AV MASS SOLDAL LUND

Cyber som operasjonsdomene

Nærmest daglig leser vi om fiendtlig cyberaktivitet og hackerangrep. Er dette noe vi bør være svært engstelige for, eller er trusselen hauset opp av aktører med produkter og kompetanse å selge? For å kunne svare på slike spørsmål, bør man starte med å fastslå hva cyberdomenet egentlig er. I denne artikkelen gir forfatteren oss et innblikk i fundamentet for dette domenet.

Mass Soldal Lund er førsteamanuensis ved Forsvarets ingeniørhøgskole og underviser i informasjonssikkerhet. (Foto: Kirsti Hovde)

NATO-toppmøtet i Warszawa i juni 2016 anerkjente cyber som operasjonsdomene.[1] Vi har i Noreg gjort noko av den same anerkjenninga gjennom oppretting av Cyberforsvaret i 2012[2] og ved å inkludere cyberoperasjonar i den siste utgåva av Forsvarets fellesoperative doktrine.[3] På trass av dette ser det ut til å herske usikkerheit om tydinga av «cyber». Dette er ei usikkerheit i dobbelt forstand; det er usikkerheit om kva vi skal forstå med omgrep som *cyberdomenet, cyberoperasjon, cybervåpen, cybermakt* og andre som startar med prefikset *cyber-*, og det er usikkerheit om kor viktig cyber er og vil vere for pågåande og framtidige konfliktar.[4] Den siste av desse usikkerheitene heng openbert saman med den fyrste; det vil vere vanskeleg å vurdere om cyber er hype eller game changer om ein ikkje har ei slags forståing av kva som ligg i omgrepet.

Når ein ønskjer klarheit og semje om omgrep er definisjonar ei mykje nytta tilnærming. Diverre er til dømes «FDs cyberretningslinjer»[5] frå 2014 eit eksempel på det motsette, at det å freiste lage presise definisjonar for noko ein ikkje fullt ut forstår har god sjanse for å mislykkast. Mange av definisjonane i dokumentet er sirkulære eller innbyrdes motseiande, men det finst òg andre problem. Dokumentet definerer cybermakt som «[e]vne til å anvende eller projisere makt i eller gjennom cyberdomenet».[6] Problemet er at definisjonen implisitt føreset at makt lèt seg anvende eller projisere i eller gjennom cyberdomenet, men utan å gjere oss noko visar om korleis dette skal arte seg. I staden for å klargjere dyttar han på problemet; før vi veit noko meir om cyberdomenet og moglegheita til å projisere makt gjennom det, veit vi eigentleg ikkje noko meir om cybermakt enn før vi hadde definisjonen.

Denne artikkelen vil ta føre seg den fyrste av dei to usikkerheitene rundt cyber, korleis vi skal forstå dette nye domenet. Sjølv om ein diskusjon om relevansen av det på sett og vis er meir interessant, synest ei djupare forståing av domenet å vere ein føresetnad. Som eit alternativ til å freiste definere seg ut av problemet er målet med artikkelen å skildre nokre særdrag ved cyber – eit forsøk på å avdekke grunnleggjande og essensielle eigenskapar ved domenet.

Definisjon vs. særdrag

Skilnaden på definisjon og skildring av særdrag kan illustrerast med to sitat frå kapittelet om «luftdimensjonen» i Forsvarets fellesoperative doktrine:

(1) «Stridskrefter knyttet til luftdimensjonen består først og fremst av aerodynamiske objekter (fly, missiler og lignende) som utnytter jordens atmosfære som operasjonsdimensjon ...»

(2) «Luftstyrkenes grunnleggende fortrinn er høyde, hastighet og rekkevidde. Høyde kombinert med avanserte sensorsystemer gir et unikt overblikk. Hastighet og rekkevidde gir evne til å bevege seg over store avstander ...»[7]

Sjølv om sitat (1) kan seiast å vere ein meir presis definisjon, bør det vere liten tvil om at sitat (2) gjev mest innsikt i luftdimensjonen og er det beste utgangspunktet for å forstå luftmakt. Grunnen til dette er at sjølv om sitat (1) fortel oss noko faktisk om domenet er det sitat (2) som gjev innsikt i dei eigenskapane ved domenet som gjer at luftmakt skil seg frå andre formar for maktutøving.

Sett på spissen har vi så langt vore for opptekne av «jordens atmosfære» og «aerodynamisk objekter» i cyber og for lite opptekne av «høyde, hastighet og rekkevidde».[8] I det følgjande er målet å sjå på nokre særdrag ved cyber, fyrst og fremst med utgangspunkt i teknologi. Vonleg kan dette seie noko om moglegheiter og avgrensingar som ligg i domenet, og opplyse oss om kva ei «evne til å anvende eller projisere makt i eller gjennom» det kan vere.

Cyber som teknologi

FDs cyberretningslinjer definerer cyberdomenet som «[f]ysiske og logiske sammenkoblinger av informasjonssystemer, herunder nettverksenheter, kommunikasjonsinfrastruktur, lagringsmedia og data».[9] Denne definisjonen er, som definisjonen

av cybermakt i same dokument problematisk; fyrst og fremst av di han svarer til luftdomenets «jordens atmosfære» og «aerodynamiske objekter», men også på grunn av alt han utelèt og då spesielt aktivitetar og handlingar.[10]

Det gjev likevel meining å sjå på cyberdomenet som teknologi, spesifikt som informasjons- og kommunikasjonsteknologi (IKT). Det vil sjølvsagt vere feil å hevde at det er bruk av teknologi som gjer cyberdomenet spesielt; krigføring har til alle tider utnytta og fremja teknologi. Den avgjerande skilnaden er at cyberdomenet ikkje eksisterer utan teknologien og difor er fullt og heilt menneskeskapt; dei «naturlege» domena eksisterer utanom teknologi, sjølv om vi brukar teknologi for å få tilgang til og utnytte dei. Denne skilnaden har to konsekvensar når vi søkjer å forstå cyberdomenets ibuande eigenskapar:

(1) Det vil gjelde andre lovar for cyberdomenet enn dei andre, «naturlege» domena. Informasjons- og kommunikasjonsteknologi har, i form av nettverk, prosessorar og lagringsmedium, ei fysisk side som må «lyde dei fysiske lovane» på same måte som alle andre fysiske objekt. Men sidan cyberdomenet ikkje kan skiljast frå informasjons- og kommunikasjonsteknologien må det lyde avgrensingar – og får eigenskapar – som er spesifikke for denne teknologien.
(2) Cyberdomenet har, som alt menneskeskapt, eit føremål som dei «naturlege» domena vantar. Alle dei menneska som har bidrege til å skape cyberdomenet – som har konstruert, designa, bygd og finansiert det – har gjort det med mål og intensjonar som er med å forme det.[11]

Desse to konsekvensane (eller prinsippa om ein vil) har vidare konsekvensar og kan nyttast som eit slags rammeverk for ei vidare utforsking av domenet. Til dømes er ein konsekvens av (1) at bestemte eigenskapar ved informasjons- og kommunikasjonsteknologien gjer det umogleg lage perfekte antivirusprogram.[12] Eit eksempel på ein konsekvens av (2) kan vere «det frie og grenselause» internett.[13] At dette ikkje er naturgjeve men eit resultat av intensjon kan illustrerast ved «den kinesiske brannmuren» som avgrensar fridomen for kinesiske internettbrukarar, og som er eit resultat av andre mål og intensjonar.[14]

Cyber som kapabilitet

Like mykje som cyberdomenet er skapt av informasjons- og kommunikasjonsteknologi er det skapt av ein ny type kapabilitet: evna til å utføre cyberåtak i ulike variantar. Anerkjenninga av cyber som eit eige domene (og opprettinga av ulike lands cyberforsvar eller *cyber commands*) er ein reaksjon på eksistensen av denne evna til å utføre cyberåtak, og kanskje spesielt ein reaksjon på at nokon nyttar eller kan nytte denne evna mot oss.[15] Utan eksistensen av cyberåtak er det liten grunn til å skulle snakke om cyber som operasjonsdomene.

Den sentrale plassen cyberåtak må ha for at vi skal akseptere cyber som eit eige operasjonsdomene illustrerer godt mangelen ved definisjonen av cyberdomenet sitert ovanfor. Men viktigare er det ein peikepinn på kvar ein bør sjå for ei betre forståing av cyberdomenet; kva som er særprega ved cyberdomenet vil i stor grad vere bestemt av kva som er særprega ved cyberåtak. Det er sjølvsagt også avgjerande for evna til å «anvende eller projisere makt i eller gjennom cyberdomenet».

To viktige faktorar som gjer cyberåtak mogleg er det som gjerne vert omtala som allestadsnærvær og konnektivitet. Kombinasjonen av desse, at «alle» system har IKT-komponentar og er kopla saman, kjenner vi igjen i konsept som nettverksbasert forsvar (NbF) og tingas internett (*Internet of Things;* IoT). Når IKT gjennomsyrar alle aktivitetar og system vert måla som kan bli ramma av åtak mot informasjons- og kommunikasjonsteknologien tilnærma uavgrensa. Når stadig fleire system vert kopla saman vil fleire åtakarar kunne nå fleire mål.[16]

Dette er likevel ikkje tilstrekkeleg for å forklare cyberåtak. Den grunnleggjande årsaka til cyberåtak er at teknologien er utnyttbar. Cyberdomenet er en artefakt forma av intensjonane til skaparane, eigarane og brukarane av nettverk, system, maskinvare og programvare. Det som kjenneteiknar eit cyberåtak er at nettverk, system,

Gir det lenger noen mening å snakke om «det digitale rom»? (Foto: Daniel Nordby/Cyber/Forsvaret.)

maskinvare og programvare vert nytta på måtar som ligg utanfor intensjon med dei – at informasjons- og kommunikasjonssystema vert nytta på måtar dei ikkje er meint å verte nytta på av personar som ikkje er meint å skulle nytte dei, for å oppnå noko som ikkje ligg i intensjonen til eigarane, skaparane og brukarane av systema.

Det fyrste spørsmålet vert kva i teknologien som gjer han utnyttbar på denne måten. Ein del av svaret er dårleg kvalitet. Programvarefeil, dårleg designa kommunikasjonsprotokollar og dårleg brukarvenlegheit skapar sårbarheiter som åtakarar kan utnytte for å få systema og teknologien til å gjere ting dei ikkje er meint å gjere.[17] Det er likevel ikkje heile svaret. Grunnlaget for informasjons- og kommunikasjonsteknologien er prinsippet om programlagring: det at kode (dvs. instruksjonane som utgjer program og applikasjonar som datamaskiner utfører) kan handsamast – lagrast og manipulerast – på sama måte som data. Denne oppdaginga la grunnlaget for informasjons- og kommunikasjonsteknologien slik vi kjenner han i dag med datamaskiner som kan utføre vilkårlege oppgåver.[18]

Men dette prinsippet er også det same som gjer cyberåtak mogleg. Eit sentralt element i eitkvart cyberåtak er for åtakaren å få eksekvert sin eigen kode på målsystemet – noko åtakaren kan gjere sidan kode kan overførast over nettverk og skjulast som vilkårlege data. Cyberåtak er difor ei ibuande moglegheit i IKT og betre kvalitet i systema kan berre delvis løyse problemet. Dersom vi ser cybersikkerheit som tiltak for å hindre åtakarar i å eksekvere kode kan det aldri lykkast fullt ut sidan det vil innebere å hindre datamaskiner i å gjere det dei er laga for: eksekvere vilkårleg kode.

Cyberforsvar kan i denne ramma sjåast som eit strev for å oppretthalde intensjonen i systema i møte med cyberåtak. På same måte som cyberåtak er med å skape cyberdomenet kan vi difor seie at cyberåtak er med å skape cyberforsvar.[19]

Alt vi har, nesten, har IKT-komponenter. (Foto: Torgeir Haugaard/Forsvaret)

Cyber som våpen

Cyberåtak er utnytting av IKT-system mot intensjonen til systema for å oppnå noko. Det neste spørsmålet vert kva det er ein kan nytte cyberåtak til å oppnå. Er det mogleg å karakterisere cyber som våpen?

Det er vanleg å skilje mellom *Computer Network Exploitation* (CNE) og *Computer Network Attack* (CNA). CNE er åtak der ein hentar ut informasjon frå motstandarens IKT-system – det ein kanskje vil kalle cyberspionasje – medan CNA er åtak for å skade eller forstyrre motstandarens IKT-system.[20] For ein systematisk analyse er denne inndelinga ikkje tilstrekkeleg. Meir dekkjande kan vi setje opp tre kategoriar av cyberåtak:

(1) Åtak retta mot informasjon.
(2) Åtak retta mot IKT-system og -tenester.
(3) Åtak retta mot fysiske system med IKT-komponentar.

CNE vil gå inn kategori (1) som åtak retta mot konfidensialiteten av informasjon. I tillegg vil denne kategorien omfatte åtak mot integriteten av informasjon (ulike formar for manipulasjon av informasjon) og tilgjengelegheita av informasjon (t.d. den typen datavirus som går under nemninga *ransomware*).[21] Dette er åtak vi relaterer til informasjonssikkerheit. Kategori (2) av åtak svarer til CNA slik det normalt er definert og er åtak vi relaterer til cybersikkerheit.

Når ein nyttar omgrepet «cybervåpen» er det gjerne åtak av kategori (3) ein ser føre seg. Dersom eit cyberåtak skal ha fysisk (kinetisk) effekt er ein avhengig av at målet for åtaket er ein kombinasjon av eit IKT-system som kan verte ramma av eit cyberåtak og eit fysisk system som kan skape den fysiske effekten. Slike system vert nokre gonger refererte til som «cyberfysiske» system og er, med referanse til allestadsnærværet av IKT, kanskje vanlegare enn mange tenkjer over. Sjølv om dei er få finst det nokre kjente eksempel på åtak av type (3), til dømes åtaket mot det iranske anlegget for oppriking av uran i Natanz i 2009-2010 (det såkalla Stuxnet-åtaket),[22] demonstrasjonar av åtak mot personbilar[23] og åtaket mot tre ukrainske kraftleverandørar i desember 2015.[24]

Men sjølv om det kan vere mogleg å skape fysisk effekt og skade ved å ta kontrollen over IKT-delen av eit «cyberfysisk» system vil skade på alt anna enn målsystemet sjølv vere indirekte. Slike system er som alle andre artefakt konstruerte for visse føremål og har innebygd ein intensjon. Det å gjere slike system til våpen vil innebere å nytte dei til noko dei ikkje er laga for. Konsekvensane av det er at dei vil vere langt mindre effektive enn faktiske våpen (som er konstruerte for å skade) og at den faktiske effekten vert langt vanskelegare å føresjå.[25]

Cyber som *space*

Cyberdomenet vert ofte framstilt som eit slags virtuelt rom. Vi kjenner dette igjen i det engelske *cyberspace*, men også i FDs cyberretningslinjer som gjev «det digitale rom» som synonym til cyberdomenet.[26] Det er gjort mange forsøk på å skildre dette rommet. Eit eksempel frå tida før tilgang til (og kjennskap til) internett vart allemannseige skildrar det som at «[c]yberspace is the "place" where a telephone conversation appears to occur ... The indefinite place OUT THERE, where the two of you, two human beings, actually meet and communicate.»[27] Utgangspunktet for denne romlege kjensla kan vere informasjons- og kommunikasjonsteknologiens evne til å vere usynleg – den store avstanden mellom funksjon og fysisk realisering.[28] Men det er grunn til å tru at ideen om cyberspace (og i forlenginga cyberdomenet)

som eit virtuelt rom ein kan gå inn i, opphalde seg i og bevege seg rundt i er spesifikk for dei generasjonane som kunne «oppdage» cyberspace og har liten gjenklang hjå yngre generasjonar som er oppvaksne med internett om ein del av kvardagen.[29] Ein kan òg argumentere for at cyberspace ikkje lenger eksisterer som noko på sida av den «røynlege verda» men i staden er vorte ein underliggjande funksjon som gjennomsyrar alle sektorar og delar av samfunnet, og dei militære domena for den sakas skuld.[30]

Av grunnar som dette bør vi spørje oss om «det digitale rom» som metafor er fruktbart eller om det bør forlatast. Det kan vere andre sider ved topologien til cyberdomenet som det er grunn til å leggje større vekt på. Det finst til dømes oppfatningar av cyberdomenet (eller i det minste internett) som fritt og grenselaust. Slike oppfatningar har openbert mykje i seg; det har sidan starten vore grunnleggjande eigenskapar ved internett. Som vi alt har sett har det konsekvensar som at fleire åtakarar får tilgang til fleire system utan å vere vidare hemma av geografisk avstand. Samtidig er det viktig å vere klar over at dette er eit resultat av design, og dimed intensjon.[31] Eksempelet med «den kinesiske brannmuren» illustrerer at andre intensjonar kan gje domenet andre eigenskapar, som i dette tilfelle ein nasjonal «grensekontroll».

Ein hovudlærdom er at cyberdomenet er formbart. Det er i tråd med at det er menneskeskapt, men også med den sterke avhengnaden til IKT – som er spesielt formbar teknologi.[32] Den eine sida av det er at domenet veks og utviklar seg i takt med utviklinga av teknologien og utbygginga av infrastruktur. Den andre er at ein gjennom design kan freiste gje IKT-system og -nettverk ein har kontroll eller eigarskap over ønskte eigenskapar. I konteksten av cyberforsvar kan det vere å gjere nettverk og system lettare å forsvare, til dømes gjennom å gjere dei lettare å overvake eller gjere det enklare å setje inn mottiltak for å avgrense konsekvensane av cyberåtak.[33] Dette vert i nokre samanhengar omtala som «å forme [cyber]lendet».[34] Sjølv om «lende» som metafor for cyberdomenet fell i same kategori som «rom/*space*» og kanskje burde avvisast, er det all grunn til å merkje seg den formbare karakteren til domenet og søkje ein måte å uttrykke denne sentrale eigenskapen.

Avslutning

Den etterkvart ganske omfattande, og tidvis ukritiske bruken av prefikset cyber-, i kombinasjon med uklarheitene rundt det vi omtalar som eit nytt operasjonsdomene, kan lett få ein til å avvise det heile som *hype*. Men sjølv om bruken av ordet er langt frå konsistent og ein til tider kunne ønskje seg eit meir presist omgrep, kan innføringa av *cyber* vere nyttig som ein markør for at vi står overfor ein ny situasjon. Den nye situasjonen har ikkje oppstått av di bruk av informasjons- og kommunikasjonsteknologi naudsynleg er nytt av året. Han er eit resultat av at utbreiinga og avhengnaden av teknologien og utviklinga av cyberåtak som kapabilitet utover 2000-talet nådde eit punkt der utnyttinga av IKT for etterretning og sabotasje er vorte realitetar som må reknast med.[35] At dette har vore ei gradvis utvikling er ikkje det sama som at «ingenting eigentleg er nytt»; sjølv «teknologiske revolusjonar» skjer gradvis i den forstand at alt som er nytt bygg på det som fanst frå før.[36]

Denne artikkelen har drøfta eigenskapar ved cyberdomenet frå eit teknologisk utgangspunkt. Sjølv om desse kan verke motsetnadsfylte er dei i realiteten ikkje det, men visar at domenet har (enorme) moglegheiter og (reelle) avgrensingar som er annleis enn i dei klassiske fire. Samtidig

Også cyberdomenet kan gjøres til gjenstand for nøktern analyse. (Torgeir Haugaard/Forsvaret)

viser artikkelen at cyberdomenet kan verte utsett for nøktern analyse.

Det er også mykje artikkelen ikkje har teke føre seg og analysen er langt frå fullstendig; mykje vert utelate i ei teknologisk tilnærming, til dømes kva slags påverknads-, operasjonelle eller politiske effektar cyberåtak kan ha. Eit anna tema som ikkje er handsama er korleis cyberdomenet vert utnytta på andre måtar enn gjennom cyberåtak.[37] Det er framleis mykje som er uavklart, men då bør målet vere meir analyse – med ulike tilnærmingar og fortrinnsvis med utgangspunkt i empiriske casar.

Referanser:

1 Warsaw Summit Communiqué, 9. juli 2016.
2 Et Forsvar for vår tid. Prop. 73 S (2011-2012), s. 102-103.
3 Forsvarets fellesoperative doktrine (FFOD 2014), s. 122.
4 M. Libicki. The Cyber War that Wasn't. I Cyber *War in Perspective:Russian Aggression against Ukraine,* s. 49-54, NATO CCD COE Publications, 2015; H. I. Langø. Den akademiske debatten om cybersikkerhet *Internasjonal politikk,* 71(2): 229-240, 2013.
5 Forsvarsdepartements retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren, «FDs cyberretningslinjer», 2014.
6 FDs cyberretningslinjer, s. 21.
7 FFOD 2014, s. 111.
8 Det at ein kan argumentere for at «høyde, hastighet og rekkevidde» ikkje er eit tilstrekkeleg grunnlag for ein luftmaktteori (H. Høiback. Luftmakt – høyde, hastighet og rekkevidde. *I Krigens vitenskap – en innføring i militærteori*, s. 253-301, Abstrakt forlag, 2012, s. 253) gjer ikkje saka noko betre.
9 FDs cyberretningslinjer, s. 4, 5, 21.
10 D. T. Kuehl. From Cyberspace to Cyberpower: Defning the Problem. I *Cyberpower and National Security*, s. 24-42, Potomac Books, 2009, s. 28.
11 H. A. Simon. *The Science of the Artificial*, 3. utgåve. MIT Press, 1996, s. 3-18.
12 F. Cohen. *Computer viruses*. University of Southern California, 1985, s. 23-25, 72-73.
13 T. Rasmussen. *Kampen om Internett*. Pax forlag, 2007, s. 184-191.
14 B. Marczak et al. An Analysis of China's «Great Cannon». I *5th USENIX Workshop on Free and Open Communications on the Internet* (FOCI'15), 2015.
15 W. J. Lynn III. Defending a New Domain. The Pentagon's Cyberstrategy. *Foreign Affairs*, 89(5): 97-108, 2010.
16 P. J. Denning og D. E. Denning. Cybersecurity Is Harder Than Building Bridges. *American Scientist*, 104(3): 154-157, 2016, s. 157.
17 *Ibid.*
18 Prinsippet om programlagring er attribuert til Alan Turing og John von Neumann gjennom det som i ettertida er omtala som universelle Turing-maskiner og von Neumann-arkitektur (B. J. Copeland. Introduction. I *Alan Turing's Automatic Computing Engine*, s. 1-11, Oxford University Press, 2005, s. 1; P. Ceruzzi. Crossing the Divide: Architectual Issues and the Emergence of the Stored Program Computer, 1935–1955. *IEEE Annals of the History of Computing,* 19(1):5-12, 1997, s. 6).
19 D. Pavlovic. Gaming Security by Obscurity. I *Proceedings of the New Security Paradigms Workshop 2011*, s. 125-139, ACM, 2011, s. 126.
20 Sjå t.d. FFOD 2014, s. 212-213.
21 K. Zetter. Hacker Lexicon: A Guide to Ransomware, the Scary Hack that's on the Rise. *Wired*, 17. september 2015.
22 K. Zetter. *Countdown to zero day. Stuxnet and the launch of the world's first digital weapon.* Crown Publishers, 2014.
23 A. Greenberg. The Jeep hackers are back to prove car hacking can get much worse. *Wired*, 1. august 2016.
24 R. M. Lee et al. Analysis of the Cyber Attack on the Ukrainian Power Grid. SANS ICS og E-ISAC, 18. mars 2016.
25 T. Rid. *Cyber war will not take place*. Hurst & Company, 2013, s. 12-15; R. E. Siedler. Hard Power in Cyberspace: CNA as a Political Means. I *8th International Conference on Cyber Conflict: Cyber Power,* s. 23-36, NATO CCD COE Publications, 2016.
26 FDs cyberretningslinjer, s. 4, 5, 21. FFOD 2014 på si side slår fast at «[c]yberdimensjonen oppstår gjennom sammenkopling av informasjonssystemer, ...» og gjev både «det digitale rom» og «det datamaskingenererte rom» som synonym (s. 122).
27 B. Sterling. *The hacker crackdown. Law and disorder on the electronic frontier.* 1994.
28 Simon, *The Science of the Artificial,* s. 6-7, 17-18.
29 H. E. Røislien. When The Generation Gap Collides With Military Structure: The Case of Norwegian Cyber Offisers. *Journal of Military and Strategic Studies,* 16(3): 23-44, 2015, s. 31, 37-38.
30 P. Dombrowski og C. C. Demchak. Cyber war, cybered conflict, and the maritime domain. *Naval War College Review,* 67(2): 71-96, 2014, s. 75.
31 Rasmussen, *Kampen om Internett,* s. 184-191.
32 Simon, *The Science of the Artificial,* s. 17-18; M. S. Mahoney. *Histories of Computing.* Harvard University Press, 2011, s. 59.
33 R. Johnsen. Cyberkrigføring og Forsvarets operative evne. *Internasjonal politikk,* 71(2): 241-251, 2013, s. 244, 247.
34 *Ibid.*, s. 244.
35 Zetter, *Count down to zero day,* s. 205-226.
36 Mahoney, *Histories of Computing,* s. 36-37.
37 J. A. Lewis. 'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine. I *Cyber War in Perspective,* s. 39-47.