SCANDINAVIAN JOURNAL OF MILITARY STUDIES

Øving på cybersikkerheit: Ein casestudie av ei cybersikkerheitsøving

COLLECTION:
WAR GAMING

PRACTICE-ORIENTED ARTICLE

MASS SOLDAL LUND

SCANDINAVIAN MILITARY STUDIES

SAMANDRAG

Denne artikkelen presenterer ein casestudie av ei cybersikkerheitsøving i militær utdanning, og nyttar denne casestudien til å drøfte nokre utfordringar med cybersikkerheitsøvingar til utdanningsføremål. Casestudien gjer greie for sentrale avgjerder i designet av øvinga, evaluering av øvinga og utfordringar i øvingskonseptet. Gjennom ein litteraturgjennomgang samanliknar vi øvinga med liknande øvingar, og ser på korleis desse øvingane har blitt evaluert. Avslutningsvis nyttar vi casestudien og litteraturgjennomgangen til å gjere betraktningar om vidare undersøkingar av cybersikkerheitsøvingar.

ABSTRACT

This article presents a case study of a cyber security exercise in military education, and uses this case study to reflect on some challenges with cyber security exercise for educational purposes. The case study discusses central decisions in the design of the exercise, the evaluation of the exercise, as well as challenges with the exercise concept. Through a survey of the literature, we compare the exercise with similar exercises, and have a look at how these exercises are evaluated. Finally, we use the case study and the literature survey to reflect on how further investigations into cyber security exercise could be made.

CORRESPONDING AUTHOR:

Mass Soldal Lund

Inland Norway University of Applied Sciences, NO

mass.lund@inn.no

NØKKELORD:

Utdanning; øving; cybersikkerheit; defensive cyberoperasjonar; CDX; cyberrange

KEYWORDS:

Education; exercise; cyber security; defensive cyberspace operations; CDX; cyber range

TO CITE THIS ARTICLE:

Lund, M. S. (2022). Øving på cybersikkerheit: Ein casestudie av ei cybersikkerheitsøving. *Scandinavian Journal of Military Studies*, 5(1), pp. 244–256. DOI: https://doi.org/10.31374/sjms.119

DOI: 10.31374/sjms.119

INTRODUKSJON

> Cyberingeniørskolen skal etablere og [...] drifte et fremskutt cybersikkerhetssenter [...] underlagt Cyberforsvarets Cybersikkerhetssenter [...] etablere sikkerhetsovervåkning av [...] sivil/militære grensesnitt [og] være forberedt på å gjennomføre defensive cyberoperasjoner [...] med den hensikt å sikre handlefrihet i cyberdomenet ved mottak og understøttelse av allierte styrker.

Dette var ordren ei gruppe kadettar ved Cyberingeniørskolen ved den norske Forsvarets høgskole fekk ved staren av operasjonsfasen til Øving Vinterdrill II 2021. For dei 13 militære ingeniørstudentane med fordjuping i cyberoperasjonar var dette den avsluttande øvinga i utdanningslaupet. I laupet av dei neste seks dagane skulle militære og ingeniørfaglege ferdigheiter opparbeidde gjennom to og eit halvt år setjast på prøve og sjåast i samanheng, og kadettane bryne seg på cybersikkerheitsmessige og militære utfordringar.

Utdanninga og øvinga ved Cyberingeniørskolen går inn i ein større trend. Cybersikkerheit har dei siste tiåra vakse fram som fagfelt, i takt med den aukande avhengnaden vår av digital teknologi og ein stadig meir påtrengande cybersikkerheitstrussel. For å dekkje det aukande behovet for cybersikkeheitskompetanse er det etablert utdanningsprogram i cybersikkerheit ved utdanningsinstitusjonar på alle nivå. Både i militære og sivile cybersikkerheitsutdanningar blir ulike formar for øvingar utnytta som arenaar for læring (Katsantonis et al. 2017; Karjalainen & Kokkonen 2020b).

Denne artikkelen vil ta føre seg bruk av øvingar i cybersikkerheitsutdanning. På trass av at det etter rapportane å døme vert arrangert eit stort tal cybersikkeheitsøvingar på verdsbasis – der føremålet kan vere konkurranse, utdanning, eller trening og øving av responsorganisasjonar (Seker & Ozbenli 2018; Enisa 2015: 14) – ser det ut til å eksistere relativt få studiar av cybersikkerheitsøvingar som pedagogisk verkemiddel. Det finst heller ikkje mange rapportar som gjev detaljerte skildringar av cybersikkerheitsøvingar.

Hensikta med artikkelen er todelt. For det fyrste ønskjer vi å introdusere cybersikkerheitsøvingar for eit breiare publikum og vise korleis dei nyttast i militær cybersikkeheitsutdanning. For det andre ønskjer vi å bidra til ein vaskande, men førebels relativt liten litteratur om cybersikkerheitutdanning generelt og bruk av øvingar i cybersikkerheitutdanning spesielt. For båe desse føremåla vil vi nytte ei cybersikkerheitsøving gjennomført ved Cyberingeniørskolen ved den norske Forsvarets høgskole i 2021 som casestudie. Casestudien vil drøfte vurderingar som vart gjort i designet av øvinga, kva evalueringar av øvinga viste, og utfordringar med øvingsformatet som vart vald. Målet er at denne casestudien kan fungere både som eit informativt eksempel på ei cybersikkerheitsøving, og som eit grunnlag for eller bidrag til seinare komparative studiar. Ei utfordring, både med cybersikkerheitsøvingar generelt og med casestudien i denne artikkelen spesielt, er korleis vi evaluerer om øvingane har hatt ønskt effekt. Denne utfordringa freistar vi kaste lys over, både med eit kritisk blikk på vår eigen casestudie og ved å sjå korleis andre har takla denne utfordringa.

Artikkelen har struktur som følgjer: Vi startar med ein introduksjon til cybersikkerheitsøvingar, før vi presenterer casestudien av Øving Vinterdrill II 2021. Deretter drøftar vi utfordringa med evaluering av cybersikkeheitsøvingar, før vi i oppsummeringa presenterer nokre tankar om vidare forsking og utvikling på feltet.

CYBERSIKKERHEITSØVINGAR

Grovt sett eksisterer det to ulike typar cybersikkerheitsøvingar. I ein *Capture the Flag* (CTF) er målet å løyse tekniske oppgåver som krev cybersikkerheitsferdigheiter. CTFar har sitt opphav i det ein litt laust kan kalle «hackar-konkurransar», der ein skal samle poeng ved å finne meldingar kalla «flagg» gøymde i datasystem. Den andre tradisjonen er *Cyber Defence Exercises* (CDX), som spring ut av militære og andre organisasjonar som søkjer å øve på realistiske scenario med handtering av cybersikkerheitshendingar. Denne typen øvingar har gjerne som mål å øve andre ferdigheiter, som til dømes kommunikasjon og team-arbeid, i tillegg til dei reint cybersikkerheitstekniske (Ošlejšek et al. 2021: 3425).

CTFar er i utgangspunktet konkurransar der deltakarane bryt seg inn i datasystem for å finne dei gøymde «flagga». Katsantonis et al. (2017) viser i ein studie av CTFar at sjølv om dei kan

DOI: 10.31374/sjms.119

nyttast til pedagogiske føremål, har dei også visse utfordringar: Dei er fyrst og fremst designa for å utnytte ferdigheiter i å gjennomføre cyberåtak. Sjølv om dei kan illustrere og vise fram sårbarheiter i datasystem, og også kan ha element av forsvar (i CTFar med fleire som lag som samtidig må gå til åtak på og forsvare seg mot andre lag), gjev dei ikkje trening i handtering av cybersikkerheitshendingar. Vidare har dei eit konkurranseelement som kan setje læring i baksetet, og kan fremje praksisar som er effektive i ein konkurranse men som elles vil verte sett på som dårlege.

CDXar vert gjennomførte i heile spekteret av øvingsformar, frå diskusjonsøvingar og speløvingar til funksjonsøvingar og fullskalaøvingar. I europeisk samanheng er øvingane Locked Shields, Cyber Coalition og Cyber Europe dei største og mest kjente CDXane. Ofte vil øvingspublikum vere eit cybersikkerheitssenter, men det kan også vere ein beredskapsorganisasjon (DSB 2016: 35–40; Seker & Ozbenli 2018).

Eit cybersikkerheitssenter er ein dedikert organisasjon eller gruppe personar med ansvar for å forhindre, detektere og handtere cybersikkerheitshendingar. Typiske arbeidsoppgåver i eit cybersikkerheitssenter består av ulike formar for passiv og aktiv datainnsamling (til dømes tapping av eit datanettverk eller uthenting av data frå minnet til ei datamaskin), ulike formar for passiv og aktiv deteksjon av hendingar (til dømes bruk av nettverksensorar eller aktive søk basert på tekniske indikatorar), ulike formar for analyse og syntese (til dømes analyse av nettverkstrafikk, datamaskinminne og skadevare, korrelering av data og bygging av tidsliner), handtering eller lukking av hendingar (til dømes installasjon av sikkerheitsoppdateringar, fjerning av skadevare og sikring av bevis), og rapportering. I tillegg kan eit cybersikkerheitssenter ha aktivitetar som trusselanalyse, sårbarheits- og sikkerheitsvurderingar, policyutvikling, erfaringslæring, bevisstgjering og kompetanseheving. Relevant i samanheng med øvingar vil også vere planlegging, kommunikasjon med organisasjonar cybersikkerheitssenteret støttar, og deployering. Det er verdt å merke seg at handtering av cybersikkerheitshendingar ofte vil ha rom for taktiske vurderingar (til dømes: Skal vi fjerne eller observere ein uautorisert aktør i systema?), og at eit cybersikkerheitssenter difor må ha eller vere underlagt eit system for å ta avgjerder. I ein militær samanheng vil ein assosiere handtering av cybersikkerheitshendingar med defensive cyberoperasjonar (Adnan et al. 2015; Forsvaret 2019: 229–230; Lund 2018; Trent et al. 2019).

Når CDXar er nytta som pedagogisk verkemiddel i cybersikkerheitsutdanning og -opplæring, er det funksjonsøvingar og fullskalaøvingar som dominerer mellom dei cybersikkerheitsøvingane som er skildra med nokon grad av detaljar i litteraturen. Brilingaitė et al. (2020), Geers (2010), Granåsen & Andersson (2016), Karjalainen et al. (2020), og Vykopal et al. (2017, 2018) rapporterer frå funksjons- eller fullskala CDXar nytta til opplæringsføremål. I terminologien til rapportane er forsvararane – hovudpublikum for øvingane – omtala som *Blue Team*, personell som gjennomfører cyberåtak mot dei forsvarte systema som *Red Team*, og øvingsleiing for *White Team*. I tillegg vert det i nokre av rapportane nytta *Purple Team* om personell som spelar eigarar og brukarar av systema, og *Green Team* om personell som står for teknisk drift av øvingsomgjevnaden.

Karjalainen et al. (2020) gjev ikkje mykje detaljar, men ser ut til å rapportere frå ei todagars funksjonsøving med 86 deltakarar (Blue Team) frå eit masterprogram i cybersikkerheit. Brilingaitė et al. (2020) rapporterer frå øvinga Amber Mist 2018. Øvinga var ei femdagars felles sivil/militær fullskalaøving der fire Blue Teams med til saman 24 deltakarar skulle forsvare industrikontrollsystem. I tillegg til desse hadde øvinga fem Purple Teams med til saman 14 deltakarar, eit Red Team med ni deltakarar, og minst 23 personar i White Team. Vykopal et al. (2017, 2018) rapporterer frå Cyber Czech, ei eindagsøving med rundt 50 deltakarar som var arrangert i seks omgangar i perioden 2015–2017. I éi av gjennomføringane vart fleire Blue Teams med til saman 24 deltakarar øva av eit White Team av åtte personar, eit Red Team av tolv personar og eit Green Team av fem personar; éi gjennomføring hadde 40 deltakarar der 20 personar utgjorde fem Blue Teams. Granåsen & Andersson (2016) og Geers (2010) rapporterer frå øvinga Baltic Cyber Shield 2010, ei todagars øving der seks Blue Teams frå fire nordeuropeiske land og ulike typar organisasjonar (statlege, militære, akademiske) forsvarte industrikontrollsystema til kvart sitt energiselskap. Dei seks Blue Teama hadde til saman omtrent 50 deltakarar, og Red Team bestod av 20 personar. Storleiken på White og Green Teams er uspesifisert, men øvinga hadde meir enn 100 deltakarar, så vi kan rekne med at dei til saman utgjorde rundt 30 personar.

DOI: 10.31374/sjms.119

Alle dei omtalte øvingane nytta ei form for *cyberrange*. Vi kan sjå ein cyberrange som ein infrastruktur for øving og trening på cybersikkerheit der virtualiseringsteknologi vert nytta til å byggje opp nettverk av emulerte system. I alle øvingane vart det lagt vekt på at det skulle vere ein realistisk og kompleks omgjevnad som liknar på reelle system (Brilingaitė et al. 2020; Geers 2010; Karjalainen & Kokkonen 2020a; Vykopal 2017). Yamin et al. (2020) gjer ein gjennomgang av litteratur om cyberranges. Dei viser at cyberranges, som med cybersikkerheitsøvingar, er eit framveksande fenomen. Ein stor del av desse – som i øvingane rapportert frå her – nyttar virtualiseringsteknologi til å byggje emulerte system der eit Red Team kan gjennomføre cyberåtak mot forsvararane i Blue Teams, men langt frå alle. Det finst òg cyberranges som i større grad nyttar simulering, og cyberranges der føremålet er utprøving av teknologi heller enn trening av personell. Sjølv om Yamin et al. (2020) også registrerer virtualisering og realisme som trendar, legg dei – i motsetnad til dei refererte øvingsrapportane – større vekt på automatisering av cyberåtak og scoring av deltakarane, og ser på dette som viktige trendar for effektivisering og skalerbarheit av cyberranges og cybersikkerheitsøvingar.

Ein gjennomgåande trend ved øvingane som det vert referert til, er at rammene for øvingane som regel er avgrensa til prosessar for handtering av cybersikkerheitshendingar, det vil seie spennet frå tekniske ferdigheiter, via analyse, til rapportering av cybersikkerheitshendingar. Slike øvingar har openberr eigenverdi, men i kontekst av ei profesjonsutdanning – som vil ha læringsmål utover den konkrete hendingshandteringa – er det også mogleg å argumentere for at ei slik avgrensing representerer ei tapt moglegheit. I det følgjande vil vi rapportere frå ei cybersikkerheitsøving der elementa frå ein typisk CDX vart integrert inn i ei meir tradisjonell militærøving, for å kunne øve eit breiare spektrum av ferdigheiter enn dei som er direkte relatert til handtering av cybersikkerheitshendingar.

CASE STUDIE: ØVING VINTERDRILL II 2021

Øving Vinterdrill II 2021 var ei øving gjennomført ved Cyberingeniørskolen ved Forsvarets høgskole, det norske Forsvarets utdanningsinstitusjon for utdanning av offiserar og befal. Dette var den siste øvinga for eit kull av kadettane ved Cyberingeniørskolen før uteksaminering, og målet var å prøve kadettane i heilskapen av kunnskap, ferdigheiter og kompetanse dei har tileigna seg gjennom studiet, eller med andre ord å øve dei som profesjonsutøvarar. I øvinga vart kadettane delte etter spesialisering, slik at 13 kadettar med spesialisering i cyberoperasjonar gjennomførte ein CDX, medan dei resterande vart øva i militære IKT-system og CIS-støtteoperasjonar. I den vidare framstillinga er det berre CDX-delen av øvinga som vert skildra.

I terminologien nytta over var dette ein liten, fullskala CDX. I det følgjande vil vi gje ein presentasjon av denne øvinga der vi går gjennom øvinga sin plass i utdanninga ved Cyberingeniørskolen, gjennomføringa av øvinga og hovudelementa i designet av øvinga. Til slutt vil vi oppsummere evalueringane av øvinga, og peike på utfordringar i øvingsdesignet.

Presentasjonen av øvinga støttar seg på tre hovudkjelder: (1) Dreieboka for øvinga, (2) dei ordrane og etterretningsrapportane som øvingspublikummet mottok gjennom øvinga, og (3) observasjonar gjort av forfattaren av denne artikkelen – som er identisk med leiaren av CDX-aktiviteten på øvinga. Evalueringa av øvinga er basert på (1) fire skriftlege tilbakemeldingar gjevne av personell i øvingsstaben ved avslutninga av øvinga, samt ei samla skriftleg tilbakemelding frå øvingspublikummet og (2) forfattaren sine eigne observasjonar.

BAKGRUNN OG MÅLSETTING

Øving Vinterdrill II (seinare endra namn til Øving Finale) er ei øving for kadettar på sisteåret ved Cyberingenørskolen. Utdanninga er ei treårig kombinert ingeniør- og befalsutdanning, som kvalifiserer uteksaminerte kandidatar til å arbeide som ingeniørar i det norske Forsvarets spesialistkorps. Studiet har 40 plassar og ein gjennomføringsgrad på 90–100 %. Studieprogrammet følgjer den nasjonale rammeplanen for elektroingeniør og gjev spesialisering i telematikk (UHR 2020). I tillegg til elektrofag inkluderer programmet ei rekkje typiske IKT-emne som *Datakommunikasjon* (10 ECTS credits; 2. semester) og *Operativsystem* (10 ECTS credits; 3. semester). Alle kadettane må ta emna *Informasjonssikkerheit* (5 ECTS credits; 3. semester) og *Cybermakt* (5 ECTS credits; 6. semester), og ca. ein tredel får valemnet *Cyberoperasjonar* (10 ECTS

DOI: 10.31374/sjms.119

credits; 5. semester). Emnet *Cyberoperasjonar* er utvikla med utgangspunkt i at kandidatane skal verte førebudde på å arbeide i cybersikkerheitssenteret til det norske Cyberforsvaret og nyttar også personell frå cybersikkerheitssenteret som undervisarar. Emnet *Cyberoperasjonar* kan sjåast som eit innføringsemne i deteksjon og handtering av cyberhendingar, og dekker tema som sårbarheitskartlegging, nettverksovervaking, skadevareanalyse, digital etterforsking og hendingshandteringsmetodikk, medan *Cybermakt* gjev innføring i politiske, rettslege og etiske rammer for bruk av cybermakt, norske og allierte doktrinar, og bruk og planlegging av cyberoperasjonar i ein militær kontekst (FHS u.å.). Som ein del av utdanninga har Cyberingeniørskolen i ei årrekkje gjennomført CDXar for kadettane (Jøsok et al. 2019: 4–5; Nikolaisen 2016; Naas 2014), men som med anna fagutvikling er desse øvingane i kontinuerleg utvikling. Øving Vinterdrill II/Finale er difor ikkje ein kopi, men ei vidareutvikling av tidlegare øvingar.

Medan tidlegare CDXar ved Cyberingeniørskolen var meir typiske CDXar, var målsettinga for Øving Vinterdrill II 2021 å øve heilskapen i profesjonsutøvinga. Det vil seie å øve alle ferdigheitene kadettane har tileigna seg som er relevante for defensive cyberoperasjonar i kontekst av militære operasjonar, ikkje berre einskildferdigheiter som digital etterforsking eller skadevareanalyse. I tillegg til dei tekniske ferdigheitene var det difor eit mål å inkludere øving av ferdigheiter som planlegging, kommunikasjon, rapportskriving og leiing. Bakgrunnen for dette kan seiast å vere todelt: For det fyrste er det eit mål at kadettane skal tileigne seg ei forståing for rolla som eige fagfelt spelar i ein større samanheng. Dette følgjer frå læringsmål i utdanninga som eksempelvis at kadettane skal tileigne seg kunnskap om «cyberingeniørens rolle i Forsvaret og i samfunnet, og konsekvenser av utvikling og anvendelse av teknologi» og «prosedyrer, taktikker og begreper innenfor cybermilitær virksomhet, herunder […] cybermakt og cyberoperasjoner». For det andre er øvingsdøgn ein knappheitsressurs, som også må utnyttast for å nå dei generelle læringsmåla for utdanninga, slik som kunnskap om «ulike verktøy for gjennomføring av militære operasjoner, herunder plan og beslutningsprosess (PBP) og risikovurdering» og bruk av «relevante verktøy og uttrykksformer for å fungere som militær leder i gjennomføring av militære operasjoner på lavere taktisk nivå» (FHS u.å.).

GJENNOMFØRING

Øving Vinterdrill II vart gjennomført over to veker i februar 2021, der den fyrste veka (måndag til fredag) utgjorde ein klargjeringsfase og den andre veka (laurdag til torsdag) ein operasjonsfase. I vekene før øvinga hadde kadettane vore gjennom ein planleggingsfase. Øvinga hadde såleis dei tre fasane planlegging, klargjering og operasjon, modellert etter militære operasjonar.

Scenarioet for øvinga er ei (tenkt) stor NATO-øving der allierte styrkeelement skal deployere til Noreg, modellert etter NATO-øvinga Trident Juncture i 2018 (Nato 2018). Under slike internasjonale øvingar vil Forsvaret etablere ein organisasjon for vertslandsstøtte, som er bindeleddet mellom dei allierte styrkane og sivile leverandørar i Noreg av forsyningar til styrkane. IKT-system som blir etablert for å administrere vertslandsstøtte vil i det følgjande bli omtalt som «vertslandsstøttesystem». Oppdraget til kadettane var å etablere eit cybersikkerheitssenter for å avlaste det norske Cyberforsvarets Cybersikkerheitssenter og styrke Forsvarets evne til å handtere cybersikkerheitshendingar medan det er allierte styrker i landet. Dette midlertidige cybersikkerheitssenteret var i scenarioet underlagt Cyberforsvarets Cybersikkerheitssenter, men hadde eit spesielt ansvar for å forsvare vertslandsstøttesystema mot cyberåtak.

I klargjeringsfasen var oppgåva til kadettane å klargjere IKT-materiell til det midlertidige cybersikkerheitssenteret, og å definere sin eigen organisasjon og arbeidsprosessar. I operasjonsfasen var oppgåva fyrst å gjere ei sårbarheitsklartlegging av vertslandsstøttesystema og å installere cybersikkerheitsovervaking av systema. Deretter var oppdraget å monitorere systema for cybersikkerheitshendingar, og å handtere detekterte hendingar. Gjennom operasjonsfasen vart systema utsette for i alt tre cyberåtak av aukande alvorsgrad: sabotasje mot organisasjonen sine websider (såkalla *web defacement*), løysepengevirus på organisasjonens arbeidsstasjonar, og uthenting av informasjon frå organisasjonens e-posttenar ved hjelp av skadevare som gav åtakaren uautorisert tilgang til systema. For kvar av desse hendingane måtte kadettane gjennomføre hendingshandtering både teknisk (analyse av nettverkstrafikk, skadevare, osb.) og taktisk (utleiing av ulike handlingsalternativ), og dei måtte rapportere både skriftleg og munnleg. Cybersikkerheitssenteret fekk i tillegg også nokre mindre

DOI: 10.31374/sjms.119

oppdrag ved sidan av hovudscenarioet for å sørgje for at arbeidsbelastninga var jamn gjennom operasjonsfasen. Desse oppgåvene dekka også spekteret frå teknisk analyse, via taktiske vurderingar, til rapportering og presentasjonar.

CDX-delen av øvinga hadde ein øvingsstab på til saman elleve personar. Dette inkluderte leiar av CDX-aktiviteten (identisk med artikkelforfattaren) som også spelte vertslandsstøtteelementet, to personar med ansvar for den tekniske infrastrukturen (Green Team) som også spelte IKT-personell hjå vertslandsstøtteelementet og underleverandørar, to personar som spelte den overordna avdelinga (Cyberforsvarets Cybersikkerheitssenter), tre personar som gjennomførte cyberåtaka i hovudscenarioet (Red Team), og ein person med ansvar for tilleggsoppdrag. I tillegg vart kadettane følgde av to erfarne cybersikkerheitsanalytikarar som mentorar gjennom operasjonsfasen.

Kadettanes cybersikkerheitssenter vart styrt gjennom oppdrag i form av ordrar frå den overordna avdelinga og korrigert gjennom tilbakemeldingar på skriftlege og munnlege rapportar dei måtte avgje. Frå den overordna avdelinga kom det også daglege etterretningsrapportar med oppsummeringar og analysar av situasjonen i cyberdomenet, inkludert vurderingar av cyberåtak andre stader, og dessutan vurderingar av den overordna politiske og militære situasjonen. Ordrane og rapportane bidrog til å byggje scenarioet og konteksten for øvinga, men vart også nytta til å gje kadettane hint om kva slags cyberåtak som var i vente.

Cybersikkerheitssenteret til kadettane var i hovudsak sjølvorganisert. Sjef og nestkommanderande var peika ut av øvingsstaben, men utover det definerte dei sin eigen organisasjon og plasserte sjølv personell i ulike roller, slik som analytikar og lagførar for underseksjonar i cybersikkerheitssentereret. Dei organiserte eigne møter for planlegging, statusoppdateringar og erfaringslæring, støtta av mentorane. Unntaket var to pausar i spelet styrt av øvingsstaben. I desse «stridspausane» vart hendingar gjennomgåtte i fellesskap av øvingspublikum og øvingsleiing. I ein av desse pausane vart òg rollene i cybersikkerheitssenteret roterte ved at øvingsstaben peikte ut ny sjef og nestkommanderande, og gav dei i oppgåve å definere ein ny organisasjon med personell i nye roller. På slutten av øvinga var det òg ein avsluttande gjennomgang av hendingane i fellesskap.

HOVUDELEMENT

I designet av øvinga vart det lagt vekt på realisme og heilskap. Dette vart ikkje gjort etter nokon streng metodikk, men vi kan i retrospekt identifisert tre hovudelement i designet av øvinga som vi meiner fangar opp tiltaka for å oppnå dette i praksis, og som kan fungere som forklaring for designavgjerder: 1) ein infrastruktur å gjennomføre øvinga på, 2) ein kontekst for øvinga, og 3) eit spel. I det følgjande vil vi gå gjennom desse elementa og forklare tanken bak dei som ledd i å nå dei overordna målsettingane i øvinga.

Infrastruktur

Øvinga nytta Cyberingenørskolens cyberrange, som har fått namnet CyberLab. I denne omgjevnaden sette vi opp både vertslandsstøttesystema kadettane hadde i oppdrag å forsvare og ein «fiendtleg» infrastruktur som åtaka kom frå. Det virtuelle nettverket i infrastrukturen var sett opp slik at einskilde internettadresser (dei som vart nytta av vertslandsstøttesystema og den fiendtlege infrastrukturen) og datatrafikken mellom desse adressene vart haldne innanfor CyberLab, medan all anna internettrafikk vart ruta til det faktiske internettet. På den måten kan ein seie at infrastrukturen også emulerte to små lommer av internett. Fordelen med dette er at det emulerte systemet har ein har normal (og difor realistisk) tilgang til internett og også vert utsett for støy frå internett. Samtidig vil cyberåtak frå den emulerte fiendtlege infrastrukturen mot det emulerte systemet generere realistisk internettrafikk, sjølv om alt vert halde i ein lukka omgjevnad og er utan bruk av reell, tredjeparts internettinfrastruktur.

Systemet kadettane skulle forsvare, kan sjåast som eit relativt standard kontornettverk sett opp med arbeidsstasjonar, brannmur, fildeling, e-post, osb., i tillegg til webtenarar med websider og webapplikasjonar. Sett bort frå at det var noko nedskalert og utan spesielt god sikkerheit, er det ingenting i systemet som skil seg prinsipielt frå eit reelt kontorsystem og ein reell webtenar. Dette i kombinasjon med ruting av internettrafikk som skildra ovanfor gjev ein høg grad av realisme.

DOI: 10.31374/sjms.119

Kadettanes cybersikkerheitssenter hadde ein eigen infrastruktur bestående av nettverkssenorar, arbeidsstasjonar, analysemaskiner osb. Det hadde vore mogleg å emulere også denne infrastrukturen, men vi valde likevel å la kadettane byggje opp sin eigen infrastruktur. Det var fleire grunnar til dette: For det fyrste er det ein måte å oppfylle eit læringsmål om at kadettane skal kjenne verktøya til eit cybersikkerheitssenter. For det andre var det for å skape eit klårt skilje mellom cybersikkerheitssenteret og den organisasjonen og det systemet dei var sette til å støtte og beskytte. Ved bruk av virtualisering kan det vere ei utfordring å ha klårt føre seg «kva som er kva»; ved å la kadettane byggje opp ein eigen infrastruktur åtskild frå virtualiseringsomgjevnaden kunne vi unngå misforståingar om kva som var ein del av det forsvarte systemet og ikkje. For det tredje var sjølve deployeringa eit eige element i øvinga, knytt til læringsmål om oppdragsløysing, som vart gjort eksplisitt for eksempel ved at kadettane måtte setje opp sin eigen nettverkssensor og bringe han til eit bestemt lokale for å installere han i det forsvarte systemet. For det fjerde understøtter det læringsmål om generelle kunnskapar og ferdigheiter i oppsett av IKT-infrastruktur.

Kontekst

Øvinga var som tidlegare nemnt ikkje ei rein teknisk øving, men også ei øving av dei operasjonelle sidene ved hendingshandtering og defensive cyberoperasjonar. Dette inkluderer øving på ferdigheiter som planlegging, organisering, leiing, kommunikasjon og rapportering. For å nå slike læringsmål er det ikkje tilstrekkeleg med ein infrastruktur (som skildra over) som legg til rette for øvinga av dei tekniske ferdigheitene. Det er også naudsynt å setje oppgåvene og utfordringane inn i ein kontekst som legg til rette for øving også av dei ikkje-tekniske ferdigheitene.

For Øving Vinterdrill II 2021 kan vi seie at denne konteksten hadde to hovudkomponentar: (1) eit scenario som skildra kva for hendingar som skjer elles i verda og samfunnet og (2) ein operasjon med oppdrag til teamet av kadettar. Scenarioet vart presentert for kadettane gjennom ulike situasjonsrapportar (som ein del av ordrane), trusselvurderingar, og etterretningsprodukt som vart gjeve før og under øvinga. Desse ulike rapportane skildra både overordna situasjon og hendingar («Situasjonen er så tilspisset at den kan utvikle seg til en konfrontasjon»), lokale hendingar («en multinasjonal stridsgruppe på om lag 1000 soldater […] deployeres til Østerdalen garnison») og hendingar i cyberdomenet («Nasjonalt Cybersikkerhetssenter (NCSC), Direktoratet for samfunnssikkerhet og beredskap (DSB) og Kommune-CSIRT varslet i januar 2021 i felleskap om et pågående angrep knyttet til løsepengevirus mot Østre Toten kommune»). Føremålet med dette var todelt: for det fyrste at kadettane skulle trenast i å byggje trusselbilete og situasjonsforståing, og for det andre å bidra til å skape ei realistisk ramme rundt øvinga. Kadettar med spesialisering i militære IKT-system og CIS-støtteoperasjonar øvde i parallell, men med det same overordna scenarioet, og dei var såleis også ein del av konteksten.

Oppdrag til kadettane vart gjevne gjennom ordrar. Den fyrste ordren – ein ordre om eit beredskapsoppdrag for å «forsterke Cyberforsvaret med en deployerbar enhet for sikkerhetsmessig overvåkning og defensive cyberoperasjoner» – vart gjeven fire veker før øvingsstart. Som ein del av emnet *Cybermakt* (sjå over) gjennomførte kadettane ein plan- og beslutningsprosess der hensikta var «å utvikle et operasjonskonsept som gir den mest optimale løsningen for anvendelse av det materiellet vi har tilgjengelig for å nå de operative kravene […] på en mest effektiv måte». Planleggingsfasen skulle også «resultere i en god forståelse for fiendens cyberkapabiliteter og en detaljert plan for klargjøringsfasen». Kadettane måtte med andre ord planleggje struktur, organisering, rutinar, materiell og infrastruktur for det midlertidige cybersikkerheitssenteret. Eit føremål med å la kadettane gjere ordreanalyse og si eiga planlegging var openbert å gje dei trening i bruk av desse ferdigheitene. Samtidig er det også mogleg å seie at ein kontekst som den vi skapte, var ein føresetnad for å kunne øve denne typen ferdigheiter.

Etableringa av ein kontekst var også naudsynt for å synleggjere handlingsalternativ og konsekvensar av både eigne og motstandaranes handlingar utover det reint tekniske. Kva tyder det for vertslandsstøtteelementet at ein fiendtleg aktør har tilgang til e-posttenaren, og kva er den beste handlemåten for å handtere ein slik situasjon? I tillegg var det å tvinge kadettane til å setje seg inn i konteksten – både den «globale», overordna konteksten og den «lokale», organisatoriske konteksten – ein måte å fremje forståing for heilskapen, og for kompleksiteten i defensive cyberoperasjonar og handtering av cybersikkerheitshendingar. Kva for prosedyrar må til for å deployere ein sensor i nettverket til ei anna verksemd?

DOI: 10.31374/sjms.119

Spel

I tillegg til tekniske ferdigheiter var det eit mål med øvinga å øve kommunikative ferdigheiter. For å gjere det, er det behov for å ha nokon å kommunisere med. Som ein del av konteksten skildra ovanfor vart det difor etablert eit spel der personellet i øvingsstaben spelte ulike aktørar som kadettane måtte forhalde seg til og kommunisere med: representantar for organisasjonen som cybersikkereheitssenteret skulle støtte, representantar for avdelinga som cybersikkerheitssenteret var underlagt, osb. Kommunikasjonen føregjekk både på e-post, telefon og fjes-til-fjes, og det vart lagt vekt på å ikkje leggje for mykje avgrensingar i kven kadettane fekk kommunisere med, men heller skape nye roller ved behov. Som ein del av dette spelet måtte kadettane også rapportere dagleg både skriftleg og munnleg. I tillegg til å fungere som trening i rapporteringsrutinar gav det ei moglegheit for øvingsstaben å korrigere utan å måtte gå inn i rolla som mentor.

Som med infrastrukturen og konteksten skildra ovanfor, var ei målsetting med dette spelet også å freiste å skape ein realisme i øvinga (til dømes det å ha moglegheit til å ringe nokon for å spørje om noko) for å fremje motivasjon og innleving hjå øvingspublikum, og også stimulere til sjølvstendig tenking og kreativitet. Samtidig gav det ei moglegheit til å skape noko av den kompleksiteten som kjem av å måtte forhalde seg til aktørar som kan ha eigne og motstridande interesser. Nettopp for å styrke truverdet og realismen i øvinga freista vi å halde eit tydeleg skilje mellom dei rollene som øvingsstaben spelte og mentorane som fylgde kadettane og var utanfor spelet.

Vi meinte samtidig at det var behov for tilbakemeldingar og refleksjonar undervegs i øvinga. Det var difor lagt inn to avbrekk eller «stridspausar» i spelet der kadettane fekk tilbakemeldingar, fekk diskutere hendingshandteringa med øvingsleiinga, og fekk reflektert og omorganisert seg.

EVALUERING

Ved avslutning av øvinga leverte deltakarane skriftlege tilbakemeldingar der dei vart bedne om å summere opp kva som fungerte bra («bør behaldast til neste øving») og kva som fungerte mindre bra («bør forbetrast til neste øving»). Den følgjande evalueringa er basert på fem slike skriftlege tilbakemeldingar: éi skriven av dei 13 kadettane i lag, tre skrivne av til saman fire av personane i øvingsstaben, og éi skriven av forfattaren sjølv.

Den viktigaste tilbakemeldinga for arrangørane av øvinga var sjølvsagt at kadettane rapporterte at øvinga hadde gjeve mykje læring og at dei opplevde meistring. Dette er konsistent med tilbakemeldingane frå øvingsstaben, som melde at dei observerte læring og meistring hjå kadettane. Kadettane rapporterte at realistiske casar hadde bidrege til læring. Dette må truleg attribuerast til ein kombinasjon av infrastrukturen og cyberåtaka utført av Red Team. Øvingsstaben var i sine tilbakemeldingar meir opptekne av at casane hadde passande vanskegrad og kompleksitet, og at kadettane fekk tilstrekkeleg med tid til å løyse dei før det kom nye utfordringar.

Både kadettar og øvingsstab rapporterte at spelet bidrog til innleving og dimed fremja motivasjon og læring. Samtidig vart det òg oppsummert at mentorane som stod utanfor spelet var viktige, og at «stridspausar» med tilbakemeldingar og hint frå Red Team var motiverande og lærerike. Det var ein fordel at pausane representerte tydelege brot i spelet. Likevel vart det peika på at skiljet mellom når personar i øvingsstaben var i ein administrativ funksjon, når dei spela ei rolle og når dei opptredde som mentorar, med fordel kunne vore tydelegare, og at mangel på tydelege skilje kunne føre til misforståingar og frustrasjon. Det kan med andre ord sjå ut som det finst avvegingar ein må gjere om kor mykje ein ønskjer å avbryte det kontinuerlege spelet og korleis ein disponerer øvingsstaben.

Vurderingane av freistnaden på å etablere ein kontekst rundt øvinga var meir blanda. Øvingsstaben meinte det fungerte godt at kadettane stod for eigen planlegging og leiing, men at det krev tett oppfølging og mentorering, i tillegg til god tid. Vidare oppsummerte dei at interaksjonen med den overordna øvinga og scenario var eit gode, og at han kunne vore meir omfattande, men at kadettane sine handlingar burde hatt meir operative konsekvensar i den overordna konteksten. I tillegg var munnleg, ikkje-teknisk rapportering til «utanforståande» viktig for øvinga og noko det ideelt sett burde vore meir av. Kadettane, på den andre sida, synast å oppfatte den overordna konteksten meir som eit forstyrrande element. Sjølv om dei var positive

DOI: 10.31374/sjms.119

til å gjere eigen planlegging og klargjering, fekk den overordna øvinga og scenarioet for stor plass i planleggings- og klargjeringsfasen, og gjekk ut over meir konkrete førebuingar til teknisk handtering av cybersikkerheitshendingar. Spesielt arbeidet med kommunikasjonsløysingane til cybersikkerheitssenteret vart opplevd som mindre relevant. Derimot fungerte relasjonen til den overordna avdelinga godt, og særleg tilbakemeldingane på dei skriftlege produkta dei leverte vart oppsummert som nyttige.

På same øving vart det òg gjennomført ein studie der standardiserte spørjeskjema vart nytta til å undersøkje relasjonen mellom sjølvregulering og lagprestasjonar hjå kadettane (Ask et al. 2021). Sjølv om dette kan fortelje noko om kva slags evner og eigenskapar som er nyttige hjå personell i eit cybersikkerheitssenter, er studien på eit detaljnivå der han seier lite om korleis det overordna designet av øvinga påverka læringsutbytet.

UTFORDRINGAR

Som vi har sett, hadde CDX-delen av Øving Vinterdrill II 2021 eit øvingskonsept der det vart lagt stor vekt på å skape realisme. I det følgjande vil vi sjå på nokre av utfordringane som ligg i dette konseptet.

For at dei emulerte systema involvert i øvinga skal framstå som realistiske, er det naudsynt at dei har ein viss storleik og kompleksitet. Å definere og setje opp systema i infrastrukturen (CyberLab) krev difor ein del ressursar. Dette vart til ein viss grad løyst ved at hovuddelen av dei forsvarte systems var eit generisk kontorsystem som i stor grad var gjenbruk frå tidlegare øvingar. Ei utfordring med dette er at systemet kan verte for generisk og at det er lite i det som gjenspeglar den fiktive organisasjonen som i scenarioet er eigarane og brukarane av systemet. I tillegg var «malen» som vart nytta eit «blankt» system, dvs. utan data som normalt vil akkumulere ved bruk over tid. I og med at cyberåtaka som systemet vart utsett for i øvinga, inkluderte eksfiltrasjon av data og eit løysepengevirus (som krypterer og held data som «gissel»), vil mangelen på data redusere realismen og kompleksiteten i handteringa av åtaka. På den andre sida vil det å byggje opp eit informasjonssystem med truverdige data auke ressursbruken i oppsettet betydeleg.

Vi hadde ei tilsvarande utfordring med datatrafikk i det emulerte nettverket. Normalt vil brukaraktivtetar generere trafikk i nettverket, men sidan systemet ikkje hadde reelle brukarar, var det heller ikkje noko reell datatrafikk. Ei løysing på dette er openbert å ha personell til å spele brukarar, men det vil igjen representere ei betydeleg auke i ressursbruken. Vi kompenserte delvis ved å nytte ei programvare som simulerte brukaraktivtetar (i praksis internettsurfing), men det er utfordrande å lage gode simulatorar, og den vi nytta var relativt enkel. Samtidig er det opent kvar den «nedre grensa» for realisme i den tekniske infrastrukturen ligg før det byrjar å gå utover læringsutbytet.

Elektronisk kommunikasjon var ei utfordring vi ikkje fann nokon god løysing på i øvinga. Kadettanes cybersikkerheitssenter hadde behov for å kommunisere både med overordna avdeling og organisasjonen dei støtta. I utgangspunktet hadde dei sjølv ansvar for dette som ein del av å definere sin eigen infrastruktur, men det viste seg vanskeleg å få på plass eit fungerande system. Sidan kommunikasjon var ein sentral del av øvinga bestemte vi oss for å gå over til å nytte personlege e-postkontoar og mobiltelefonar for å ikkje la problem med kommunikasjonssystema gå utover kommunikasjonen. Problemet med denne avgjerda er todelt. For det fyrste er det å få på plass gode kommunikasjonsløysingar ei reell utfordring som det i seg sjølv er verdt å øve på, og det same er kommunikasjonsutfordringar med opphav i manglande kommunikasjonsløysingar. For det andre er det ei reell problemstilling korleis ein skal kommunisere når ein må anta ta kommunikasjonssystema er kompromittert, slik som var tilfelle for e-postsystemet til den fiktive organisasjonen i øvingsscenarioet (Lund 2021: 103–104). Som vi har sett skapte utfordringane med kommunikasjonssystemet frustrasjon hjå kadettane og det vart eit forstyrrande element som tok fokuset bort frå hovudoppgåvene til cybersikkerheitssenteret. Då vi gjekk over til kommunikasjonssystem utanfor øvingas infrastruktur og scenario fjerna vi eit forstyrrande element, men samtidig reduserte vi også realismen og kompleksiteten i øvinga. Det kan stå som eit eksempel på ei avveging i designet av slike øvingar: Skal ein leggje mest vekt på å øve cybersikkerheitsferdigheiter eller på å handtere kompleksiteten i defensiv cyberoperasjon.

Som alt antyda var ressursbruken i øvinga relativt høg. I alt elleve personar var involvert i operasjonsfasen for å øve 13 kadettar. Samtidig er det vanskeleg å sjå korleis ein kan redusere dette vesentleg utan at det går utover den relativt høge graden av interaksjon som det vart lagt opp til. Det ser heller ikkje ut til at skalerbarheita er spesielt god. Ved å ha fleire team som arbeidde i parallell med dei same oppgåvene, kunne ein hatt eit større øvingspublikum, men ein måtte samtidig hatt ein større stab for å mentorere og å handtere interaksjonen med dei ulike aktørane. Likevel ser ikkje ressursbruken ut til å vere uvanleg samanlikna med liknande øvingar. I den vanlege terminologien for CDXar hadde Øving Vinterdrill II 2021 eit Blue Team med 13 personar, eit Red Team med tre personar og eit kombinert White, Green og Purple Team på åtte personar. Det gjev eit forholdstal på 13:11, eller ca. 1:1 mellom dei som blir øva (Blue Team) og dei som på ulike måtar legg til rette (White, Red, Green og Purple Teams). I gjennomgangen av andre øvingar skildra i litteraturen finn vi igjen det same forholdstalet: Amber Mist 2018 hadde 24:46, Cyber Czeck hadde 24:25 og 20:20, og Baltic Cyber Shield hadde 50:50.

EVALUERING AV CYBERSIKKERHEITSØVINGAR

Over har vi sett at ressursbruken ved CDXar er stor. Til det kan vi leggje til at planlegginga av slike øvingar kan ta fleire veker eller månader (6–7 veker for Øving Vinterdrill II 2021). Det er difor ikkje urimeleg å stille spørsmålet om øvingane har den læringseffekten vi ønskjer oss. Eit spørsmål i forlenginga av det er korleis vi kan undersøkje læringseffekten av slike øvingar.

Dette er ikkje ei ny problemstilling, og felles for øvingsrapportane refererte i denne artikkelen er at det i alle tilfella er gjort forsøk på å evaluere utbyte frå øvingane. Karjalainen et al. (2020) gjennomførte ei spørjeundersøking mellom 21 av dei 86 deltakarane om læringsutbyte på 44 læringsområde. Resultatet viser at respondentane rapporterer som svakt læringsutbyte på dei fleste av læringsområda. Brilingaitė et al. (2020) gjennomførte ei spørjeundersøking mellom Blue, Red og Purple Teams før og etter Amber Mist 2018, men hadde i tillegg observatørar i laga og gjorde ei samanstilling av svar på spørjeundersøkingane med den faktiske prestasjonen. Spørjeundersøkinga viste at deltakarane opplevde læring gjennom øvinga, men også at laga hadde overdriven tru på eigne prestasjonar samanlikna med dei observerte prestasjonane. Ved ei av gjennomføringane av Cyber Czeck i 2017 lét Vykopal et al. (2018) dei 20 deltakarane frå fem Blue Teams svare på to spørjeundersøkingar rett etter øvinga, og igjen etter at dei hadde blitt presentert for ei tidsline over scoring knytt til hendingar under øvinga. Resultata viste at deltakarane tykte øvinga var utfordrande, men nyttig, og at feedbacken dei fekk gjennom tidslina var nyttig. Granåsen & Andersson (2016) presenterer ei brei undersøking av Baltic Shield 2010 der det vart nytta spørjeundersøkingar, observatørar i laga, rapportar frå Red og Blue Teams, After Action Reviews og intervju i etterkant, i tillegg til opptak av video, lyd og skjermbilete, og innsamling av chat-loggar, e-postkommunikasjon og tekniske data frå infrastrukturen. Det vart også gjort scoring undervegs i øvinga basert på oppetida til dei forsvarte systema. Mellom resultata var at deltakarane var motiverte og oppfatta vanskegraden til øvinga som god. Spørjeundersøkingane gav nyttig informasjon om korleis laga vurderte seg sjølv, men viste også at sjølvevaluering og -rapportering er upålitelege mål for prestasjon og effektivitet. Observatørrapportar og hendingsrapportar frå laga var dei mest verdifulle for å få innsikt i lagprestasjonane; automatisk scoring kan gje eit røft bilete av prestasjonane til laga, men gjev lite innsikt i korleis laga arbeider.

Brilingaitė et al. (2020), Karjalainen & Kokkonen (2020b) og Vykopal et al. (2017) gjev alle metodikk for planlegging og gjennomføring av cybersikkerheitsøvingar, men det er vanskeleg å sjå at desse følgjer frå dei systematiske undersøkingane refererte til over. Vi må difor leggje til grunn at desse metodikkane er baserte på eigne og andres erfaringar, og kjennskap til ulike pedagogiske modellar. Meir direkte nyttar Vykopal et al. (2018) resultata frå undersøkinga si til å argumentere for viktigheita av raske og detaljerte tilbakemeldingar til deltakarane. Til skilnad var føremålet med analysen til Granåsen & Andersson (2016) å evaluere ulike metodar for å vurdere Blue Teams på seinare øvingar.

Denne gjennomgangen viser ulike former for evaluering av øvingar, som ikkje er heilt utan utfordringar. Både Brilingaitė et al. (2020) og Granåsen & Andersson (2016) peikar på det problematiske i å basere seg utelukkande på sjølvrapportering frå deltakarane. Lessons learned-rapportar, som denne artikkelen representerer, er heller ikkje uproblematiske. Enisa

DOI: 10.31374/sjms.119

(2015: 28–29) peikar på den openberre faren for at slike rapportar har den biasen at øvinga av politiske eller andre grunnar «må» lykkast.

I evalueringa av Øving Vinterdrill II 2021 oppsummerte vi at øvinga hadde gjeve læring og meistring. Samtidig må vi passe oss for å trekkje for sterke konklusjonar frå denne evalueringa. Som peika på over er det ikkje uproblematisk å basere seg på sjølvrapportering; vi kan ikkje ta for gjeve at deltakarane si kjensle av læring i augneblinken korrelerer med tileigning av ønskte kunnskapar og ferdigheiter. Det ligg også ei betydeleg utfordring i å nytte rapportar frå arrangørane i evaluering av øvingar, til dømes faren for bias i retning av å vere nøgd med eller forsvare eigne avgjerder og eige arbeid. Spørsmålsstillinga i evalueringa, om kva som fungerte og ikkje fungerte i øvinga, kan ha både fordelar og ulemper. Ulemper er både at det ikkje er spørsmål om læring og måloppnåing, og at det oppmuntrar til å trekkje fram «det viktigaste». Spørsmålsstillinga eignar seg difor dårleg for å få detaljert kunnskap om oppfylling av læringsmål. Ein fordel ved spørsmålsstillinga kan vere at det gjev konkrete svar om spesielt gode eller dårlege sider ved øvinga (Pettersen 2005: 294–295). Dette vil potensielt kunne utfordre dei grunnleggjande premissa for øvingsdesignet på ein måte som ei meir målretta evaluering av læringsutbyte moglegvis ikkje vil fange opp.

Eit alternativ til eigenrapportering kan vere å basere evaluering av øvingar på manuell eller automatisk scoring, dvs. ulike formar for metrikkar for oppgåveløysing. Det vil kunne gje meir objektive mål, men samtidig er det ei fare for å redusere evalueringa til løysing av einskildoppgåver. Ei utfordring vil då vere korleis ein målar heilskapsforståinga som vi har sett som eit sentralt læringsmål. Ei anna utfordring er at eit mål på deltakarane sine prestasjonar på ei øving ikkje naudsynleg gjev eit mål for læring eller for deira framtidige virke som profesjonsutøvarar.

OPPSUMMERING

Vi har presenter Øving Vinterdrill II 2021 – ein CDX gjennomført for 13 kadettar ved Cyberingeniørskolen ved Forsvarets høgskole. Vi har framheva element i designet av øvinga vi meiner var sentrale. Ei kort oppsummering er at vi la stor vekt på å lage ein realistisk og truverdig omgjevnad (infrastruktur, kontekst, scenario, spel) for å fremje innleving, motivasjon og læring av både tekniske og ikkje-tekniske ferdigheiter. Vi har gjort ein gjennomgang av tilbakemeldingar frå øvingsstab og øvingspublikum, og også oppsummert utfordringar ved øvingskonseptet.

Ein gjennomgang av litteratur om cybersikkerheitsøvingar viser at Øving Vinterdrill II 2021 har store likskapar med andre øvingar av same type. Likevel – i eit spekter frå funksjonsøving til fullskala-øving – plasserer øvinga seg kanskje som eit ytterpunkt med stor vektlegging av kontekst og scenario, og av øving på ferdigheiter som organisering, leiing, rapportering og kommunikasjon i tillegg til dei tekniske ferdigheitene. Vidare hadde øvinga lite vektlegging av scoring, stress og konkurranse.

Både i Øving Vinterdrill II 2021 og liknande øvingar presentert i litteraturen har ressursbruken vore stor. I kva grad desse øvingane har ønskt effekt og utbyte, blir difor eit relevant spørsmål. Som vi har sett, er det heller ikkje eit trivielt spørsmål. I militære utdanningar har vi også den tilleggsutfordringa – som i tilfellet med Øving Vinterdrill II 2021 – at ein samtidig ønskjer å øve andre sider av den militære profesjonen som ikkje er direkte knytt til cybersikkerheitsferdigheiter.

Cybersikkerheitsøvingar blir ofte gjennomførte på IKT-plattformer som vi omtalar som *cyberranges*. Ein kan argumentere for at ein måte å redusere ressursbruken på er å utnytte potensialet for automatisering (til dømes av cyberåtak og scoring) som ligg i desse plattformene. Vi vil derimot argumentere for at det å investere ressursane i automatisering kan føre til at ein låser seg til bestemte måtar å organisere øvingane på før vi har tilstrekkeleg kunnskap om kva som gjev best utbyte.

For vidare utvikling av cybersikkerheitsøvingar til utdannings- og opplæringsføremål vil det vere behov for fleire og større undersøkingar. Vi ser føre oss tre moglege vegar å gå: (1) Breie evalueringar med samansette metodar slik som rapportert av Granåsen & Andersson (2016). I slike evalueringar bør ein leggje særleg vekt på observasjonar av øvingspublikum, og analysar av dei munnlege og skriftlege produkta og rapportane som øvingspublikummet produserer undervegs i ei øving. Vidare bør evalueringane funderast i analysar av relasjonen

mellom læringsmål og aktivitetar, slik som presentert av til dømes Karjalainen & Kokkonen (2020b). (2) Meta-studiar av øvingsrapportar. Rapportar frå einskildøvingar kan som vist ha bias og svakheiter, men vonleg kan det vere mogleg å handtere svakheitene og å trekkje ut allmenngyldige lærdomar dersom ein kan samanhalde rapportar frå mange øvingar. (3) Undersøkingar mellom personell i responsorganisasjonar som har delteke på cybersikkerheitsøvingar. Dette vil vonleg kunne kaste lys over læringseffekten på lengre sikt enn berre rett etter at ei øving er gjennomført – og ser for oss ut til å vere ein av dei få metodane vi har for å undersøkje langtidseffektar av øvingar.

ETIKK OG SAMTYKKE

All bruk av skriftlege tilbakemeldingar i denne artikkelen er etter skriftleg, informert samtykke. Prosjektet er vurdert og godkjent av Norsk senter for forskningsdata (NSD) og Forsvarets forskningsnemnd.

TAKK

Takk til Cyberingeniørskolen ved Forsvarets høgskole som aktivt oppmodar til erfaringsdeling og forsking på øvingar, og spesiell takk til kadettar og forsvarstilsette som har late meg nytte tilbakemeldingane deira i arbeidet med denne artikkelen. Takk også til den anonyme fagfellen som gjennom kommentarane sine har bidrege til store forbetringar av artikkelen.

KONKURRERANDE INTERESSER

Forfattaren var tilsett ved Cyberingeniørskolen og leidde aktiviteten det blir rapportert frå i denne artikkelen.

AUTHOR AFFILIATION

Mass Soldal Lund orcid.org/0000-0002-5286-982X
Inland Norway University of Applied Sciences, NO; Norwegian Defence University College, NO

REFERANSAR

Adnan, M., Just, M., Baillie, L., & **Kayacik, H. G.** (2015). Investigating the work practices of network security professionals. *Information & Computer Security, 23*(2), 347–367. DOI: https://doi.org/10.1108/ICS-07-2014-0049

Ask, T. F., Sütterlin, S., Knox, B. J., & **Lugo, R. G.** (2021). Situational States Influence on Team Workload Demands in Cyber Defense Exercise. I. C. Stephanidis et al. (Red.), *HCI International 2021 – Late Breaking Papers: Cognition, Inclusion, Learning, and Culture* (LNCS Bd. 13096, s. 3–20). Springer. DOI: https://doi.org/10.1007/978-3-030-90328-2_1

Brilingaitė, A., Bukauskas, L., & **Juozapavičius, A.** (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security, 88*, artikkel 101607. DOI: https://doi.org/10.1016/j.cose.2019.101607

Direktoratet for samfunnstryggleik og beredskap (DSB). (2016). *Rettleiar i planlegging, gjennomføring og evaluering av øvingar. Grunnbok: Introduksjon og prinsipp.* Henta frå https://www.dsb.no/globalassets/dokumenter/rapporter/rettleiar_i_planlegging_og_gjennomforing_ovelser_grunnbok_nynorsk.pdf

Enisa. (2015). *The 2015 Report on National and International Cyber Security Exercises. Survey, Analysis and Recommendations*. Henta frå https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises/at_download/fullReport

Forsvaret. (2019). *Forsvarets fellesoperative doktrine*.

Forsvarets høgskole (FHS). (u.å.). *Bachelor ingeniør – telematikk*. Forsvaret. Henta 21. august 2022 frå https://www.forsvaret.no/utdanning/utdanninger/ingeniorfag-studieretning-telematikk

Geers, K. (2010). Live Fire Exercise: Preparing for Cyber War. *Journal of Homeland Security and Emergency Management*, *7*(1), artikkel 74. DOI: https://doi.org/10.2202/1547-7355.1780

Granåsen, M., & **Andersson, D.** (2016). Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. *Cognition, Technology & Work*, *18*(1), 121–143. DOI: https://doi.org/10.1007/s10111-015-0350-2

Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., & **Helkala, K.** (2019). Self-regulation and cognitive agility in cyber operations. *Frontiers in Psychology, 10*, artikkel 875. DOI: https://doi.org/10.3389/fpsyg.2019.00875

Karjalainen, M., & **Kokkonen, T.** (2020a). Comprehensive Cyber Arena; The Next Generation Cyber Range. I *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW 2020)* (s. 11–16). IEEE. DOI: https://doi.org/10.1109/EuroSPW51379.2020.00011

Karjalainen, M., & **Kokkonen, T.** (2020b). Review of Pedagogical Principles of Cyber Security Exercises. *Advances in Science, Technology and Engineering Systems Journal, 5*(5), 592–600. DOI: https://doi.org/10.25046/aj050572

Karjalainen, M., Puuska, S., & **Kokkonen, T.** (2020). Measuring Learning in a Cyber Security Exercise. I *12th International Conference on Education Technology and Computers (ICETC 2020)* (s. 205–209). ACM. DOI: https://doi.org/10.1145/3436756.3437046

Katsantonis, M., Fouliras, P., & **Mavridis, I.** (2017). Conceptual Analysis of Cyber Security Education Based on Live Competitions. I *IEEE Global Engineering Education Conference (EDUCON 2017)* (s. 771–779). IEEE. DOI: https://doi.org/10.1109/EDUCON.2017.7942934

Lund, M. S. (2018). CND-konsept for taktiske nettverk. I Ø. Jøsok & B. J. Knox (Red.), *Ledelse i Cyberdomenet* (s. 35–47). Forsvarets ingeniørhøgskole.

Lund, M. S. (2021). Kommunikasjonssystemer for beredskap og krisehåndtering – teknologi og utfordringer. I A.-K. Larssen (Red.), *Beredskap og krisehåndtering. Utfordringer på sentralt, regional og lokalt nivå* (s. 86–108). Cappelen Damm.

Nato. (2018, 29. oktober). *Trident Juncture 2018*. North Atlantic Treaty Organization. Henta 4. mars 2022 frå https://www.nato.int/cps/en/natohq/157833.htm

Nikolaisen, P.-I. (2016, 21. januar). – Er det IS eller Russland? Slik øver fremtidens norske cybersoldater. *Teknisk Ukeblad, 163*(1), 28–35.

Naas, T. (2014). Øvelse Cold Matrix. *Soldatnytt, 35*(11), 14–15.

Ošlejšek, R., Rusňák, V., Burská, K., Švábenský, V., Vykopal, J., & **Čegan, J.** (2021). Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training. *IEEE Transactions on Visualization and Computer Graphics, 27*(8), 3425–3437. DOI: https://doi.org/10.1109/TVCG.2020.2977336

Pettersen, R. C. (2005). *Kvalitetslæring i høgere utdanning. Innføring i problem- og praksisbasert didaktikk*. Universitetsforlaget.

Seker, E., & **Ozbenli, H. H.** (2018). The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation. I *International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2018)*. IEEE. DOI: https://doi.org/10.1109/CyberSecPODS.2018.8560673

Trent, S., Hoffman, R. R., Merritt, D., & **Smith, S.** (2019). Modelling the cognitive work of cyber protection teams. *The Cyber Defense Review*, 4(1), 125–135.

Universitets- og høgskolerådet (UHR). (2020). *Nasjonale retningslinjer for ingeniørutdanning*. Henta frå https://www.uhr.no/_f/p1/i0cb3d399-4d21-4317-8978-e4f44c2306c1/nasjonale-retningslinjer-for-ingeniorutdanning-vedtatt-av-uhr-mnt-november-2020.pdf

Vykopal, J., Ošlejšek, R., Burská, K., & **Zákopčanová, K.** (2018). Timely feedback in unstructured cybersecurity exercises. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE 2018)* (s. 173–178). ACM. DOI: https://doi.org/10.1145/3159450.3159561

Vykopal, J., Vizváry, M., Oslejsek, R., Celeda, P., & **Tovarnak, D.** (2017). Lessons learned from complex hands-on defence exercises in a cyber range. In *IEEE Frontiers in Education Conference (FIE 2017)*. IEEE. DOI: https://doi.org/10.1109/FIE.2017.8190713

Yamin, M. M., Katt, B., & **Gkioulos, V.** (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security, 88*, artikkel 101636. DOI: https://doi.org/10.1016/j.cose.2019.101636

TO CITE THIS ARTICLE:
Lund, M. S. (2022). Øving på cybersikkerheit: Ein casestudie av ei cybersikkerheitsøving. *Scandinavian Journal of Military Studies*, 5(1), pp. 244–256. DOI: https://doi.org/10.31374/sjms.119

Submitted: 22 October 2021
Accepted: 09 June 2022
Published: 19 September 2022