Figur 1 Illustrasjon hentet fra Istock og gjengitt med tillatelse.

Cyberhendelser i Norge ved en krise eller konflikt: Science fiction eller virkelighet?

Håkon Haukeland
01.06.2018

Universitet i Bergen
Institutt for sammenlignende politikk

SAMPOL 650 – Masteroppgave i Demokratibygging

Vår 2018

Forord

For noen år tilbake tenkte jeg at noe masteroppgave kommer jeg aldri til å skrive. Så feil kan man ta. Etter at en kollega viste meg dette studiet bestemte jeg meg for å søke. Jeg startet denne studiereisen høsten 2015 og har i perioden truffet mange nye mennesker, fått en hel del ny lærdom, som også er relevant i min jobb i Forsvaret. Så dette studiet vil jeg anbefale andre i Forsvaret å gjennomføre.

Så er det flere jeg må takke for at jeg har klart å stå løpet ut. Først er det rådgiver ved etter- og videreutdanning på UiB, Bjørg Hildeskår. Når jeg søkte opptak ble det kluss i innsending av papirene mine. De ble returnert fra UiB til meg uten at de var innom opptakskontoret for studiet. Hildeskår fant en god løsning på situasjonen slik at jeg kunne starte på studiet. Hildeskår har også hjulpet med ulike utfordringer i studieperioden når det har vært behov for det.

Det har vært en spennende reise med ny lærdom som har vært inspirerende og utfordrende. Takk til Terje Knudsen for et godt tilrettelagt og interessant studietilbud.

Så må jeg takke mine to veiledere ved Forsvarets Forskningsinstitutt. Torbjørn Kveberg og Torgeir Broen. De har holdt ut med mine spørsmål og eposter som har kommet ofte. De har gitt gode råd på veien, som jeg har lært mye av. Uten deres veiledning ville ikke dette vært mulig.

Jeg må også takke Liv Torill Lindgren som har vært trofast som korrekturleser gjennom hele studieperioden.

Sist men ikke minst må jeg takke min familie som har holdt ut med studiene mine i tillegg til pendlerhverdagen min mellom Askøy og Gardermoen. Uten støtte og tilrettelegging fra dem hadde ikke dette vært mulig.

Håkon Haukeland
Askøy 31. mai 2018

Sammendrag

I et demokrati er det viktig med ytringsfrihet og pressefrihet. Denne friheten er også nedfelt i de universelle menneskerettighetene. I Norge er ytringsfriheten nedfelt i grunnloven. I dag er mye av disse ytringene flyttet over i det digitale rom. Norge har hatt en stor digital utvikling i de senere år hvor stadig nye programmer, hjelpemidler og applikasjoner har ført til en effektivisering av menneskers hverdag. Norske allmenkringkastere og norske myndigheter har deltatt i denne utviklingen og tilbyr i dag mange nyhets-, radio- og tv tjenester via internett. Kommunikasjonen mellom norske myndigheter og den norske befolkningen har som hovedregel også blitt digital. Men hvor sårbart er dette i en krise eller konflikt? Problemstillingen for masteroppgaven er: *Hvordan kan cyberhendelser i krise og konflikt utfordre norske allmenkrigkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon?* Problemstillingen besvares gjennom å finne eksempler på hendelser ved å studere cyberhendelser i Estland, Georgia og Ukraina og deretter intervjue NRK og Kommunikasjonsenheten i Forsvarsdepartementet. Oppgaven slutter at cyberproblematikk har stor prioritet i sikkerhetsarbeidet for å kunne håndtere slike hendelser dersom de skulle inntreffe. Det ble også identifisert flere typer av hendelser i cyberdomenet som kan påvirke norske allmenkringkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon.

Innholdsfortegnelse

Introduksjon

Det norske samfunnet blir stadig mer digitalisert. I følge FNs oversikt over internettbrukere er Norge et av de mest digitaliserte land i verden (FN 2018). Men økt digitaliseringen gir også grobunn for sårbarheter som kan ramme digital kommunikasjon (Nasjonal Sikkerhetsmyndighet 2018). Problemstillingen til denne masteroppgaven er:

Hvordan kan cyberhendelser i krise og konflikt utfordre norske allmenkrigkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon?

I 2015 kom det ut en Norsk Offentlig Utredning kaldt *Digital sårbarhet – sikkert samfunn.* Den beskriver hvordan hverdagen til mennesker i Norge har blitt endret de siste 20 årene. Teknologi og internett er blitt inkludert i et stadig større utvalg av teknologiske hjelpemidler. Med det fortsetter internett å vokse som infrastruktur og blir stadig viktigere i menneskers liv. Ikke bare blir slik teknologi inkludert i apparater som hvitevarer, men kritisk infrastruktur og samfunnsmessige funksjoner er også blitt digitalisert og sentralisert (NOU 2015:13: 15-19). Utredningen viser hvor viktig og hvor avhengig Norge og den norske befolkningen er blitt av det digitale rom. Men utviklingen fører også med seg nye sårbarheter som kan utnyttes for kriminalitet eller de kan utnyttes i statlige krise eller konflikter (NOU 2015:13: 19 og Nasjonal Sikkerhetsmyndighet (NSM) 2018). Når så store deler av hverdagen og livet til mennesker dreier seg rundt digitale hjelpemidler, der i blant pc, mobiltelefon og nettbrett, er det også i det digitale rom norske allmenkringkastere og norske myndigheter må være for å kommunisere med sitt publikum og befolkningen for øvrig.

De første norske avisene kom på internett i 1995. Først ut av de riksdekkende avisene var Dagbladet, som kom ut 8. mars 1995 (Omdahl 2010). Fra da og frem til i dag har den digitale utviklingen for mediene ført til at medienes nettutgaver har større lesertall enn den tradisjonelle papiravisen. (Medienorge 2018a). Øvrige nyhetsmedier har fulgte etter, og i dag har alle de store riksdekkende mediene som NRK og TV2, egnet nettsider hvor nyheter publiseres både under og etter en hendelse. En utvikling hvor mediene sin digitale virksomhet stadig ekspanderer i det digitale rom, gjør dem mer sårbare for uønskede hendelser. Dette kan påvirke medienes muligheter for å publisere nyhetssaker og viktig informasjon, som norske myndigheter ønsker å meddele norske borgere.

Norske myndigheter har digitalisert sin kommunikasjon ut til den norske befolkning, og har opprettet et eget direktorat, Direktorat for Forvaltning og IKT (Difi), for å ivareta den digitale omstillingen (Direktorat for forvaltning og IKT 2018). I dag er hovedregelen at kommunikasjon mellom en norsk innbygger, stat, fylkeskommune og kommune skal være digital (Direktorat for forvaltning og IKT 2014). Kommunikasjonen med den enkelte innbygger innebærer at den enkelte bruker må logge seg inn på nettsider eller applikasjoner på nettbrett eller mobiltelefon. Det betyr at en bruker må logge seg inn gjennom nettsider på en pc eller applikasjoner på nettbrett eller mobiltelefon. Det mest fremtredende eksempelet på digital kommunikasjon mellom norske myndigheter og en innbygger i Norge er skattemeldingen. Den sendes digitalt til hver enkelt innbygger via den digitale plattformen Altinn. Her må den enkelte bruker logge seg på for å lese og gjøre eventuelle endringer i skattemeldingen, før den leveres elektronisk gjennom samme plattform.

Men de nye mulighetene for effektivitet og økt produksjon gir også større sårbarhetsflater som kan utnyttes av en tredjepart til kriminelle handlinger eller politiske aksjoner (NSM 2018). Ved bruk av cybermakt kan tredjeparten nekte tilgang til bestemte nettsteder, endre innholdet på ulike nettsider, eller de kan søke etter informasjon som igjen kan selges videre for profitt (NOU 2015:13).[1] Hendelser i cyberdomenet er ikke en ny ting. En av de første hendelsene ble oppdaget i 1986.[2] Tyske hackere ble avslørt i å bryte seg inn i forskningssenter og militære installasjoner for å søke etter hemmelig informasjon som kunne selges til KGB (Healey 2013). Den mest avanserte hendelsen ble oppdaget i Iran og ble kjent som Stuxnet. En dataorm som var programmert til å fysisk ødelegge sentrifuger som iranerne brukte i sitt atomprogram (Rid 2013).

I 2007 kom, det som til da, var den mest alvorlige bruken av cybermakt. Både offentlige og private aktører i Estland ble rammet av cyberangrep.[3] Resultatet var at estiske myndigheters nettsider var tidvis utilgjengelige, kommunikasjon mellom departementene ble rammet og mediebedrifter måtte begrense sin virksomhet med å blokkere forespørsler fra utenlandske nettbrukere for å kunne opprettholde sin virksomhet (Russell 2014). Estland hadde på det

[1] Cybermakt er en samlebetegnelse for handlinger i cyberdomenet som har ondsinnede hensikter
[2] Cyberdomenet er fysiske og logiske sammenkoblinger av flere informasjonssystemer. Dette inkluderer ulike nettverksenheter, infrastruktur for kommunikasjon, også mobiltelefoni, lagringsmedier og data (Forsvarsdepartementet 2014).
[3] Cyberangrep er et "angrep" i cyberdomenet og må ikke forveksles med maktbruk mellom to parter.

tidspunktet digitalisering som et satsingsområde. Da Estland ble rammet av cybermakt ble så mye som 95 prosent av alle finanstransaksjoner gjort digitalt (Russell 2014).

Jeg vil i denne masteroppgaven studere cyberhendelser i tre caser, Estland, Georgia og Ukraina. Casene vil danne grunnlag for intervjuer hvor casene og intervjuene vil forsøke å svare på problemstillingen.

Teori

I et autoritært styre eller i et konfliktområde vil myndighetene kunne bruke media til å utøve propaganda overfor befolkningen for å sikre sympati for sitt styre eller sitt syn. (Jarstad og Sisk, 2008:87). Da Vladimir Putin ble president i Russland i år 2000 startet han med å innføre et nytt styresystem. Systemet som ble innført ligner på en pyramide hvor presidenten er på toppen, og institusjoner som parlament, domstoler, regionale myndigheter og presse styres av presidenten (Bogen, 2018). Pressen i Russland vil ikke lenger være en fri presse, og ytringsfriheten vil ikke bli ivaretatt. På denne måten vil president Putin også kontrollere hvilken informasjon som blir gitt ut til befolkningen, og det er ikke rom for kritiske ytringer (Bogen 2018).

I et demokrati vil man finne den motsatte situasjon. Pressen skal være uavhengig av myndighetene, slik at den kan gjengi meninger, rapportere om politiske saker og være kritisk til den sittende makten. Publisering av viktig informasjon som må ut til befolkningen er også en sentral oppgave for media. (Jarstad og Sisk, 2008: 87).

Ytringsfrihet er en viktig bærebjelke i et demokrati. Ytringsfrihet er nedfelt i de universelle menneskerettighetene paragraf 19 heter det:

> *Enhver har rett til menings- og ytringsfrihet. Denne rett omfatter frihet til å hevde meninger uten innblanding og til å søke, motta og meddele opplysninger og ideer gjennom ethvert meddelelsesmiddel og uten hensyn til landegrensen* (FN 1948).

Norske styresmakter har gjennom den norske grunnloven ytterligere presisert retten til ytringsfrihet i Grunnlovens paragraf 100 (Grunnloven, §100, 2014). Diamond (2008: 21-22) presiserer at det ikke kan være demokrati dersom det ikke er ytringsfrihet. Medias rolle er en

forlenget arm til ytringsfriheten. Den gir en stemme til mennesker og organisasjoner i det offentlige rom, og stemmen kan gjerne være kritisk til et lands myndigheter.

I Norge har mediene selv tatt samfunnsansvar. I 1936 vedtok Pressens faglige utvalg *Vær Varsom-plakaten.* Dette er et sett med etiske retningslinjer som gjelder for radio, TV, trykt presse og nettpublikasjoner i Norge. Plakaten har vært revidert en rekke ganger, sist i 2015. Gjennom *Vær Varsom-plakaten* har mediene vedtatt og definert sitt eget samfunnsoppdrag. Allerede under punkt én kommer dette til syne (Presseforbundet 2015):

1. *Pressenes Samfunnsrolle*
   - *1.1. Ytringsfrihet, informasjonsfrihet og trykkefrihet er grunnelementer i et demokrati. En fri og uavhengig presse er blant de viktigste institusjoner i et demokratisk samfunn.*
   - *1.2. Pressen ivaretar viktige oppgaver som informasjon, debatt og samfunnskritikk. Pressen har et spesielt ansvar for at ulike syn kommer til uttrykk.*
   - *1.3. Pressen skal verne om ytringsfriheten, trykkefriheten og offentlighetsprinsippet. Den kan ikke gi etter for press fra noen som vil hindre offentlig debatt, fri informasjons formidling og fri tilgang til kildene. Avtaler om eksklusiv formidling av arrangementer skal ikke være til hinder for fri nyhetsformidling.*
   - *1.4. Det er pressens rett å informere om det som skjer i samfunnet og avdekke kritikkverdige forhold. Det er pressenes plikt å sette kritisk søkelys på hvordan mediene selv fyller sin samfunnsrolle.*
   - *1.5. Det er pressens oppgave å beskytte enkeltmennesker og grupper mot overgrep eller forsømmelser fra offentlige myndigheter, institusjoner og private foretak eller andre.*

Alle redaktører og journalister har et ansvar for å følge *Vær Varsom-plakaten* i sitt daglige virke. Når mediene har dette som et etisk ståsted, legger det til rette for at norske medier har plikt og rett til å formidle meningsytringer, og formidle viktig informasjon ut til den norske befolkning. Dette gjelder også det som kritiserer myndighetene og deres samarbeidspartnere.

Norge har en statlig eid allmenkringkaster, NRK. I 2007 vedtok Stortinget et måldokument for NRK som blir kalt NRK-plakaten. Denne ble sist revidert i 2017 gjennom Stortingsmeldingen *Eit moderne og framtidsretta NRK*. Formålet med NRK-plakaten som måldokumentet er at den skal sette rammene for NRK sitt samfunnsoppdrag, og inngå i NRK sine vedtekter. NRK sitt samfunnsansvar er spesifisert i paragraf 12, 13 og 14, hvor det står at NRK skal styrke

demokratiet, verne om ytringsfriheten og ytringsvilkårene samt at NRK har et selvstendig ansvar for å sikre dette (NRK, 2018). Til tross for at mediekanalen NRK er eid av norske myndigheter, slår Stortinget altså fast at NRK skal operere uavhengig av myndighetene i sitt redaksjonelle innhold.

I NRK-plakaten har Stortinget også gitt NRK et beredskapsansvar ovenfor den norske befolkningen. I paragraf 23 heter det: *NRK skal ha et særlig beredskapsansvar. NRK skal legge til rette for at styremaktene kan nå ut til befolkningen med informasjon over kringkastingsnettet ved nasjonale kriser eller katastrofer* (NRK 2018a). Paragrafen gir NRK et klart ansvar for å gi ut viktig informasjon til den norske befolkningen dersom det skulle oppstå en krise i Norge. Det skal de kunne gjøre gjennom bruk av sitt kringkastingsnettverk. Kringskastingsnettverket skal være tilgjengelig på minst en distribusjonsplattform for hele befolkningen, noe som gjør NRK godt egnet til formålet - å nå ut til hele befolkningen i en krisesituasjon (NRK, 2018a).

En stat står alltid overfor utfordringer som spionasje, sabotasje og subversjon. Av disse tre er subversjon den mest utfordrende, og har eksistert lenge før cyberdomenet kom til. (Rid 2013: 113). Begrepet subversjon ble til på 1700-tallet da den irske taleren Edmund Burke skrev: *To make a revolution is to subvert the ancient state of our country* (Rid 2013: 116-117). Gjennom tiden har begrepet endret seg noe. Subversjon kan defineres som aktivitet hvor myndigheters troverdighet, integritet og grunnlov blir undergravd av aktivister. Målet med subversjon kan være å kaste den etablerte makten i et land. En mer vanlig variant av subversjon er at aktiviteten rettes mot mindre organisasjoner eller enkeltpersoner for å skade deres sak eller autoritet (Rid 2013: 116). Eksempler på subversjon kan være protester som den arabiske våren, dyrevernaktivisme eller Anonymous hacktivister (Rid 2013: 113-114).

Subversjon er altså drevet av en motivasjon for en felles sak som samler aktivister (Rid 2013: 123). Cyberhendelser som har en politisk agenda kan betegnes som subversjon (2013: 113-116). I Estland og Georgia ble cybermakt benyttet mot medier og myndigheter hvor det originale innholdet på nettsidene ble endret ved nettsidevandalisme, eller gjort utilgjengelig med tjenestenektangrep (Rid 2013: 6-8).[4] Slike angrep mot media kan få konsekvenser for medienes muligheter for å publisere sitt redaksjonelle innhold (Healey 2013). I dagens

[4] Tjenestenektangrep, eller Distributed Denial of Service Attacks (DDoS), er et koordinert angrep som instruerer datamaskiner til å sende store mengder trafikk mot et bestemt mål for å overbelaste båndbredden og serverens evne til å svare på forespørsler. Et slikt angrep kan gjøre tjenester og nettsider utilgjengelig (Russell 2014).

teknologiske samfunn, hvor aktivister har tilgang på internett, er verktøyene for å starte en aksjon blitt mye mer tilgjengelig. Aktivister kan, gjennom sosiale medier eller andre elektroniske kommunikasjonsmidler, enklere samles og koordinere angrep eller en aksjon i cyberdomenet. Men selv om verktøyene er blitt mer tilgjengelige, betyr ikke dette at subversjon er blitt enklere å gjennomføre (Rid, 2013: 115).

Cyberhendelser som har en politisk agenda kan betegnes som subversjon (2013: 113-116). I Estland og Georgia ble cybermakt benyttet mot medier og myndigheter hvor det originale innholdet på nettsidene ble endret ved nettsidevandalisme, eller gjort utilgjengelig med tjenestenektangrep (Rid 2013: 6-8).[5] [6] Slike angrep mot media kan få konsekvenser for medienes muligheter for å publisere sitt redaksjonelle innhold (Healey 2013). I dagens teknologiske samfunn, hvor aktivister har tilgang på internett, er verktøyene for å starte en aksjon blitt mye mer tilgjengelig. Aktivister kan gjennom sosiale medier eller andre elektroniske kommunikasjonsmidler enklere samle seg og koordinere seg. Også for å koordinere en aksjon i cyberdomenet.

Med den digitale utviklingen er nå mediene lett tilgjengelig ved bruk av en pc, nettbrett eller mobiltelefon. Som tidligere nevnt øker dette den digitale sårbarheten til mediene. En undersøkelse utført av Newscycle Solutions viser, ifølge Marsh (2015), at over 50 prosent av nyhetsmediene som deltok i undersøkelsen har vært utsatt for cyberhendeleser rettet mot sin virksomhet. Av disse hendelsen var 49 prosent tjenestenektangrep. Studien sier ikke noe om konsekvensene eller alvorlighetsgraden av tjenestenektangrepene, men det var de hendelsene som vakte størst bekymring. Tjenestenektangrepene virket å ha en politisk agenda, og var utført av hactivister. I samme undersøkelse kommer det frem at så mange som 39 prosent av mediebedriftene i undersøkelsen ikke hadde en form for beredskap eller sikkerhet rundt hendelser i cyberdomenet (Marsh, 2015).

[5] Tjenestenektangrep, eller Distributed Denial of Service Attacks (DDoS), er et koordinert angrep som instruerer datamaskiner til å sende store mengder trafikk mot et bestemt mål for å overbelaste båndbredden og serverens evne til å svare på forespørsler. Et slikt angrep kan gjøre tjenester og nettsider utilgjengelig (Russell 2014).
[6] Nettsidevandalisme er en form for hærverk hvor en aktør kaprere en nettside og publisere sitt eget innhold eller budskap gjennom tekst eller bilder på bekostning av det opprinnelige innholdet (TrendMicro 2018).

Metode

For å besvare problemstillingen gjennomføres først en kvalitativ komparativ casestudie av hendelser i cyberdomenet under en krise eller konflikt fra et utvalg caser. Denne studien anvendes til å generere et utvalg hendelser som kan skje i Norge dersom Norge skulle komme i en situasjon av krise eller konflikt. Resultatet vil danne grunnlag for intervjuer med relevante samfunnsaktører. For denne masteroppgaven vil det begrense seg til Kommunikasjonsenheten i Forsvarsdepartementet og NRK. Dette kapitelet vil forklare hvordan dette gjennomføres og drøfte styrker og svakheter opp mot å besvare problemstillingen.

Casene vil først bli studert og hendelser i cyberdomenet vil bli presentert for hver enkelt case slik hendelsene er blitt rapportert. I presentasjonen av casene vil det bli tatt med bakgrunnsinformasjon om konflikten, samt flere cyberhendelser som fant sted i konflikten. Dette illustrerer at hver enkelt case ikke var en isolert hendelse, men en del av en større kontekst.

Landene som er valgt som caser til oppgaven har en annen bakgrunnshistorie enn Norge. Estland, Georgia og Ukraina har alle vært en del av Sovjetunionen, som har vært en stor kontrast til Norge. Der Norge har vært en fri nasjon med medlemskap i NATO og senere også EØS, har det tre landene vært utsatt for et autoritært og undertrykkende styre gjennom Sovjetunionen (Egge 2017). Etter Sovjetunionens fall har alle de tre landene sett i retning vesten. I 2004 ble Estland medlem av NATO (NATO 2018). Georgia har et tett samarbeid med NATO, og har hatt det over en lenger periode (Russell 2014). I 2013 fremforhandlet Ukraina og EU en assosieringsavtale som ville ført Ukraina et steg nærmere medlemskap i EU (FN 2016). Overføringsverdien mellom hendelsene i disse landene og til Norge kan deles i to. Den ene er teknologisk. Cyberangrep har som mål og utnytte sårbarheter i et digitalt system, kompromittere nettsteder eller stjele passord informasjon (Andress og Winterfeld 2014: 22). På den måten er det teknologiske aspektet interessant i en norsk kontekst. Den andre årsaken er mer sikkerhetspolitisk. Norge har i likhet med de tre landene en grense til Russland. Det gjør at alle har et naboskap med en stormakt. Som casene senere vil vise, har alle landene et politisk anstrengt forhold til Russland. Gjennom flere uttalelser og hendelser i de senere årene er tonen mellom Russland og Norge også blitt mer anstrengt (Bogen 2018). NRK oppsummerer flere hendelser som understreker endringer i forholdet mellom Norge og Russland. Når norske myndigheter vedtok at amerikanske soldater kunne øve i Norge, kom det skarp kritikk fra

Russland. Når PST gikk åpent ut for å advare mot russiske agenter, førte det til en ny runde med skarp kritikk av Norge. En russisk avis, Kommersant, laget en reportasje om at norsk Svalbardpolitikk kan føre til en militær konfrontasjon. (NRK 2018b). For casene med Estland er det også en overføringsverdi i forhold til at både Norge og Estland er medlem av NATO. Når et NATO land blir utsatt for en serie hendelser i cyberdomenet i en krise eller konflikt er ikke det utenkelig at Norge kan oppleve det samme.

Den komparative casestudien vil forsøke å kartlegge på hvilken måter medier og myndigheter har vært utsatt for cybermakt i de krisene og konfliktene som har funnet sted. Intervjuene, som vil baseres på casene, vil bli gjennomført som samtaleintervju. Dette er en mer uformell intervjuform som egner seg for dybdeintervju (Ringdal 2013:242-244). Samtaleintervjuene vil søke å finne svar på hvordan NRK kan bli utsatt for cybermakt. Som igjen kan påvirke deres evne til å løse sitt samfunnsoppdrag og hvilke konsekvenser det kan ha for norske medier. I dette tilfellet NRK. Mål på hvordan evnen til krisekommunikasjon kan rammes, innhentes med samtaleintervju med Kommunikasjonsenheten i Forsvarsdepartementet, hvor masteroppgaven søker å finne svar på hvordan krisekommunikasjon ut til befolkningen kan ivaretas dersom norske myndigheter blir utsatt for cybermakt. Intervjuene gjennomføres som samtaleintervju via telefon.

Årsaken til samtaleintervju via telefon er de geografiske avstandene mellom Bergen, hvor studiet gjennomføres, og Oslo hvor NRK og Kommunikasjonsenheten i Forsvarsdepartementet har sine kontorer. Reisekostnadene er også betydelig større enn kostnadene for en telefonsamtale. Svakheten ved å gjennomføre intervjuet via telefon er at det ikke er mulig å observere kroppsspråk og reaksjoner som intervjuobjektet har underveis i intervjuet (Ringdal 2013: 242-244). Min vurdering er at tematikken i masteroppgaven ikke er av en slik karakter at slike observasjoner vil ha noen innvirkning på informasjonen som informanten kan bidra med. Ved samtaleintervju over telefon er det viktig med oppfølgingsspørsmål, for å oppklare eventuelle uklarheter i informasjonen som informanten gir. Intervjuobjektene vil bli tilbudt sitatsjekk for å sikre at intervjuobjektet er tolket riktig og at de kan stå inne for det som blir presenteres i oppgaven.

Et samtaleintervju følger ikke en fastlagt mal, noe som gir intervjuformen en mulighet for å gå i dybden på et tema. Formen på intervjuet er uformell slik at det kan bli en diskusjon rundt et bestemt tema framfor et spørreskjema som har en fast mal. (Ringdal 2013: 242-244). Men selv

om ikke et samtaleintervju ikke trenger en fast mal, vil jeg i denne masteroppgaven utarbeidet et intervjuskjema som baserer seg på funn gjort i casene. På den måten sikrer jeg å få med riktig og relevant informasjon fra intervjuobjektene (Se vedlegg 1 og 2).

Avgrensinger

Ideelt sett burde det bli intervjuet flere medier for å få en bredere datainnsamling til å svare på problemstillingen. Valget om å gjennomføre intervju kun med ett mediehus, NRK, er tatt på bakgrunn av tid tilgjengelig, all den tide masteroppgaven gjennomføres som et deltidsstudium. NRK er valgt på bakgrunn av at de er en statseid nyhetsformidler som har et fastlagt samfunnsansvar som er vedtatt i Stortinget.

I tilfeller hvor det er definert en trussel, kan det være utarbeidet beredskapsplaner for å hindre eller motstå en hendelse. Nasjonal Sikkerhetsmyndighet (NSM) anbefaler at bedrifter utarbeider en slik plan for hendelser i cyberdomenet (NSM 2018). Masteroppgaven vil ikke se på eventuelle beredskapsplaner som mediebedrifter eller norske myndigheter kan ha utarbeidet, eller på hvilken effekt de kan eller vil ha dersom Norge skulle rammes av cybermakt. Masteroppgaven vil bare se på hvilke typer hendelser i cyberdomenet som kan påvirke medias evne til å løse sitt samfunnsoppdrag, og på norske myndigheters evne til krisekommunikasjon.

Konflikten i Ukraina har ikke funnet en permanent løsning og pågår fortsatt. Som casebeskrivelsen vil vise ble det undertegnet en våpenhvileavtale i 2015. Selv om denne roet situasjonen noe har den ikke fått slutt på konflikten. For å begrense omfanget, men samtidig få med de viktigste hendelsene, vil masteroppgaven konsentrere seg om cybermakt under Euromaidan-revolusjonen, cybermakt som var rettet mot presidentvalget på våren i 2014, cybermakt i forbindelse med parlamentsvalget høsten 2014 og hacking av det ukrainske strømnettet i 2015 og 2016.

Begrepsavklaringer

Masteroppgaven kommer til å bruke en del begreper som ikke alle bruker til daglig. En del begreper har også flere betydninger, avhengig av hvilken kilde som brukes for å finne en forklaring på begrepet. Et eksempel er begrepet *cyberdomenet* hvor FN har sin definisjon, NATO har en annen definisjon, mens USA har flere definisjoner (Andress og Winterfeld 2014). Målet med dette kapitelet er å beskrive og avklare hva denne masteroppgaven legger i begrepene som brukes.

I følge Forsvarsdepartementet (FD) (2014) sine retningslinjer er cyber et prefiks. Det vil si at det settes foran et meningsbærende ord med en henvisning til noe som skjer i cyberdomenet. For eksempel cyberangrep eller cybertrussel. Med cyberdomenet menes fysiske og logiske sammenkoblinger av flere informasjonssystemer. Det inkluderer nettverksenheter, infrastruktur for kommunikasjon, lagringsmedier og data. Dette inkludere også Mobiltelefoni (FD 2014). Cyberangrep, slik de er beskrevet i denne oppgaven, er handlinger som har til hensikt å skade eller påvirke personer, materiell eller konfidensialitet, integriteten, tilgjengeligheten eller autentisiteten til den som er utsatt for cyberangrep. Denne typen av angrep må ikke forveksles med maktbruk utenfor cyberdomenet. Cybermakt brukes her som samlebetegnelse for handlinger i cyberdomenet som har ondsinnede hensikter.

Hactivist er et begrep som første gang oppstod i Texas. En gruppe hackere kjempet mot myndigheter som drev sensur på internett. Gruppen hevdet at tilgang til informasjonen på internett var en menneskerett, og arbeidet deres førte til dannelse av prosjektet Hacktvismo. Hactivist er sammenslått av to ord, hacker og aktivist. Målet for en hactivist er å benytte den nyeste tilgjengelige teknologien for å gjøre sivil ulydighet, skape uro eller protestere mot en politisk beslutning. Forskjellen på en aktivist og en hacktivist er de teknologiske mulighetene for å handle raskt, gjennomføre aktivismen på tvers av landegrensene og anonymt (Singer og Friedman 2014).

Casestudier av cyberhendelser

Dette kapittelet vil presenter casene som masteroppgaven bygger på. Jeg vil vise at hendelsene i cyberdomenet ikke var isolerte hendelser, men en del av en større kontekst. For å beskrive dette vil jeg først helt kort oppsummere bakgrunnen for den krisen, eller konflikten som oppstod i case landene. Så vil jeg presentere cyberhendelsene sammen med hendelsene utenfor cyberdomenet, slik at ikke cyberhendelsene står igjen som isolerte hendelser. På den måten vil jeg vise at hendelsen i cyberdomenet var del av en større kontekst.

Estland

Oppbygging til konflikt

Bakgrunnen for krisen i 2007 ligger i estere og russeres vidt forskjellige perspektiv på den russiske frigjøringen og okkupasjonen i følge med andre verdenskrig (Russell 2014). Esterne ser på frigjøringen som et bytte av okkupasjonsmakt, mens russerne på sin side mener esterne er utakknemlige. I forbindelse med frigjøringen reiste Sovjetunionen et krigsminnesmerke i bronse av den ukjente soldat og den ble reist i 1947 (Healey 2013 og Russell 2014). Bronsesoldaten er iført en sovjetisk uniform, som var samme uniformen sovjetiske soldater brukte når de drepte eller deporterte esterne som deltok i andre verdenskrig på Nazi-Tysklands side (Jackson 2007).

I 2005 var det seksti år siden andre verdenskrig var over, og i den forbindelse ble den estiske presidenten invitert til Moskva for å markere slutten på krigen. Den estiske presidenten takket nei til invitasjonen, med den begrunnelse at slutten på andre verdenskrig markerte begynnelsen på russisk okkupasjon. Hendelsen førte til en opphetet politisk diskusjon i Estland, hvorpå det den 9. mai 2006 (den russiske frigjøringsdagen) ble arrangerte en stor demonstrasjon av etniske russere ved *Bronsesoldaten*. En etnisk ester dukket opp under demonstrasjonen, han veivet med et estisk flagg og ropte slagord. Vedkommende ble tatt hånd om av politiet, men hendelsen førte til store overskrifter i avisene om at et estisk flagg ikke var velkommen ved monumentet (Healey 2013 og Russell 2014).

I januar 2007 ble det vedtatt å flytte bronsesoldaten fra sentrum av Tallin til en militær kirkegård rett utenfor byen (Healey 2013). I mars 2007 ble det holdt valg i Estland og monumentet ble en del av valgkampen (Healey 2013). Partiet som satt ved makten, Reform, økte sin oppslutning med 10 prosent og ble dermed sittende ved makten (Jackson 2007). Vedtaket om å flytte

bronsesoldaten ble opprettholdt. Den 23. april utstedte Russland en protest på vedtaket av flyttingen av statuen, og de advarte mot at flyttingen ville kunne få store konsekvenser for Estland. Esterne lot seg ikke presse, og opprettholdt flyttevedtaket, da de ikke mente et veikryss var et verdig sted å ha et minnesmerke (Russell 2014).

Den 26. april 2007 startet arbeidet med å flytte *Bronsesoldaten*. Området ble inngjerdet og klargjort (Healey 2013). I ukene som fulgte ble gravene til soldatene som var lokalisert sammen med statuen flyttet til den militære kirkegården. Arbeidet med flyttingen skapte en serie med hendelser. Det ble opprør i Tallin og i byene Johvi og Kohtla-Jarve nordøst i Estland. Det ble kastet steiner og flasker, og viftet med russiske flagg. Biler ble satt i brann, og butikkvinduer knust og ramponert. Opprøret førte til at en person ble drept, 150 mennesker ble skadet og over 1000 ble arrestert (Russell 2014). Opptøyene døde ut etter to netter, den 29. april (Lander og Markoff 2007). I Moskva, utenfor den estiske ambassaden, oppstod det flere demonstrasjoner. Demonstrantene viste sin misnøye med å rive ned det estiske flagget, noe som er brudd på internasjonale diplomatiske regler. Etter seks dager brøt demonstrantene barrierene og stormet inn i ambassaden, men ble stoppet av estiske sikkerhetsstyrker før de rakk frem til ambassadøren (Russell 2014).

Russerne fordømte flyttingen og russiske medier brukte uttrykk som *barbarer*, *motbydelig* og *blasfemi*. Enkeltpersoner i den russiske Dumaen oppfordret til boikott av estiske varer. Mange fulgte oppfordringen og tok estiske varer ut av sine butikkhyller. Broer og veier mellom Estland og Russland ble plutselig stengt, med begrunnelse i behov for akutt vedlikehold. Russland styrket ikke sikkerheten rundt den estiske ambassaden under de aggressive demonstrasjonene. De få sikkerhetsstyrkene som var der observerte bare hendelsene, uten å gripe inn. (Russell 2014).

Hendelser på Internett

Hillar Aarelaid, som var ansvarlig for cybersikkerheten, uttalte *"if there are fights in the street, there are going to be fights on the internet"* (Lander and Markoff 2007).Slike uttalelser fra en sikkerhetasansvarlig tyder på at hendelser i cyberdomenet ikke var uventet. Esterne hadde allerede før flyttingen av krigsmonumentet fanget opp signaler om at cyberangrep kunne bli utført (Lander and Markoff 2007). I midten av april var det flere russiskspråklige nettforumer som søkte støtte til, og oppfordret til å gjennomføre tjenestenektangrep (DDoS), rettet mot

estiske servere. De la også ut hackerprogrammer sammen med instrukser om når programmene skulle brukes (Healey 2013). På den måten oppfordret hackerforumene aksjonister med lav kompetanse på cyberangrep om å delta i aksjonene mot Estland.

Healey (2013) deler cyberangrepene inn i to faser, hvor fase en startet 27. april, og fase to varte fra 30. april til 18. mai. Angrepene bestod av tjenestenektangrep og nettsidevandalisme, som er enkle former for cyberangrep. Angrepene var rettet mot offisielle nettsteder, som nettsidene til statsminister Andrus Ansip og andre politiske ledere. Angrepene var så omfattende at epostserveren til den estiske regjeringen ble overbelastet med trafikk, og midlertidig utilgjengelig. Nyhetsnettsteder som Postimees ble også utsatt for to tjenestenektangrep, hvorpå de ble nødt til å stenge tilgangen for utenlandske nettsteder. Dette var med på å hindre kommunikasjon og varsling ut over estiske grenser. Diskusjonsforumer ble spammet ned med nedsettende kommentarer og fornærmelser rettet mot statsministeren (Healey 2013). Internettrafikken som var rettet mot regjeringens nettside var over ti ganger høyere enn de høyeste daglige trafikktoppene. Infrastrukturen på dette tidspunktet var ikke dimensjonert for å takle så store mengder trafikk. Konsekvensen var en nedetid på 8 timer i strekk den 28. april. I de to dagene som fulgte var nettsidene påfallende sene med å laste innholdet, og til tider var det ikke mulig å laste siden. Angrep som dette var og er fremdeles dagligdagse, men den mengden som Estland ble utsatt for gjorde situasjonen vanskelig. Rundt klokken 01:00 den 28. april erklærte Estland at de var under cyberangrep (Healey 2013).

Den 30. april endret cyberangrepene karakter og fase to startet. Fra å være angrep som var organisert gjennom nettforum og synkronisert i tid av enkeltmennesker ble cyberangrepene nå mer sammensatte. Angriperne begynte nå å benytte botnets.[7] Botnets benytter seg av flere infiserte datamaskiner verden over, og er kontrollert av en eller få brukere som da kunne oppnå en større effekt (Russell 2014). Andre fase deler Healey (2013) inn i 4 bølger. Den første bølgen varte til og med 8. mai. Uken var relativt rolig uten store utfordringer, men angrepene toppet seg den 4. mai med tjenestenektangrep rettet mot regjeringsmedlemmer og Domaine Name Service (DNS) sine systemer (Healey 2013). DNS kan sammenlignes med en telefonbok for internett. De inneholder en rekke domenenavn, og oversetter disse til Internett Protokoll (IP) adresser (Network Soultions 2018). Et angrep på DNS kan føre til at domenenavn og IP-

[7] Botnet er et nettverk av datamaskiner som er kapret gjennom ulike typer av skadevare. Oppgaven til et botnet kan være å søke gjennom nettsider for informasjon, sende søppel post eller utføre tjenestenektangrep (IKTnytt.no 2018).

adresser ikke blir koblet og et nettsted ikke blir lastet ned. Den 9. mai er den russiske frigjøringsdagen og esterne forventet at det ville komme flere cyberangrep (Russell 2014). Forventingene ble innfridd og bølge nummer to startet den 9. mai. Målene for angrepene var myndighetenes nettsider og finansielle institusjoner (Healey 2013). Flere målere av internettrafikk, som er plassert rundt i verden, målte angrep som hadde varighet på opptil ti timer (Nazario 2009). Det ble anslått at cirka 1 million datamaskiner verden rundt deltok i angrepene uten at eierne visste om det (Russell 2014). Flere banker ble rammet av cyberangrep, der iblant Estlands største bank, Hansabank (Lander og Markoff 2007). De to største bankene ble tvunget til å stenge sine nettjenester i en periode på 45 til 90 minutter (Healey 2013). Dagen etter rapporterte Hansabank at deres nettjenester ikke var tilgjengelig på morgenen, og at folk ville oppleve at banktjenestene ville være ustabile utover dagen. Hansabank informerte videre at kunder som var utenfor Estland ville bli nektet tilgang til bankens tjenester (Healey 2013). Først på ettermiddagen den 10. mai avtok angrepene, og på en slik måte at det kan se ut som om angriperens leietid på botnet gikk ut (Lander og Markoff 2007).

De sterkeste angrepene var nå over. De to påfølgende bølgene relativt ubetydelig, selv om de var rettet mot regjeringen og finansnæringen (Lander og Markoff 2007).

Konsekvenser

Russell (2014) skiller mellom politiske-, sosiale- og økonomiske konsekvenser. Cyberangrepene oppstod i en periode med indre uro i Estland. Angrepet som ble rettet mot de politiske nettstedene gjorde det vanskelig for estiske myndigheter å kommunisere viktig informasjon rundt hendelsene i landet. (Lander og Markoff 2007). Russell (2014) hevder at cyberangrepene ikke fikk noen politiske konsekvenser. Men det kan argumenteres for at NATO Cooperativ Cybder Defence Center of Excellence (CCD COE) ble opprettet og lagt til Estland som en konsekvens av den cybermakten Estland ble utsatt for. CCD COE er i dag en viktig del av NATO, og er viktig for trening og øving i cyberdomenet (CCD COE 2018). Cyberangrepene kan med det ha hatt en positiv politisk konsekvens.

De sosiale konsekvensene var derimot merkbare. Infrastrukturen for kommunikasjon ble for første gang angrepet i fredstid. Manglende informasjon som følge av angrepene førte til større uro. Selv om angrepene ikke varte mer enn noen uker, var det ikke mulig å forutse angrepenes varighet under selve hendelsene. Som følge av dette ble det en del frykt i det estiske samfunnet,

basert på historien og forholdet til Russland. De fryktet at cyberangrepene skulle være starten på en russisk invasjon (Russell 2014).

De økonomiske konsekvensene var små i det store bildet. Konflikten stoppet nesten all handel med Russland, (Russell 2014), men denne utgjorde bare om lag 10 prosent av Estlands totale utenlandshandel, og var derfor ikke en avgjørende del i angrepet (Jackson 2007). Bankenes tap i cyberangrepene kan være vanskelig å beregne. Den beste måten å måle tapene på er tap av økonomiske muligheter i markedet. Dette gjør at de økonomiske tapene ikke er beregnet til å være større enn cirka 1 million USD (Healey 2013 og Russell 2014). En annen forklaring på hvorfor ikke de økonomiske tapene ble større er at bankene, inkludert Hansabank, hadde laget planer for å bekjempe cyberangrep som var rettet mot bankene, og at bankene samarbeidet med det estiske Computer Emergancy Response Team (CERT) (Collier 2007).

Hvem stod bak?

Både Healey (2013) og Russell (2014) fremhever at Estland ved flere anledninger beskyldte russiske myndigheter for å stå bak angrepene. Den estiske utenriksministeren fremhevet også at noen av de angripende datamaskinene hadde IP adresser på innsiden av president Putins administrasjon (Russell 2014). Beskyldningene har også bakgrunn i at oppfordringer og organisering av angrep ble gjort via russiskspråklige nettsider. Flere av mottiltakene som ble brukt i kampen mot angrepene var å blokkere nettsteder som hadde landskode ru. Dette fikk i enkelte tilfeller en god effekt. I følge Russell (2014) så bygger dette opp under påstanden om at Russland stod bak

Selv om mange av IP-adressene kom fra innsiden av Russland så ble tjenestenektangrep gjennomført fra datamaskiner fra hele verden. Botnets angrep ble registrert fra både USA og Peru. Det gjør disse typene angrep til cyberangrep som lett kan benektes. Både Healey (2013) og Russell (2014) benytter begrepet *plausible deniability* om denne typen angrep. Det gir med andre ord store muligheter for å skjule hvem som faktisk stod bak angrepene.

Etterforskningen av cyberangrepene førte til arrestasjon av en 19 år gammel, etnisk russisk ester. Han var i første omgang bare mistenkt for å hjelpe til med organiseringen av angrepene, men ble senere dømt. (Russell 2014). Estland kontaktet også Russland for å få støtte til å

etterforske angrepene, men Russland gav hverken støtte eller tillatelse til en etterforskning på russisk side. Også dette er med på å forsterke mistankene mot Russland (Healey 2013).

Selv om etterforskningen ikke førte til at de skyldige ble avslørt eller tatt, har det kommet to uttalelser om hvem som er skyldige. I 2009 påtok en aktivist, som var medlem av Nasi, en russisk ungdomsorganisasjon, seg ansvaret for angrepet (Lowe 2009). Etter aktivistens innrømmelse kom Sergei Markov, en representant i den russiske Dumaen, med en uttalelse om at det var hans assistent som stod bak cyberangrepne på Estland. Det festet liten troverdighet til en slik uttalelse, da angrepenes natur gjør at det er mer sannsynlig at en gruppe, snarere enn en enkeltperson, har gjennomført cyberangrepene (Leyden 2009).

Georgia

Georgisk selvstendighet har historisk vært utfordret av både indre uro og ytre erobrere. Uroen har alltid vært påvirket av interesser utenfra, som har hatt noe å tjene et ustabilt Georgia (Stotlz 2009).

I 1991 ble Georgia igjen en selvstendig stat. Som tidligere ble det en indre uro i Georgia også denne gangen. Sør-Ossetia og Abkhasia ønsket en løsrivelse fra Georgia, noe som førte til krigshandlinger mellom Sør-Ossetia og Georgia fra 1991 til 1992, og mellom Abkhasia og Georgia fra 1992 til 1993 (Øverland 2009). Konfliktene endte med våpenhvile uten at konfliktene ble løst, og Organisasjon for Sikkerhet og Samarbeid i Europa (OSSE) opprettet en fredsbevarende styrke. Styrkene var en sammensatt styrke som kom fra Russland, Georgia og Sør-Ossetia (Tikk, Kaska og Vihul 2010). Samarbeidet innad i styrken ble vanskelig, og det utviklet seg større spenninger hvor georgiere var på den ene siden og russisk støttede separatister på den andre (Tikk et al. 2010). Konfliktene med Sør-Ossetia og Abkhasia førte til at Georgia mistet kontrollen over store deler av sitt eget land (Øverland 2009).

Oppbygging til konflikt

I 2004 ble Mikheil Saakasjvili president i Georgia. Et av hans valgløfter var å samle Georgia igjen, ved å innlemme Adjar-provinsen, Abkhasia og Sør-Ossetia i Georgia på nytt. Første forsøket gjorde han i 2004. Adjar-provinsen er i sør og grenser til Tyrkia. Innlemmelsen av Adjar-provinsen ble gjennomført uten problemer. I Sør-Ossetia var motstanden mye større og han gikk på et nederlag. Sør-Ossetia demonstrerte at de var villige til å sloss for sin

uavhengighet (Pukhov 2010). Etter nederlaget begynte Saakasjvili å forsterke de georgiske styrkene i samarbeid med amerikanske myndigheter. Dette førte til et skifte i maktbalansen, hvor de Georgiske styrkene ble overlegne de militære kreftene som var i Sør-Ossetia og Abkhasia (Lavrov 2010). Eneste måten å forsvare utbryterrepublikkene på var om russiske styrker ble direkte involvert (Lavrov 2010). Georgia ønsket å bli medlem av NATO, og i en eventuell utvidelse av forsvarsalliansen østover var det Ukraina og Georgia som var aktuelle land (Øverland 2009). Georgia sitt ønske om NATO-medlemskap var begrunnet i et ønske om å sikre seg mot Russland (Øverland 2009).

Russland mente at en utvidelse av NATO østover var en trussel, og dessuten brudd på løfter fra den vestlige verden. Etter at de baltiske landene ble medlem av NATO, og etter utplassering av et rakettforsvar i Polen og Tsjekkia, mente Russland at NATO nå begynte å komme farlig nært. (Pallin og Westerlund 2009). Som et svar på utvidelsen av NATO startet Russland i 2006 en serie med øvelser, Caucasus Frontier. Øvelsene økte i omfang år for år, og sommeren 2008 var det over 10 000 soldater og flere hundre pansrede kjøretøy som deltok (Pallin og Westerlund 2009).

Den militære konflikten startet 7. august 2008 ved at Georgia gikk inn for å ta kontroll over Sør-Ossetia (Pukhov 2010). Etter sin årlige øvelse i regionen hadde Russland etterlatt flere militære styrker i området. Da georgierne startet sin militære offensiv fikk russerne raskt ordre om å krysse grensen inn i Sør-Ossetia (Lavrov 2010). Den militære konflikten som fulgte varte i fem dager, hvor russerne avanserte utover utbryterrepublikkene Sør-Ossetia og Abkhasia før det ble inngått en våpenhvile (Pallin og Westerlund 2009).

Teknologisk sårbarhet

Den konfliktfylte utviklingen etter at Georgia fikk sin selvstendighet har påvirket den teknologiske utviklingen negativt. Landet var derfor et stykke bak den teknologiske utviklingen til Estland på samme tidspunkt (Russell 2014). Også land som Nigeria, Bolivia og El Salvador lå foran Georgia i teknologisk utvikling (Markoff 2008). Med et slikt utgangspunkt var Georgia potensielt mindre sårbar for bruk av cybermakt (Markoff 2008). En direkte sammenligning fra 2007 viser at Estland hadde 57 internettbrukere per 100 innbygger, mens Georgia hadde syv brukere per 100 innbygger (Tikk et al. 2010). Dette forteller midlertidig ikke hele sannheten. I

2006 økte bruken av internett og nettbaserte tjenester, hvorpå den største økningen var brukere av bredbånd (Tikk et al. 2010).

I 2008 var over halvparten av Georgias internettrafikk avhengig av fysiske koblinger som var lagt gjennom Russland. En ny kabel var under utbygging gjennom Svartehavet og over til Vest-Europa, men var ikke klar før i november 2008 (Tikk et al. 2010). Den nye kabelen var altså ikke klar før etter konflikten med Russland.

Cyberangrepene

Før selve konflikten startet rapporterte Shadowserver at den georgiske presidentens nettside var under tjenestenektangrep i mer enn 24 timer, fra den 19. til 20. juli 2008 (Adair, 2008a).[8] Jose Nazario, fra Arbor Networks, oppdaget at cyberangrepet inneholdt en melding som gjentok seg gjennom hele angrepet. Meldingen var: ”win+love+in+russia” (Markoff 2008). Cyberangrepet fikk liten internasjonal oppmerksomhet ettersom president Saakasjvili selv nedskalerte betydningen av cyberangrepet (Healey 2013).

Georgia startet sin militære offensiv for å innlemme Sør-Ossetia tilbake i Georgia den 7. august (Tikk, Kaska, Runnimeri, Kert, Taliharm og Vihul 2008). Dagen etter svarte Russland ved å krysse grensen for å forsvare Sør-Ossetia mot Georgias militære fremstøt (Friedman 2008). Rett i forkant, sent 7. august, startet cyberangrepene. Det ser derfor ut til at cyberangrepene og den militære aktiviteten til Russland har vært synkronisert i tid (Tikk et al. 2008). Cyberangrepene var rettet mot georgiske myndigheters nettsider og nyhetsnettsider (Russell 2014).

Mellom det første cyberangrepet som ble registrert i juli og frem til starten på cyberangrepene sent 7. august, registrert ikke Shadowserver noen Command & Control (C&C) servere med aktivitet rettet mot Georgia (Adair 2008b).[9] Finansnæring ble den 9. august rammet av cyberangrep ved at Georgias største kommersielle bank, TBC ble utsatt for tjenestenektangrep (Tikk et al. 2008).

[8] Shadowserver Foundation er en frivillig organisasjon som jobber med å spore, følge og rapportere på skadevare, botnet aktivitet og e-svindel. De ønsker å forbedre sikkerheten på internett gjennom å øke bevisstheten rundt skadelige servere, ondsinnede angrep og spredning av skadevare (Nazario og DiMino, 2008).

[9] Command & Control servers (C&C) er datamaskiner som gir kommandoer eller ordre til botnet (WhatIs, 2017)

Ved hjelp av en nyopprettet blogg kunngjorde det georgiske utenriksdepartementet den 11. august følgende tekst: *"A cyber warfare campaign by Russia is seriously disrupting many Georgian websites, including Ministry of Foreign Affairs"* (Tikk et al. 2008). Cyberangrepene som rammet presidentens nettside var heller ikke over, men endret karakter fra nettsidevandalisme til tjenestenektangrep (Adair, 2008c). Den militære delen av konflikten over på fem dager og var dermed over den 12. august (Pallin og Westerlund 2009). Bruken av cybermakt fortsatte. Den 13. august oppdaget Shadowserver et nytt stort tjenestenektangrep som var rettet mot Georgiske myndigheters nettsider. Angrepene kom fra flere russiske datamaskiner som var spredt utover hele Russland og fordelt på alt fra bredbåndsbrukere til brukere med analoge linjer (Tikk et al. 2008). Det største cyberangrepet som rammet det georgiske cyberdomenet kom den 27. august. Igjen var det det georgiske myndighetssider og spesielt siden til det georgiske utenriksdepartementet som ble rammet. Tjenestenektet var så kraftig at andre nettsteder også ble skadelidende da angrepet var så stort at hele infrastrukturen ble påvirket. (Tikk et al. 2008).

Hovedvekten av cyberangrepene som ble brukt ved konfliktens startet var tjenestenektangrep og nettsidevandalisme (Tikk et al. 2008). Tjenestenektangrepene var satt sammen av flere botnets som var under kontroll av flere C&C servere (Adair, 2008c). Nettsidevandalisme var rettet mot politiske mål som presidentens nettside, den georgiske nasjonalbanken og mot det georgiske utenriksdepartementet (Tikk et al. 2008). Som regel var nettsidevandalisme pro-russisk propaganda. Et eksempel av nettsidevandalisme som fremgår i flere kilder (Adair 2008b; Tikk et. al. 2008; Healey 2013 og Russell 2014) beskriver en bildekolleksjon som ble lagt ut på presidentens nettside, hvor president Saakasjvili blir sammenlignet med Hitler. I bildekolleksjonen er det valgt ut bilder hvor Saakasjvili og Hitler har like positurer.

Et tredje typeangrep ble også identifisert. Lobbyorganisasjoner hadde utarbeidet en epostliste over georgiske politikere. Listen av epostadresser ble offentligjort og misbrukt av ulike hackere til å sende store mengder spam (Tikk et al. 2008). Jose Nazario og Andre DiMino (2008) utarbeidet en statistikk for tjenestenektangrepene den første dagen. Et gjennomsnittlig tjenestenektangrep varte i 2 timer og 17 minutter, mens det lengste angrepet var på over 6 timer. Både private og offentlige nettsteder ble utsatt for cyberangrep.

Ulike typer av nettsider ble utsatt for tjenestenektangrep (Tikk et al. 2008):

Statlige nettsider:

- www.parlament.ge, Georgias parlament.
- www.president.gov.ge, Georgias president.
- www.mes.gov.ge, Georgias Utdanning og Forsknings departement.
- www.naec.gov.ge, Nettside som organiserer standardiserte tester for utdanning.

Nyhetsmedier:

- www.forum.ge, det største nettforumet i Georgia.
- www.civil.ge, Georgias største engelskspråklige nyhetsside.
- www.presa.ge, nettavis.
- www.apsny.ge, nettavis.
- www.rustavi2.com, privat tv selskap.
- www.news.ge, engelskspråklig nettavis.
- interpress.ge, nettavis.
- www.tbilisiweb.info, en nyhetsportal.

Finansinstitusjoner:

- www.tbc.ge Georgias største kommersielle bank.

Andre nettsteder:

- www.hacking.ge Georgiske hackeres nettside.
- www.newsgeorgia.ru, nyhetsportal.
- www.os-inform.com, privat nyhetsside.
- www.kasparov.ru, nettsiden til en representant fra et russisk opposisjonelt parti.

Konsekvenser av cyberangrepene

CERT Estland avdekket at to av de største leverandørene av internett, United Telecom and Caucasus Network og United Telecom of Georgia, ble rammet av cyberangrep.[10] Trafikken som nettverkene ble utsatt for ble for stor (Tikk et al. 2008), og selskapene hadde problemer med å levere sine tjenester over en periode på flere dager (Tikk et al. 2010). Georgiske

[10] CERT er en mye brukt benevnelse for en avdeling som har til oppgave å overvåke cybersikkerhet. I Norge har vi NorCERT som er en del av Nasjonal Sikkerhetsmyndighet. Det er egentlig en forkortelse og står *Computer Emergancy Response Team*.

myndigheter hadde derfor store utfordringer når deres offisielle nettsider ble utsatt for tjenestenektangrep, og leverandørene av internett hadde problemer med å levere sine tjenester (Tikk et al. 2008). En konsekvens av dette var at georgiske myndigheter ble forhindret i å gi ut informasjon til den georgiske befolkningen, som støttet opp under den georgiske siden av konflikten. (Healey 2013). Jart Armin, grunnlegger av HostExpolit, kom med en advarsel til georgierne og uttalte at dersom de klarte å laste inn georgiske myndigheters sine nettsider kunne innholdet være falskt.[11] For å kontrollere innholdet burde leserne se om innholdet var av en nyere dato, eller om innholdet var foreldet (Swain 2008).

Da finansnæringen ble utsatt for cyberangrep valgte bankene en helt egen strategi for å redusere effekten. På ordre fra den georgiske nasjonalbanken ble alle elektroniske banktjenester stoppet (Russell 2014). Ved å velge en slik strategi sørget bankene for at det ikke ble skade på bankenes cyberinfrastruktur (Rohdes 2011). Bankenes elektroniske tjenester ble ikke åpnet igjen før den 18. august. Da hadde det ikke vært mulig å bruke elektroniske banktjenester på ti dager (Tikk et al. 2010). Som konsekvens av at den elektroniske handelen ble stoppet ble dagliglivet til vanlige georgiere påvirket. Det var ikke muligheter for å benytte bankkort, og kontanter var vanskelig å få tak i. Hendelsen førte til at handelsstanden fikk færre kunder og etterspørselen av varer gikk ned (Healey 2013).

Den tredje metoden i bruk av cybermakt var utsendelse av store menger med spam og skadevare. Resultatet ble at epost servere ble overbelastet, noe som også reduserte kommunikasjonsmuligheten ytterligger. (Russell 2014).

Jose Nazario uttalte til media etter konflikten at det ikke virket som bruken av cybermakt mot Georgia hadde en kraftig eller langvarig effekt. Det baserte han på at Georgia ikke var kommet så langt i sin digitale utvikling. Han understreker likevel at bruken av cybermakt påvirket informasjonsflyten innad i georgiske myndigheter (Tikk et al. 2008).

Bekjempelse av cyberangrepene.

Et amerikansk selskap, Tulip Systems Inc, tilbyde georgiske myndigheter hjelp, ved å flytte presidentens nettside og tv-kanalen rustavi2.com over på selskapets servere i USA. Det georgiske utenriksdepartementet opprettet en bloggkonto via bloggspott.com (Keizer 2008).

[11] HostExploit er en organisasjon som forsker på cyberkriminalitet for å avsløre aktiviteten (HostExploit 2018).

Etterhvert opprettet Estland egne nettsider for Georgias utenriksdepartement (Tikk et al. 2010). Civil.ge, den største engelskspråklige nyhetsnettsiden, benyttet seg av samme fremgangsmåte ved å bytte over til en bloggkonto i tilfelle cyberangrepene skulle bli langvarige. Kontoret til den polske presidenten valgte å gjøre plass på sine nettsider for viktige pressemeldinger fra georgiske myndigheter (Tikk et al. 2010).

I 2008 var CERT Georgia en organisasjon som var formet og gitt i oppgave å støtte i teknisk- og sikkerhetsspørsmål for institusjoner innenfor høyere utdanning (Tikk et al. 2010). De var ikke dimensjonert for å håndtere den cybermakten som Georgia ble utsatt for. Georgia fikk hjelp fra CERT Polen som analyserte IP data, CERT Frankrike som hjalp til med å samle og lagre ulike typer loggfiler og CERT Estland sendte to spesialister til Georgia for å bistå (Tikk et al. 2010). Med det fikk Georgia god hjelp fra utsiden for å håndtere cybermakten.

Etter cyberangrepet den 27. august sluttet i stor grad cyberangrepene, mye på grunn av bekjempelse hvor cyberangrepene ble blokkert (Tikk et al. 2008).

Hvordan ble cyberangrepne gjennomført?

I likhet med cyberangrepene i Estland var det flere russiske forumer og russiskspråklige nettsider som la ut script (oppskrift) for gjennomføring av cyberangrep mot Georgia. En av nettsidene hadde også gjort scriptet tilgjengelig i et program: ”war.bat” (Tikk et al. 2010). Nettsiden stopgerogia.ru (eller stopgeorgia.info som den også het) ble brukt aktivt for å rekruttere nybegynnere. På nettsiden ble det gjort tilgjengelig verktøy som var klargjort for cyberangrep mot Georgia, i tillegg til lister over georgiske nettsider som skulle angripes (Carr 2008). Oppskriftene inneholdt beskrivelser om hvordan tjenestenektangrep og nettsidevandalisme kunne gjennomføres (Tikk et al. 2010).

Gjennom sine analyser identifiserte Shadowserver seks C&C servere som var involvert i cyberangrepene. Det bekrefter at det var flere botnet som hadde rettet sin aktivitet mot Georgia (Adair 2008b). Dette understreker også Nazario og DiMino (2008) sine funn som viste at cyberangrepene ikke bare kom fra Russland, men fra store deler av verden. Botnetene som ble brukt i angrepene ble gjenkjent for å være ”DDoS for hire” eller ”DDoS for extortion” og er normalt rettet mot ikke kommersielle nettsteder (Johnsen 2008).[12] Bruken av cybermakt skiller

[12] DDoS er Ditributet Denial of Service angrep som oversettes til norsk som tjenestenektangrep.

seg derfor ut fra vanlig cyberkriminalitet ved at de angriper ikke kommersielle nettsteder som georgiske myndigheters nettsider (Tikk et al. 2010).

Under selve konflikten gikk en gruppe med ekspertise fra cyberdomenet sammen om å etterforske bruken av cybermakt mot Georgia. Deres funn ble etter konflikten utgitt i en rapport kalt *Project Grey Goose*. Prosjektet gikk gjennom over 200 innlegg på nettsiden xakep.ru og stopgeorgia.ru. Ved analyse av postene fant prosjektet at cyberangrepene kunne deles inn i 5 stadier (Carr 2008):

1. Oppfordre nybegynnere ved hjelp av patriotisme og retorikk til å involvere seg i cyberangrep mot Georgia.
2. Publisere en målliste over georgiske myndigheters nettsider, som var blitt utsatt for tester gjennom IP adresser fra Russland og Litauen.
3. Diskusjoner og utvelgelse av skadevare som skulle brukes mot en nettside.
4. Gjennomføre cyberangrepene.
5. Evaluere resultatet av cyberangrepene.

Hvem stod bak cyberangrepene?

Som med Estland er det vanskelig å bevise hvem som faktisk stod bak bruken av cybermakt. Tatt i betrakting at Russland krysset grensen til Georgia med full militær styrke, og at bruken av cybermakt startet på omtrent samme tid, var det ikke unaturlig å tro at Russland stod bak hendelsene i cyberdomenet. Georgia var også tidlig ute med å anklage Russland for cyberangrepene (Keizer 2008). Russland har kategorisk nektet for å stå bak, eller å ha kjennskap til cybermakt rettet mot Georgia (Markoff 2008). Bevisene som er funnet peker i retning mot russiske nettsider, blogger og nettforum. En side peker seg spesielt ut som svært aktiv i å koordinere, oppfordre og gjennomføre cybermakten mot Georgia og det er stopgeorgia.ru (Carr 2008).

Flere nettsider enn de som er listet opp under avsnittet Cyberhendelser ble utsatt for cyberangrep. Dette er ifølge Johnson (2008) nettsider innenfor følgende kategorier:

- Pornonettsteder.
- Nettsider for prostitusjon.
- Nettsider som fremmer hvite som en overlegen rase.

- Nettsider forbundet med kredittkortsvindel.
- ”Virtual currency” sider (sider som minner om PayPal, men som ikke har samme legitimitet).
- Russiske nyhetsmedier.

En vurdering fra Shadowserver sier at det er lite sannsynlig at russiske myndigheter står bak bruken av cybermakt. Som et argument fremfører Shadowserver at nettsidene ikke har noen tilknytning til konflikten (Johnson 2008).

Etter at konflikten var over begynte analytikere fra ulike miljøer å analysere hendelsene som hadde skjedd i det georgiske cyberdomenet. Analysene viste at de aller fleste av cyberangrepene kom fra servere som var plassert i Russland (Healey 2013). Russian Business Network (RBN) ble tidlig utpekt til å være en aktør som kunne stått bak bruken av cybermakt (Markoff 2008). Organisasjonen har base i St. Petersburg, og er kjent for å stå bak kriminalitet som barnepornografi, identitetstyveri og spam (Markoff 2008). Minst en av serverne ble identifisert som en ”MachBot controller” som er mye brukt av russiske hactivister og er et kjent verktøy for RBN (Tikk et al. 2010). Men om det var RBN som stod bak bruken av cybermakt, eller om de bare hospiterte for cyberangrepene er uklart. Shadowserver gav tidlig utrykk for at det er russere som står bak, men at det ikke er russiske myndigheter eller RBN som gjennomførte cyberangrepene (Johnson 2008). Flere kilder fremhever nettsiden stopgeorgia.ru som hovedkilde til å stå bak cybermakten mot Georgia (Carr 2008; Tikk et al. 2010 og Nazario og DiMino 2008). Men hvem som faktisk står bak siden finnes det ingen klare bevis på (Tikk et. al. 2010).

Project Grey Goose viser sammenhenger mellom hendelsen som skjedde på bakken i Georgia og hendelsene i cyberdomenet.[13] De mener at russiske hackere må ha blitt informert fra russisk offisielt hold når den militære operasjonen startet. Som bevis på denne påstanden viser prosjektet til opprettelsen av nettsiden stopgeorgia.ru. Nettsiden var oppe og tilgjengelig bare timer før bakkeangrepene startet, og var da allerede klar med lister over aktuelle mål for cyberangrep (Carr 2008). Bevisene som rapporten baserer seg på er indisier og ikke direkte beviser på russiske myndigheters deltagelse i cyberangrepene (Tikk et al. 2010). Indisiene er

[13] Project Grey Goose er et prosjekt som ble etablert 22. august 2008 for å etterforske cyberhendelsene i konflikten mellom Georgia og Russland. Prosjektet gav ut rapporten Russia/Georgia Cyber War – Findings and Analysis (Carr 2008).

hentet fra, og basert på, historier fra to konflikter i Tsjetsjenia, og uttalelser som kommer fra offisielt russisk hold (Carr 2008).

En gruppe russiske hackere som har kalt seg "The representatives of Russian hako-undergound" har tatt på seg ansvaret for hendelsene i cyberdomenet. Årsaken var oppgitt å være et ønske om å leve i en verden fri fra aggresjon og løgner. De fremhevet også at de ikke handlet på bakgrunn av ordre fra en statsmakt, men med bakgrunn i patriotisme (Nazario og DiMino 2008). En talsperson for den russiske ambassaden i USA, Yevgeniy Khorshko, kunne ikke utelukke at russiske personer var involvert i cyberhendelsene. Han mente at det kunne være personer som ikke var enige i et standpunkt, og uttrykte det. Videre poengterte han at også USA hadde mennesker som demonstrerte sin motstand mot standpunkter de var uenige i (Markoff 2008).

Selv om russiske myndigheter ikke direkte står bak bruken av cybermakt er det helt klart at Russland ikke gjorde noe for å stoppe cybermakten som Georgia ble utsatt for (Krebs 2008).

Ukraina

Landområdene som utgjør Ukraina i dag har historisk sett vært delt mellom ulike riker. Den vestlige delen har vært underlagt Polen i lange periode, før Østerrike tok herredømmet frem til 1918 (Kolstø 2018). De østlige landsdelene har vært underlagt russisk herredømme i lange perioder av historien. Som et resultat av det russiske herredømme har befolkningen i denne delen av Ukraina vært sterkt påvirket av russisk kultur og russiske verdier (Kolstø 2018). De vestlige delene av Ukraina gjorde det første forsøke på å opprette en selvstendig stat i 1918. Men bare noen år senere, i 1923, ble den ukrainske staten en unionsrepublikk i Sovjetunionen. (Kolstø 2018). I 1957 vedtok Sovjetunionen at Krim-halvøya, som frem til da var russisk, skulle underlegges sovjetrepublikken Ukraina. Vedtaket hadde ingen stor betydning da både Krim og Ukraina begge var underlagt styret i Moskva (FN 2016). Ved oppløsningen av Sovjetunionen ble Ukraina en selvstendig stat på ny. Krim som nå var en del av Ukraina etter vedtaket i 1957, ble fortsatt værende en del av Ukraina, til tross for at flertallet av innbyggerne på Krim var etnisk russiske (FN 2016). Utviklingen til Ukraina etter Sovjetunionens fall har ført med seg en del uro. Ved to anledninger har uroen ført til store nasjonale kriser. I 2004 kom Oransjerevolusjonen, som førte til at det måtte holdes nytt valg av president (Kolstø 2018). I 2014 førte presidentens avgjørelse om å ikke signere en assosieringsavtale med EU til store

protester. Dette ledet til voldeligheter, som igjen førte til at den ukrainske presidenten ble avsatt (Kolstø 2018).

Ukrainas geografiske plassering med grenser til både EU og Russland gjør at landet har interesse i å opprettholde et godt forhold til både EU og Russland. Ved presidentvalget i 2010 var det en pro-russisk kandidat, Viktor Janukovitsj, som gikk av med seieren (FN 2016). Selv om han var pro-russisk ønsket han også et godt forhold til EU. Historien til Ukraina gjør at landet er delt i to i synet på EU og synet på Russland. Vestlige deler har i stor grad en favorisering til EU, mens det i de østlige delene av landet har en favorisering til Russland (FN 2016). Etter forhandlinger med EU ble Ukraina i 2013 tilbudt en såkalt assosieringsavtale. Avtalen var en frihandelsavtale med EU, som ville gitt Ukraina tilgang på europeiske markeder, og hadde ført Ukraina nærmere EU (Kolstø og Paulsen 2018). En betingelse i avtalen var at Ukraina ikke kunne signere en avtale med Russland og bli en del av den russiskledede økonomiske unionen som Russland hadde etablert med Hviterussland og Kasakhstan (FN 2016).

Som Ukrainas historie har vist, er det et skille i landet mellom øst og vest. Dette skillet var fremdeles fremtredende i 2013, og derfor var befolkningen delt i synet på assosieringsavalen med EU. I vest var det et sterkt ønske om at avtalen måtte signeres og i øst var det et større ønske om å få et nærmere forhold til Russland. (FN 2016 og Kolstø og Paulsen 2018).

Betingelsene i assosieringsavtalen gjorde at president Janukovitsj ble tvunget til å velge mellom EU og Russland (FN 2016). Det førte til at Janukovitsj avslo å signere assosieringsavtalen i november 2013 (Kolstø og Paulsen 2018). Han valgte i stedet å signere en avtale med Russland (FN 2016). Presidentens valg førte til at flere demonstranter samlet seg i en fredelig demonstrasjon på Maidan-plassen utenfor parlamentet i Kiev. Gjennom helgen den 24. – 25. november økte demonstrasjonene i omfang, og gikk fra rundt 1 500 demonstranter til at titusener av mennesker sluttet seg til (Szostek 2014).

Demonstrasjonene var av en fredelig karakter frem til politiet økte voldsbruken for å bryte opp demonstrasjonen den 30. november. I stedet for at demonstrasjonen ble oppløst ble resultatet økt oppslutning for demonstrasjonene, som eskalerte ytterligere (Szostek 2014). Eskaleringen gjorde at president Janukovytsj gikk i forhandlinger med opposisjonen. Forhandlingene var

støttet av EU og Russland, hvor det ble enighet om endringer i grunnloven, utlysning av nyvalg og en våpenhvileavtale. Hele avtalen ble signert 21. februar 2014 (Kolstø og Paulsen 2018). Noen dager før signeringen hadde politiet tatt i bruk skarpe våpen mot demonstrantene, og det ble en ytterligere eskalering av demonstrasjonene (Pakharenko 2015). Samme kveld som avtalen ble signert forlot Janukovytsj Ukraina. Dagen etter, 22. februar, vedtok parlamentet å avsette Janukovytsj som president (Kolstø og Paulsen 2018).

På Krimhalvøya og i de østlige deler av Ukraina førte disse handlingene til et politisk opprør (Kolstø og Paulsen 2018). På Krimhalvøya og i byen Sevastopol ble sentrale bygninger okkupert av maskerte menn som enten var russiske, eller russiskstøttede (Kolstø og Paulsen 2018). Som en følge av hendelsen ble det holdt folkeavstemning på Krim for en tilbakeføring til Russland. Folkeavstemmingen var svært omstridt og ble gjennomført uten internasjonale valgobservatører. Resultatet ble et overveldende flertall for en gjenforening med Russland (Kolstø og Paulsen 2018). Som et resultat av disse hendelsene annekterte Russland Krim (FN 2016).

Motsetningene mellom dem som ønsket å nærme seg vesten og EU i Vest-Ukraina og ønsket i Øst-Ukraina om et nærmere forhold til Russland førte til et væpnet opprør i øst. Myndigheten i Kiev møtte separatistene i øst med det de kalte en ”anti-terrorist operasjon” for å ta tilbake kontrollen i øst (Kolstø og Paulsen 2018). Operasjonen viste seg å bli vanskelig for ukrainske myndigheter, ettersom de ukrainske militære styrkene var i dårlig forfatning, og separatistene i øst var støttet av Russland (Kolstø og Paulsen 2018).

Ved to anledninger har det vært fremforhandlet en våpenhvileavtale. I september 2014 ble det undertegnet en våpenhvileavtale i Minsk. Denne avtalen brøt umiddelbart sammen (Kolstø og Paulsen 2018). I februar 2015 ble det gjort et nytt forsøk. Denne gangen deltok Organisasjon for Samarbeid og Sikkerhet i Europa (OSSE). Avtalen ble signert av OSSE, Ukraina, Russland og den selvutnevnte folkerepublikken i Øst-Ukraina (Kolstø og Paulsen 2018).

Teknologisk sårbarhet

I 2013, ved utbruddet av den siste konflikten, hadde Ukraina 41 internettbrukere per 100 innbygger (Internet live stats 2018). Til sammenligning hadde Georgia ti internettbrukere per 100 innbygger da Georgia ble utsatt for cybermakt (FN 2018). Det utbygde nettet deler landet i to deler, i urbane og ikke-urbane strøk. Nettleveransen i urbane strøk er relativt god, mens den

er dårligere utbygd i ikke-urbane strøk (Freedomhouse 2016). Den største økningen av internettbrukere var på mobile enheter over telefonnettet (Freedomhouse 2016). Ukraina hadde og har over 400 ulike leverandører av internett. I de ulike regionen er det ofte lokale bedrifter som tilbyr internett, og de er gjerne avhengig av større bedrifter i det området de tilbyr sine tjenester. Dette er en organisering som gjør strukturen sårbar for korrupsjon (Freedomhouse 2016).

Cyberangrepene

Konflikten i Ukraina skiller seg ut fra konfliktene i Estland og Georgia fordi konflikten enda ikke har funnet en løsning. Det ble inngått en våpenhvile i 2015 som reduserte kamphandlinger og roet konflikten, men den ble forble uløst (Kolstø og Paulsen 2018). Dette kapittelet vil beskrive hvordan Ukraina har vært utsatt for bruk av cybermakt frem til og med 2016. Under er en spesifisert liste av cyberhendelser som masteroppgaven vil fokuserer på for å vise hva Ukraina har vært utsatt for:

- Cybermakt under Euromaidan revolusjonen.
- Cybermakt mot presidentvalget våren 2014.
- Cybermakt mot parlamentsvalget høsten 2014.
- Cyberangrepet mot strømnettet i 2015.
- Cyberangrepet mot strømnettet i 2016.

Euromaidan revolusjonen

De første hendelsene i cyberdomenet startet noe før selve Euromaidan-revolusjonen. Den 28. oktober 2013 annonserte Anonymous Ukraine at de startet sin ”Operation Independence”. Anonymous Ukraine skilte ikke på EU, NATO eller Russland, men stod for et helt uavhengig Ukraina (Kovacs 2013a), noe dette sitatet fra Anonymous Ukraine viser:

> *Ukraine must be free. We do not want to be dependent on other countries or organization. Ukraine people do not need speculative Association agreement with the European Union. Ukraine does not need to be a part of Russia-led Eurasian customs union. We do not need to be servants of NATO* (Kovacs 2013a).

I forbindelse med Euromaidan-revolusjonen ble de første cyberangrepene registret i helgen 24-25. november 2013. Cyberangrepne var tjenestenektangrep rettet mot nyhetsnettstedet Ukrainska Pravda, hvor det blir hevdet at pro-russiske hactivister sto bak (Baezner og Robin 2017: 17). De ble fulgt opp med tjenestenektangrep på TV-kanalen Hromadske sin nettside dagen etter. Samme dag ble også nyhetsnettsiden censor.net utsatt for et cyberangrep, som slettet alt innhold på nettstedet. Alle disse angrepene ble utført av pro-russiske hactivister (Baezner og Robin 2017: 17).

Det var ikke bare nettsteder som dekket demonstrasjonene som ble utsatt for cybermakt. 31. november ble nettsiden til innenriksdepartementet utsatt for tjenestenektangrep fra sympatisører til euromaidanbevegelsen (Baezner og Robin 2017: 17). I månedsskifte mellom november og desember økte myndigheten innsatsen for å få fjernet demonstrantene med hjelp av økt voldsbruk. Parallelt med myndighetenes økning i bruk av makt økte også hendelsen i cyberdomenet. 2. desember ble opposisjonenes nettsider utsatt for kraftige tjenestenektangrep (Pakharenko 2015: 61).

De påfølgende ukene ble flere nyhetsmedier som dekket de økende demonstrasjonene utsatt for tjenestenektangrep, i forsøkt på å stenge ned sidene. Radio Free Europa er et stort uavhengig mediehus som har tatt på seg oppgaven å kringkaste usensurerte nyheter til steder i verden som ikke har en fullt ut fri presse (Radio Free Europa 2018). 8. desember ble deres nettsted utsatt for et større tjenestenektangrep, som førte til at deres nettside var nede i tre timer (Kovacs 2013b). Den 14. desember klarte nyhetsnettstedet liga.net å publisere at de var under tjenestenektangrep, dette gjorde de via sosiale medier (Vtaliymoroz 2013).

I de påfølgende to månedene ble flere nettsteder utsatt for tjenestenektangrep. Nyhetsmedier ble utsatt for tjenestenektangrep gjentatte ganger av pro-russiske sympatisører, og ukrainske myndigheter fikk flere av sine nettsider angrepet fra aktivister som støttet Euromaidan-protestene (Baezner og Robin 2017: 17-18 og Pakharenko 2015: 61). Dette var nettsider som:

- Det Ukrainske Innenriksdepartementet.
- Pro-russiske nyhetsnettstedet Ukrainskaya Pravda.
- Ukrainske TV kanal 5.
- Nettstedet til Euromaidan.

- Nettsiden til den Greskortodokse kirken i Ukraina.
- Nettsiden til TV-kanalen espresso.tv.

Den 18. februar endret protestene igjen karakter, da myndigheten begynte å bruke skarpe våpen mot demonstrantene. Cyberangrepene endret også karakter, og mobiltelefoner tilhørende opposisjonens medlemmer ble spammet ned av tekstmeldinger og oppringinger slik at telefonene ikke kunne brukes. Opposisjonens muligheter for å organisere mottrekk ble på den måten forhindret (Baezner og Robin 2017:18 og Pakharenko 2015:61). Utenfor opplevde demonstranter som oppholdt seg i en bestemt gate å bli mottakere av en tekstmelding som truet med at de ville bli tiltalt for sin deltagelse i demonstrasjonene (Pakharenko, 2015: 61). Det er ikke klart hvem som faktisk stod bak dette angrepet (Baezner og Robin 2017:18). Som et resultat av voldelighetene, og at demonstrasjonene fortsatte selv da dødelig makt ble benyttet, forlot president Janukovytsj Ukraina på kvelden den 21. februar. Dagen etter ble det satt inn et nytt styre (Kolstø og Paulsen 2018 og Pakharenko 2015: 61).

Ikke lenge etter at Janukovytsj forlot Ukraina begynte russiske soldater å ta kontroll over militærbasen Sevastopol og den internasjonale flyplassen Simferopol på Krimhalvøy. I samme operasjon ble det også utført fysisk sabotasje på internettkablene mellom fastlands Ukraina og Krimhalvøya (Maurer og Janz 2014). Selskapet Ukrtelecom ble også raidet og selskapet mistet all teknisk kontakt mellom Ukraina og Krimhalvøya (Maurer og Janz 2014). De neste dagene opplevde medlemmer av det ukrainske parlamentet at de fikk mobiltelefonene sine blokkert. Gjennom helgen 1. – 2. mars 2014 var hovedsiden www.kmu.gov.ua tatt ned. Siden var nede i totalt 72 timer i strekk (Polityuk og Finkel 2014).

Cybermakt mot presidentvalget våren 2014

Da president Janukovytsj ble avsatt den 22. februar, var det behov for en ny president. Det ble klargjort for valg av ny president og valget fant sted 25. mai (OSSE 2014). I perioden 22. – 26. mai ble Central Election Commision (CEC) utsatt for flere tilfeller av cybermakt. Det ble påvist noen dager før valget at flere viktig filer i programvaren som valgkommisjonen benyttet var slettet, slik at programvaren ikke vil fungere (Clayton 2014). Selv om dette angrepet kom over internett, blir det hevdet at noen på innsiden må ha hjulpet hackerne ved å slå av sikkerhetsfunksjoner. En fremtredende årsak til denne påstanden var at passordet som ble tastet inn når viruset ble installert var tastet inn korrekt på første forsøk (Gorchinkaya, Rudenko og

Schreiber 2014). Hele systemet ble raskt gjenopprettet fra backupsystemer, og var oppe igjen på ettermiddagen 22. mai (Clayton 2014 og Gorchinkaya et al. 2014).

To typer av cyberhendelser ble avslørt og bekjempet på selve valgdagen. Nettsidene til CEC ble utsatt for nettsidevandalisme (Baezner og Robin 2017:18). Den andre hendelsen var langt mer alvorlig. CEC oppdaget skadevare som var plassert på sine servere. Skadevaren hadde et forhåndsprogrammert valgresultat hvor en høyreradikal nasjonalist, Dmytro Yarosh, ville vunnet valget med 37 prosent av stemmene, og Petro Poroshenko ville fått 29 prosent. Det reelle resultatet var at Poroshenko vant valget, mens Yarosh fikk under en prosent oppslutning (Clayton 2014 og Security Service of Ukraine 2014). En russisk TV-kanal, Russia One, må ha vært informert om det falske valgresultatet på forhånd. Kanalen publiserte valgresultatet slik det var programmert i skadevaren. TV-kanalen hevdet å ha hentet informasjonen på CEC sine hjemmesider, men siden skadevaren var fjernet fra deres servere ble aldri skadevarens valgresultat offentliggjort på deres nettsider (Stopfake.org 2014 og Security Service of Ukraine 2014).

I løpet av natten til den 26. mai opplevde CEC flere tjenestenektangrep som var rettet mot kommunikasjonslinjene fra valgdistriktene og inn til CEC. Som eneste konsekvens ble det en forsinkelse av valgresultatet, slik at dette ikke var klart før på morgenen den 26. mai (Clayton 2014).

CyberBerkut har på sin blogg fra 2014 påtatt seg ansvaret for bruken av cybermakt som har vært rettet mot det Ukrainske presidentvalget (CyberBerkut 2014). CyberBerkut er en pro-russisk hactivistgruppe som har hentet navnet sitt fra det ukrainske spesialpolitiet, Berkut. Oversatt til norsk betyr det Kongeørn. Ikke bare har de tatt navnet fra spesialpolitiet, men de har også tatt logoen og tilpasset den til navnet CyberBerkut (TrendMicro 2015). I en rekke blogginnlegg som startet 22. mai gikk CyberBerkut hardt ut mot presidentvalget og kalte det for et illegitimt valg. De hevdet også at de stod bak flere av forsøkene på ødeleggelser som ble gjort i de ukrainske serverne til CEC (CyberBerkut 2014). Det kan virke til at CyberBerkut har en viss tilknytning til Russland, men hvorvidt de er en del av det russiske statsapparatet, eller bare en gruppe som sympatiserer med Russlands synspunkter, er ikke bevist (Bing 2017).

Cybermakt mot Parlamentsvalget høsten 2014

Ukraina avholdet Parlamentsvalg søndag 26. oktober. Hendelsene i cyberdomenet startet fredagen før valget. Elektroniske reklameskilt i Kiev ble hacket, og viste bilder av ødelagte bygninger og døde mennesker sammen med flere kandidater i parlamentsvalget. Bildene hadde påskriften *Krigsforbrytere*. CyberBerkut tok på seg ansvaret for hendelsen (Lange-Ionatamishvili og Svetoka 2015: 106). Dagen før valget ble Central Election Commision (CEC) utsatt for cybermakt på ny, da nettsidene deres, www.cvk.gov.ua, ble utsatt for et tjenestenektangrep. Security Service Ukraine (SSU) var de første til å rapportere om angrepet, noe de gjorde via sine Facebook-sider. Nyhetsbyrået RIA Novosti rapporterte at det ukrainske valgsystemet var blitt ødelagt i angrepet, og hevdet å ha informasjonen fra den ukrainske statsadvokatens nettsider. SSU på sin side sier at angrepet var forutsigbart, og at de hadde gjort forberedelser for å hindre denne typen angrep. En talsperson fra den ukrainske statsadvokaten rykket også ut og tilbakeviste opplysningene fra RIA Novosti som "fake news" (Agence France Presse 2014).

Cybermakt rettet mot Ukrainas strømnett i 2015

I desember 2015 ble flere energiselskaper offer for cybermakt. På ettermiddagen den 23. desember ble det et stort strømbrudd som gjorde 225 000 kunder strømløse. Det viste seg at en tredjepart hadde overtatt kontrollen over styringssystemene som kontrollerte distribusjonen av strøm (Lee, Assante og Conway 2016). Angrepet var blitt mulig gjennom bruk av fire ulike måter å få tilgang til systemet, spear phishingi eposter, ulike varianter av BlackEnergy-skadevare og gjennom manipulerte Microsoft Office-dokumenter som inneholdt ulike typer med skadevare.[14] Resultatet var at angriperne fikk «en fot» innenfor programvaren slik at de kunne hente ut brukernavn, passord og informasjon som kunne utnyttes i angrepet (Lee et al. 2016). Ved å gjennomføre angrepet viste de ansvarlige at de hadde gode kunnskaper i bruk av dataprogrammet som styrer strømdistribusjonen, og hvordan de kunne ta ut relestasjoner og etterlate de ubrukelige. For å gjøre situasjonen mer krevende arrangerte angriperen flere tusen telefonoppringninger som førte til at kunder ikke kom gjennom til kundeservice for å rapportere om strømbrudd (Lee et al. 2016). Denne bruken av cybermakt viser at de som stod bak hadde gode ressurser og evner til å gjennomføre en operasjon som krever lang tid for å rekognosere og lære seg programvaren (Lee et al. 2016).

[14] Spear phishing angrep er epost angrep som kan inneholde skadevare og er rettet mot en bestem organisasjon eller person for å få tilgang til sensitive informasjon og systemer (SearchSecurity 2018).

I februar året etter ble det slått fast at cyberhendelsen hadde opprinnelse i det russiske språket og kom fra innsiden av Russland. Først ble det hevdet at en gruppe kalt ”Fancy Bear” var de som stod bak angrepet (Park, Summers og Walstorm 2017). Fancy Bear er oppgitt å ha forbindelse til den russiske sikkerhetstjenesten GRU (Bogen 2018). Videre etterforskning viste at det var skadevaren BlackEnergy3 som ble benyttet i angrepet. Denne skadevaren er utviklet og brukt av en annen gruppe kalt ”Sandstorm Team” (Park et al. 2017). Gruppen har tidligere utført cybermakt rettet mot både NATO og Ukraina. Den politiske orienteringen tyder også på at gruppen sympatiserer med Russlands politiske ståsted. Sandstorm Team har gjennomført aktivitet som krever lang infiltrering i systemer som angripes, noe som tyder på at gruppen har tilgang på store ressurser. Det kan tenkes at gruppen har en tilknytning til russiske myndigheter. En slik påstand er likevel ikke bevist (Park et al. 2017).

Cybermakt rettet mot Ukrainas strømnett 2016

Nesten ett år etter første angrepet, 16 desember 2016, ble strømnettet igjen utsatt for cybermakt (Park et al. 2017). Omfanget av strømbruddet denne gangen var mindre enn strømbruddet i 2015, denne gangen begynte angrepet rett før midnatt den 16. desember og varte i en time (Zetter 2017). Fremgangsmåten var identisk som året før. Det hele startet med en spear phishing kampanje som rammet flere offentlige institusjoner i juli samme år. Programvaren var skrevet på en ny og mer avansert måte, for å gjøre analysen av programvaren mer komplisert (Zetter 2017). Tiden fra juli og frem til desember gav gjerningspersonene, eller gruppen, god tid til å rekognosere og hente ut den informasjonen som var nødvendig for å gjennomføre et nytt cyberangrep. Eposten som startet det hele skal angivelig ha kommet fra en kilde som var sett på som troverdig. Det blir anslått at angriperen kunne gjort langt mer skade enn de faktisk gjorde, og at angrepet langt på vei var skjedde slik at angriperen kunne vise frem sine kapasiteter (Gooding 2017). Trolig er det Sandstorm Team som også denne gangen står bak cyberhendelsene (Park et al. 2017).

Konsekvenser

Generelt har de fleste cyberangrep en prislapp hvor økonomisk tap, omdømmetap, og kostnader knyttet til etterforskning er elementer som må vurderes. Det var i hovedsak tjenestenektangrep som rammet media i deres dekning av hendelsen under Euromaidan-revolusjonen. Her er det nok ikke et tap av inntekter som er det mest avgjørende for nyhetsmediene, men tap av

omdømme. Når mediene blir utsatt for cyberangrep på denne måten, og til stadighet blir utsatt for angrep, kan dette gå utover en befolknings tillit til deres produkt og deres evne til å takle slike hendelser. Tilliten blir redusert eller borte (Beazner og Robin 2017: 12). Ved strømbruddet i desember 2015 fikk ikke kundene kontakt med kundeservice da de prøvde å melde fra om strømbruddet, på grunn av stormen med falske telefoner mot strømselskapenes telefoner. Slike hendelser fører også til et tillitsbrudd, hvor kundene ikke har tro på at deres leverandør av en slik tjeneste er rustet for å takle en slik hendelse (Beazner og Robin 2017: 12).

I hendelsen hvor strømnettet ble hacket i 2015, hadde inntrengerne skrevet om firmware[15] på hele 16 stasjoner som leverte strøm. Dette gjorde at reparatørene ikke hadde muligheter for å logge seg på stasjonen, og de måtte styres manuelt. En del av maskinvarene hadde også blitt infisert med en skadevare som kalt ”KillDisk”. Den slettet alt innhold på datamaskinene og gjorde de ubrukelige. De kunne ikke startes på nytt, noe som førte til at all data som var lagret gikk tapt og måtte erstattes (Beazner og Robin 2017: 13).

Generering av utvalg hendelser

Casebeskrivelsene viser at det har vært flere typer av hendelser i cyberdomenet rettet mot ulike institusjoner og infrastruktur. I dette kapittelet vil jeg bruke informasjonene fra case beskrivelsene for å gjøre en sammenligning av casene. Den er ment å identifisere hvilke hendelser som har funnet sted og om det er likheter og ulikheter mellom casene. De identifiserte hendelsene skal videre danne grunnlaget for spørsmålene i intervjuene med NRK og Kommunikasjonsenheten i Forsvarsdepartementet.

Alle tre landene erfarte bruk av tjenestenektangrep. Bruken av denne teknikken i Estland og Georgia ble koordinert gjennom russiskspråklige nettsider og nettforum. Der ble lagt ut beskrivelser for hvordan denne typen av cybermakt skulle utføres og hvilke nettsider som var mål for cyberangrepene (Russell 2014 og Tikk et al. 2010). I Ukraina var denne typen angrep mye brukt i begynnelsen av konflikten, under Euromaidan-demonstrasjonene. Media som dekket demonstrasjonene ble utsatt for tjenestenektangrep (Beazner og Robin 2017: 13). I Ukraina ble det ikke avdekket nettsider eller nettforum som organiserte, eller forsøkte å verve nye mennesker til sin sak. Ved å sammenligne alle tre casene finner man at alle hendelsene med

[15] Firmware er programvare som er programmert inn i et systems hardware, og er et sett med instruksjoner for hvordan hardware skal kommunisere med andre hardware deler (Techterms 2018).

tjenestenekt har vært utført av hactivister som har hatt et politisk mål, og hvor mesteparten av dem er utført til støtte for russiske politikk. I Estland var det til støtte for demonstrantene mot flyttingingen av bronsestatuen (Russell 2014 og Healey 2013), i Georgia var det motstand mot georgiske fremstøt i Sør-Ossetia og til støtte for en russisk militæroffensiv. (Russell 2014) og i Ukraina ble media som dekket demonstrasjonene eller media som tilsynelatende støttet demonstrantene utsatt for tjenestenektangrepangrep av pro-russiske hactivister (Tikk et al. 2008 og Beazner og Robin 2017: 13).

Både i Estland og Georgia ble det utført nettsidevandalisme mot presidentens nettsider og andre myndighetssider. I Georgia ble nettsiden vandalisert med en sammenligning av presidenten og Hitler (Russell 2014 og Healey 2013). I Ukraina skiller nettsidevandalimen seg ut. Den var ikke rettet direkte mot presidenten eller mot myndighetssider, men mot til Central Election Commision (CEC) (Ukrinform 2014). Det skjedde rett i forkant av valget på ny president i 2014. CyberBerkut brukte nettsiden til CEC for å komme med en politisk ytring om at valget var illegitimt (CyberBerkut 2014). Når det gjelder media er det ikke avdekket at nettsidevandalisme er benyttet mot medier er casene.

Epost spam og skadevare via epost ble også benyttet i alle tre casene. I Estland ble epostserveren til estiske myndigheter utsatt for så mye spam at de ikke klarte å håndtere mengden med trafikk og ble utilgjengelig for estiske myndigheter (Healey 2013). Et tilsvarende scenario ble også gjennomført i Georgia hvor det ble sendt store mengder spam til en definert adresseliste som var publisert i russiske hackerforum. Også her ble konsekvensen at epostserveren ikke klarte å håndtere mengden av trafikk og ble utilgjengelig for georgiske myndigheter (Tikk et al. 2008). Epost ble brukt annerledes i Ukraina. Gjennom en spear phishing kampanje som var rettet mot offentlige institusjoner fikk en hacker med ondsinnede hensikter tilgang til det ukrainske strømnettet. Selv om ikke inntrenger gjorde stor skade og strømmen kom tilbake etter bare noen få timer kunne de gjort langt større skade (Gooding 2017). Ved å bruke epost som våpen i cyberdomenet har angriperne gjort serverne utilgjengelig i Estland og Georgia, men i Ukraina har de utnyttet epost med skadevare for å skaffe seg tilgang til strømnettet.

I Estland og Georgia ble cyberinfrastrukturen utsatt for cyberangrep. I Estland var det Domaine Name Servere (DNS) som ble utsatt for angrep (Healey 2013). Siden en DNS kobler IP-adresser sammen med domenenavn er det den helt essensiell for at en nettside skal lastes ned. I Georgia ble de to største teleselskapene utsatt for så store mengder med trafikk at de ikke klarte å levere

sine tjenester til sine kunder (Tikk et al. 2008). Et slikt scenario vil jo ramme alle kunder av et teleselskap om det skulle skje, slik at nettjenester som nyhetsmedier og myndigheter ikke er tilgjengelig for publikum.

I Ukraina var det to hendelser som ikke ble funnet i Estland og Georgia. Det var blokkering av mobiltelefoner og fysisk sabotasje på cyberinfrastruktur. Det var to tilfeller hvor mobiltelefoner ble blokkert, den ene var under Euromadian-demonstrasjonene da opposisjonen fikk sine mobiltelefoner blokkert av tekstmeldinger og telefonoppringninger (Baezner og Robin 2017:18 og Pakharenko 2015:61). I det andre tilfellet fikk flere parlamentsmedlemmer blokkert sine telefoner da russiskstøttede aksjoner sikret kontroll over Sevastopol (Polityuk og Finkel 2014). I begge tilfeller fikk dette konsekvenser for hvordan mottiltak kunne organiseres. Den andre hendelsen som bare er identifisert i Ukraina er fysisk sabotasje av cyberinfrastruktur. I aksjonen hvor den militære basen Sevastopol kom under kontroll av russiske styrker ble fiberlinjene mellom fastlandet på Ukraina og ut til Krimhalvøya utsatt for sabotasje slik at det ikke var kommunikasjonslinjer mellom Ukraina og Krim (Maurer og Janz 2014).

Cyberhendelsene som rammet Estland, Georgia og Ukraina kan kategoriseres og settes opp i en tabell. På den måten er det lettere å få en oversikt over hvilke hendelser som kan påvirke allmenkringkasteres evne til å løse sitt samfunnsoppdrag og myndigheters evne til krisekommunikasjon.

Tabell 1: Identifiserte hendelser i Estland, Georgia og Ukraina

Type cybermakt	Estland	Georgia	Ukraina
Tjenestenektangrep	X	X	X
Nettsidevandalisme	X	X	X
Epost spam og skadevare	X	X	X
Cybermakt rettet mot cyberinfrastruktur	X	X	
Cybermakt mot mobiltelefoner			X
Fysisk skade av cyberinfrastruktur			X

Den komparative casestudien skal danne grunnlaget for intervjuer med NRK og Kommunikasjonsenheten i Forsvarsdepartementet. I dette kapittelet er det blitt identifisert flere typer hendelser som har påvirket nyhetsdekning og kommunikasjon med befolkingen i caselandene. Informasjonene med tjenestenektangrep, nettsidevandalisme, epost spam og skadevare, cybermakt mot cyberinfrastruktur, cybermakt mot mobiltelefoner og fysisk skade på cyberinfrastruktur er blitt benyttet for å danne spørsmålene til spørsmålskjemaene i vedlegg 1 og 2. Spørsmålene i intervjuene er ment å avdekke hva norske allmenkringkastere, i dette tilfellet NRK, tenker om trusler i cyberdomenet og hva som er alternativene dersom et cyberangrep mot NRK skulle lykkes. Det samme gjelder for spørsmålene som er blitt utarbeidet til norske myndigheter, hvordan norske myndigheter kan håndtere denne typen av hendelser i cyberdomenet. Spørsmålene i intervjuene vil forsøke å avdekke hvordan NRK ser for seg å kunne løse sitt samfunnsoppdrag dersom de skulle bli utsatt for nettsidevandalisme og tjenestenektangrep. I tillegg til å identifisere om NRK ser på skadevare som en trussel. For Kommunikasjonsenheten i Forsvarsdepartementet vil informasjonen bli brukt for å identifisere hvilke muligheter norske myndigheter har for å opprettholde krisekommunikasjon dersom en av hendelsestypene, eller flere av dem skulle ramme de digitale kommunikasjonslinjene til norske myndigheter.

Norske medier og myndigheter om cyberhendelser i krise og konflikt

I metodekapittelet går det fram at jeg skal intervjuet NRK og Kommunikasjonsenheten i Forsvarsdepartementet. I dette kapittelet vil jeg presentere resultatet av disse intervjuene. NRK viste stor interesse, for å gjennomføre et slikt intervju, og Øyvind Vasaasen som er avdelingsdirektør for Sikkerhet og Beredskap i NRK, stilte opp til intervju. For Kommunikasjonsenheten i Forsvarsdepartementet var det Fagdirektør i Kommunikasjonsenheten, Kåre Helland-Olsen som stilte til intervju. Som nevnt i metodekapittelet så ble både Vasaasen og Helland-Olsen tilbudt sitatsjekk for intervjuene, noe begge ønsket. Presentasjonene av intervjuene under har derfor vært sent til henholdsvis Vasaasen og Helland-Olsen for sitatsjekk slik at de kan stå inne for det som er presentert.

NRKs beredskapsansvar og hendelser i cyberdomenet

Intervjuet med NRK ble gjennomført 23. mai 2018. Avsnittene under omhandler hvordan NRK ser på trusler i cyberdomenet og hvordan de kan opprettholde sitt beredskapsansvar og sin nyhetsformidling dersom de utsettes for cybermakt. Siden NRK også har et beredskapsansvar ble også dette temaet diskutert i intervjuet.

Et av de viktigste temaene som ble diskutert i intervjuet var NRK som beredskapskanal. NRK-plakaten er vedtatt av Stortinget og inngår i NRKs vedtekter, hvor § 23 omhandler beredskap (NRK 2018a). I den forbindelse har Kulturdepartementet, som eier av NRK, inngått en avtale med NRK, som skal regulere hvordan norske myndigheter skal få bruke NRKs ressurser i en krisesituasjon. I forbindelse med beredskapsansvaret er det NRK P1 som er beredskapskanalen. I kraft av å være beredskapskanal er det også NRK P1 som har størst redundans. Radiokanalen blir distribuert fra DAB-sendere som i dag dekker områdene hvor 99, 7 prosent av den norske befolkningen bor, hvorav sendere med full redundans dekker 93 prosent. Disse senderne vil være i funksjon selv om for eksempel strømforsyningen blir brutt. Men det er viktig å understreke at NRK også har et ansvar som nyhetsformidler. Det ansvaret dekker også plattformer som TV, internett og mobiltelefon. NRK har derfor lagt stor vekt på redundans også på disse distribusjonsplattformene (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

NRK har god oppslutting og høy troverdighet i det norske samfunnet og er derfor en attraktiv bedrift å ramme i cyberdomenet. Med det mener Vasaasen at NRK kan være et høyverdig mål for en aktør som ønsker å ramme en nyhetsformidler i cyberdomenet. For å opprettholde beredskapsforpliktelsene og de journalistiske forpliktelsene har NRK arbeidet med risiko- og sårbarhetsanalyser som dekker NRKs virksomhet. I det arbeidet har NRK vurdert sannsynligheten og konsekvensen av flere typer uønskede hendelser, deriblant hendelser i cyberdomenet (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

Tjenestenektangrep er ikke et ukjent fenomen for NRK, da slike angrep skjer jevnlig. Dersom et tjenestenektangrep resulterer i at nettsiden blir tatt ned har NRK en beredskapsplan for å løse problemene. I tilfeller hvor det blir helt nødvendig har NRK avtaler med en tredjepart som gjør at NRK kan flytte nettstedene sine til en annen lokasjon. Dersom en aktør rammer både NRK og en annen samfunnsinstitusjon på samme tid kan det påvirke formidlingen av nyheter. I en

periode hvor nettsiden flyttes, eller NRK må benytte andre reserveløsninger vil det ta noe tid før alle systemer er oppe igjen. I den perioden kan det være en utfordring å rapportere om kritiske hendelser (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

Et annet scenario NRK har vurdert er nettsidevandalisme. Det inkluderer også et scenario hvor en utenforstående endrer innhold i allerede publiserte artikler. Vasaasen fremhever at dette er et sannsynlig scenario som de har forberedt seg på at vil skje. Til tross for at dette er en trussel skal ikke dette styre NRKs journalistikk. NRK skal drive med den journalistikken som de mener er viktig (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

Skadevare via epost er en annen type trussel i cyberdomenet. NRK anser dette som en stor trussel. Det handler om de ansattes holdninger til å klikke på vedlegg uten å kjenne avsenderen eller opphavet til eposten. Et arbeid opp mot de ansattes holdninger mot en slik trussel foregår kontinuerlig. Det gjør epost systemet sårbart for angrep. NRK har blitt utsatt for slik skadevare tidligere og regner med at det kommer til skje igjen. Derfor har de også rutiner og planer for å håndtere en slik hendelse. Skulle epost systemet bli utsatt for et cyberangrep hvor epost blir utilgjengelig understreker Vasaasen at epost er et administrativt verktøy og som ikke vil påvirke NRK sin evne til å opprettholde sine nasjonale forpliktelser (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

I Estland, og spesielt i Georgia, førte bruk av cybermakt til at leverandørene av digitale tjenester ikke kunne levere tjenestene sine. Et tilsvarende scenario i Norge vil kunne påvirke NRKs nyhetsformidling. Men det er viktig å ikke glemme NRKs grunnpilarer som er radio og TV. Spesielt viktig i beredskapssammenheng er radio. DAB nettet er helt selvstendig fra det digitale nettet i Norge noe som gjør at en slik hendelse ikke vil påvirke nyhetsformidling via radio. Også TV-distribusjonen via internett har fått større redundans ved å benytte flere CDN-leverandører. (Content Delivery Network/nettverk for levering av innhold). NRK benytter seg av skytjenester, og de kan bli rammet i et slikt scenario, men NRK har spredt lokasjonene for skytjenestene til flere land. Ved bortfall av mobilnettet har NRK en rekke andre muligheter for internkommunikasjon for å kunne formidle intervjuer og nyhetssaker. Vasaasen forteller at NRK har egne fibernettverk, parabolspeil, et system med HF-radio hvor det er HF-speil plassert ut i hele landet og tilgang til satellitt-telefon. I tillegg er NRK godkjent bruker av nødnettet og er i ferd med å teste dette. Selv om mobiltelefon er et viktig verktøy i det daglige arbeidet er

ikke NRK avhengig av denne for å løse sine oppdrag (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

Ved tilfeller hvor et mediehus blir utsatt for cyberangrep gjentatte ganger kan dette påvirke tilliten til mediehuset. Vasaasen bruker begrepet *Digital tillit.* I NRK er digital tillit en viktig verdi som omfatter hele NRKs drift. Tillit bygges ved at en bruker føler det trygt å legge igjen kredittkort informasjon og andre personopplysninger på et nettsted og føler seg trygg på at det blir behandlet på en god måte. På samme måte som en bruker skal ha tillitt til at nyhetssaken vedkommende trykker på er sannferdig. Problematikken om tillit er bredere enn bare cyberproblematikk, tillitsarbeid er et møysommelig arbeid. Den tilliten som er bygget opp kan raskt bli revet ned dersom det inntreffer hendelser i cyberdomenet. Da handler det om brukeren faktisk har tillit til NRK som en aktør (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

Norske myndigheter om cyberhendelser som kan påvirke evnen for krisekommunikasjon.

Kåre Helland-Olsen har tidligere erfaring som kommunikasjonsdirektør i Forsvarsdepartementet, og har også erfaring som pressetalsmann. Spørsmålene til intervjuet er basert på hendelser i casene som er presentert tidligere. Avsnittene under viser hva Helland-Olsen trekker frem som utfordringer og temaer basert på disse spørsmålene, og hvilke problemstillinger Norge prioriterer i cyberdomenet, sett i kontekst av krise og konflikt (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

For krisekommunikasjon ved større hendelser er det Krisestøtteenheten (KSE) i Justisdepartementet som er den viktigste kommunikasjonskanalen for norske myndigheter. KSE har stor kompetanse og flere muligheter for å opprette nettsider for å legge ut informasjon. De kan også ta i bruk sosiale medier. En viktig forutsetting for å kunne benytte KSE sine muligheter er at infrastrukturen er intakt, og alle kommunikasjonslinjer er åpne (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

En kommunikasjonskanal som norske myndigheter kan benytte for å spre informasjon er media. Norge har en statseid og statsfinansiert kanal, NRK. Det kan være rimelig at de har et beredskapsansvar til hjelp for norske myndigheter. NRK har en paragraf i NRK-plakaten som

gir NRK er særlig beredskapsansvar. Tidligere hadde en representant ved Statsministerens kontor direkte kontakt med NRK. Dette er ikke lenger tilfelle. Som kommunikasjonskanal blir NRK behandlet likt med alle andre medier. NRK skal ha et redaksjonelt innhold som er uavhengig av norske myndigheters påvirkning. Dersom norske myndigheter skulle komme og "bestille plass" hos NRK, vil det kunne stilles spørsmål ved NRKs uavhengighet. Den eneste årsaken som kan gjøre at NRK vil stille sine ressurser til rådighet for norske myndigheter, er om det ved Kongen i Statsråd erklæres krig (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Den aktiviteten som norske myndigheter er minst bekymret for i cyberdomenet, er nettsidevandalisme. Norske myndigheter legger til grunn at nettsidevandalisme vil forsøke å påvirke en stemning og få publikum til å tenke annerledes. For at det skal skje må publikummet være mottakelig for et slikt budskap. Det foregår noe forebyggingsarbeid for å unngå at dette skal kunne få alvorlige konsekvenser. Norske myndigheter forsøker å satse på å spre kunnskap om hvilke virkemidler som kan bli tatt i bruk under krise og konflikt. Men det å få den norske befolkning til å godta et slikt budskap, uten å koble det til fakta, mener norske myndigheter er vanskelig av flere årsaker. Norge har åpne politiske systemer som bidrar til å gjøre det norske samfunnet gjennomsiktig. Dette fører til at forsøk på påvirkning blir vanskeligere. Norske myndigheter er derimot mer bekymret for langsiktig påvirkning for å skape konfliktskillelinjer. Men som stunt i en krise eller konflikt mener norske myndigheter at nettsidevandalisme vil ha minimal effekt (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Hovedplattformen som den norske befolkningen mottar informasjon på i dag er en digital plattform, og det er her norske myndigheter må forsøke å nå befolkningen. Men den digitale plattformen kan bli utsatt for tjenestenektangrep som kan hindre den digitale kommunikasjonen. Det gjør tjenestenektangrep til en type angrep som kan påvirke norske myndigheters evne til krisekommunikasjon. For at angrepet skal ha en effekt, må den ramme de digitale kommunikasjonslinjene til norske myndigheter. Konsekvensen av et slikt angrep, dersom det skulle finne sted, er at myndighetene internt har muligheter for kommunikasjon, men vil ha problemer med å nå ut til befolkningen. Alternative kommunikasjonsplattformer kan være å ta i bruk FM-nettet, men mengden av radioapparater som tar inn FM er synkende. Skulle det oppstå en situasjon hvor Norge blir utsatt for et så sterkt tjenestenektangrep, mener Helland-Olsen at det vil være sannsynlig at andre typer hendelser som kan påvirke kommunikasjonen også vil finne sted. Hendelser som fysisk sabotasje på cyberinfrastruktur, eller en kampanje

med elektronisk krigføring som vil hindre radiosamband. I et scenario hvor alle disse kombineres, har ikke Norge noen systemer som kan motstå et slikt angrep.[16] Selv om dette er situasjonen i dag, så er det et prioritert arbeidsområdet som Norge bruker mye ressurser på å forebygge. Samtidig kan dette sammenlignes med et rustningskappløp. Etterhvert som det utvikles gode mottiltak i cyberdomenet, vil ondsinnede aktører stadig utvikle mer sofistikerte måter å utføre sabotasje på (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Helland-Olsen mener at det er en viktig problemstilling om norske myndigheters epostservere vil bli overbelastet dersom de utsettes for et cyberangrep. Han gjør en sammenligning med det å sprenge postkasser. Det er vanskelig å levere viktig informasjon når postkassen er borte. En antatt strategi fra en motstander i en krise eller konflikt er at de ønsker å påvirke beslutningsevnen til beslutningssystemene. Ved å ta ut epostserverne vil beslutningsevnen bli påvirket. Dette er helt klart en hendelse som vil kunne påvirke norske myndigheters evne til krisekommunikasjon. Også dette er et område hvor norske myndigheter bruke mye tid og ressurser, slik at norsk infrastruktur blir skjermet mot en overbelastning av servere. Helland-Olsen sier at norske myndigheter er klar over at det finnes aktører i cyberverden som har høy kompetanse som gjør et slikt scenario aktuelt. Om mottiltakene til norske myndigheter vil fungere vet ingen før situasjonen faktisk har oppstått (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

I en situasjon hvor cyberinfrastrukturen er målet for selve cyberangrepet, vil angrepet kunne ramme evnen norske myndigheter har til å drive krisekommunikasjonen. Et stadig tilbakevendende tema innenfor cyberproblematikk som påvirker kommunikasjonen, er om Norge har en alternativ kanal for å distribuere informasjon. I den grad noen klarer å lamme den norske digitale infrastrukturen er det vanskelig for norske myndigheter å kommunisere ut til befolkningen. Det finnes ikke et helt opplagt alternativ for kommunikasjon, men Helland-Olsen trekker frem to muligheter. Norge kan ta i bruk FM-nettet og spre informasjon via sendinger der. En svakhet er at færre og færre mennesker har et radioapparat som kan ta inn FM nett. I tillegg ligger det en mulighet i å utnytte at Norge har et stort nett av organisasjoner og nettverk som kan benyttes. Som eksempel kan norske myndigheter opprette dirkete kontakt med fylkesmenn rundt i Norge, som igjen kan utnytte kontaktpunkter ut i kommunene. På denne

[16] Elektronisk Krigføring er her ment som utsendelse av elektromagnetisk energi som forstyrrer radiofrekvenser til radiosamband (Børresen 2014).

måten kan informasjon komme ut til små grupper og samfunn. Her vil Direktoratet for Samfunnssikkerhet (DSB) sammen med KSE ha en viktig rolle. I en slik situasjon vil det være vanskelig med et scenario hvor man stiller opp statsministeren på en talerstol for å tale til hele nasjonen (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Mobiltelefon er et viktig verktøy for norske myndigheter. Helland-Olsen understreker at han *snakker med store ord* når han omtaler dette temaet. Dersom bare enkeltpersoners mobiltelefoner blir rammet, vil norske myndigheter kunne drive kommunikasjon gjennom de fleste digitale plattformer, for da har man tross alt kommunikasjonslinjer. Men skulle en situasjon oppstå der mobiltelefonene var et mål i seg selv tar Helland-Olsen det for gitt at mobiltelefonnettet blir rammet og tatt ned. Det vil å så fall kunne påvirke norske myndigheters evne til krisekommunikasjon i stor grad (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Området som vekker aller størst bekymring, er sikring av kritisk norsk infrastruktur. Dette inkluderer telekommunikasjon og digitalt samband. I løpet av de siste to til tre årene har norske myndigheter satt inn store ressurser for å sikre infrastruktur. Når det finnes konkrete eksempler, slik som at Ukrainas strømnett ble rammet, er ikke dette lenger et tenkt scenario, men en trussel som kan bli en realitet i morgen. I dette arbeidet har Olje og Energidepartementet vært sterkt involvert, sammen med norsk oljenæring som er en viktig næring for Norge. Helland-Olsen understreker flere ganger at det er satt inn betydelige ressurser for å forhindre et scenario hvor norsk infrastruktur havner under kontroll av andre aktører. Skulle kontrollen av slik infrastruktur havne i andres hender, har Norge problemer (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

I et scenario hvor digital kommunikasjon på en eller annen måte blir utsatt for cybermakt har Norge få, om noen, alternative kommunikasjonslinjer for krisekommunikasjon. Norge satser stort på å sikre den norske cyberinfrastrukturen for å hindre inntrengere tilgang. Hvor langt dette arbeidet er kommet og nøyaktig hva det innebærer, er gradert informasjon (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Drøfting

I dette kapitelet vil masteroppgaven drøfte hendelsen i casene og hvordan de kan ramme norske mediers evne til å løse sitt samfunnsoppdrag og hvordan norske myndigheters evne til krisekommunikasjon kan bli påvirket av hendelser i cyberdomenet. Drøftingen vil også bygge på intervjuene med Øystein Vasaasen fra NRK og Kåre Helland-Olsen fra Kommunikasjonsenheten i Forsvarsdepartementet.

Tjenestenektangrep rettet mot media

Tjenestenektangrep som ble benyttet i casene hindret pressen i å fritt rapportere fra de hendelsene som fant sted. Det kan sees på som forsøk i å hindre ytringsfriheten. Tjenestenektangrep mot media kan også knyttes opp mot subversjon hvor angrepene undergraver nettsidens troverdighet og evner til å beskytte seg. Når tjenestenektangrep blir benyttet kan det føre til tap av tillitt og tap av omdømme ved gjentatte og vellykkede tjenestenektangrep. Når tjenestenektangrep blir rettet mot media betyr det at deres tjenester som nyhetsformidler kan bli påvirket. I Estland ble flere medier utilgjengelig utenfor Estland sine landegrenser, noe som gjorde det vanskelig å få god mediedekning og varsle til samfunnet utenfor Estland (Healey 2013). I Georgia ble flere nyhetsmediers evne til å rapportere fra hendelsene under konflikten satt på prøve, og gjorde det vanskelig å komme ut med en dekning av konflikten som kunne støtte opp under Georgias versjon (Healey 2013). Pro-russiske hacktivster forsøkte å hindre dekningen av demonstrasjonene på Euromaidanplassen, ved å rette tjenestenektangrep mot media som dekket demonstrasjonene (Beazner og Robin 2017: 8). Potensielt kan en slik måte å angripe media på hindre en direktesending av viktige begivenheter under en demonstrasjon. I sine beredskapsplaner har NRK sett for seg et slikt scenario. Dersom NRK skulle bli utsatt for et så kraftig tjenestenektangrep at de ikke lenger kan levere sine tjenester har NRK avtaler med en tredjepart hvor de kan flytte nettsidene sine til en annen lokasjon. I en periode hvor overgangen skjer kan det være en utfordring å få dekket en kritisk hendelse, slik som Euromaidan-demonstrasjonene i Ukraina var. I Georgia ble bruk av cybermakt synkronisert i tid med hendelser i den virkelige verden (Carr 2008). Dersom et scenario i Norge skulle skje hvor media blir utsatt for kraftige tjenestenektangrep samtidig som det skjer en stor uønsket hendelse i Norge, kan det by på utfordringer for medier. En flytting av nettstedet og de digitale tjenestene vil ta noe tid og kan føre til mangelfull dekning av viktig hendelser i en periode (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018).

I de tre casene er det tjenestenektangrep som går mest igjen. I Georgia viste de innledende tjenestenektangrepene at tjenestenektangrep kan inneholde meldinger eller skadevare (Markoff 2008). Dersom nettsiden blir skadet som følge av tjenestenektangrep, kan disse gjenopprettes forholdvis raskt ved hjelp av backup- prosedyrer som gjør at nettsiden igjen vil være tilgjengelig for publikum. Dette var tilfellet for hjemmesiden og serverne til Ukrainas Central Election Commision (CEC) (Ukrinform 2014). Men dette er avhengig av mediebedriftens sikkerhetsnivå og beredskapsplaner for å håndtere hendelser i cyberdomenet (NSM 2018). NRK har gjennomført risiko- og sårbarhetsanalyser for å redusere sin egen risiko for å bli rammet av tjenestenektangrep (Samtaleintervju med Øyvind Vasaasen, gjennomført 23. mai 2018). Dersom en medieaktør eller andre blir rammet gjentatte ganger av vellykkede tjenestenektangrep kan det også føre til et tap av omdømme (Baezner og Robin 2017: 12).

Casene viser at skulle det bli en krise eller konflikt i Norge er det store sjanser for at media blir rammet av tjenestenektangrep. I casene påvirket tjenestenektangrepene medias evne til å drive nyhetsformidling. NRK ser også for seg at de kan bli utsatt for en slik type angrep dersom situasjonen skulle tilsi det. Selv om NRK har planer for hvordan de skal håndtere tjenestenektangrep, vil det kunne være en periode, mens NRK relokaliserer seg, at de ikke klarer å drive god nyhetsformidling. Tjenestenektangrep er med det en type cyberhendelse som kan påvirke medias evne til å løse sitt samfunnsoppdrag.

Tjenestenektangrep som kan påvirke krisekommunikasjon

De tre landene opplevde også å få nettsidene tilhørende myndighetene utsatt for tjenestenektangrep. Men her er det en viktig forskjell på Estland og Georgia på den ene siden og Ukraina på den andre. Euromaidan-demonstrasjonene var rettet mot president Janokovytsj og hans regjering, og dermed myndighetene. Tjenestenektangrepene som var rettet mot ukrainske myndigheter var utført av støttespillere til Euromaidan-evegelsen og ikke av pro-russiske aktivister slik som ellers har vært tilfellet (Baezner og Robin 2017: 17).

Tjenestenektangrepene som var rettet mot myndighetene i Estland og Georgia, førte til at myndigheten mistet tilgang til egne nettsider og i noen perioder tok det lang tid å laste ned sidene (Markoff og Landler 2007; Healey 2013 og Swain 2008). De estiske og georgiske myndighetene mistet da en distribusjonskanal for informasjon ut til sin befolkning. I Georgias tilfellet var det også en militær konflikt, og informasjonsbehovet ut til det georgiske folket var

derfor stort (Pukhov 2010). Som casene viser kan tjenestenektangrep hindre digital kommunikasjon. I Norge er hoveddelen av kommunikasjonen mellom norske myndigheter og befolkningen digital. Kommunikasjonen blir da ekstra sårbar ved tjenestenektangrep (Samtaleintervju med Helland-Olsen gjennomført 7. mai 2018). Dersom Norge skulle oppleve en nasjonal krise hvor myndighetene blir utsatt for tjenestenektangrep har NRK et beredskapsansvar (NRK 2018a). Ansvaret reguleres i en egen avtale mellom Kunnskapsdepartementet og NRK. Dersom den digitale informasjonskanalen skulle falle bort for norske myndigheter vil det fremdeles være en mulighet for norske myndigheter å benytte NRK og NRK P1 for å distribuere viktig informasjon til befolkningen.

Noen uker før konflikten i Georgia startet var det et tjenestenektangrep rettet mot den georgiske presidentens nettside. Dette angrepet varte i overkant av 24 timer (Adair 2008a). Skulle norske myndigheter være de eneste som blir utsatt for tjenestenektangrep vil ikke det påvirke norske myndigheters evne til krisekommunikasjon i spesielt stor grad. Norske myndigheter kan kommunisere gjennom media og NRK P1 som beredskapskanal. Mobiltelefon vil også være tilgjengelig som et varslingsverktøy hvor norske myndigheter kan publisere mediesaker eller informasjon gjennom sosiale medier. (Samtaleintervju med Kåre Helland Olsen 2018 og Øyvind Vasaasen 2018). I casene Estland og Georgia skjedde ikke tjenestenektangrepene isolert mot en aktør som media eller myndighetene, men mot begge aktørene på samme tid (Russell 2014 og Healey 2013). Med bakgrunn i disse casene er det sannsynlig at det samme vil skje i Norge. I Georgias tilfellet var det en russisk militæroperasjon i Georgia da tjenestenektangrepene mot myndighetene og media startet (Carr 2008). En slik fremgangsmåte gjør at politiske hactivister kan forsinke eller blokkere viktig informasjon i å komme frem til befolkningen i en fase hvor informasjon kan være svært viktig.

Dersom et tjenestenektangrep blir rettet kun mot norske myndigheters nettsider trenger ikke det å ha så mye å si for norske myndigheters evne til krisekommunikasjon. Men dersom det kombineres med tjenestenektangrep også mot media kan det få konsekvenser. Norske myndigheter har fremdeles NRK P1 som beredskapskanal for viktig informasjon.

Nettsidevandalisme rettet mot media og myndigheter

Nettsidevandalisme er en enkel form for cybermakt, men som kan medføre potensielt stor skade for den som er offeret for et slikt cyberangrep (Baezner og Robin 2017:15). Om en

sammenligner nettsidevandalisme med et tjenestenektangrep kan nettsidevandalismen ha noen av den samme effektene. Nettsiden som blir angrepet blir kapret av en inntrenger, og blir utilgjengelig for eier av nettsiden. Den inneholder gjerne et politisk budskap gjennom bruk av tekst eller bilder (Trendmicro 2018). En annen mulighet er at en hacktivist går inn og endrer innholdet i en allerede publisert artikkel hos en medieaktør (Samtaleintervju med Øyvind Vasaasen gjennomført den 23. mai 2018). Bruk av nettsidevandalisme kan være for å påvirke et publikum. For at en slik påvirkning skal lykkes, forutsetter det at publikummet er mottakelig for den propagandaen som blir fremlagt i vandalismen. Nettsidevandalisme kan også knyttes til subversjon. Når en hactivist publiserer sitt budskap eller endrer innholdet i en artikkel er det for å demonstrere sin politiske mening, samtidig som de undergraver og svekker tilliten til aktøren de rammer. Ved gjentatte vellykkede forsøk på å vandalisere en nettside er dette med på å svekke brukerens tillit til nettstedet.

I casene har nettsidevandalismen vært rettet mot myndighetssider med en politisk ytring til støtte for et russisk politisk syn. Kapringen av nettsiden gjør det vanskelig for eieren av siden å publisere sin informasjon på nettsidene. Selv om nettsidevandalismen ikke gjør nettsiden utilgjengelig slik som tjenestenektangrep kan gjøre, blir innholdet endret slik at siden ikke publiserer den informasjonen som er ment. Det gjør at oppnådd effekt for en hactivist er ganske lik som ved tjenestenektangrep hvor nettsiden ikke er tilgjengelig for publikum.

I casene med Estland og Georgia er tjenestenektangrep og nettsidevandalisme brukt på samme tid og om hverandre (Russell 2014 og Tikk et al. 2010). Ukraina er den beste eksempelet, hvor Central Election Commison (CEC) ble utsatt for nettsidevandalisme i forbindelse med presidentvalget 25. mai 2014 (Baezner og Robin 2017:18). Organisasjonene CyberBerkut tok på seg ansvaret for hendelsen, og er kjent for å ha et pro-russisk ståsted (CyberBerkut 2014). Ut fra casene ser det ikke ut til at media har vært noe hovedmål for nettsidevandalisme. Det kan ikke utelukkes at media kan bli utsatt for slike cyberhendelser og er et scenario som NRK har utredet og har planer for å håndtere (Samtaleintervju med Øyvind Vasaasen gjennomført den 23. mai 2018).

Siden nettsidevandalisme kaprer en nettside og fører til at eieren ikke kan publisere sin egen informasjon, kan den påvirke medias evne til å løse sitt samfunnsoppdrag. Norske allmenkringkastere har flere muligheter for å nå ut med sin nyhetsformidling. NRK sin grunnpilar er fortsatt radio og tv. Isolert sett vil ikke nettsidevandalisme alene kunne påvirke

norske allmenkringkasteres evne til å løse sitt samfunnsoppdrag. Norske myndigheter er heller ikke spesielt bekymret for nettsidevandalisme. Det politiske budskapet vil ikke nødvendigvis være sammenfallende med fakta, og vil dermed ha liten effekt på den norske befolkning. Gjennom KSE har Norge flere muligheter for å nå ut med sin informasjon til den norske befolkning dersom norske myndighetssider skulle bli utsatt for nettsidevandalisme (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018). Nettsidevandalisme kan påvirke medias evne til å løse samfunnsoppdraget, men kan bekjempes med en god beredskapsplan (NSM 2018). Når det gjelder myndighetenes evne til krisekommunikasjon vil nettsidevandalisme isolert sett bare ha en begrenset eller ingen effekt så lenge myndighetene har andre tilgjengelige kommunikasjonskanaler.

Epost spam og skadevare

I Estland var trafikken mot epostserverne så stor at de ble overbelastet og utilgjengelig for brukerne (Healey 2013). I Georgia ble en adresseliste med eposter utarbeidet av lobbyorganisasjoner fanget opp og misbrukt av hacktivister. Resultatet ble at personer som stod på adresselisten ble offer for store mengder med spam (Tikk et al. 2008). Mengden med spam førte til at epostserverne til Georgia, som i Estland, ble overbelastet slik at muligheten for å kommunisere via epost ikke var mulig (Russell 2014). En slik hendelse kan, som Helland-Olsen gjorde, sammenlignes med å sprenge postkasser. Det vil ikke være mulig å kommunisere digitalt når serverne ikke fungerer. Siden den norske befolkning får hovedvekten av informasjon digitalt, vil også myndighetene motta mye informasjon digitalt. Når epostserverne ikke fungere er faren stor for at en del informasjon ikke kommer frem til beslutningstakerne i beslutningssystemene. Helland-Olsen fremhever at nettopp denne formen for angrep er viktig å skjerme seg mot. Dette er en type angrep som kan ramme beslutninger som norske myndigheter må fatte i en krise eller konflikt (Samtaleintervju med Helland-Olsen gjennomført 7. mai 2018). Resultatet kan bli at norske myndigheter mister en kommunikasjonskanal eller at beslutningstagere ikke får nødvendig informasjon. Får ikke myndighetene informasjon kan det føre til at de ikke har informasjon å kommunisere ut til befolkningen. Vasaasen i NRK fremhever at epost er et administrativt verktøy for NRK. De har alternativer for kommunikasjon gjennom egne fibernett, HF-radio og satellittkommunikasjon. På den måte vil bortfall av epost og epostservere ikke ha innvirkning på NRKs evne til å løse sitt samfunnsoppdrag.

Hvor det i Estland og Georgia var en overbelastning av epostserverne som gjorde dem utilgjengelig, ble bruken av epost skadevare og spam brukt mer målrettet mot spesifikke mål i Ukraina, eksempelvis da man angrep det ukrainske strømnettet (Gooding 2017). Her har målet vært å få tilgang til det ukrainske strømnettet ved hjelp av skadevare som er sendt ut via epost. Gruppen som mottok eposten var ikke tilfeldig, men en gruppe mennesker som satt med tilgang til datasystemene som styrte produksjon og distribusjon av strøm (Lee et al. 2016). NSM (2018) gjennomførte en simulert spear phishing kampanje mot en avdeling innen for norsk forvaltning. Der klarte flere personer å aktivere en simulert skadevare. Det viser at fremgangsmåten kan overføres til andre systemer enn selve strømnettet. I masteroppgaven er det ikke gjort funn i de tre casene som beskriver at cybermakt av denne typen har vært benyttet direkte mot media. NRK rammes derimot av epost med skadevare fra tid til annen i fredstid. Det gjør at NRK har et holdningsskapende arbeide for at ansatte ikke skal være ukritisk til hva de trykker på av lenker i mottatte eposter. Inntrengingen i NRK sine datasystemer er også en del av NRK sin risiko- og sårbarhetsanalyse, slik at NRK har utarbeidet rutiner for hvordan slike hendelser skal håndteres (Samtaleintervju med Øyvind Vasaasen gjennomført den 23. mai 2018).

For krisekommunikasjon er myndighetene avhengig av å ha kommunikasjonslinjer. Cyberangrep som har vært rettet mot cyberinfrastruktur finnes i både Estland og Georgia hvor infrastrukturen ble overbelastet med trafikk (Healey 2013; Russell 2014 og Tikk et al. 2010). Hactivister har med det vist vilje til å angripe cyberinfrastruktur. Et sted hvor en spear phishing kampanje kan rettes mot er cyberinfrastruktur på samme måte som ved hackingen av strømnettet i Ukraina. En inntrenger kan infiltrere kommunikasjonsinfrastrukturen hvorpå inntrengeren da kan slå av etter mønster fra kontrollsystemene i Ukrainas strømnett. Norske myndigheter har definert spear phishing og skadevare via epost som en av de største truslene i cyberdomenet og bruker mye ressurser på å forhindre et slikt scenario (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Om ikke hackingen av det Ukrainske strømnettet i seg selv har så mye å si for medias evne til å løse sitt samfunnsoppdrag eller myndighetenes evner til krisekommunikasjon, kan fremgangsmåten i angrepet overføres til andre sektorer. Dette gjør at fremgangsmåten med spear phishing og skadevare via epost kan ha påvirkning for medias evne til å løse sitt samfunnsoppdrag og myndigheters evne for krisekommunikasjon. Som ved strømnettet i Ukraina kan en inntrenger ta kontroll over en kringkasters styringssystemer eller andre styringssystemer som er sentral i den digitale infrastrukturen.

Cybermakt rettet mot cyberinfrastruktur

En analyse av casene Estland og Georgia viser at cyberinfrastrukturen har vært utsatt for cybermakt. I Estland ble det i første bølge av cyberangrepene utført angrep som var rettet mot Domain Name Servere (DNS) som kobler nettsidens navn opp til en IP adresse. (Healey 2013 og Network Soultions 2018). Et angrep her kan føre til at en DNS ikke klarer å koble et domenenavn opp til en IP-adresse. Resultatet blir at nettsidene ikke vil lastes ned til en bruker siden domenenavnet ikke blir oversatt til en IP-adresse (Network Solutions 2018). I Georgia ble de to største internettleverandørene rammet av cyberangrep. Internettrafikken var så stor at United Telecom and Caucasus Network og United Telecom of Georgia ikke klarte å levere sine tjenester i en periode på flere dager (Tikk et al. 2008 og Tikk et al. 2010).

Denne typen angrep ser ut til å ramme alle som er brukere av leverandøren som blir rammet. Det er helt klar et scenario som kan påvirke en allmenkrigkasters evne til å løse sitt samfunnsoppdrag. Selv om mediene ikke er direkte berørt, vil en allmenkringkaster bli påvirket. Mediene blir da indirekte berørt, siden nettleverandøren ikke leverer tjenester.

I dag finnes det ikke gode alternativer for digital kommunikasjon. Dersom et cyberangrep skulle ramme cyberinfrastrukturen, eller nettleverandørene ikke klarer å levere sine tjenester, vil dette uten tvil påvirke norske myndigheters evne til krisekommunikasjon (Samtaleintervju med Helland-Olsen gjennomført 7. mai 2018). Det første alternative for å kommunisere ut til befolkningen blir da NRK P1 som beredskapskanal. DAB-nettet dekker 99,7 prosent av områdene der befolkningen bor. DAB-nettet er helt uavhengig av det digitale nettet, så bortfall av det digitale nettet vil ikke påvirke DAB. Skulle strømmen i DAB-nettet kuttes er DAB-nettet utstyrt med redundans slik at boområdene til 93 prosent av befolkningen fremdeles vil være dekket (Samtaleintervju med Øyvind Vasaasen gjennomført den 23. mai 2018). Helland-Olsen trekker også frem to andre alternativ. Ta i bruk det som er igjen av FM-nettet eller bruke det store nettet av organisasjoner og nettverk som Norge har (Samtaleintervju med Helland-Olsen gjennomført 7. mai 2018).

Cybermakt som er rettet mot cyberinfrastruktur vil kunne påvirke en allmenkringkasters evne til å løse sitt samfunnsoppdrag ved at de ikke får benyttet de digitale tjenester fra sin tjenesteleverandør. NRK har alternativer til nyhetsformidling gjennom DAB-nettet som ikke er

avhengig av disse tjenesten. Norske myndigheter vil kunne miste tilgang på nettsider og sosiale medier i en slik situasjon. Men igjen har de tilgang på NRK P1 som beredskapskanal for å nå ut til befolkningen. Krisekommunikasjonene kan bli påvirket, men ikke nødvendigvis stoppet.

Cybermakt mot mobiltelefoner.

I to tilfeller har det vært hendelser rettet mot parlamentsmedlemmer sine mobiltelefoner i Ukraina. Det første tilfellet var da ukrainske myndigheter begynte å bruke dødelig makt under Euromaidan-protestene (Baezner og Robin 2017:18 og Pakharenko 2015: 61). Mobiltelefonene til opposisjonen mottok så mange oppringinger og tekstmeldinger at mobiltelefonene ikke kunne benyttes. Opposisjonens mulighet for å koordinere et mottiltak mot myndighetenes bruk av makt ble påvirket av hendelsen. Samtidig fikk flere demonstranter tekstmelding om at deres deltagelse i demonstrasjonen var registrert (Pakharenko 2015:61). Når russiske soldater sikret den militære Sevastopol basen på Krim, ble også kontorene til Ukrtelecom raidet. Etter denne hendelsen fikk flere av parlamentsmedlemmene sine mobiltelefoner blokkert, slik at de ikke kunne benyttes (Polityuk og Finkel 2014).

Mobiltelefon er i dagens Norge blitt et viktig verktøy for både private bedrifter og offentlige institusjoner. Den brukes til alt fra å koordinere møter via telefon eller tekstmeldinger, til å lese nyheter gjennom nettaviser og sosiale medier. Når eieren er ute av sin arbeidsplass kan telefonen kobles opp til epostkontoen til vedkommende, slik at viktige eposter kan bli lest og besvart. For norske myndigheter er mobiltelefon et svært sentralt og viktig verktøy som kan brukes til krisekommunikasjon ut til den norske befolkning (Samtaleintervju med Helland-Olsen gjennomført den 7. Mai 2018). For norske allmennkringkastere er mobiltelefonen også et viktig verktøy. Men Vasaasen understreker at NRK ikke er avhengig av den. Som tidligere nevnt har NRK alternative kommunikasjonsmidler med egne fibernett, satellitt-telefon og HF radio. Ved hjelp av disse kanalene for kommunikasjon kan nyhetssaker fortsatt distribueres internt og publiseres. En blokkering av mobiltelefon vil da ikke ha noen betydning for NRK sin evne til å løse samfunnsoppdraget. krisekommunikasjon.

I Ukraina ser det ut til at en blokkering har hatt til hensikt å hindre kommunikasjon for å koordinere mottiltak for henholdsvis opposisjonen under Euromaidan-revolusjonen og hindre ukrainske myndigheters kommunikasjonsmuligheter under aksjonen hvor Sevastopol-basen ble

sikret av russiske soldater. Bruken av denne typen cybermakt kan da ha vært med på å skaffe et overtak for et pro-russiske syn, eller for de russiske aksjonene på Krim-halvøya.

Det ble ikke avdekket cybermakt som var rettet direkte mot medias mobiltelefoner. Det kan ikke utelukkes at journalister tilstede under Euromaidan-protestene fikk tekstmeldingen på sine mobiltelefoner hvor det står at de er registrert som deltagere i demonstrasjonen, men en tekstmelding alene vil ikke kunne påvirke medias evne til å utfør sitt samfunnsoppdrag. Det vil først kunne skje dersom mobiltelefonen blir utsatt for så store mengder oppringinger og mottak av tekstmeldinger at telefonen ikke kan benyttes. Analysen av casene fant ikke slike cyberhendelser i Ukraina.

Dersom et utvalg av medlemmer av den norske regjeringen eller medlemmer på Stortinget skulle bli utsatt for lignende bruk av cybermakt, vil ikke dette ha så stor effekt, da norske myndigheter har flere muligheter enn enkeltpersoners mobiltelefon. Men skulle en slik hendelse ende med å ta ned hele mobiltelefonnettet, noe Helland-Olsen mener er mer sannsynlig, vil det kunne ramme evnen for krisekommunikasjon ganske betraktelig. Mobiltelefonen er kanskje det viktigste verktøyet, for der finnes alle sosiale kanaler. (Samtaleintervju med Helland-Olsen gjennomflrt den 7. mai 2018). Selv om norske myndigheter skulle miste mobiltelefon som kommunikasjonsmiddel er ikke det den eneste muligheten for å drive krisekommunikasjon. NRK P1 er fortsatt en alternativ kanal for krisekommunikasjon.

Ut fra hendelsen i Ukraina er det lite trolig at media vil være mål for en slik bruk av cybermakt. Skulle det skje har en allmenkringkaster som NRK gode alternativer for kommunikasjon slik at en slik cyberhendelse vil ha liten eller ingen effekt på en allmenkringkasters evner til å løse sitt samfunnsoppdrag. Det vil kunne ha en effekt på norske myndigheters evne til krisekommunikasjon, men myndigheten vil ha alternativer for krisekommunikasjon.

Fysisk skade på infrastruktur

I aksjonen hvor den militære basen Sevastopol ble sikret av russiske soldater, ble de fiberoptiske kablene mellom fastlandet og Krim-halvøya fysisk ødelagt. Sammen med raidet på Ukrtelecom ble konsekvensen av sabotasjen at det ikke var kommunikasjonslinjer mellom Ukraina og Krim-halvøya (Maurer og Janz 2014). En slik hendelse kan påvirke medias mulighet til å rapportere om hendelsene fra den isolerte sonen. For myndighetene kan det være vanskelig å få

tak i viktig informasjon om hendelser i det isolerte området (NOU 2015:13: 109). Når det ikke er kommunikasjonslinjer inn eller ut av et område, kan det bli vanskelig for media å løse sitt samfunnsoppdrag ovenfor det isolerte samfunnet, og myndighetene får ikke gitt innbyggerne viktig informasjon om den pågående konflikten.

I Norge er infrastrukturen bygget opp av et kjernenett, regionalnett og aksessnett. Kjernenettet dekker all digital kommunikasjon i Norge, som telefoni, mobiltelefoni, bredbånd, nødnettsamband og TV, og har som oppgave å distribuere det utover til de andre nettene. To selskaper eier all infrastrukturen i kjernenettet, Telenor og Broadnett. Deler av denne infrastrukturen er lagt i samme trasé, noe som gjør infrastrukturen mer sårbar for fysisk skade. For å redusere sårbarheten, har Telenor lagt infrastrukturen som to parallelle nettverk som fysisk er skilt fra hverandre. Den er også lagt i en ringstruktur, hvor trafikken normalt går i sirkel, men kan rutes i motsatt retning og likevel komme frem til mottageren dersom det oppstår fysisk skade på nettverket. De regionale nettene har tilsvarende oppbygging for å ivareta nettets integritet dersom en skade skal oppstå i nettet (NOU 2015:13: 97-101). For å isolere brukere av digitale systemer som bruker disse nettene, må det saboteres på flere steder for å hindre kommunikasjonen ved fysisk skade. Aksessnettet er nettet som knytter brukeren av internett, TV og telefoni sammen med de regionale nettene, og videre til kjernenettet. Skader i aksessnettet vil ikke kunne ramme store områder siden de er relativt små, sammenlignet med de regionale nettene (NOU 2015:13: 100). I Norsk Offentlig Utredning 2015:13 er det utarbeidet en oversikt over mulige konsekvenser dersom all digital kommunikasjon skulle falle bort i en femdagers periode. Det blir anslått at konsekvensene for samfunnsstabilitet er svært store, og manglende informasjon fra myndigheter trekkes frem som en av årsakene til vurderingen (NOU 2015:13: 109).

I masteroppgaven er det ikke vurdert hvor sannsynlig det er at en slik sabotasje kan finne sted i en krise eller konflikt, da det ikke er en del av problemstillingen som masteroppgaven forsøker å belyse. Men det er klart at fysisk sabotasje av cyberinfrastruktur kan få konsekvenser for medias evne til å utføre sitt samfunnsoppdrag, dersom det utføres fysisk sabotasje mot kjernettet eller regionalnettene. En allmenkringkaster som NRK har alternative kommunikasjonsmidler som satellitt-telefon og HF-radio som ikke er avhengig av den samme infrastrukturen. NRK vil derfor ha mulighet for kommunikasjon med en journalist som befinner seg i et isolert område. Skulle fysisk sabotasje skje i Norge vil NRK kunne rapportere fra området, og gjennom DAB-nettet fortsatt kunne drive nyhetsformidling og opprettholde sitt samfunnsoppdrag. Internt har

norske myndigheter muligheter for å drive kommunikasjon via krypterte sambandsmuligheter. For å opprettholde krisekommunikasjon vil norske myndigheter være avhengig av NRK P1, som beredskapskanal. Kommunikasjon ut til den norske befolkning i det isolerte området vil bli mer utfordrende for norske myndigheter når eneste tilgjengelige kommunikasjonskanal er NRK P1. Helland-Olsen mener det ikke er usannsynlig at Norge kan rammes av en kampanje av elektronisk krigføring i et slikt tilfelle (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018). Elektronisk krigføring kan forstyrre radiofrekvenser som både NRK bruker i sin kommunikasjon med HF radio og det krypterte sambandet som norske myndigheter benytter for internkommunikasjon. Skulle det bli scenariet kan også frekvensene til DAB-nettet være et mål for elektronisk krigføring.

Temaet i denne masteroppgaven er hvordan cyberhendelser i cyberdomenet kan påvirke allmenkrigkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne for krisekommunikasjon. Det er derfor ikke vurdert eller drøftet hvordan elektronisk krigføring kan påvirke de samme evnene for allmennkringkastere eller norske myndigheter. Men skulle elektronisk krigføring bli brukt mot Norge i en krise eller konflikt har det potensiale for å påvirke både en allmennkringkasters evner til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon (Samtaleintervju med Helland-Olsen gjennomført den 7. mai 2018).

Konklusjon

I denne masteroppgaven har det nå vært gjennomført en komparativ studie av tre caser. De tre casene dannet grunnlaget for intervjuer med NRK og Kommunikasjonsenheten i Forsvarsdepartementet. Med bakgrunn i dette har oppgaven svart på følgende problemstilling:

Hvordan kan cyberhendelser i krise og konflikt utfordre norske allmenkrigkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon?

Analysen har vist at det er flere typer av cyberhendelser som kan utfordre norske allmenkringkasteres evner til å løse sitt samfunnsoppdrag, og norske myndigheters evne til krisekommunikasjon. Bruk av teknikker som nettsidevandalisme, tjenestenektangrep, cyberangrep rettet mot cyberinfrastruktur, cyberangrep mot mobiltelefoni, fysisk sabotasje av

cyberinfrastruktur og hacking av infrastruktur til telekommunikasjon og internett er alle teknikker som skaper utfordringer.

Nettsidevandalisme kan utfordre norske allmenkringkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon ved at en hacktivist tar over nettsidene deres. Slik kan gruppen eller organisasjonen publiserer et politisk budskap, enten i form av tekst eller bilder. Ved å gjøre det prøver de å spre sitt politiske syn og påvirke publikummet som vanligvis benytter nettsiden. Nettsidevandalisme er ikke den hendelsen som vekker størst bekymring i cyberdomenet.

Bruk av tjenestenektangrep kan ha langt større effekt enn nettsidevandalisme. Casene viser at tjenestenektangrep gjorde nettsider for media utilgjengelig i en periode hvor informasjon ut til befolkningen var kritisk. Om norske myndigheter blir utsatt for et tjenestenektangrep som er vellykket, kan det påvirke norske myndigheters evne til å drive krisekommunikasjon. Her er det noen forutsettinger for at det skal ha en påvirkning. Blir myndighetene angrepet uten at nyhetsmedier blir utsatt for tjenestenektangrep, har norske myndigheter muligheter for kommunikasjon gjennom nyhetsmedier og sosiale medier. Dersom mediene og allmenkringkasterne blir utsatt for tjenestenekt samtidig som norske myndigheter blir mulighetene færre for krisekommunikasjon. Fremdeles vil det være mulig å benytte NRK P1 som beredskapskanal i DAB-nettet og kommunisere viktig informasjon til norske borgere. NRK har også en avtale med en tredjepart for å flytte sine nettider og vil kunne komme opp igjen for å fortsette viktig nyhetsformidling. Tjenestenektangrep kan påvirke både allmenkringkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krise kommunikasjon, men både NRK og Kommunikasjonsenheten mener å ha løsninger tilgjengelig slik at det ikke vil skape betydelige problemer.

Et cyberangrep som rettes mot selve infrastrukturen til cyberdomenet kan få store konsekvenser. Blir DNS serveren utsatt for et cyberangrep er det ikke sikkert DNS serveren vil være i stand til å gjøre sin oppgave. Om det skulle skje med en DNS server hvor norske allmennkrigkastere og norske myndigheter har sine IP-adresser vil ikke nettsiden lastes. Det vil påvirke norske allmenkrigkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon. I det norske kjernenettet til digital kommunikasjon går trafikken for telefoni, mobiltelefoni, internett og TV. Dersom kjernenettet skulle bli angrepet og overbelastet vil det kunne påvirke all den trafikken som er lagt i infrastrukturen. Uten telefoni,

internett eller tv vil dette kunne påvirke både medias evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon. Men også her er det muligheter for norske myndigheter og opprettholde krisekommunikasjon gjennom NRK P1. Med DAB-nettet vil det da også være mulig for en allmenkringkaster å opprettholde nyhetsformidling.

Mobiltelefon er i dag et av de viktigste verktøyene for digital kommunikasjon. Når det ikke er tilgjengelig for bruk vil det kunne gå utover informasjonsutveksling og koordinering. Dersom enkeltpersoners telefoner blir tatt ut kan det omgås. Kommunikasjonsenheten i Forsvarsdepartementet mente det var mer realistisk at hele mobilnettet ble tatt ned i tilfelle en krise eller konflikt. Dersom det skulle bli scenariet vil det kunne påvirke digital kommunikasjon som går over mobiltelefonnettet. En slik hendelse kan ha begrenset effekt på medias evne til å løse sitt samfunnsoppdrag all den tid en allmenkringkaster som NRK har alternative kommunikasjonslinjer for å få nyhetssaker frem til redaksjonen. Norske myndigheter sin krisekommunikasjon mister et viktig verktøy for å nå den norske befolkningen med sitt budskap. Samtidig har norske myndigheter andre kanaler, da spesielt NRK P1 som en distribusjonskanal.

Den norske cyberinfrastrukturen er bygget opp av kjernenettverk, regionalnett og aksessnett. Kjernenettverket er lagt i en ring, slik at brudd på kablene kan rutes i motsatt retning og likevel komme frem. Fysisk sabotasje må derfor gjøres flere steder for at det skal ha effekt. Ved at det i en krise eller konflikt skulle skje en fysisk sabotasje på flere steder av kjernenettverket vil det påvirke all kommunikasjon som ligger i nettverket. Det er telefoni, mobiltelefoni, TV og internett. Igjen er ikke DAB en del av kjernettverket og vil ikke bli påvirket av fysisk sabotasje når kjernetettet blir det. Nyhetsformidling på DAB og krisekommunikasjon gjennom NRK P1 vil fortsatt være mulig. Men det vil påvirke allmenkringkasteres evne til å løse sitt samfunnsoppdrag på de andre plattformene som tv, internett, telefoni og mobiltelefon. Norske myndigheter vil kunne miste sin hovedkanal for kommunikasjon som er via digitale kommunikasjonslinjer, men har fortsatt muligheten for krisekommunikasjon gjennom NRK P1 på DAB-nettet.

Fremgangsmåten som ble brukt ved hacking av strømnettet i Ukraina kan overføres til annen type infrastruktur der i blant cyberinfrastruktur. En inntrenger kan få tilgang til styringssystemer og kan slå av og på deler av det norske cyberdomenet. Et slikt scenario hvor en utenforstående

har kontroll på cyberinfrastrukturen kan påvirke norske allmenkringkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon.

I de tre casene har hendelser som nettsidevandalisme, tjenestenektangrep, cyberangrep mot cyberinfrastruktur, epost spam og skadevare, cyberangrep mot mobiltelefoni, og fysisk sabotasje av infrastruktur påvirket den digitale kommunikasjonen. Intervjuene bekrefter at disse teknikkene også kan påvirke den digitale kommunikasjonen i Norge. Selv om disse teknikkene har potensialet for å påvirke norske allmenkringkasteres evne til å løse sitt samfunnsoppdrag og norske myndigheters evne til krisekommunikasjon er norske allmenkringkastere og norske myndigheter bevist på trusselen som hendelser i cyberdomenet kan utgjøre og har planer for hvordan dette skal håndteres. Så selv om de skulle utsettes for cybermakt har norske allmenkringkastere flere alternativer for å kunne løse sitt samfunnsoppdrag, og de gjelder også for norske myndigheters krisekommunikasjon.

Litteraturliste

Adair, Steven. 2008a. “The Website for the President of Georgia Under Attack – Politically Motiveated?” *Shadowserver Foundation.* Lest 05. april .2018. https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720.

Adair, Steven. 2008b. Georgian Websites Under Attack –DDoS and Defacement. *Shadowserver Foundation.* Lest 05. april 2018. https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080811.

Adair, Steven. 2008c. “Georgian Attacks: Remember Estionia?” *Sadowserver Foundation.* Lest 05. april 2018. https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080813.

Agence France Presse. 2014. ”Hackers Target Ukraine´s Election Website”. Lest 16. april 2018. https://www.securityweek.com/hackers-target-ukraines-election-website.

Alnes, Espen 2018, ”Kan være på veg mot ein ny kald krig”. *NRK*. Lest 28. februar 2018. https://www.nrk.no/urix/kan-vere-pa-veg-mot-ein-ny-kald-krig-1.13981960.

Andress, Jason og Steve Winterfeld. 2014. *Cyber Warefare Techniques, Tactics and Tools for Security Practitioners.* Waltham USA: Syngress

Baezner, Marie og Patrice Robin. 2017. *Cyber and Information warfare in the Ukrainian conflict.* Center for Security Studies. Zurich

Bing, Chris. 2017. “Russian hacker group ”CyberBerkut” returns to public light with allegations against Clinton”. *Cyberscoop.* Lest 27. april 2018. https://www.cyberscoop.com/cyberberkut-returns-hillary-clinton/.

Bogn, Øystein. 2018. *Russlands Hemmelige Krig Mot Vesten.* Kagge Forlag. Oslo

Bratberg, Øyvind. 2014. *Tekstanalyse for samfunnsvitere.* Oslo: Cappelen Damm A/S

Carr, Jeff (2008): *Project Grey Goose,* Washington DC.

Central Intelligence Agency. 2018. “World Factbook: Estonia”. *CIA.* Lest 30. mars 2018. https://www.cia.gov/library/publications/resources/the-world-factbook/geos/en.html.

Clayton, Mark. 2014. “New Details of Massive Cyber Attack During Last Month´s Ukrainian National Elections”. *Christian Science Monitor.* Lest 21. mars 2018. http://www.matthewaid.com/post/89154062321/new-details-of-massive-cyber-attack-during-last.

Collier, Mike. 2007. “Cyber Superpower: Estonia is getting a reputation for being security savvy. Just ask the hackers”. *Transition Online: Regional Intelegance.* Lest 30. mars 2018. http://www.tol.org.pva.uib.no/client/article/19241-cyber-superpower.html.

CyberBerkut. 2014. Blogg. Lest 21. mai 2018. https://cyber-berkut.org/en/olden/index3.php.

Direktorat for forvaltning og IKT. 2014. ”Regelverk for digital kommunikasjon”. Lest 07. april 2018. https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/regelverk-digital-kommunikasjon.

Direktorat for Forvaltning og IKT. 2018. ”Om DIFI”. Lest 14. mai 2018. https://www.difi.no/om-difi.

Egge, Åsmund. 2017. ”Sovjetunionen”. *Store Norske Leksikon*. Lest 25. mars 2018. https://snl.no/Sovjetunionen.

Filseth, Gunnar og Fredrik Thordarson. 2016. ”Georgias Historie”. *Store Norske Leksikon.* Lest 01. april 2018. https://snl.no/Georgias_historie.

FN. 1948. ”FNs Verdenserklæring om menneskerettigheter”. Lest 19. mai 2018. https://www.fn.no/Om-FN/Avtaler/Menneskerettigheter/FNs-verdenserklaering-om-menneskerettigheter.

FN. 2016. ”Ukraina”. Lest 25. mars 2018. https://www.fn.no/Konflikter/Ukraina.

FN. 2018. ”Internettbrukere”. Lest 26. april 2018. https://www.fn.no/Statistikk/Internettbrukere.

Forsvarsdepartementet. 2014. *Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i Forsvarssektoren*. Oslo: Forsvarsdepartementet

Freedomhouse. 2016. “Freedom on the Net 2016”. Lest 27. april 2018. https://freedomhouse.org/report/freedom-net/2016/ukraine.

Friedman, George. 12. august 2008. “The Russi-Georgian War and the Balance of Power”. *Stratfor*. Lest 05. april 2018. http://blog.cafewall.com/wp-content/uploads/2008/09/rus-v-geo-analysis.pdf.

Gooding, Dan. 2017. “Hackers triger yet another power outage in Ukraine”. *Ars Technica.* Lest 16. april 2018. https://arstechnica.com/information-technology/2017/01/the-new-normal-yet-another-hacker-caused-power-outage-hits-ukraine/.

Gorchinkaya, Katya, Olga Rudenko og William Schreiber. 2014. “Authoraties: Hackers foild in big to rig Ukraine presidential election result”. *Kyiv Post*, 25. mai 2014. (Lest 21. mars 2018). https://www.kyivpost.com/article/content/may-25-presidential-election/authorities-hackers-foiled-in-bid-to-rig-ukraine-presidential-election-results-349288.html.

Grassglobal. 2012. ”DDoS attacks target media covering protestes in Ukraine”. Lest 21. mai 2018. https://grassglobal.com/2013/12/14/ddos-attacks-target-media-covering-protests-in-ukraine/

Grunnloven. *Kongeriket Norges Grunnlov av 1814.* Sist endret 27. mai 2014. http://grunnloven.lovdata.no.

Healey, Jason. 2013. *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Arlington: Cyber Conflict Studies Association

HostExploit. 2018. “About”. Lest 15. mai 2018. http://hostexploit.com/?p=about

Internet Live Stats. 2018. “Ukraine Internet Users”. Lest 27. april 2018. http://www.internetlivestats.com/internet-users/ukraine/.

IKTnytt.no. 2018. ”Hva er en zombie/botnet?” Lest 03. april 2018. http://iktnytt.no/zombie-botnet.

Jackson, Patric. 2007. “Playing Estonia´s plotical cards”, *BBC*, 12. mai 2007. (Lest 14. Januar 2018). http://news.bbc.co.uk/2/hi/europe/6645789.stm

Jarstad, Anne K og Tomothy D. Sisk. 2008. *From War to Democracy.* Cambridge University Press, New York

Johnson, Mike. 13. august 2008. “Georgian Websites Under Attack – Don´t Believe the Hype*”. Shadowserver Foundation.* Lest 05. april 2018. https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080812.

Keizer, Gregg (2008): “Cyberattacks knock out Georgia´s Internet precence”. *Computerworld*. Lest 26. januar 2018. https://www.computerworld.com/article/2532289/cybercrime-hacking/cyberattacks-knock-out-georgia-s-internet-presence.html.

Komputer for alle. 2015. ”Hva er malware?” Lest 15. mai 2018. http://komputer.no/sikkerhet/malware/hva-er-malware.

Kovacs, Eduardo. 2013a. “Anonymous Ukraine Launches OpIndependence, Attacks European Investment Bank”. *Softpedia news.* Lest 20. mars 2018. http://news.softpedia.com/news/Anonymous-Ukraine-Launches-OpIndependence-Attacks-European-Investment-Bank-395790.shtml.

Kovacs, Eduardo. 2013b. “Radio Free Europa Website Hit by DDoS Attack During Kiev Protests”. *Softpedia news*. Lest 20. mars 2018. http://news.softpedia.com/news/Radio-Free-Europe-Website-Hit-by-DDOS-Attack-During-Kiev-Protests-407319.shtml.

Landler Mark og John Markoff. 2007. “Digital Fears Emerge After Data Siege in Estionia”. *The New York Times,* 29. mai 2007. (Lest 14. januar 2018). http://www.nytimes.com/2007/05/29/technology/29estonia.html.

Lang-Ionatamishvili, Elina og Sanda Vetoka. 2015. ”Strategic Communication and Social Media in the Russia Ukraine Conflict”. i *Cyberwar in perspective: Russian Aggression Against Ukraine*, redigert av Kenneth Geers. 103-113. NATO CCD COE Publications: Tallin

Lavrov, Anton. 2010. “Timeline of Russian-Georgian Hostilities in August 2008”. i *The Tanks of August,* redigert av Pukhov, Ruland. 37-76. Center for Analysis of Strategies and Technologies: Moskva

Lee, Robert M. Michael J. Assante og Tim Conway. 2016. *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Electricity Information Sharing and Analysis Center. Washington DC.

Leyden, John. 2009. "Russian politician: My assistant started Estonian cyberwar". *The Register*. 10. mars 2009. (Lest 14. januar 2018). https://www.theregister.co.uk/2009/03/10/estonia_cyberwarfare_twist/.

Lowe Christian. 2009. "Kremlin loyalist says launched Estonia cyberattack", *Reuters* 13. mars 2009. (Lest 14. januar 2018). https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313.

Lied, Finn og Torolf Rein. 2014. "Elektronisk Krigføring". *Store Norske Leksikon.* Lest 15. mai 2018. https://snl.no/elektronisk_krigføring.

Markoff, John. 2008. "Before the Gunfire, Cyberattacks", The New York Times. 12. august 2008. (Lest 22. januar 2018). http://www.nytimes.com/2008/08/13/technology/13cyber.html.

Marsh, Peter. 22 oct 2015. *"Daily Miracle 2.0: Time to Fight Back". Editor&Publisher.* 22. oktober 2015. (Lest 24. april 2018). http://www.editorandpublisher.com/columns/daily-miracle-2-0-time-to-fight-back/.

Maurer, Tim og Scott Janz. 2014. *The Russian-Ukraine Conflict: Cyber and information warefare in a Regional Context.* Center for Security Studies. Zurich

Medienorge. 2018a. "Lesing av papiraviser og nettaviser en gjennomsnittsdag". *Universitetet i Bergen og Statistisk Sentralbyrå*. Lest 14.05.2018 http://www.medienorge.uib.no/statistikk/medium/avis/360

Medienorge. 2018b. "Andel med tilgang til internett – resultat". *Universitetet i Bergen og Statistisk Sentralbyrå*. Lest 20. april 2018. http://www.medienorge.uib.no/statistikk/medium/ikt/347.

Nasjonal Sikkerhetsmyndighet. 2018. "Risiko 2018, Verdifulle individer, Verdifulle virksomheter, Verdufull infrastruktur". Lest 21. mai 2018. https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf.

NATO. 2018. "Member countries". Lest 25. mars 2018. https://www.nato.int/cps/en/natohq/topics_52044.htm.

Nazario, Jose. 2009: "Politically Motivated Denial of Service Attacks" i *The Viritual Battlefield: Perspective on Byberwarefare,* redigert av Czosseck, Christaian og Kenneth Geers. 163-181. Amterdam: IOS Press

Nazario, Jose og Andre M. Dimino. 2008. "An In-Depth Look at the Georgia-Russia Cyber Conflikt of 2008". *Arbor Networks*. Lest 26. januar 2018. http://www.shadowserver.org/wiki/uploads/Shadowserver/BTF8_RU_GE_DDOS.pdf.

Network Solutions. 2018. “Managing Domain Name Servers”. Lest 02. mai. 2018. http://www.networksolutions.com/support/what-is-a-domain-name-server-dns-and-how-does-it-work/.

NOU 2015:13. 2015. *Digital sårbarhet – sikkert samfunn – Beskytte enkeltmennesker og samfunn i den digitalisert verden.* Oslo: Departementenes sikkerhets- og serviceorganisasjon Informasjonsforvaltningen. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/.

NRK. 2018a. ”NRK-plakaten”. Lest 23. april 2018. https://www.nrk.no/informasjon/nrk-plakaten-1.12253428.

NRK. 2018b. ”Forholde Norge-Russland oppsummert”. Lest 24. april 2018. https://www.nrk.no/nyheter/forholdet-norge-_-russland-1.12423222.

Nye, Joseph S. 2014. ”Putin´s Calculus”. *Project Syndicate*. 10. april 2014 (Lest 21. januar 2018). https://www.project-syndicate.org/commentary/joseph-s--nye-asks-whether-russia-s-short-term-gains-in-ukraine-will-be-worth-the-long-term-loss-of-soft-power.

Organisasjon for Sikkehet og Sammarbeid i Europa. 2014. *OSCE/OIDHR Election Observation Mission - Final report.* Warswa

Omdahl Jan. 09.03.2010. ”For 15 år siden fantes det ikke nettaviser i Norge*”. Dagbladet.* 09. mars 2010. (Lest 14. mai 2018). https://www.dagbladet.no/kultur/for-15-ar-siden-fantes-ikke-nettaviser-i-norge/64988291.

Pakharenko, Glib. 2015. “Cyber Operations at Maidan: A First-Hand Account”. i *Cyberwar in perspective: Russian Aggression Against Ukraine*, redigert av Kenneth Geers. NATO CCD COE Publications: Tallin

Pallin, Carolina Vendil og Fredrik Westerlund. 2009. “Russia´s war in Georgia: lessons and consequnences”. *Small Wars & Insurgencies* vol. 20 (2): 400-424

Polityul, Pavel og Jim Finkel. 2014. “Ukraine says communications hit, MPs phones blocked”. *Reuters*. 04. mars 2014. (Lest 26. april 2018). https://www.reuters.com/article/ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSL6N0M12CF20140304.

Presseforbundet. 2015. ”Vær Varsom-plakaten”. Lest 23.04.2015. http://presse.no/pfu/etiske-regler/vaer-varsom-plakaten/ [23.04.2015]

RadioFreeEuropa. 2018. ”About us”. Lest 26. april 2018. https://pressroom.rferl.org/p/6091.html.

Rafati, Mohammad. 27. mai 2018. “Cyber Attacks on Ukraine Elections Servers came from Russia”. *Cyberwarzone*. Lest 20. mars 2018. https://cyberwarzone.com/cyber-attacks-ukraine-elections-servers-came-russia/.

Rid, Thomas. 2013. *Cyber war will not take place.* New York: Oxford University Press

Ringdal, Kristen. 2013. *Enhet og Mangfold.* Bergen: Fagbokforlaget
Bergen: Fagbokforlaget

Rodhes, Ron. 2011. *Cyber Meltdown.* Eugene, Oregon: Harvest House Publishers.

Russell, Alison Lawlor (2014): *Cyber Blockades*, Washington DC: Georgetown University Press.

SearchSecurity. 2018. "Spear phishing". Lest 15. mai 2018. https://searchsecurity.techtarget.com/definition/spear-phishing.

Security Service of Ukrane. 2014. "Security Service of Ukraine ensured protection and safe function of telecommunication system of the Central Election Commision during elections of the President of Ukraine". *SSU Press Center.* 27. mai 2014 (Lest 21. mars 2018). http://ssu.kmu.gov.ua/sbu/control/en/publish/article;jsessionid=29500438081F244E522F8D6E37C38423.app2?art_id=126126&cat_id=124945.

Stoltz, Thomas. 2009. "The Paradox of Living in Paradise: Georgia´s Decent into Chaos". i *The Guns of August 2008 Russia´s war in Georgia,* redigert av Cornel, Svante E. & S. Fredrick Starr. 10-28. New York: M.E. Sharp Inc

Techterms. 2018. *Firmware.* Lest 15. Mai.2018. https://techterms.com/definition/firmware.

Tikk Eneken, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm og Liis Vihul. 2008. *Cyber Attacks Against Georgia: Legal Lessons Identified.* Tallin: Cooperativ Defence Center of Excellence (CCD COE)

Tikk Eneken Kadri Kadri og Liis Vihull. 2010: *International Cyber Incidents Legal Considirations.* Tallin: Cooperativ Defence Center of Excellence (CCD COE)

Trend Micro. 2015. "Hactivisk Group CyberBerkut Attacks German Official Websites." Lest 27. april 2018. https://blog.trendmicro.com/trendlabs-security-intelligence/hacktivist-group-cyberberkut-behind-attacks-on-german-official-websites/.
Trend Micro. 2018. "Website Defacement". Lest 15. mai 2018. https://www.trendmicro.com/vinfo/us/security/definition/website-defacement.

Ukrinform. 2014. "SBU neutralizes virus intended to destroy election results". Lest 21. mai 2018. https://www.ukrinform.net/rubric-politics/1665990-sbu_neutralizes_virus_intended_to_destroy_election_results_321822.html.

Vtaliymoroz. 2013. "DDoS attacks target media covering protests in Ukraine". *Grassglobal*. 13. desember 2013. (Lest 20. mars 2018). https://grassglobal.com/2013/12/14/ddos-attacks-target-media-covering-protests-in-ukraine/.

WhatIS. 2017. "Command-and-control server (C&C center)". Lest 05. april 2018. https://whatis.techtarget.com/definition/command-and-control-server-CC-server.

Zetter, Kim. 2017. "The Ukrainian Power Grid Was Hacked Again". *Motherboard*. 10. januar 2017. (Lest 20. mars 2018). https://motherboard.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report.

Øverland, Indra. 2009. ”Georgia og Russland”*, Norsk Utenrikspolitisk Institutt (NUPI)* 15. februar 2009. (Lest 26. januar 2018). http://hvorhenderdet.nupi.no/Publikasjoner/Innsikt-og-kommentar/Hvor-hender-det/HHD-2009/Georgia-og-Russland.

Vedlegg 1. Intervjuskjema for Kommunikasjonsenheten i Forsvarsdepartementet

1. Hva er din stilling og hva innebærer det?

2. Hva er den viktigste informasjonskanalen kanalen for norske myndigheter for å dele viktig informasjon i en krise eller konflikt?

3. NRK er definert som en beredskapskanal for informasjon ut til befolkningen for norske myndigheter gjennom §23 i NRK plakaten. Dersom NRK er utsatt for et cyberangrep som forhindrer NRK i å publisere informasjonene, hvilke andre kanaler har norske myndigheter for å nå ut med sin informasjon?

4. Dersom en tjenestenekt eller liknende angrep rammer norske myndigheters datasystemer, hvordan kan det påvirke norske myndigheters evner for krisekommunikasjon ut til den norske befolkningen?

5. I hvor stor grad ser norske myndigheter på nettsidevandalisme som en trussel for norske myndigheters evne til krisekommunikasjon?

6. I Estland og Georgia ble det sendt store mengder med spam som førte til at epost serverne til myndigheten ble overbelastet og utilgjengelig. Dersom epost blir utilgjengelig for norske myndigheter, hvordan kan det påvirke evnen for krisekommunikasjon?

7. I casene Estland og Georgia ble cyberinfrastruktur angrepet, slik at de store nettleverandører fikk problemer med å lever sine tjenester. Kan en slik hendelse påvirke norske myndigheters evne for informasjon og krisekommunikasjon?

8. Hvor viktig vil kommunikasjon via mobiltelefon være i en krise eller konflikt?

9. I Ukraina ble offentlig strømnettet hacket og satt ut av drift etter en epost kampanje rettet mot offentlige institusjoner. Fremgangsmåten kan benyttes for å få tilgang også til andre systemer. I Estland og Georgia viste cyberangriperne vilje til å ta ut cyberinfrastruktur. Om samme fremgangsmåte rettes mot kommunikasjonslinjer fremfor strømnettet, har norske myndigheter noen tanker om det?

Vedlegg 2. Intervjuskjema for NRK

1. Har NRK beredskapsplaner for hendelser i cyberdomenet evt. hvorfor?

2. Mener NRK at de som et stort mediehus er spesielt utsatt for hendelser i cyberdomenet?

3. Dersom NRK skulle bli utsatt for tjenestenektangrep, vil NRK kunne være raskt oppe igjen dersom nettsiden skulle bli skadet?

4. Kan medier som NRK skille på nyheter som er tidskritiske og ikke tidskritiske?

5. Har NRK noen tanker om hvordan tilliten til NRKs produkt kan påvirkes av hendelser i cyberdomenet?

6. Har NRK noen tanker om hvordan nettsidevandalisme kan påvirke NRKs publisering av nyheter på nett?

7. Er epost spam og skadevare en trussel for NRK?

8. Dersom leverandøren / leverandørene av digitale tjenester til NRK skulle bli utsatt for cyberangrep som gjør at de ikke er i stand til å levere sine tjenester, hvilke konsekvenser kan det ha for NRK?

9. I NRK plakatens §23 er NRK gitt et beredskapsansvar. Har NRK noe tanker om hvordan det skal løses dersom NRK blir utsatt for cyberhendelser
   - §23 nevner at informasjonene fra myndighetene skal være tilgjengelig på minst en av distribusjonsplattformene, hva legger NRK i det?
     - Holder det at NRK klarer å distribuere informasjonen på en av sine distribusjons kanaler som radio, TV eller på sine nettsider?
     - Eller er tolkningen av beredskapsansvaret slik at budskapet skal være tilgjengelig på alle distribusjonsplattformer slik at Norges befolkning får det med seg på minst en av plattformene?

10. Hvor viktig er mobiltelefon og telenettet for NRK dersom det oppstår en krise eller konflikt?

11. Som beredskapskanal, har NRK og norske myndigheter en egen kommunikasjonskanal som ikke er avhengig av mobiltelefon eller telenettet?

12. I Ukraina ble strømnettet hacket gjennom bruk av skadevare som ble sendt ut i en epost. En inntrenger fikk tilgang på distribusjonssystemene til det Ukrainske strømnettet og klarte å stenge strømmen til 225 000 innbyggere etter å ha kartlagt systemet over enger tid.