye sårbarheter? Hvordan nye teknologier og organisasjonsformer påvirker robusthet og beredskapsevne for IKT-hendelser ved et sykehus* (1452). Hentet fra https://samforsk.no/publikasjoner/ikt-nye-grensesnitt-og-nye-sarbarheter-hvordan-nye-teknologier-og-organisasjonsformer-pavirker-robusthet-og-beredskapsevne-for-ikt-hendelser-ved-et-sykehus

Almklov, P. G., Antonsen, S., Størkersen, K. V. & Roe, E. (2018). Safer societies. *Safety Science*, 110, 1-6. https://doi.org/10.1016/j.ssci.2018.03.018

Antunes, D., Palma-Oliveira, J.M., Linkov, I. (2017). Enhancing Organizational Resilience Through Risk Communication: Basic Guidelines for Managers. I: Linkov, I., Palma-Oliveira, J. (red.) *Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security*. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-1123-2_18

Arias-Vargas, M., Sanchis, R. & Poler, R. (2023). Gamification for Awareness of the Importance of Enterprise and Supply Chain Resilience. I: García Márquez, F.P., Segovia Ramírez, I., Bernalte Sánchez, P.J., Muñoz del Río, A. (red.) *IoT and Data Science in Engineering Management. CIO 2022. Lecture Notes on Data Engineering and Communications Technologies*, vol 160. Springer, Cham. https://doi.org/10.1007/978-3-031-27915-7_61

Atkinson, P. (2015). *For ethnography*. Sage Publishing

Bagheri, S., Ridley, G. & Williams, B. (2023). Organisational cyber resilience: management perspectives. *Australasian Journal of Information Systems*, 27, 1 – 28. https://doi.org/10.3127/ajis.v27i0.4183

Beck, U. (1992a). *Risk society. Towards a new modernity*. Sage Publishing.

Beck. U. (1992b). From industrial society to the risk society: Questions of survival, social structure and ecological enlightenment. *Theory, Culture & Society*, 9, s. 97-123.

Beck, U. (2006). Living in the world risk society. *Economy and Society*, 35(3), 329-345. https://doi.org/10.1080/03085140600844902

Björck, F., Henkel, M., Stirna, J., Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. I: Rocha, A., Correia, A., Costanzo, S., Reis, L. (red.) *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol 353. Springer, Cham. https://doi.org/10.1007/978-3-319-16486-1_31

Boin, A. & van Eeten, M. J. G. (2013). The resilient organization. *Public Management Review*, 15(3), 429 – 445. https://doi.org/10.1080/14719037.2013.769856

Brinkmann, S. & Kvale, S. (2019). *Doing interviews*. Sage Publications Ltd. https://doi.org/10.4135/9781529716665

Broadhurst, R., Grabosky, P., Alazab, M. & Chon, S. (2014). Organizations and Cybercrime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 8(1), 1-20.

Broekema, W., van Kleef, D. & Steen, T. (2017). What factors drive organizational learning from crisis? Insights from the Dutch food safety services' response to four veterinary crises. *Journal of Contingencies and Crisis Management*, 25(4), 326 – 340. https://doi.org/10.1111/1468-5973.12161

Bruvoll, J. A., Thuv, A. & Enemo, G. (2020*). Håndtering av IKT-sikkerhetshendelse i Helse Sør-Øst og fylkesmannsembetene – en vurdering* (FFI-rapport 20/01560). Hentet fra: https://www.ffi.no/aktuelt/nyheter/dataangrepene-mot-helse-sor-ost-og-fylkesmennene

Bungum, B., Forseth, U. & Kvande, E. (2016). Internasjonalisering og den norske modellen. I: Bungum, B., Forseth, U. & Kvande, E. (red.). *Den norske modellen. Internasjonalisering som ufordring og vitalisering*. Bergen: Fagbokforlaget.

Council of Europe (2001). Convention on cybercrime (23.XI.2001). Hentet fra https://www.coe.int/en/web/cybercrime/the-budapest-convention

Creswell, J. W. & Creswell, J. D. (2018). *Research design. Qualitative, quantitative & mixed methods approaches* (5. Utg). Los Angeles: Sage.

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cyber Security*, 5(1), 1 – 17. https://doi.org/10.1093/cybsec/tyz013

Dynes, R. R. (1993). Disaster reduction: The importance of adequate assumptions about social organization. *Sociological Spectrum*, 13(1), 175 – 192. https://doi.org/10.1080/02732173.1993.9982022

Egan, M. J. (2007). Anticipating future vulnerability: Defining characteristics of increasingly critical infrastructure-like systems. *Journal of Contingencies and Crisis Management*, 15(1), 4-17. https://doi.org/10.1111/j.1468-5973.2007.00500.x

Engen, O. A. H., Kruke, B. I., Lindøe, P. H., Olsen, K. H., Olsen, O. E. & Pettersen, K. A. (2016). *Perspektiver på samfunnssikkerhet*. Oslo: Cappelen Damm Akademisk.

Eskola, M. (2012). From risk society to network society: preventing cybercrimes in the 21st century. *Journal of Applied Security Research*, 7, 122-150. https://doi.org/10.1080/19361610.2012.631446

Eurostat (2021, juni). ICT specialists – statistics on hard-to-fill vacancies in enterprises. Hentet fra https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises

Eurostat (2023, mai). ICT specialists in employment. Hentet fra https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment#Number_of_ICT_specialists

Flin, R., O'Connor, P. & Crichton, M. (2008). *Safety at the sharp end. A guide to non-technical skills*. CRC Press.

Foucault, M. (1978). *The history of sexuality. Volume 1: An introduction*. New York: Pantheon House, Inc.

Foucault, M. (2002). *Forelesninger om regjering og styringskunst*. Oslo: Cappelen akademisk.

Giacomello, G. & Pescaroli, G. (2019). Managing Human Factors. I: Kott, A., Linkov, I. (red.) *Cyber Resilience of Systems and Networks. Risk, Systems and Decisions*. Springer, Cham. https://doi.org/10.1007/978-3-319-77492-3_11

Ham, D.-H. (2020). Safety-II and resilience engineering in a nutshell: An introductory guide to their concepts and methods. *Safety and Health at Work*, 12(1), 10-19. https://doi.org/10.1016/j.shaw.2020.11.004

Hammersley, M. (2017). Interview data: a qualified defence against the radical critique. *Qualitative research*, 17(2), 173-186. https://doi.org/10.1177/1468794116671988

Heldal, F. & Antonsen, S. (2014). Team leadership in a high-risk organization: the role of contextual factors. *Small Group Research*, 45(4), 376 – 399. https://doi.org/10.1177/1046496414533617

Holling, C. T. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4, 1 – 23. http://www.jstor.org/stable/2096802
Hollnagel, E. (2013). Resilience engineering and the built environment. Building Research & Information, 42(2), 221 – 228. https://doi.org/10.1080/09613218.2014.862607
Hollnagel, E. (2015). Introduction to the Resilience Analysis Grid (RAG). A technical note. Hentet fra https://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf
Hollnagel, E., Wears, R. L. & Braithwaite, J. (2015). From Safety-I to Safety-II. A white paper. Hentet fra https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf
Hult, F. & Sivanesan, G. (2013). What good cyber resilience looks like. *Journal of Business Continuity & Emergency Planning*, 7(2), 112 – 125. https://www.ingentaconnect.com/content/hsp/jbcep/2014/00000007/00000002/art00004
Hydro (2014, 7. november). Vellykket bruk av Lean-prinsipper i Hydro. https://www.hydro.com/no-NO/media/news/2014/vellykket-bruk-av-lean-prinsipper-i-hydro/
Hydro (2019, 20. september). Hydro tildeles pris for åpenhet etter cyberangrepet. https://www.hydro.com/no-NO/media/news/2019/hydro-tildeles-pris-for-apenhet-etter-cyberangrep/
Hydro (2020, 14. oktober). Cyberangrep på Hydro. https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/
Haavik, T. K., Antonsen, S., Rosness, R. & Hale, A. (2019). HRO and RE: A pragmatic perspective. Safety Science, 117, 479-489. https://doi.org/10.1016/j.ssci.2016.08.010
Johansen, J. P., Almklov, P. G. & Mohammad, A. B. (2016). What can possibly go wrong? Anticipatory work in space operations. *Cogn Tech Work*, 18, 333-350. https://doi.org/10.1007/s10111-015-0357-8
Kongsvik, T., Albrechtsen, E., Antonsen, S., Herrera, I. A., Hovden, J. & Schiefloe, P. M. (2018). *Sikkerhet i arbeidslivet*. Fagbokforlaget.
Kripos (2023). *Cyberkriminalitet 2023. Politiets årlige temarapport om kriminalitet mot datasystemer og kriminalitet støttet av datasystemer*. Hentet fra https://www.politiet.no/aktuelt-tall-og-fakta/aktuelt/nyheter/2023/03/29/ny-cyberkrim-rapport---na-ser-vi-organiserte-cyberkriminelle-i-norge/
Kusenbach, M. (2003). Street phenomenology: the go-along as ethnographic research tool. *Ethnography*, 4(3), 455 – 485. https://doi.org/10.1177/146613810343007
Kvale, S. (1996). *Interviews, an introduction to qualitative research interviewing*. Thousand Oaks, CA: SAGE.
Linkov, I. & Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. I: Linkov, I. & Kott, A. (red.) *Cyber Resilience of Systems and Networks. Risk, Systems and Decisions*. Springer, Cham. https://doi.org/10.1007/978-3-319-77492-3_1
Linkov, I., Trump, B.D. & Fox-Lent, C. (2016). Resilience: approaches to risk analysis and governance. I: Florin, M. -V. & Linkov, I. (red.) *IRGC resource guide on resilience*. Lausanne: EPFL International Risk Governance Center (IRGC). https://doi.org/10.5075/epfl-irgc-228206
Mark, M. S., Tømte, C. E., Næss, T. & Røsdal, T. (2019). Leaving the windows open – økt mangel på IKT-sikkerhetskompetanse i Norge. *Norsk Sosiologisk Tidsskrift*, 3(3). https://doi.org/10.18261/issn.2535-2512-2019-03-02
Mathiesen, I. H. & Volckmar-Eeg, M. G. (2022). En abduktiv tilnærming til institusjonell etnografi – et bidrag til sosiologisk kunnskapsutvikling. *Norsk Sosiologisk Tidsskrift*, 6(1), 9 – 23. https://doi.org/10.18261/nost.6.1.2

McGuire, M. (2012). *Organised Crime in the Digital Age*. London: John Grieve Centre for Policing and Security.
Miljødirektoratet (2023*). Microplastics in Norwegian coastal areas, rivers, lakes and air* (MIKRONOR1). Hentet fra https://www.miljodirektoratet.no/publikasjoner/2023/januar-2023/microplastics-in-norwegian-coastal-areas-rivers-lakes-and-air-mikronor1/
Mo, A. K. (2021, 1. september). Når krisen kommer. *NRK*. Hentet fra https://www.nrk.no/innlandet/xl/beredskap-i-norge_-slik-er-norske-kommuner-forberedt-pa-krise-1.15612587
Nasjonal Sikkerhetsmyndighet (2022a, 23. mars). *Sikkerhetskonferansen 2022*. Hentet fra https://nsm.no/aktuelt/sikkerhetskonferansen-2022
Nasjonal Sikkerhetsmyndighet (2022b). *Nasjonalt digitalt risikobilde* (nasjonalt digitalt risikobilde 2022). Hentet fra: https://nsm.no/aktuelt/digitalt-risikobilde-2022-cyberangrep-har-blitt-hverdagskost
Nasjonal Sikkerhetsmyndighet (u.å. a). Dette er NSM. Hentet fra: https://nsm.no/om-oss/dette-er-nsm/
Nasjonal Sikkerhetsmyndighet (u.å. b). Dette gjør NSM. Hentet fra: https://nsm.no/om-oss/ledige-stillinger/dette-gjor-nsm/
Naylor, R. T. (2003). Towards a general theory of profit-driven crimes. *The British Journal of Criminology*, 43(1), 81-101. http://www.jstor.org/stable/23638918
NOU 1985:31 (1985). *Datakriminalitet – straffelovrådets utredning om datakriminalitet*. Oslo: Justis- og politidepartementet.
NOU 2015:13 (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Oslo: Departementenes sikkerhet- og serviceorganisasjon.
NTB (2022, 16. september). Etterforskere fant krypteringsnøkler og hjalp Hydro å få tilbake stjålne data. *Dagsavisen*. Hentet fra https://www.dagsavisen.no/nyheter/innenriks/2022/09/16/etterforskere-fant-krypteringsnokler-og-hjalp-hydro-a-fa-tilbake-stjalne-data/
Næringslivets Sikkerhetsråd (2022). *Mørketallsundersøkelsen 2022*. Hentet fra https://www.nsr-org.no/aktuelt/morketallsundersokelsen-2022-er-na-tilgjengelig
Patriarca, R., Bergström, J., Gravio, G. D. & Costantino, F. (2018). Resilience engineering: current status of the research and future challenges. *Safety Science*, 102, 79 – 100. https://doi.org/10.1016/j.ssci.2017.10.005
Payne, G. & Williams, M. (2005). Generalization in qualitative research. *Sociology*, 39(2), 295-314. https://doi.org/10.1177/0038038505050540
Petroleumstilsynet (2017). *Prinsipper for barrierestyring i petroleumsvirksomheten – barrierenotat 2017*. Hentet fra https://www.ptil.no/fagstoff/utforsk-fagstoff/fagartikler/2017/barrierenotat/
Politiet (u.å. a). Nasjonalt cyberkrimsenter. Hentet fra https://www.politiet.no/om-politiet/organisasjonen/sarorganene/kripos/kripos-hovedarbeidsomrader/nasjonalt-cyberkrimsenter/
Politiet (u.å. b). Organisert kriminalitet. Hentet fra https://www.politiet.no/rad/organisert-kriminalitet/
Politiets sikkerhetstjeneste (2022a, 11. Februar). Nasjonal Trusselvurdering 2022. Hentet fra https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/
Politiets sikkerhetstjeneste (2022b, 18. Mars). PST vurderer etterretningstrusselen fra Russland i Norge som økt. Hentet fra https://www.pst.no/alle-artikler/pressemeldinger/oppdatert-trusselvurdering-pst-ser-en-okt-etterretningstrussel-fra-russland-i-norge/

Ragusa, A., Notarstefano, V., Svelato, A., Belloni, A., Gioacchini, G., Blondeel, C., …Giorgini, E. (2022). Raman Microspectroscopy Detection and Characterisation of Microplastics in Human Breastmilk. *Polymers*, 14(13), 1 – 14. https://doi.org/10.3390/polym14132700

Regjeringen (2019). *Nasjonal strategi for digital sikkerhet*. Hentet fra https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Regjeringen (2021, 14. oktober). Digital sikkerhet. Hentet fra: https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/digital-sikkerhet/id2340011/

Roege, P.E. et al. (2017). Bridging the Gap from Cyber Security to Resilience. I: Linkov, I., Palma-Oliveira, J. (red.) *Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security*. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-1123-2_14

Roulston, K. (2010). Considering quality in qualitative interviewing. *Qualitative research*, 10(2), 199 – 228. https://doi.org/10.1177/1468794109356739

Schiefloe, P. M. (2017). Pentagonanalyse – en helhetlig modell for sikkerhet i organisasjoner. I: Antonsen, S., Heldal, F. & Kvalheim, S. A. *Sikkerhet og ledelse* (281-301). Oslo: Gyldendal Akademisk.

Schjølberg, S. (2017). *Cyberkriminalitet*. Oslo: Universitetsforlaget.

Schultz, E. (2005). The human factor in security. *Computers & Security*, 24, 425-426. https://doi.org/10.1016/j.cose.2005.07.002

Sohlberg, P. & Sohlberg, B. M. (2020). *Kunnskapens former. Vetenskapsteori, forskningsmetod och forskningsetik*. Stockholm: Liber.

Solbakken, H. (2021, 10. januar). Sensitiv pasientinformasjon kan være på avveie etter dataangrep. *NRK*. Hentet fra: https://www.nrk.no/innlandet/ostre-toten-kommune-angrepet-av-hackere-_-pasientinformasjon-og-helsedata-kan-vaere-pa-avveie-1.15321398

Solms, R. V. & Niekerk, J. V. (2013). From information security to cyber security. *Computers & Security*, 38, 97 – 102. https://doi.org/10.1016/j.cose.2013.04.004

Stavland, B. & Bruvoll, J. A. (2019). *Resiliens – hva er det og hvordan kan det integreres i risikostyring?* (FFI Rapport 19/00363). Hentet fra https://www.ffi.no/publikasjoner/arkiv/resiliens-hva-er-det-og-hvordan-kan-det-integreres-i-risikostyring

Steen, R., Haakonsen, G., & Patriarca R. (2022). «Samhandling»: on the nuances of resilience through case study research in emergency response operations. *Journal of Contingencies and Crisis Management*, 30(3), 257 – 269. https://doi.org/10.1111/1468-5973.12416

Stolt-Nielsen, H. & Lysberg, M. (2021). Dataangrepet kostet Hydro 800 millioner kroner. Nå er det kriminelle nettverket avdekket. *Aftenposten*. https://www.aftenposten.no/norge/i/47WR3o/dataangrepet-kostet-hydro-800-millioner-kroner-naa-er-det-kriminelle-nettverket-avdekket

Straffeloven (2005). Lov om straff. Hentet fra: https://lovdata.no/lov/2005-05-20-28

Suchman, L. (1985). *Plans and situated actions: the problem of human-machine communication*. Palo Alto, California, Xerox.

Thomstad, A. B. (2019). Totalforsvaret i et militært perspektiv. I P. M. Norheim-Martinsen (red.), *Det nye totalforsvaret* (s. 41-61). Oslo: Gyldendal.

Thon, R. (2020). Bedriftene må være åpne om dataangrep. Hentet fra https://nsm.no/hold-deg-oppdatert/meninger/bedriftene-ma-vare-apne-om-dataangrep

Tjora, A. (2018). *Kvalitative forskningsmetoder i praksis* (3. utg.). Oslo: Gyldendal.

Triplett, W. J. (2022). Addressing human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2, 573-586. https://doi.org/10.3390/jcp2030029

Trøen, M. I. N., Vogt, L. F. & Kessel, D. (2021, 30. mars). Bekreftar at personsensitiv data er lekka etter dataangrep i Østre Toten. *NRK*. Hentet fra https://www.nrk.no/innlandet/info-som-hackarar-fekk-ut-fra-ostre-toten-kommune-kan-ha-hamna-pa-det-morke-nettet-1.15439495

van der Kleij, R. & Leukfeldt, R. (2019). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. I: Ahram, T., Karwowski, W. (red.) *Advances in Human Factors in Cybersecurity. AHFE 2019. Advances in Intelligent Systems and Computing*, vol 960. Springer, Cham. https://doi.org/10.1007/978-3-030-20488-4_2

Vasudevan, S., Piazza, A. & Carr, M. (2022). Qualitative factors in organizational cyber resilience. *2022 International Conference on Cyber Resilience (ICCR*), 1 – 5. https://doi.org/10.1109/ICCR56254.2022.9995762

Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly*, 38(4), 628 – 652. https://doi.org/10.2307/2393339

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P. & Fu, X. (2018). Cybersecurity for digital manufacturing. *Journal of Manufacturing*, 48(c), s. 3-12. https://doi.org/10.1016/j.jmsy.2018.03.006

Yu, D. J. et al. (2020). Towards general principles for resilience engineering. Risk Analysis, 40(8), 1509 – 1537. https://doi.org/10.1111/risa.13494

Østby, G. & Kowalski, S. J. (2022). *Hendelseshåndtering ved cyber- angrepet mot Østre Toten kommune* (90312702 CG6321). Hentet fra https://www.ototen.no/aktuelt/rapport-etter-dataangrepet.15279.aspx

Vedlegg

Vedlegg 1: SIKTs vurdering av meldeskjema

Sikt

Meldeskjema / Bits og bytes i risikosamfunnet. En kvalitativ masteroppgave om cyb... / Vurdering

Vurdering av behandling av personopplysninger

Referansenummer	Vurderingstype	Dato
129054	Standard	19.10.2022

Prosjekttittel
Bits og bytes i risikosamfunnet. En kvalitativ masteroppgave om cyberkriminalitet mot norsk arbeidsliv

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for samfunns- og utdanningsvitenskap (SU) / Institutt for sosiologi og statsvitenskap

Prosjektansvarlig
Petter Grytten Almklov

Student
Bjørnar Husby

Prosjektperiode
01.11.2022 - 31.05.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 31.05.2023.

Meldeskjema

Kommentar
OM VURDERINGEN
Personverntjenester har en avtale med institusjonen du forsker eller studerer ved. Denne avtalen innebærer at vi skal gi deg råd slik at behandlingen av personopplysninger i prosjektet ditt er lovlig etter personvernregelverket.

Personverntjenester har nå vurdert den planlagte behandlingen av personopplysninger. Vår vurdering er at behandlingen er lovlig, hvis den gjennomføres slik den er beskrevet i meldeskjemaet med dialog og vedlegg.

VIKTIG INFORMASJON TIL DEG
Du må lagre, sende og sikre dataene i tråd med retningslinjene til din institusjon. Dette betyr at du må bruke leverandører for spørreskjema, skylagring, videosamtale o.l. som institusjonen din har avtale med. Vi gir generelle råd rundt dette, men det er institusjonens egne retningslinjer for informasjonssikkerhet som gjelder.

TYPE OPPLYSNINGER OG VARIGHET
Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til den datoen som er oppgitt i meldeskjemaet.

LOVLIG GRUNNLAG
Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake.

Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER
Personverntjenester vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til

behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER
Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), og dataportabilitet (art. 20).

Personverntjenester vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER
Personverntjenester legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

Ved bruk av databehandler (spørreskjemaleverandør, skylagring eller videosamtale) må behandlingen oppfylle kravene til bruk av databehandler, jf. art 28 og 29. Bruk leverandører som din institusjon har avtale med.

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

MELD VESENTLIGE ENDRINGER
Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til oss ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde: https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/melde-endringer-i-meldeskjema

Du må vente på svar fra oss før endringen gjennomføres.

OPPFØLGING AV PROSJEKTET
Personverntjenester vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Vedlegg 2: Informasjonsskriv sendt ut til informanter

Vil du delta i forskningsprosjektet

«Bits og bytes i risikosamfunnet: en kvalitativ masteroppgave om cyberkrim mot norsk arbeidsliv»?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å utforske sårbarheten de norske virksomhetene står ovenfor i cyberlandskapet. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Samfunnet og arbeidslivet blir stadig mer digitalisert. Norge omtales ofte som et av de mest digitaliserte landene i verden, men digitalisering kan i enkelte tilfeller introdusere nye sårbarheter og nye problemstillinger. Tidligere i år fortalte Nasjonal Sikkerhetsmyndighet at Norge kunne forvente en økende andel cyberangrep fremover, både rettet mot individer så vel som virksomheter. Prosjektet har som formål å skape ny kunnskap og nye innsikter i en særdeles ny problemstilling. Sentrale spørsmål som er av interesse i denne masteroppgaven er: *hvordan har cyberkriminalitet bidratt til endring av bedriftssårbarhet og sikkerhet i virksomheten*? *Hva tenker de ansatte om cyberrisiko*?

Masteroppgaven tar utgangspunkt i et felt som er relativt sett er lite forsket på, men behovet for denne informasjonen øker parallelt. I dette prosjektet vil jeg derfor utforske denne tematikken med et semi-strukturert intervju. Det vil si at intervjuet følger en viss grad av struktur – i form av tematiske spørsmål – men intervjuspørsmålene åpner samtidig opp for refleksjon og tanker rundt tematikken.

Spørsmålene som stilles i løpet av intervjusituasjonen har ikke som formål å få innsyn i spesifikke sikkerhetsrutiner eller sensitiv informasjon. Intervjuet vil heller ikke kunne spores til den som deltar i intervjuet.

Hvem er ansvarlig for forskningsprosjektet?
Institutt for sosiologi og statsvitenskap ved NTNU er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
På grunnlag av din interesse har du fått et spørsmål om delta i min masteroppgave. Finner du imidlertid ut at du har ombestemt deg fra da du fikk den første forespørselen til du fikk dette informasjonsskrivet, er dette i orden. Mer om dine rettigheter finner du nedenfor.

Hva innebærer det for deg å delta?
Dersom du velger å delta i prosjektet vil du få en invitasjon til et intervju på omtrent 45 minutter. For at intervjuet kan formidles så nøyaktig som mulig, og for at relevant informasjon ikke utelates, vil intervjuet foregå med lydopptak. Senere vil lydopptaket transkriberes i et dokument. Opptak og transkribering slettes når prosjektet fullføres og avsluttes. Mer om ditt personvern kan du lese om nedenfor.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket. Det er kun undertegnede, herunder Bjørnar Husby, som har tilgang til dine opplysninger. Ditt navn og dine kontaktopplysninger erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data. Vedkommende vil ikke kunne gjenkjennes når prosjektet publiseres.

Hva skjer med personopplysningene dine når forskningsprosjektet avsluttes?
Prosjektet vil etter planen avsluttes/godkjennes ved utgangen av Mai 2023. Etter prosjektslutt vil dine opplysninger anonymiseres. Ved prosjektslutt slettes dine opplysninger og alle lydopptak.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra *Institutt for sosiologi og statsvitenskap* ved *NTNU* har Personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke opplysninger vi behandler om deg, og å få utlevert en kopi av opplysningene
- å få rettet opplysninger om deg som er feil eller misvisende
- å få slettet personopplysninger om deg
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger

Hvis du har spørsmål til studien, eller ønsker å vite mer om eller benytte deg av dine rettigheter, ta kontakt med:

- Bjørnar Husby (meg), tlf: 46836530, bjorhu@stud.ntnu.no
- Petter Grytten Almklov, petter.almklov@ntnu.no
- Vårt personvernombud: Thomas Helgesen, thomas.helgesen@ntnu.no

Hvis du har spørsmål knyttet til Personverntjenester sin vurdering av prosjektet, kan du ta kontakt med:

- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 53 21 15 00.

Med vennlig hilsen

Petter Grytten Almklov (Forsker/veileder)

Bjørnar Husby

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *Bits og bytes i risikosamfunnet. En kvalitativ masteroppgave om cyberkrim mot norsk arbeidsliv*, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i intervju med lydopptak

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

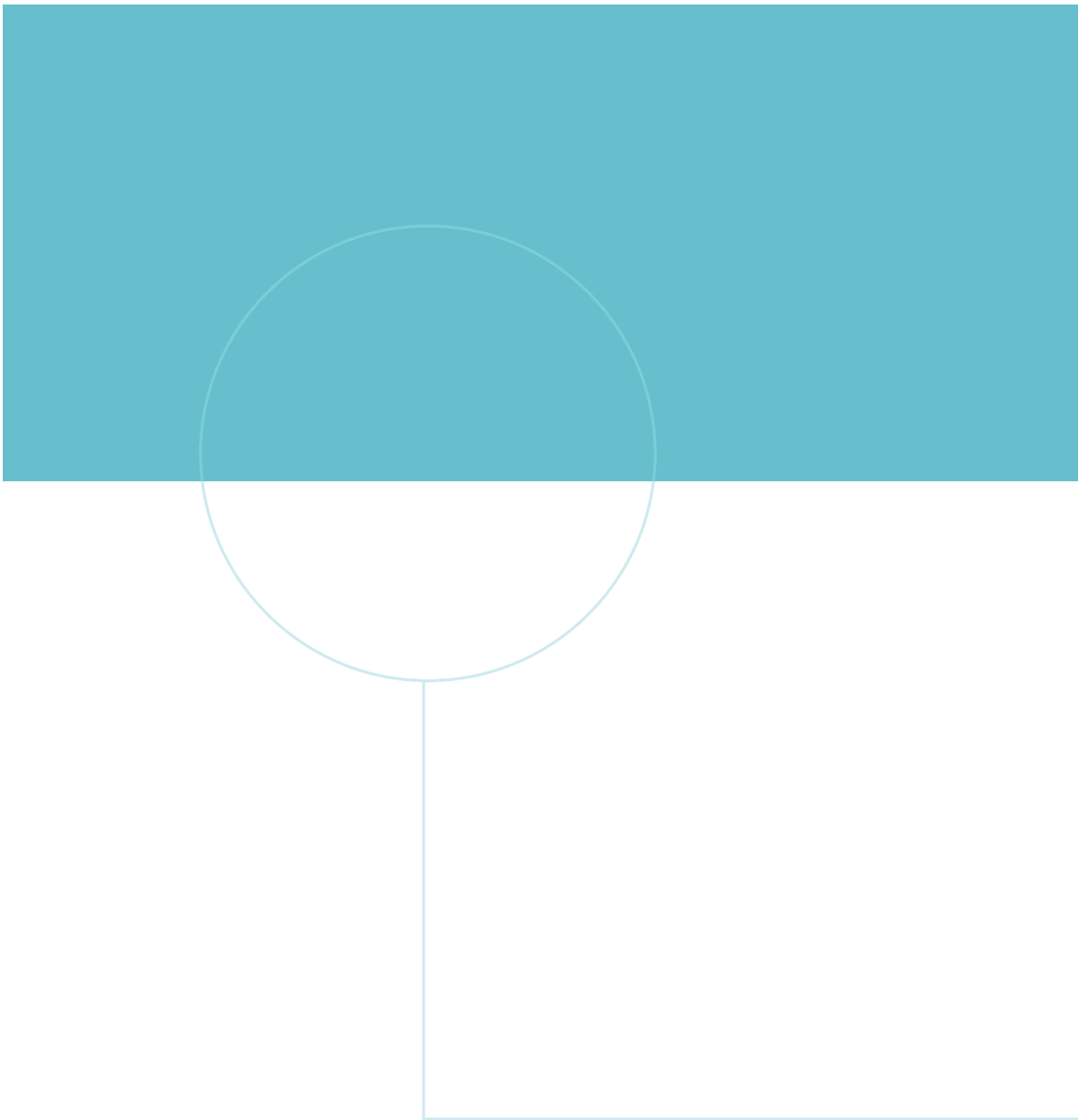
(Signert av prosjektdeltaker, dato)

Vedlegg 3: Intervjuguide

Overordnede spørsmål	Oppfølgingsspørsmål
Åpningsspørsmål 1. Hvor gammel er du? 2. Har du vært på jobb i dag?	
Den ansattes stilling i virksomheten 1. Hvor lenge har du vært ansatt i virksomheten? 2. Hvilken stilling har du? 3. Hvilken utdanning har du? Fagbrev? 4. Kan du beskrive en vanlig arbeidsdag? 5. Hvilke typiske arbeidsoppgaver har du? 6. Hvem forholder du deg vanligvis til?	Hvor lenge har du vært i stillingen? Har du noen kurs i tillegg? Har du noen som jobber under deg? Forholder du deg til interne/eksterne, i så fall; hvem?
IKT-kompetanse 1. Hva legger du i begrepet «risiko»? 2. Hva legger du i begrepet «cybersikkerhet»? 3. Kan du beskrive din IKT-kompetanse? 4. Kan du beskrive din digitale bevissthet? 5. Hvor mye av det daglige arbeidet foregår på en datamaskin / på internett? 6. Hvor mye av dette foregår innenfor OT og IT? 7. Kan du forklare hvor avhengig du er av teknologi i det daglige arbeidet?	Har du noen kurs innen IKT/informasjonssikkerhet/cybersikkerhet? I det private og i arbeid, hvilke sikkerhetstiltak gjennomfører du selv? Hvilken type arbeid er det snakk om innen IT og OT? Hvordan påvirker eventuell bortgang av systemer arbeidsoppgavene dine - og hvilke konsekvenser innebærer dette?
Før cyberangrepet 1. Før angrepet, fulgte dere råd fra sikkerhetsmyndighetene?	Kan du beskrive hvordan virksomheten forholdte seg til cybersikkerhet i forkant? Kan du beskrive virksomhetens bevissthet

2. Hvordan ble du oppdatert på sikkerhetsbildet? 3. Hadde det vært noen opplæring i cyber- og informasjonssikkerhet i forkant? 4. Ble det utarbeidet en håndteringsplan dersom et cyberangrep skulle skje?	om sårbarhet i det digitale rom i forkant av angrepet? Hvordan fikk du eventuelle oppdateringer? Hvilke faremomenter / ytre trusler var virksomheten mest opptatt av før angrepet? Hva innebar eventuelt håndteringsplanen?
Under cyberangrepet 1. Kan du beskrive den dagen du gikk på jobb og fant ut at virksomheten hadde blitt angrepet av et løsepengevirus? 2. Da angrepet skjedde, kan du fortelle om hvilke strakstiltak du gjennomførte? 3. Var du/dere i kontakt med noen under angrepet? 4. Ble det satt inn ekstra mannskap på jobb under angrepet? 5. På hvilken måte endret utførelsen av dine arbeidsoppgaver seg? Fortell konkret hva som endret seg.	Ble dere brifet / hadde møte med nærmeste leder – eventuelt hva ble diskutert i møtet? Hva ble gjort utilgjengelig? Kan du utdype de konsekvensene denne utilgjengeligheten hadde for deg? Sikre/stanse prosessnettverket? Ble forskjellige tiltak for IT/OT diskutert? Kontakt med interne og/eller eksterne?
Etter cyberangrepet 1. Mener du at sikkerhetsarbeid skal skje på sikkerhetsnivået eller noe alle bør ta del i? Eventuelt, hvordan da? 2. Etter angrepet, kan du beskrive hvordan du og virksomheten følger råd fra sikkerhetsmyndighetene? 3. Vil du si at din cyberbevissthet er annerledes i dag enn før? Kan du eventuelt forklare hvordan?	Kan du peke på tiltak enkeltpersoner kan gjøre? Gjennomfører dere kurs innenfor tematikken? Hvilke kurs? Hvordan opplever du eventuelt disse kursene? Blir ansatte direkte involvert i ulike øvelser eller scenarioer – eventuelt hvordan? Mener du at mennesker eller teknologi utgjør størst sårbarhet – kan du utdype hvorfor? Virksomheten skal etter planen introdusere ny teknologi de kommende årene – hva blir

4. I hvilken grad har dere hatt noen opplæring rundt digital sikkerhet etter hendelsen? 5. Har det vært noen treningsscenarioer? 6. Har det blitt etablert noen nye stillinger internt som har et fokus på cybersikkerhet / eller andre relevante stillinger? 7. Vet du hva du skal gjøre dersom IT- / OT-systemet er nede? 8. Hva anser du som den største sårbarheten mot cybersikkerhet i din virksomhet? Kan du utdype hvorfor? 9. Lærte du noe spesielt av cyberangrepet i ettertid?	mest krevende fremover og hvor ligger fokuset sikkerhetsmessig? Ser dere for der å ansette ny ekspertise innen sikkerhetsfaget?
Avrunding 1. Er det noe annet interessant du kan tenke deg å snakke om som ikke ble nevnt i løpet av intervjuet?	



NTNU

Kunnskap for en bedre verden