Cyberforsvar

- Er det viktig i dagens samfunn?

Kadett Aleksander Højklint

Bachelor i militære studier; ledelse og landmakt

Krigsskolen

Høst 2013

Antall ord: 7827

Innholdsfortegnelse

1. Introduksjon

1.1 Bakgrunn

«Stadig flere land anerkjenner cyberangrep som en grunnleggende trussel mot nasjonal sikkerhet» skriver Kristin Bergtora Sandvik (s 252). Roger Johansen skriver i samme utgave av bladet, *Internasjonal politikk*, at cyberdomenet stiller nasjonalstaten overfor en ny trusseldimensjon (s 242). Vi kan først stille oss følgende spørsmål: Hva er cyberdomenet? Cyberdomenet er bruken av elektroniske hjelpemidler til å utføre handlinger som å lese, lage og dele informasjon over nettet (Langø & Sandvik, 2013, s 221). Hva er det som gjør at cyberdomenet utgjør en ny trussel for nasjonalstaten og nasjonal sikkerhet? De siste 20 årene har IKT endret samfunnet (Johansen, 2013, s. 241). Jeg vil gå nærmere inn på hva denne endringen går ut på i teorikapittelet. Internett og måten vår samfunnskritiske infrastruktur er koblet opp på internett, har gjort at vi må tenke annerledes på sikkerheten rundt disse systemene. Systemer det er snakk om er mobilen din, strømnettet, vann-nettet og mye mer som sørger for at du får dekket dine hverdagslige behov. Noen av disse systemene ble koblet opp på 80-tallet, da internett var nytt og ingen enda ante hvilken innvirkning det ville ha på oss og på hverdagen vår. Sikkerheten på disse systemene er også tilsvarende lav fordi man ikke tenkte at internett ville ha så stor påvirkning på oss eller på samfunnets infrastruktur. William Lynn, viseforsvarsminister i USA, skrev i en artikkel i *Foreign Affairs* følgende om cyberdomenet *« (…) just as critical to military operations as land, sea, air and space»*. Hva slags trusler møter vi på dette området, og hvilke konsekvenser kan et cyberangrep få? Dette er spørsmål som jeg ønsker å svare på videre.

1.2 Valg av problemstilling

Med denne oppgaven ønsker jeg å belyse et tema som jeg synes det er forbausende få som har kjennskap til. Jeg har alltid hatt en interesse for informasjonsteknologi (IT). Dette medførte at jeg ønsket å se nærmere på hva cyberforsvar er, og for min egen del få mer informasjon om det og samtidig kunne formidle til andre hva cyberforsvar er. Denne oppgaven er en belysende oppgave der fokuset mitt er å opplyse om trusselen og konsekvensen. Hvordan instansene sikrer oss mot trusselen er gradert informasjon, og mitt formål med oppgaven, å belyse, ville da falt bort. Ettersom temaet om cyberdomenet er så stort, blir oppgaven noe vid. Det er vanskelig å kun se på et aspekt, som for eksempel trussel, uten å se det i en sammenheng av aktøren og konsekvensen den kunne forårsaket. Dette er

særlig viktig idag, da internett er blitt en så sentral del av alles hverdag. Noen mennesker er også avhengig av å ha tilgang til internett (Rid, 2013, s. vii). Hvem har ikke en smarttelefon i lommen eller en PC på jobben eller i stuen? Det er så lite som skal til for at noen med onde hensikter klarer å utnytte vår uvitenhet til å påføre oss, eller i et større omfang, institusjoner skade. I lys av dette er min problemstilling som følger:

Hvilke trusler står forsvarets datasystemer og samfunnskritisk infrastruktur overfor, og hvilke konsekvenser kan et cyberangrep forårsake?

1.3 Avgrensning

Som avgrensning ønsker jeg å se på et politisk overordnet bilde. Jeg skal ikke gå inn på enkeltpersoner som blir hacket, men fokusere på samfunnskritisk infrastruktur og forsvarets datasystemer som kan bli utsatt for cybertrusler. Jeg kommer også til å avgrense meg til Cyberforsvaret og Norwegian Computer Emergency Response Team(NorCERT) sitt arbeid innenfor cyberforsvar, og utelater bedrifter som har sine egne instanser til cyberforsvar. Videre kan jeg ikke gå dypt inn på hvordan de sikrer oss, da dette er gradert informasjon. Cyberforsvar er et svært vidt område, og jeg velger derfor å holde meg til Norge, og går ikke inn på hva NATO gjør i denne forbindelse. Disse avgrensningene er nødvendige for å holde meg innenfor oppgavens begrensede lengde og tid.

2. Metode

2.1 Valg av metode

Jeg har valgt å bruke kvalitativ metode for å finne svar på om cyberforsvar er viktig i dagens samfunn. Kvalitativ metode er en måte å samle inn data på ved å henvende seg til personer som sitter på relevant kunnskap og erfaring. (Johannessen, Tufte, Kristoffersen, 2010, s 103). Dette fordi jeg ønsker å få dybdeinformasjon og få kunnskap på et område som er lite kjent fra før (Enstad, 2013). Jeg kommer til å benytte en metode-triangulær tilnærming der jeg gjennomfører en dokumentanalyse av bøker og artikler som er skrevet om cyberforsvar. Deretter skal jeg gjennomføre semi-strukturerte intervjuer på et begrenset antall informanter. Metode-triangulering er å bruke flere metoder for å finne og samle inn data og styrke tilliten til funnene (Johannessen et al, s 367). Dokumentanalyse er å finne et budskap i en tekst og trekke konklusjoner som svarer på problemstillingen (Johannessen et al, 2010, s 164). Et semi-strukturert intervju er et intervju med en intervjuguide. Her har du et utvalg spørsmål som skal hjelpe deg å svare på det problemstillingen skal belyse (Johannessen et al, 2010, s 139). Grunnen til at jeg har valgt semi-strukturert intervju, er at jeg ønsker at informantene skal snakke om sine betraktninger på bakgrunn av sin utdanning og faglige kompetanse ved å stille åpne spørsmål (Johannessen et al, 2010, s 136-137). Til slutt skal jeg analysere det jeg har lest og det som er kommet frem i intervjuene.

For å løse dette baserer jeg meg på dokumentanalyse fra personer som har inngående kjennskap til temaet. Jeg har valgt å bruke Thomas Rid sin bok «Cyber War Will Not Take Place». Videre bruker jeg tidsskriftet *Internasjonal Politikk*, kvartalsrapporter fra Nasjonal sikkerhetsmyndighet (NSM)/NorCERT, samt rapporter fra Forsvarets Forskningsinstitutt (FFI).

Jeg ønsker å gjennomføre intervjuene med mennesker som har god kjennskap til cyberforsvar og truslene vi møter. Jeg skal beskrive trusselen vi møter, og dette gjør jeg ved å ha et intervju som har *«en struktur og et formål»* (Johannessen et al, 2010, s 135). Mitt formål er at jeg ønsker å få en forståelse for og beskrive (Johannessen et al, 2010, s 135) cyberforsvar og trusselen som vi møter. De som jeg skal intervjue jobber i Cyberforsvaret og i NorCERT. Jeg har utarbeidet en intervjuguide som stiller de samme spørsmålene til begge instanser. Dette for å se om de tenker likt på alle områder eller om det er områder de ser ulikt på. Jeg har vært i kontakt med mine informanter før selve intervjuet og gitt dem en forberedelse på hva som blir temaet og bakgrunnen for intervjuet. Fordi jeg har valgt semi-strukturert intervju, kan

jeg også bevege meg litt frem og tilbake mellom spørsmålene mine og ikke være låst til min egen rekkefølge av spørsmål (Johannessen et al, 2010, s 137). Jeg har valgt å bruke diktafon under intervjuet. Det gjør at jeg kan konsentrere meg om det som blir sagt og ikke forstyrre informanten. Jeg kommer til å ta notater for å merke meg viktige svar og momenter.

2.2 Utvalg

Min tanke bak valg av informanter har vært å få personer fra begge miljøene, Cyberforsvaret og NorCERT. Dette har jeg gjort for å få frem meningene til den enkelte instans. Er de enige eller er det noen meningsforskjeller? Jeg har valgt å intervjue kun én fra hver avdeling fordi de representerer en instans, og derfor vil jeg få frem et syn som har stor troverdighet. Per Le fra Cyberforsvaret er ingeniør og har jobbet i cyberforsvaret siden 2012. Han har utdanning innenfor telematikk og informasjonssikkerhet. Fra NorCERT fikk jeg intervjue Marie Moe. Hun er fungerende seksjonssjef for operasjonssenteret hos NSM. Hun har mastergrad i fysikk og matematikk, med spesialisering innenfor kryptografi. Videre har hun en doktorgrad i informasjonssikkerhet fra instituttet for telematikk hos NTNU. Hun har jobbet hos NSM og NorCERT siden 2011.

2.3 Metode- og kildekritikk

Noe som kan være en svakhet med min metode er at jeg har få informanter. I en kvalitativ undersøkelse, hevder Seidman, Kvale og Brinkman (Johannessen et al, 2010, s 104) at man bør gjennomføre intervjuer helt til man ikke får mer ny informasjon. Siden bacheloroppgaven har begrenset med tid, må jeg også begrense antall informanter. Jeg mener at ved å velge personer som representerer instanser, så vil deres mening vise til noe større enn enkeltpersonen selv, nemlig til selve instansen. Dette gjør at jeg, selv med få informanter, tror jeg får frem det som trengs for å dekke cyberforsvar på en god måte som gir dybde om trusselen og betydningen av cyberforsvar. Alt jeg bruker av informasjon fra mine informanter i oppgaven er også sitatsjekket. Dermed ivaretar jeg kvaliteten av innholdet, på bakgrunn av sitatsjekk og hvem de representerer, og trenger ikke intervjue en hel mengde personer.

Videre har dokumentanalysen vært basert på et utvalg av tekster. Jeg har brukt boken til Thomas Rid, «Cyber War Will Not Take Place», en god del. Grunnen til dette er at jeg mener at han, på bakgrunn av sin erfaring og sin utdannelse, er svært troverdig i sin fremstilling av trusselen. I tillegg har han publisert artikler i fagfellevurderte journaler om samme tema. Dette er blant annet i *The Journal of Strategic Studies (*2012). Dette er med på å gi hans bok troverdighet og validitet, da boken bygger på nettopp disse artiklene. Han har også fått god kritikk av boken fra flere hold, og professor i krigsstudier ved Kings College i London, Sir Lawrence Freedman hevder at boken gir et meget godt bilde på trusselen som vi møter (Freedman, 2013). Grunnen til at jeg har valgt å referere til hans hjemmeside, er at han via denne linker videre til personer og instanser som har anmeldt boken hans. Jeg har også brukt NSM/NorCERT sin kvartalsrapport for 1.kvartal i 2013. Her gir de en del nøkkeltall

angående hendelser, samt at de skriver litt om situasjonen i Norge angående cyberhendelser. Dette er NSM/NorCERT sin oppsummering og vurdering av risiko og hendelser mot samfunnskritisk infrastruktur. Til slutt har jeg brukt tidsskriftet Internasjonal Politikk. De hadde i nr2, 2013 et spesielt fokus på cyberspace, og i den forbindelse flere artikler knyttet til dette temaet. Ifølge dem selv er deres ønske følgende: *«(…) presentere faglig innsikt av topp kvalitet på en tilgjengelig måte»* (Nordisk tidsskriftdatabase). Ettersom det er flere forfattere som gir sitt bidrag, og disse har gode ekspertkunnskaper om sitt tema, gir dette validitet og troverdighet. I tillegg er utgiveren av Internasjonal Politikk, NUPI, en underliggende etat av kunnskapsdepartementet, og ble opprette i 1958 av stortinget. Deres formål er å drive med forskning og utredning i den hensikt å opplyse.

Intervjuene mine skal være semi-strukturerte og fremstå mer som en samtale. Dette kan gi mye informasjon som blir vanskelig å analysere i etterkant. Dette kan være en svakhet i min tilnærming. Måten jeg løser dette på, er å benytte meg av intervjuguiden min. Der har jeg spørsmål som gjør at jeg får dekket de temaene jeg trenger. Så lenge jeg bruker intervjuguiden og jobber ut fra den, vil jeg kunne samle inn data og klare å analysere i ettertid (Johannessen et al, 2010, s 139).

3. Teoridel

3.1 Historisk perspektiv

«Cyberkrig kommer!» Dette ble sagt av John Arquilla og David Ronfeldt fra RAND Corporation i 1993 (Rid 2013, s xiii), bare to år etter at World Wide Web (WWW) ble oppfunnet. Internett eksisterte lenge før «WWW» og ble brukt av bedrifter, men i første omgang ble det utviklet til forsvaret og het ARPANET (Advanced Research Project Agency Network). I 1973 koblet den første nordmann, Pål Spilling ved FFI, seg på ARPANET (Røsjø, 2012). Internett-trafikken økte kraftig etter at Microsoft la med en nettleser i Windows 95, og det har vært en enorm økning i antall brukere siden den gang. I 1995 var det på verdensbasis registrert 30 millioner brukere, i 2000 hadde antall brukere steget til 250 millioner og i 2013 er brukerantallet oppe i 2,08 milliarder (Wikipedia, URL 1). På kort tid har internett gått fra å være det noen mente var et forbigående fenomen til å bli noe som mennesker er avhengig av. Mange mener til og med at det å være «tilkoblet» og å ha digitalt utstyr definerer ens velbefinnende (Rid, 2013, s vii). Mye har skjedd på cyberfronten siden «WWW» ble oppfunnet i 1991, og vi bruker mer og mer tid på internett og flere og flere systemer blir koblet opp på internett. I dag går mye av kritisk infrastruktur på et system som heter SCADA (Supervisory Control and Data Acquisition). Kraftverk, rørledninger, vann og avløpssystemer og mye mer (Rid, 2013, s 66) er systemer som bruker denne typen teknologi, og ifølge Rid er sikkerhetsstandarden på disse systemene forbausende lav, og er dermed et lett bytte for en dyktig hacker (Rid, 2013, s 173). Dette er med på å forsterke utsagnet til Kristin Bergtora Sandvik om at cyberangrep er en grunnleggende trussel mot nasjonal sikkerhet. Hva er effekten om man mister muligheten til å styre kritisk infrastruktur? Effekten vi vil se kan kanskje være tilsvarende det som skjer under en naturkatastrofe når kritisk infrastruktur skades (Langø & Sandvik, 2013, s 224); kaos. I dagens mer og mer tekniske samfunn ser vi at det er en økning i cyberangrep mot den statlige og private sektoren (Rid, 2013, s 9). Selv med avanserte sikkerhetstiltak klarer hackere å bryte seg inn og gjøre skader. Dette klarer de ved å infisere PC-er fra utsiden, slik at privatpersoner tar dette med seg på jobben ved hjelp av lagringsmedier og infiserer bedriftens PC-er fra innsiden, strategisk webkompromittering (NorCERT, 2013, s 7). Dette gjør de selvsagt uvitende. Jeg vil komme nærmere tilbake til dette senere i kapittelet.

3.2 Cyberangrep

I takt med at teknologien utvikler seg, får vi også en økning i personer eller instanser som søker å utnytte dette. Dette kan være alt fra kriminelle som ønsker økonomisk vinning til hacking der personen(e) bak ønsker å utnytte svakheter i systemet eller få personer til å gi bort sensitiv informasjon i god tro. Hvis vi går tilbake i tid og ser på tidligere hendelser, har det skjedd flere angrep som varierer i alvorlighetsgrad. Estland ble i 2007 utsatt for et massivt angrep som stoppet det meste av informasjon på internett. Banker, tv-kanaler og regjeringens sider stoppet opp og kunne ikke brukes. Dette pågikk i nærmere tre uker (Rid, 2013, s 30). Det gikk så langt at statsministeren i Estland, Ansip, sa følgende: «*What's the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?*». Forsvarsministeren i Estland tenkte tanken å prøve å iverksette artikkel 5 i NATO-pakten, men dette ville ikke nyttet da ingen av de andre forsvarsministrene i NATO så på cyberangrep som et militært angrep på Estland (Rid, 2013, s 30). Det er svært vanskelig å finne ut hvem som står bak et cyberangrep. Internett gir ingen spesifikk adresse til den som står bak. Du kan koble deg opp via en PC som er koblet opp igjen via en annen PC i et annet land. Dette gjør identifisering vanskelig. Mye tyder på at Russland stod bak dette angrepet på Estland. Det hadde vært store opptøyer på grunn av at estlenderne flyttet en statue over falne russiske soldater 2 uker før Russlands minnemarkering over 2. verdenskrig (Rid, 2013, s 6). Dette var et angrep som var basert på Distributed Denial of Service (DDoS), det vil si et angrep som sender informasjon/pakker til mottakeren som gjør at systemet blir overarbeidet, som videre medfører at vanlig trafikk ikke slipper til. Det finnes to måter å gjøre et slikt angrep på. Den ene måten er Denial of Service (DoS), som går ut på at én PC prøver å sende nok informasjon til mottaker slik at systemet blir overarbeidet. Dette er imidlertid lite effektivt. Den mest effektive formen er DDoS, som er et nettverk av PC-er som sender informasjon til mottakeren, og som sammen vil få langt større effekt og vil overarbeide systemet (Wikipedia, URL 2**).**

Neste eksempel er angrepet på de Iranske atomsentrifugene i Natanz. Her utsatte ormen Stuxnet Irans anrikningsprosess av uran ved å skade atomsentrifugene, samt at den fikk ingeniørene til å bli usikre på seg selv og jobben de gjorde. Dette er per dags dato det eneste potente cybervåpenet som noensinne er tatt i bruk (Rid, 2013, s 105-106). Definisjonen på et cybervåpen er ifølge Thomas Rid*: «(…) computer code that is used, with aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings»*. Stuxnet hadde flere aspekter ved seg som gjorde det til et meget sofistikert og velutviklet

våpen. For det første utnyttet Stuxnet fire såkalte «Zero-day exploits». Dette er svakheter som ikke tidligere er oppdaget i et program, hvilket gjør dem svært verdifulle for en hacker. For det andre hadde utviklerne bak Stuxnet fått tak i to digitale sertifikat som gav skjult tilgang til sider man ellers ikke kunne fått tilgang til (Rid, 2013, s 45). For det tredje var Stuxnet annerledes i forhold til andre ormer når det kom til strategien den brukte. Svært mange PC-er var infisert, rundt 100 000, uten at ormen skadet dem på noen måte. Den skadet kun de PC-ene som var av betydning for oppdraget. Dette er svært uvanlig, da andre ormer gjør stor skade på PC-ene som de infiserer (Rid, 2013, s 46). Dette er den rent tekniske biten av ormen. I tillegg hadde Stuxnet en psykologisk faktor. Den søkte ikke bare å ødelegge kun det tekniske, men gjorde også ingeniørene som jobbet med atomsentrifugene usikre på både seg selv og den Iranske regjeringens evne til å utvikle atomvåpen (Rid, 2013, s 172). Måten ormen gjorde dette på, var å gå inn i systemet som styrer temperaturer i ventiler samt operasjonstemperaturer og gi falske målinger tilbake til ingeniørene. Det ormen altså gjorde var å få systemet til å skade seg selv ved å gi feil informasjon (Rid, 2013, s 44-45). Dette førte til at ingeniørene ble så usikre at de satte ingeniører til å fysisk melde tilbake med radio fra anleggene der prosessene skjedde til de som kontrollerte instrumentene (Rid, 2013, s 32). Ralph Langner er forskeren som fant Stuxnet og som blottla angrepskoden (Cherry, 2010). Langner sier følgende: *«The resources and investment that went into Stuxnet could only be mustered by a 'cyber superpower'»*. Den amerikanske regjeringen har i ettertid erkjent at de tok del i Stuxnet (Rid, 2013, s 45).

Dette er bare to eksempler på cyberangrep som har blitt gjennomført de siste årene. Angrepene er to vidt forskjellige typer cyberangrep, men de viser en trend som øker i stor grad. Vi ser cyberangrep som er større og mer alvorlige, og flere er statsstøttet. Dette gir en gråsone for hva som er et angrep på en nasjon og hva som ikke er det. Ettersom ingen eier internett, er dette svært vanskelig å si. Hvor går «landegrensene» på internett? Slike grenser finnes ikke, og det vi har å beskytte oss med er sikkerhetsinstanser som antivirus-bedrifter og tilsvarende. Vi i Norge har Cyberforsvaret og NorCERT. Dette er to forskjellige instanser, men de driver med det samme, bare for forskjellige klienter. Jeg vil nå gå litt mer inn på hva vi i Norge gjør for å møte denne trusselen ved å fortelle kort om Cyberforsvaret og NorCERT og hva de jobber med.

3.3 Cyberforsvaret

Cyberforsvaret er en avdeling i Forsvaret som har personell med spisskompetanse innenfor sitt fagfelt. Fokusområdet deres er forsvarets datasystemer. Dette sørger de for at

forblir ukompromittert, og slår tilbake eventuelle angrep som rettes mot dem. Personene som jobber med cyberforsvar har god faglig kunnskap og en militær bakgrunn, og de får utdannelsen sin ved Forsvarets ingeniørhøgskole. Her trenes de opp i militære disipliner, samt at de får en relevant og god akademisk utdanning som gjør dem rustet til å takle de nye utfordringene og den økende trenden av angrep vi ser i cyberdomenet (Forsvaret).

3.4 NorCERT

Dette er instansen innenfor cyberforsvar som ivaretar angrep mot samfunnskritisk infrastruktur. De har sine lokaler på Brynseng, hvorfra de overvåker og tar imot angrep daglig (Forsvarets forum). Dette kan være alt fra små virusanslag til større, alvorlige trusler mot bedrifter eller departement. NorCERT er en tverrsektoriell instans, og er underlagt forsvarsdepartementet og justis- og beredskapsdepartementet. De er direkte underlagt NSM, og jobber sammen med cyberforsvaret om det skulle bli behov (Forsvaret).

Mitt inntrykk er at det norske folk generelt vet lite om cyberforsvar og hvor alvorlig denne trusselen er. Espen Barth Eide (2013), tidligere utenriksminister, har sagt følgende: *«Den største utfordringen er å få folk til å forstå hvor alvorlig dette er»*. Dette er med på å underbygge min antagelse om at folk generelt vet lite om cybertrusler. Mitt mål med denne oppgaven er å belyse og skape bevisstgjørelse rundt denne trusselen og de konsekvenser den kan medføre.

4. Analyse

4.1 Generelle betraktninger

Med bakgrunn i intervjuene jeg har gjennomført og de bøkene og artiklene jeg har lest, vil jeg se på hvilke trusler cyberforsvaret og NorCERT møter og hva de gjør for å hindre at truslene gjør skade. I avsnittet om trusler skal jeg se hvilke aktører som finnes, og hvilke aktører som står bak. Til slutt ønsker jeg å se på konsekvensene som et cyberangrep kan forårsake. Jeg vil her drøfte noen scenarier og noen mulige utfall av cyberangrep. Det jeg ønsker å vise til her er hvorfor det er så viktig at vi har et cyberforsvar.

4.2 Trusler

I teorikapittelet har jeg beskrevet eksempler på to typer cyberangrep. Hva er det som skiller disse angrepene? De representer begge alvorlige hendelser som kan skape store problemer for dem som blir utsatt. Det som likevel skiller disse to angrepene er alvorlighetsgraden av dem. Et DDoS-angrep hindrer bare tilgang til systemer midlertidig. Stuxnet, derimot, var en sabotasjeoperasjon som hadde stor effekt og gjorde fysiske skader på et anlegg. I dette kapittelet vil jeg ta for meg de truslene vi ser i Norge, flere tusen anslag hvert kvartal (Moe & Le, 2013), som er rettet mot forsvaret og samfunnskritisk infrastruktur. Jeg ønsker å se på alvorlighetsgraden av truslene, og hvem som kan være de aktuelle aktørene.

Hvilke typer angrep har vi? De to typene angrep det skilles mellom er ikke-målrettede angrep og målrettede angrep, og det er store forskjeller mellom dem. Cyberforsvaret har flere tusen hendelser i året (Le, 2013) Dette innebærer falske alarmer, mindre alvorlige hendelser og alvorlige hendelser. NorCERT sier det samme om trusselbildet de ser (Moe, 2013). Det begge instanser er enig om, er at de ser mest ikke-målrettede angrep. Dette er mindre alvorlige hendelser som økonomisk kriminalitet, spear phishing, ormer og trojanere, i grove trekk (Moe & Le, 2013). Spear phishing må også sees i sammenheng med målrettede angrep, da dette kan være en måte å operere på for å få tilgang til en PC og dermed nettverket. NorCERT håndterer flest saker som er ikke-målrettet, der økonomisk kriminalitet har størst volum av hendelser (Moe, 2013). Her er det snakk om trojanere som spres på norske nettsider, og som tar over PC-en din. Dette skjer ved at det er integrert en ondsinnet kode i nettsiden som gjør at du blir lurt inn på falske sider som ser ut som, for eksempel, nettbanken din. Her logger du deg på, i god tro om at du er på riktig sted. Det som egentlig skjer, er at du har fått opp et falskt vindu

der du taster inn sensitive innloggingsdata. Samtidig sitter det en person i andre enden og taster inn denne informasjonen på det riktige innloggingsvinduet, for så å tømme bankkontoen din. Det som Cyberforsvaret derimot er mer bekymret for, er ormer og trojanere som henter ut informasjon på PC-en din. Dette i seg selv er ikke så farlig, men dersom du har tilgang til PC-er med gradert informasjon, begynner det å bli verre. Tenk deg at din PC er infisert. Du plugger i USB-sticken som du alltid bruker i din egen PC og overfører noen dokumenter. Deretter tar du den med deg på jobb og plugger den i FisBasis PC-en. Nå har du potensielt overført en skadevare over på graderte systemer. Faren nå er at skadevaren henter over gradert data og lagrer dette på sticken. Når du da kommer hjem, vil dette sendes til mottakeren over nettet. Dette kan være svært sensitiv informasjon som kan skade Norge, Forsvaret og våre allierte. En slik hendelse er rapporteringspliktig til NSM (Moe, 2013), da det er snakk om et gradert system. I tillegg kan det også være tegn på at vi har gått fra et ikke-målrettet angrep og over til et målrettet angrep, hvilket både NorCERT og Cyberforsvaret prioriterer. Dette tar oss over på målrettede angrep.

En type hendelser som har økt voldsomt i antall håndterte saker, og som er veldig vanskelig å oppdage, er spionasje (Moe, 2013). Det fremmed etterretning prøver å hente ut av informasjon, er et målrettet angrep. Dette utgjør en mye større trussel, og får størst prioritet (Le, 2013). Bak slike angrep står gjerne aktører med mye større kapasitet, flere ressurser og dyktigere folk. Så langt i år, desember 2013, har NorCERT håndtert 39 alvorlige hendelser (Moe, 2013). NSM skriver i sin kvartalsrapport for 2. og 3. kvartal følgende*: «Når vi bruker begrepet alvorlige hendelser, er det som oftest digital spionasje vi sikter til»*. Et målrettet angrep er at noen velger seg ut spesifikke mål og angriper. For Cyberforsvaret kan dette være datamaskiner som inneholder gradert informasjon (Le, 2013). Aktørene bak slike angrep er gjerne organisasjoner som ønsker å få fatt i hemmeligstemplede dokumenter som sier noe om våre kapasiteter, hvordan en avdeling er strukturert og dermed hvilke oppgaver den avdelingen kan gjennomføre. Dette kan være kritisk for oss i en krisesituasjon, da våre kapasiteter bør være ukjent. Et lignende scenario for NorCERT, som beskytter bl.a. forsvarsindustri, kan være at forretningshemmeligheter blir forsøkt lekket. Man kan se for seg et spionasjeangrep mot forsvarsindustri, industri som leverer våpensystemer til forsvaret. Fienden kan da få tilgang til spesifikasjoner om forsvarssystemer som gjør at de kan forsvare seg bedre mot dem, som igjen gjør at de får en fordel. NorCERT er nasjonalt kontaktpunkt for hendelser i Norge, og alle hendelser som går mot forsvarssektoren deler de med Cyberforsvaret (Moe, 2013). Dette gjør at Cyberforsvaret får den informasjonen de trenger

slik at de kan møte trusselen. NorCERT melder også fra om hendelser til andre sektorer som de har ansvar for. Dette gjør at de sitter på det overordnede bildet, og har kontroll på alle hendelser.

Ikke alle angrep blir oppdaget. Thomas Rid (2013) sier i sin bok at de mest vellykkede angrepene forblir hemmelige. Vi har et begrep som heter APT, Advanced Persistent Threat. Dette betyr at de som står bak angrepet ikke gir seg. De pøser på med målrettede, skreddersydde eposter, eller de har avanserte metoder for å trenge seg inn i systemer (Moe, 2013). De har store kapasiteter som støtter dem, og dette fører oss inn på aktørene. Akkurat som det er store forskjeller på truslene, så er det også stor forskjell på aktørene. I mine intervjuer med Cyberforsvaret og NorCERT kom det tydelig frem at det er forholdsvis lett å skille mellom aktørene (Moe, 2013). Problemet er å bevise hvem som faktisk står bak. Dette samsvarer med det Thomas Rid (2013) skriver angående aktører:

> *«Nearly all political cyber attacks on the empirical record – whether they were done for purposes of espionage, sabotage, or subversion – have one feature in common (…). That feature of digital conflict represents a fundamental, and in many ways disturbing, change when compared to political confrontation in earlier, analogue times, be they violent or non-violent: that change is the attribution problem».*

Her sier Rid at det i den analoge verdene var mulig å se hvem som konfronterte deg, mens dette i det digitale spekteret er blitt mye vanskeligere. Som nevnt i teoridelen, har ikke internett noen grenser. Sporbarheten på internett er ekstremt lav, og det må gjøres noen grep for at det skal kunne endres på. Dette er et problem som Admiral McConnell (2010) adresserte i et intervju til *The Washington Post.* Her foreslo han at internett burde redesignes, slik at det på svært kort tid blir mulig å finne ut hvem som gjorde hva og hvor. Han er tidligere direktør i NSA, og tidligere direktør i National Intelligence i George W. Bush sin regjering.

Hva sier så Cyberforsvaret og NorCERT om hvordan de skiller mellom aktørene? Det som begge instanser sier, er at de ved å se på alvorligheten i et angrep kan si hvilken type aktør som står bak. NorCERT ser på «modus-operandi» (Moe, 2013), og Cyberforsvaret ser på hvilke metoder som blir brukt, for eksempel om det er tidligere kjente signaturer eller om det er zero-days sårbarheter (Le, 2013). Rid (2013) beskriver denne sammenhengen mellom aktør og alvorlighetsgraden av angrepet på følgende måte sin bok: *«the attribution problem is a function of an attacks severity».*

Generalmajor Sundseth, daværende sjef for Cyberforsvaret, sa i et foredrag på Oslo Militære Samfund (2013) at det er tre typer aktører som peker seg ut; kriminelle, hacktivister og statsstøttede organisasjoner. De har forskjellige måter å operere på, og forskjellige fokusområder. Kriminelle er ute etter, for eksempel, økonomisk vinning. De bruker enkle metoder til å lure folk inn i feller der de utnytter uvitenhet og uforsiktighet. Dette kan være banktrojanere som jeg har nevnt tidligere, eller det kan være løsepenge-scam der de tar PC-en til fange ved å låse datafilene og kreve løsepenger for å låse opp datafilene (Moe, 2013). Den andre gruppen er hacktivister som gjerne har en politisk agenda. De ønsker å få frem et synspunkt på noe de er misfornøyde med eller noe de støtter. Den mest kjente hacktivist-bevegelsen er Anonymous. Dette er et internettsamfunn der hackere med variert bakgrunn slutter seg til og bruker cyberdomenet til å vise sitt standpunkt (Moe, 2013). De har absolutt muligheten til å utføre angrep som er alvorlige, men i det lange løp vil ikke alvorlighetsgraden være større enn det som den tredje gruppen får til, nemlig statsstøttede organisasjoner. Dette er de aktørene som har størst kapasitet, mest avanserte metoder og som kan gjøre mest skade. De har et stort apparat tilgjengelig, noe som gjør at de kan oppnå mye i cyberdomenet. Et eksempel er israelernes bombing av en atomreaktor nord i Syria. Det hele startet med at de angrep en radarstasjon som lå helt inntil den tyrkiske grensen ved å bruke cyberdomenet. Dette gjorde at radaren ble satt ut av spill, og var ikke lenger i stand til å se israelernes fly som fløy over grensen og gjennomførte et bombetokt (Rid, 2013, s 11).

Jeg ønsker også å belyse hvor vanskelig det kan være å tilegne noen skyld. I NSMs kvartalsrapport for 1. kvartal 2013 (NorCERT) viser de til et amerikansk sikkerhetsselskap som heter Mandiant. De slapp en rapport, APT1 report (2013), som omhandler spionasjesaker mot den vestlige verden. Her offentliggjorde de en aktør som har gjennomført angrep på Norge, «APT1». Denne gruppen kan spores tilbake til en helt spesifikk bygning i Shanghai, og den kan linkes til ca. 20 lignende saker. I tillegg hevdes det i denne rapporten at APT1 er en del av Peoples' Liberation Army (PLA) Unit 61398 (Rid, 2013, s 155). Dette er den militære delen av Communist Party of China, altså den sittende regjering. Dette gir gode indikasjoner på at det er en statsstøttet aktør, men å bevise at det er dem er en helt annen sak.

FFI kom med en rapport allerede i 2004 som beskrev dette problemet. De skriver i sin rapport Cyber Space Som Slagmark at cyberspace er en arene som ikke har et territorium det tilhører, det har ingen befolkning og ingen politiske institusjoner. Når da cyberdomenet

anvendes til maktbruk, vil det vanskeliggjøre håndhevingen for nasjonalstater fordi trusselen *«(…)i sin natur er global*» (FFI 1). Dette er en rapport som kom tidlig, og som i ettertid blir bekreftet fra flere hold, blant annet fra Mandiant sin rapport fra 2013.

Det som kommer fram av dette kapittelet, er at av de flere tusen hendelser som inntreffer hvert kvartal, er de fleste ikke-målrettede angrep. Dette er mindre alvorlige hendelser som ikke er kritisk for forsvarets datasystemer eller samfunnskritisk infrastruktur. Det som derimot er mer bekymringsverdig, er økningen av målrettede angrep der aktører går etter spesifikke mål, og ønsker å hente ut etterretning og informasjon som de ikke skal ha. Her ser både Cyberforsvaret og NorCERT en økning i antall hendelser. I denne sammenheng må vi se an hvilke type aktører som står bak, da de er med på å tilegne trusselen alvorlighetsgraden. Enkeltpersoner kan helt klart utgjøre en stor trussel, men det er de statsstøttede organisasjonene som utgjør den største trusselen. Som nasjonalstat er det umulig å gjøre noe overfor et domene som ikke har et territorium. Dette støttes både av en rapport av FFI (FFI 1) og det Admiral McConnel (2010) snakket om i sitt intervju i *The Washington Post*. Dette kom også tydelig frem av DDoS-angrepet på Estland, der regjeringen stod maktesløs i forhold til å reagere militært på angrepet.

4.3 Konsekvenser

Hvilke konsekvenser kan et cyberangrep få? Generalløytnant Kjell Grandhagen, sjef for etterretningen, sier han ikke ser bort i fra at det neste 22. juli kan komme fra det digitale rom (2013). Leon Panetta, daværende CIA-sjef, sa i 2011 at *«The next Pearl Harbor could very well be a cyber attack»*. Dette er svært alvorlige uttalelser fra høytstående og innflytelsesrike personer. Det er mange mulige scenarioer på et eventuelt cyberangrep, og det er dette jeg ønsker å drøfte i dette avsnittet. Jeg vil se på hva Cyberforsvaret og NorCERT mener og tenker, samt at jeg kommer til å trekke inn noen av Thomas Rid sine betraktninger omkring temaet.

I og med at Cyberforsvaret og NorCERT har forskjellige fokusområder på hva de beskytter, trekker de frem forskjellige konsekvenser av et potensielt cyberangrep. For Cyberforsvaret kommer det frem at kommunikasjon er det som kan skape de største konsekvensene (Le, 2013). Dette understøttes av følgende sitat fra Roger Johansen (2013): *«De norske cyberstyrkenes mest grunnleggende oppgave blir derfor å etablere en fleksibel og robust informasjonsinfrastruktur (…)»*. Han sier altså at den viktigst oppgaven for Cyberforsvaret er å etablere et sikkert og stabilt kommunikasjonsnettverk. Dette medfører at

Cyberforsvarets viktigste oppgave blir å beskytte forsvarets kommunikasjonsnettverk fra å bli kompromittert og ødelagt. Dette kommer også klart frem av Generalmajor Sundseth sitt foredrag i Oslo Militære Samfund (2013), hvor han trekker frem et eksempel. Under en vinterøvelse i 2005 klarte to cyberoperatører å ta kontroll på sambandssystemet til en divisjon. Ved å få tilgang til et sambandsknutepunkt, kunne de nå lytte på trafikken. Det betydde at fienden hadde tilgang til all informasjon som divisjonen sendte. Dette er absolutt en kritisk hendelse i en krisesituasjon. Hadde dette vært i Afghanistan, og Al-Qaida hadde fått tilgang til vårt samband, ville de hatt mulighet til å lokalisere våre posisjoner og fått etterretning om tid og sted for neste angrep. Det ville vært katastrofalt for vår del. Dette eksempelet går på at vår kommunikasjon blir kompromittert. Hva om vi mistet forbindelsen til våre soldater?

Per Le fra Cyberforsvaret kom med følgende eksempel: La oss si at antenner eller satellitter blir tatt ut på en eller annen måte ved bruk av cyber. Da vil vi blant annet miste muligheten til å kommunisere med hverandre og til å kontakte ledelseselementer i Afghanistan og Norge. Vi vil miste muligheten til å be om forsterkninger, artilleri-dekning og flystøtte. Vi vil altså bli helt isolert uten muligheter for støtte. I et slikt tilfelle ville liv gått tapt, det er det ingen tvil om. Vi har hatt mange situasjoner i Afghanistan der vi har vært avhengig av å kunne opprette kommunikasjon med støtteavdelinger for å komme oss helskinnet ut av situasjoner vi ikke hadde klart å håndtere på egenhånd. NorCERT ser også på kommunikasjonsnettverk som kritisk å ramme (Moe, 2013). Dette gjelder militært så vel som sivilt. Moe (2013) ser for seg at noen kan komme inn udetektert i forsvarets datasystemer og plante en bakdør. Denne bakdøren kan de ha klar til når de trenger den. Denne bakdøren kan for eksempel brukes til å ta ned kommunikasjon under et kritisk punkt i en operasjon, eller den kan brukes ved et fysisk anslag mot oss og ta ned vår kommunikasjon slik at det blir vanskelig for oss å møte situasjonen. Dette er scenarioer som hovedsakelig vil ramme forsvaret. NorCERT ser også for seg scenarioer som rammer samfunnet i større grad.

Hvis du ønsker å skape ødeleggelse, er det *«industrielle prosesser, offentlige tjenester og sivile samt militære kommunikasjonsnettverk du bør ta ned»* (Rid, 2013, s 41). De systemene som gir størst sannsynlighet for uttelling i forhold til ødeleggelse, er SCADA-systemene som jeg har snakket om i teoridelen og i eksempler tidligere. Veldig mange prosesser overvåkes av SCADA-systemer. Dette er «*en måte å kontrollere prosessene ved hjelp av datamaskiner»* (Moe, 2013). Dersom sabotasje er det du ønsker å oppnå, bør du altså gå etter SCADA-systemene. Et godt eksempel på hvilke konsekvenser et slikt cyberangrep kan få, er hva Stuxnet klarte å få til. Her ble et helt prosessanlegg satt ut av spill på grunn av

en orm. Hva om vi trekker linjene til norsk oljeindustri? Hva vil skje om oljeindustrien blir rammet av lignende hendelser? Det er mange mulige scenarioer som kan utspille seg da. En mulighet er at plattformer blir utsatt for sabotasje, slik at for eksempel pumper som drar opp olje slutter å fungere. Dette får ikke så store konsekvenser i seg selv, men hva om dette pågår over lang tid? Et slikt scenario kan få store innvirkninger på den norske økonomien blant annet. Et annet scenario er også sabotasje, men i større omfang. En borerigg bruker SCADA-systemer til å overvåke prosessene om bord. De er med på å overvåke sikkerhetssystemene på plattformen, og gjør at teknikerne kan monitorere prosessene og hindre ulykker. Hva om overvåkningsprosessene på disse systemene blir manipulert, og man får en feil i systemet som ikke oppdages? Det kan være man får en situasjon lik deepwater-horizon ulykken. Dette var en eksplosjon ombord på en plattform på grunn av av en gasslekkasje. Hvis sikkerhetssystemer som skal detektere og forhindre slike feil er manipulert, øker risikoen for at slike ulykker kan skje. I deepwater-horizon ulykken omkom 11 personer, og flere ble skadet. Boreriggen sank, og nærmere 800 millioner liter olje (BBC news, 2010) rant ut i havet.

Hva om et cyberangrep utfører flere slike operasjoner samtidig for å skape størst mulig effekt, og dette i forkant av et militært angrep? La oss se på et scenario der vann og elektrisitet slutter å virke på grunn av et massivt cyberangrep. Dette varer i en dag eller to, og så forsvinner kommunikasjonen. Ingen får ringt ut, og Forsvaret klarer ikke å kommunisere avdelingene imellom. Store internettsider og tv-kanaler som formidler informasjon blir utsatt for DDoS-angrep og hacking, som gjør at kritisk informasjon til sivilbefolkningen ikke når ut, samt at statsministerens twitter-konto blir hacket og meldinger som maner til panikk legges ut. Dette vil føre til panikk blant befolkningen, og de vil kreve informasjon og spørre om hva som skjer og hvorfor ikke noe blir gjort. Deretter blir man utsatt for et militært angrep. Dette er selvsagt et eksempel på et svært massivt angrep som ville vært vanskelig, om ikke umulig, å gjennomføre i denne skalaen. Et realistisk scenario vil derimot være at noen funksjoner rammes. Om elektrisiteten og kommunikasjonsnettverket forsvinner, kan det skape store problemer for folk flest, og vil gi en effekt lik den i et katastrofeområde (Langø & Sandvik, s 224).

En annen type konsekvens er den vi får av å ha et trusselbilde. Vi ønsker å sikre oss mot trusler, og fatter dermed tiltak som skal sørge for dette. Et godt eksempel på slike tiltak er sikkerhet på flyplasser. Det var i 2006 at et terroristangrep ble avverget, der terroristene planla å sprenge syv passasjerfly ved hjelp av flytende sprengstoff. Sprengstoffet hadde de tenkt å

smugle inn ved hjelp av brusflasker og lignende. Denne hendelsen førte til at sikkerheten ble innskjerpet på flyplasser verden over. Passasjerer kan ikke få med seg inn større beholdere enn 1dl, samt at alle flasker og væskebeholdere må få plass i en pose som rommer 1l når den er lukket. Dette er en tydelig konsekvens av en reel trussel som merkes av den enkelte.

At vi vil få en krig som kun utspiller seg i cyberdomenet, er lite trolig. Det er også noe som Thomas Rid (2013) argumenterer for i sin bok. Utsagn som at neste 22. juli kan komme fra det digitale rom, kan ikke støttes opp av noen hendelser så langt. Forsker ved FFI og tidligere forsvarssjef, General Diesen, sa i FFI forum i Oslo Militære Samfund (2013) at det er lite sannsynlig at vi vil se rene cyberkriger. Årsaken til dette er at det er enklere for terrororganisasjoner å forsøke å sprenge samfunnskritisk infrastruktur, da de ikke like lett vil kunne oppnå det samme resultatet ved bruk av et rent cyberangrep. Dette støtter opp om Rid sitt syn. Det er klart at vi vil kunne se sabotasjeaksjone, men ikke med tap av menneskeliv i så stort omfang. Det eneste angrepet som har vært potent til noe slik,t var Stuxnet. Heller ikke her gikk liv tapt, kun materielle skader. Et angrep som er støttet av cyberangrep derimot, er svært sannsynlig. Her kan vi kanskje se lignende hendelser som 22. juli eller som et ledd i en militær aksjon. Det har vi jo allerede sett eksempel på i forbindelse med flyangrepet Israel gjorde i Syria, da de med hjelp av cyber tok ut en radarstasjon. Min konklusjon angående konsekvenser er altså at vi vil kunne se sabotasjeaksjoner, enten alene eller som en del av en større operasjon, samt spionasjeoperasjoner der fremmed etterretning ønsker å skaffe seg informasjon angående våre styrker, handlemåter og våpensystemer.

5. Sammendrag og konklusjon

5.1 Sammendrag av oppgaven

Det er ingen tvil om at vårt samfunn er i stadig teknologisk forandring. Stadig flere av våre systemer blir koblet opp på internett og gjøres lettere tilgjengelig for oss. Med en stadig økende trend av cyberangrep i dette domenet, medfører det at vi må ta noen grep. Min oppfatning er at folk generelt har lite kunnskap på dette området, og jeg ønsket med denne oppgaven å vise til viktigheten av cyberforsvar ved å se på truslene som man møter og aktørene bak, samt konsekvensene som kan oppstå som følge av et cyberangrep. Min problemstilling ble derfor som følger:

Hvilke trusler står forsvarets datasystemer og samfunnskritisk infrastruktur overfor, og hvilke konsekvenser kan et cyberangrep forårsake?

For å klare å løse denne oppgaven, så jeg på hvilke instanser vi har i Norge og hvordan de jobber. Jeg prøvde med mine intervjuer å finne ut hvilke trusler de møter, samt hvor ofte de blir angrepet. Når jeg så på truslene, var det også nødvendig å se på aktørene som står bak. Dette sier noe om alvorlighetsgraden av selve angrepet. Til slutt har jeg gått inn på hvilke konsekvenser et cyberangrep kan ha. Jeg har valgt å fokusere på mer omfattende angrep som påvirker samfunnet i større grad.

5.2 Konklusjon

Med flere tusen anslag i kvartalet og ca. én alvorlig hendelse i uken (Moe, 2013) ser vi en økende trend av cyberangrep. Vi ser stadig flere alvorlige hendelser med sterke indikasjoner på at aktøren er en statsstøttet organisasjon. Dette er en foruroligende utvikling. Selv om jeg har valgt å se på denne oppgaven i en større kontekst enn den personlige PC-en, så er det her man kan begynne. Flesteparten av angrepene kommer nemlig mot denne delen av befolkningen. Dersom folk generelt blir mer bevisste rundt datasikkerhet, kan svært mange angrep avverges. Økt bevissthet omkring cybersikkerhet i hjemmet kan avverge mange målrettede angrep. Dette fordi aktørene finner ut hvilke sider ansatte innen en bestemt instans surfer på, og infiserer disse internettsidene (NorCERT). I dag når nesten alt er koblet sammen med digitale hjelpemidler, vil det være vanskelig å gå tilbake til et analogt samfunn. Man er i dagens samfunn avhengig av strøm- og kommunikasjonsnettverk fordi det meste av utstyr er koblet opp mot et kommunikasjonsnettverk og trenger strøm for å fungere. Internett er blitt en livline for oss i dagens stadig mer teknologiske samfunn. Så konsekvensene av ikke å kunne forsvare seg på cyberområdet vil bare bli større og større, ikke i liv som går tapt, men i systemer og dermed viktige funksjoner i samfunnet som blir rammet. I min analyse av trusler og aktører bak, samt konsekvenser av et eventuelt cyberangrep, kommer det tydelig frem at cyberforsvar er svært viktig i dagens samfunn. Uten et godt cyberforsvar ville vi stått helt åpne for angrep. Det ville vært som om vi i Norge, med vår lange kystlinje, ikke hadde hatt et sjøforsvar til å forsvare oss og hevde vår suverenitet. Dette ville jo vært utenkelig. Derfor er det viktig at vi nå anerkjenner cyberangrep som en reell trussel, og øker fokuset på dette området i vårt forsvar av Norge.

5.3 Veien videre

Andre land satser stort på cyber. Russland og Kina er begge nasjoner som har gjennomført cyberangrep i stor skala, og sistnevnte har gjennomført angrep i Norge (APT1 report). Derfor er det nå viktig at også vi satser på cyberforsvar. I min samtale med Cyberforsvaret sier de at kompetanse er nøkkelen til å kunne forsvare Norge i cyberdomenet (Le, 2013). Det trengs folk med kompetanse innenfor informasjonssikkerhet og telematikk. General Harald Sunde (2013) sa at cyberdomenet blir like mye brukt av det militære og det sivile samfunn som land-, sjø og luftdomenet, og likevel er det nettopp i cyberdomenet vi er svakest. Det er altså her vi må øke vår kapasitet. Jeg mener vi må rekruttere flere fremtidige cybersoldater som kan være med på å forsvare Norge i cyberdomenet. I fremtidige konflikter tror jeg at cyberangrep vil være like mye brukt som andre former for angrep. Derfor er det bra å se at man nå begynner å ta tak i dette, ikke bare i Norge, men også NATO. I mars utviklet NATO en doktrine for cyberforsvar. Her er bl.a. informasjonsdeling, samarbeid og økt kapasitet viktige prinsipper.

FFI skrev i en rapport om krisehåndtering at vi i Norge er for dårlig samkjørt. Vi hadde ikke per dags dato gjennomført øvelser i større skala, øvelser der flere sektorer er med og det brukes et større geografisk område. Økt fokus på sivilt/militært samarbeid ble også etterlyst (FFI 2). I år, 2013, ble øvelse Cyber Dawn gjennomført. Dette var en øvelse som Telenor, Cyberforsvaret og NorCERT gjennomførte sammen. Denne øvelsen ble i tillegg satt sammen med øvelse Hovedstad. Scenarioet i Cyber Dawn var at Norge ble utsatt for et digitalt angrep som var alvorlig for nasjonale interesser. Formålet md øvelsen var å avdekke eventuelle mangler og sårbarheter i samarbeidet mellom de forskjellige etatene. Forsvaret stod for å evakuere og forflytte Telenors ansatte fra Fornebu til en alternativ lokasjon, slik at Cyberforsvaret, støttet av NorCERT, kunne løse situasjonen (Teknisk ukeblad, 2013). Dette er øvelser som det må fokuseres mer på; militære øvelser med scenarioer som inkluderer cyberdomenet i større grad. Som nevnt tidligere i oppgaven er det ikke usannsynlig at vi vil se militære angrep som er støttet av et eller flere cyberangrep mot kritisk infrastruktur.

Jeg håper at jeg med denne oppgaven har klart å belyse viktigheten av cyberforsvar, samt å bevisstgjøre deg som leser. Ved å være bevisst og selv ta ansvar, kan også du som enkeltperson gjøre en forskjell.

Referanseliste

1. Johannessen, Asbjørn., Tufte, Per Arne, & Christoffersen, Line. (2010). *Introduksjon til samfunnsvitenskapelig metode.* Oslo: Abstrakt forlag.
2. Rid, Thomas. (2013). *Cyber war will not take place.* United Kingdom: C.Hurst & Co.

3. FFI 1. (2004). FFI/RAPPORT-2004/01666. Kjeller: Johansen, Iver.
4. FFI 2. (2007). FFI-rapport 2007/01204. Kjeller: Fridheim, Håvard & Hagen, Janne.
5. Nasjonal sikkerhetsmyndighet. (2013). Q2/Q3 2013. Oslo: forfatter.
6. NorCERT: Nasjonal Sikkerhetsmyndighet. (2013). *Kvartalsrapport for 1. kvartal 2013*. Oslo: NorCERT.

7. Johansen, Roger. (2013). Cyberkrigføring og Forsvarets operative evne. *Internasjonal politikk,* 71, (2), s 241-251.
8. Langø, Hans-Inge & Sandvik, Kristin Bergtora. (2013). Cyberspace og sikkerhet. *Internasjonal politikk*, 71, (2), s 221-228.
9. Rid, Thomas. (2012) Cyber war will not take place. *The Journal of Strategic Studies*, 35, (1), s 5-32.

10. Forsvarets forum. (2013, April). Cybervakten. S 24.
11. Grandhagen, Kjell. (2013, April). Cybervakten. *Forsvarets forum,* s 24.
12. Eide, Espen Barth. (2013, April). Cybervakten. *Forsvarets forum*, s 26.
13. Lynn, William. (2010, September-oktober) *Foreign affairs.* Council on Foreign Relations.

14. Diesen, Sverre. (2013, 27/11). Cybermakt – og Forsvarets rolle. FFI-forum i Oslo Militære Samfund.
15. Enstad, Kjetil. (2013). Leksjon i kvalitativ metode.
16. Le, Per. (2013) Intervju på Jørstadmoen.
17. Moe, Marie. (2013) Intervju hos NorCERT.
18. Sunde, Harald. (2013, 14/01) Forsvaret – status. Foredrag i Oslo Militære Samfund.
19. Sundseth, Roar. (2013, 18/02). Cyberoperasjoner – utfordringer i Cyber. Foredrag i Oslo militære Samfund.

20. BBC news. (2010). Lokalisert [10/12-13] på http://www.bbc.co.uk/news/science-environment-10851837
21. Cherry, Steven. (2013). Lokalisert [10/12-13] på http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook
22. Forsvaret. Lokalisert [10/12-13] på http://forsvaret.no/om-forsvaret/organisasjon/cyberforsvaret/Sider/cyberforsvaret.aspx
23. Freedman, Sir Lawrence. (2013). Lokalisert [10/12-13] på http://thomasrid.org/cyber-war-will-not-take-place/
24. Nordisk tidsskriftdatabase. Lokalisert [11/10-13] på http://www.idunn.no/ts/ip
25. NSM. Lokalisert [10/12-13] på https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/Om-NorCERT/
26. Røsjø, Bjarne. (2012). Lokalisert [10/12-13] på http://www.forskning.no/artikler/2012/januar/311616
27. Teknisk ukeblad. (2013). Lokalisert [10/12-13] på http://www.tu.no/it/2013/08/28/telenor-banker-og-cyberforsvaret-far-bryne-seg-pa-et-ekte-dataangrep
28. Wikipedia URL 1. Lokalisert [10/12-13] på http://no.wikipedia.org/wiki/Internett
29. Wikipedia URL 2. Lokalisert [10/12-13] på http://no.wikipedia.org/wiki/Tjenestenektangrep

Vedlegg

Vedlegg 1 – Intervjuguide.

Vedlegg 2 – Sammendrag av intervju med Marie Moe.

Vedlegg 3 – Sammendrag av intervju av Per Le.

Vedlegg 4 – Ordforklaringer.

Vedlegg 1

Intervjuguide

Innledning

Si litt om hvem jeg er.
Informere om bacheloren.
Hva er betydningen av at du er med på intervjuet.
Hvordan dokumenterer jeg intervjuet.
Anonymitet vs ikke anonym.
Retten til å kunne avbryte intervjuet når som helst.
Hvor lang tid intervjuet vil ta.

Faktaspørsmål

- Hva fikk deg interessert i cyber?
- Hvor lenge har du jobbet med cyber?
- Hvilken utdannelse har du?
- Hva er din jobb, hvilke oppgaver utfører du?
- Hva anser du som det viktigste/mest kritiske innfor cyberforsvar?

Introduksjonsspørsmål

- Hva tenker du når du hører cyberforsvar? (Hva menes med det)
- Hva er samfunnskritisk infrastruktur?
- Cyberforsvaret jobber med sikring og forsvar av forsvarets datasystemer, nettverk og høyteknologiske plattformer mot angrep i og fra cyberdomenet. Kan du si noe om hva dette innebærer?

Overgangsspørsmål

- Hvilken trussel ser du mest av? Hvilke typer skadevare?
- Hva er mest utbredt, sabotasje eller spionasje? Andre former for angrep?

Nøkkelspørsmål

- Hva er mest utsatt for cyberangrep slik du ser det?
- Hvor stor er økningen av cyberangrep fra år til år?
- Hvor ofte er det angrep på systemer dere beskytter og hva er alvorlighetsgraden av angrepene?
- Hvilke aktører ser dere mest av? Hacktivister eller stats støttede organisasjoner?
- Hva er den største konsekvensen du ser som følge av et cyberangrep generelt?
- Hva tenker du om at et cyberangrep kan brukes som i et ledd før en militær aksjon?

Avsluttning

Si at nå nærmer vi oss slutten.
Er det andre ting du ikke har fått sagt eller som du mener er viktig å få med seg?

Vedlegg 2

Sammendrag av Marie Moe

NorCERTs jobb og hvordan de løser det.

- Deres oppgaver er bl.a. å monitorere et såkalt VDI-sensornettverk. Dette er et Varslingssystem for Digital Infrastruktur. Her ser de etter tegn på hendelser mot nasjonalkritisk infrastruktur. Dette er infrastruktur som samfunnet er avhengig av for å fungere. For å gjennomføre banktransaksjoner så må internett fungere, skal du kjøre til jobben så må olje og gass industrien kunne levere råolje til prosessering. Videre så er NorCERT nasjonalt kontakt punkt for hendelser i Norge. Alt om kommer inn om hendelser i cyber kommer til NorCERT. Her deler de informasjon med andre sektorer som driver med tilsvarende oppgaver. Videre så har NorCERT ansvaret for å ha et oppdatert bilde på IKT-trusselbildet og bistå virksomheter som er rammet av dataangrep.

Det viktigste inne cyberforsvar

- Det å detektere statlige aktører som prøver å gjennomføre spionasje er en av de viktigste aspektene innen cyberforsvar. Dette vil de prioritere høyere enn andre pågående saker så fremt de ikke er veldig alvorlige, dette for å hindre at andre nasjoner får kjennskap til våre kapasiteter og operasjons mønster, samt bedriftshemmeligheter. Det å bevisstgjør bedrifter, og den enkelte, om viktigheten av å ha gjennomført en risikoanalyse på det som bedriften holder på med er også et viktig aspekt, det å opplyse om trusselen og en bevisstgjøring av folkemassen. Sabotasje er noe som ikke er så utbredt enda, men de er bekymret for dette pga. systemene som dette angår er dårlig sikret, SCADA, og å gjøre noe med disse systemene betyr fysisk skade på utstyr, samt at å sabotere SCADA-systemer kan medføre skade på personer i tilknytning til systemene.

Trusselen

- Den trusselen som det blir sett mest av er kriminalitet og hacking. Her er det flere typer angrep som kan gjennomføres. Du har DDoS-angrep og økonomisk kriminalitet som er de hyppigste. De som driver med økonomisk kriminalitet kan for eksempel ta over PCen din og låse den og få deg til å betale for å få den låst opp, eller de kan ta over din sesjon når du er på vei inn i nettbanken din. De som sprer disse virusene/trojanerne er gjerne store norske nettsider som er blitt infiserte som sprer dette videre. Det de er mest bekymret for er spionasje. Her har de hatt en veldig stor økning de siste årene. Dette rammer i hovedsak forsvarsindustri, olje og gass, departementer og forskning og utvikling. Det er veldig vanskelig å oppdage da det ofte er statsstøttede operasjoner. Sabotasje er noe vi har hatt svært lite av i Norge, men som de er bekymret for at kan skje. SCADA-systemene er dårlig sikret og utgjør en trussel mot samfunnskritisk infrastruktur.

Konsekvensene av et cyberangrep

- Det er mange konsekvenser som kan komme som følge av et cyberangrep. Det som i hvert fall er sikkert er at om du tar ut de riktige tingene så kan det oppleves som en naturkatastrofe der du mister viktig infrastruktur. Dette gjelder da særlig om du tar ned strømnett, vann-nett og det finansielle. Konsekvensen av det Stuxnet gjorde er kanskje det som gir de største konsekvensene, å gå inn og ødelegge kritisk infrastruktur. Stanse olje-produksjon, stanse finansielle transaksjoner. Mer alvorlige hendelser kan medføre at liv går tapt. Ta strømmen til store deler av befolkningen på vinteren o.l. I et militørt perspektiv så kan konsekvensene her være at noen har klart å plante inn bakdører i systemene til forsvaret. Det gjør at du kan gå inn i systemene på kritiske tidspunkter å lamme for eksempel kommunikasjon, det vil jo få store konsekvenser om du tar det ut under operasjoner. Det kan gi fienden en god forståelse om vår taktikk og bruk av våpensystemer om de klarer å hente ut informasjon om handlemåter og operasjonsmønster.

Vedlegg 3

Sammendrag av Per Le

Cyberforsvarets jobb og hvordan de løser det.

- Deres oppgaver er å monitorere forsvarets nettverk ved hjelp av sensorer som tar opp trafikkstrømmen som forsvarets nettverk produserer. Dette er all internett trafikk som går internt og eksternt. På Fisbasis og via to-nivå løsningen. Her sitter ingeniører å ser på trafikken som går gjennom kablene som alle PCene er koblet opp på og ser på alarmer som har gjenkjent en signatur som kan indikere en trussel av noe slag.

Det viktigste innen cyberforsvar

- Det viktigste som han ser innenfor cyberforsvar er samarbeidet med andre avdelinger og sporbarhet. Med samarbeidspartnere mener han at ved hjelp fra andre kan de få verdifull informasjon om angrep eller signaturer som de har bruk for, NorCERT er et eksempel på en samarbeidspartner. Med sporbarhet så mener han logger. Med en logg kan du gå tilbake å se på en hendelse som har skjedd og analysere den. Denne hendelsen kan være ondartet eller det kan være en falsk indikasjon på noe. Skulle det vise seg å være en ondsinnet hendelse kan loggen brukes til å analysere hendelsen og finne ut hva som var hensikten til skadevaren.

Trusselen

- Den trusselen som de ser mest av er ikke-målrettede angrep i form av ormer eller trojanere. Dette rammer hovedsakelig privatpersoner og er lett å forsvare seg mot. Har du oppdatert alle programmene dine så er de aller fleste sikkerhetshull tettet. Dette kommer i form av spear phising eller vannhulls angrep. Dette oppdages oftest ved at ansatte tar kontakt når de oppdager forsøk på disse typer angrep. De truslene som får mest fokus er de målrettede angrepene der, som oftest, statlige aktører står bak. Dette er gjerne spionasje og forsøk på å tilegne seg etterretning. Det er vanskelig å finne ut hvem bakmennene er, men ved å se på hvor sofistikert angrepet er gir en god indikasjon. Hvis det er zero-day sårbarheter eller tidligere kjente sårbarheter som brukes, så sier det litt om nivået.

Konsekvensene av et cyberangrep

- Det som er den største konsekvensen av et cyberangrep er at samfunnet stopper opp. Dette innebærer jo at flere systemer blir rammet samtidig og kan medføre at situasjonen oppleves som under en naturkatastrofe der vann, strøm, kommunikasjon og andre kritiske systemer slutter å fungere. Eksempler på slike angrep eller systemer er DDoS angrep som kan lamme all internett trafikk eller SCADA-systemer som vil ta ut industrielle kontroll systemer og annen sivil infrastruktur som kan bidra til fysiske ødeleggelser. For forsvarets del er kommunikasjon det som er den største konsekvensen at vi, og kritisk om man, mister. Det hindrer oss i å gjennomføre de oppdragene vi skal og/eller få en samlet innsats.

Vedlegg 4

Ordforklaringer

ARPANET – Advanced Research Project Agency Network. Den første versjonen av internet. Ble laget for militær bruk. Den første noden utenfor USA ble plassert i Norge ved FFI.

NSM – Nasjonal sikkerhetsmyndighet.

NorCERT – Norwegian Computer Emergency Response Team.

Cyberforsvaret – Forsvarets avdeling for beskyttelse i cyberdomenet.

Cybervåpen – Kode som er ment å skade psykisk, fysisk og funksjon på strukturer, systemer og levende vesner.

Stuxnet – Det første potente cybervåpen.

Zero-day exploits – Dette er sikkerhetshull I programmer o.l som ikke er oppdaget før.

Spear phishing – Dette er for eksempel mailer som blir sendt ut og som utgir seg for å være noen andre. Dermed kan de lure til seg sensitiv informasjon. La oss si din bank. De har et problem som du kan løse ved å taste inn navn og bankkontonr. og passord. Dermed tømmer de kontoen din.

Trojaner – Dette er ondsinnet kode som utgir seg for å være noe bra. Det er det ikke.

Ormer – Dette er et datavirus som jobber på egenhånd. Den har all informasjon den trenger til å gjøre alt på egenhånd. Dette kan være å ødelegge helt spesifikke ting eller dokumenter som omtaler et emne. Den kan settes av etter en viss tid. Den har mange bruksområder

SCADA – Supervisory Control and Data Acquisition. Dette er datasystemer som benyttes i stort sett alt av infrastruktur og prosesseringsanlegg som er automatisert. Det overvåker systemer og gir tilbakemelding på fysiske hendelser til en kontrollskjerm.

DDoS – Distributed Denial og Service. Dette er et nettverk av PC-er som er tatt over av en person og som brukes til å sende pakker til mottakeren og stenger tilgangen til systemet. Dette fordi det ikke takler så stort press. Du kan nekte folk tilgang til aviser, banker og andre internett sider ved å bruke et slikt angrep.