Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 77, Nummer 3, side 241-251, 2019, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert september 2019

Fokus: Cybersikkerhet

NATOs offensive cyberspaceoperationer. Muligheder og udfordringer ved NATOs forespørgselsdrevne og effektbaserede tilgang

Jeppe Teglskov Jacobsen
Institut for Militær Teknologi, Forsvarsakademiet, Danmark

Sammendrag

NATO har i det seneste årti orienteret sig mod de defensive aktiviteter i cyberspace, men i slutningen af 2017 gjorde alliancen det klart, at fremtidig planlægning af militære operationer også kommer til at indeholde muligheden for offensive cyberspaceoperationer (OCO). Inklusionen af OCO sker ved hjælp af en såkaldt "effektbaseret model". Ifølge denne model efterspørger NATOs øverstkommanderende – igennem det nyoprettede NATO Cyber Operations Centre – en specifik cybereffekt hos medlemsstaterne. Nærværende artikel peger på modellens muligheder og udfordringer. For selvom OCO indeholder et potentiale som redskab for løbende forstyrrelser af modstanderens netværk, så indeholder OCO også en række begrænsninger og faldgruber, når de skal integreres i en forespørgselsdreven og effektbaseret model: Det gælder i særlig grad manglende koordination omkring effekter (risiko for kollisioner) samt vanskeligheder ved inddæmning og vurdering af effekter. Disse begrænsninger svækker signalet om, at alliancen nu mestrer og for alvor vil gøre brug af cyberdomænet. Ønsker NATO at sende et klart signal, bør alliancen drøfte internt, hvordan man forholder sig til de aktiviteter, der ikke blot knytter sig til væbnet konflikt, som cyberspace også – og primært – tilbyder.

Nøgleord: cyberkrigsførelse · cyberangreb · NATOs operationelle planlægning · integration

*Kontaktinformasjon: Jeppe Teglskov Jacobsen, e-post: jeja@fak.dk

Citation: Jeppe Teglskov Jacobsen (2019). NATOs offensive cyberspace operationer. Muligheder og udfordringer ved NATOs forespørgselsdrevne og effektbaserede tilgang. Internasjonal Politikk, 77(3): 241–251. http://dx.doi.org/10.23865/intpol.v77.1393

Indledning

Udgør oprettelsen af et NATO Cyber Operations Centre, der skal integrere medlemsstaternes cybervåben ind i alliancens operationer, en drastisk forandring af alliancens cyberpolitik? Spørges Rizwan Ali, som var med til at etablere NATO's cyberprogram, er denne ikke i tvivl om: at svaret er "ja" (Ali, 2017). Selvfølgelig sender et nyt Cyber Operations Centre et signal om, at NATO tager cyberdomænet seriøst. Eller som Daniel Moore og Max Smeets (2018) formulerer det, er det muligvis et forsøg på at etablere en troværdig afskrækkelse.

Hvis NATOs generalsekretær Jens Stoltenbergs ord står til troende, er centeret oprettet for at give NATO endnu et redskab, hvormed trusler mod alliancen kan imødegås (Stoltenberg, 2017). Uanset om centeret vitterligt er et signal til Rusland eller blot fremstår som et naturligt næste skridt efter NATOs annoncering af cyberspace som et domæne for militære operationer, er et afgørende spørgsmål stadig, om og på hvilken måde medlemsstaternes cybervåben vil blive brugt til at påføre effekter i alliancens fremtidige operationer. Er integrationen af medlemsstaters cybereffekter i NATOs operationer forbundet med så mange vanskeligheder, at cybervåben kun i mindre omfang vil blive brugt, sender det fx ikke et seriøst signal til eksempelvis Rusland.

Artiklens hovedargument er, at cybervåben som direkte militær støttefunktion kun vanskeligt lader sig integrere i NATOs operationelle planlægningscyklus. Lever offensive cyberspaceoperationer (OCO) i stedet sine egne liv parallelt med de militære operationer, kan de forårsage forstyrrelser, irritationer og tvivl hos fjenden, hvilket indirekte kan understøtte NATOs strategiske mål. Artiklens sekundære argument er, at en åben anerkendelse af behovet for at bevæge sig videre end til blot at se cybervåben som "endnu et militært værktøj" styrker signalet om, at NATO for alvor er en spiller, der skal tages seriøst i cyberdomænet.

Artiklen giver eksempler på, hvordan offensive cyberspaceoperationer (OCO) i NATO kan vise sig nyttige i en operationel kontekst, ligesom artiklen peger på en række generelle karaktertræk ved OCO, der kan vanskeliggøre en meningsfuld integrationen i NATOs operationelle planlægning.

OCO: Et nyt militært værktøj

Cyberangreb forstyrrer, manipulerer eller ødelægger it-systemer, oftest ved at udnytte fejl og sårbarheder i disse systemer (Libicki, 2016, s. 19–20). Cyberspionage er derfor ikke et cyberangreb, for selvom processen, hvorigennem de eksterne cyberangreb udnytter fejl og sårbarheder, langt hen ad vejen overlapper, er en afgørende forskel, at cyberspionage ikke har til hensigt at skade eller forstyrre it-systemet. Cyberspionage ønsker kun manipulation med indhentning af data for øje.

Libicki karakteriserer ydermere cyberangreb som værende midlertidige og reversible. Antagelsen om disse karakteristika skaber en forhåbning om, at cyberangreb bidrager til den militære værktøjskasse med mulige effekter, der kan undgå disproportional skade på eksempelvis civile (ibid., s. 28–31; Smeets, 2017). Den

stigende globale afhængighed af sammenkoblede it-systemer gør samtidig, at det ikke er vanskeligt at forestille sig de militære muligheder ved cyberangreb. Kan man opnå adgang til og manipulere eller sabotere fjendtlige radar- og missilaffyringssystemer, eller kan man forstyrre kritiske kommunikationsnetværk på afgørende tidspunkter, vil det givetvis kunne have afgørende betydning for effekten af en militær operation.

En succesfuld israelsk bombning af et syrisk atomanlæg i 2007, Operation Orchard, udgør et vigtigt referencepunkt for, hvordan strategiske tænkere og praktikere i dag forestiller sig militære brug af cyberangreb. Bombningen blev muliggjort af et cyberangreb, der manipulerede syriske radarsystemer. Den succesfulde operation har resulteret i, at OCOs militære potentiale hovedsageligt ses som støttefunktioner til militære operationer på linje med konventionelle våben (Smeets, 2018).

NATO-medlemslande har også egenhændigt benyttet sig af cyberangreb både som en del af en militær konflikt og i fredstid. Disse cyberangreb fungerer imidlertid ikke primært som militære støttefunktioner. USA udviklede (i samarbejde med Israel) Stuxnet-ormen, som saboterede atomcentrifuger i Iran (Sanger, 2018, s. 7–37). Og USA og Storbritannien forstyrrede ISIS' kommunikation med cyberangreb (Bond, 2018; Jacobsen & Ringsmose, 2017). Alligevel dominerer idéen om, at OCO for at være succesfulde skal spille en mærkbar (og målbar) rolle i nedkæmpningen af fjenden. Således erklærede Ashton Carter, amerikansk forsvarsminister i perioden 2015–7, sig efterfølgende skuffet over de cybereffekter, det amerikanske cybermilitær leverede (Carter, 2017).

De følgende tre afsnit afdækker, hvorledes cyberbegivenheder fremhæver en række karakteristika, som vanskeliggør en succesfuld integration af cyberangreb i NATOs – eller en medlemsstats egen – operationelle planlægning. Artiklen peger specifikt på, hvordan begrænsningerne knytter sig til måden, hvorpå cybervåben udvikles og ændres, vanskeligheden ved at vurdere effekt samt risikoen for negative konsekvenser for andre medlemsstaters arbejde i cyberspace (kollisioner). Artiklens sidste afsnit diskuterer, hvordan cyberangreb mest effektfuldt kan bruges, herunder hvordan NATO kan sende et stærkere signal om, at alliancen tager cyberdomænet seriøst.

Udvikling af cybervåben

På den ene side er cyberangreb i reglen karakteriseret ved, at de rammer pludseligt (Lynn III, 2010). Selvom dette oftest er tilfældet, er det ikke den pludselige effekt, der er interessant for integrationen af OCO. Det er hastigheden, hvormed den udvikles. Som det gælder med traditionelle våben i det militære arsenal, tager fremstillingen af cybervåben tid. Men for cybervåben gælder det videre, at udviklingen er mere afhængig af den specifikke sammensætning af det mål (it-system), der ønskes angrebet, samt at afdækningen og klargørelsen af målet også ofte tager længere tid end i den "fysiske" verden. Viden om målet er således ikke blot relateret til brugen af våbnet, som det er tilfældet med eksempelvis et missil, men derimod også

til våbnets udvikling. Den politiske, juridiske og militære beslutningstager, der skal tage beslutningen om at påføre effekter i cyberspace, er fuldstændig afhængig af et "terræn", som bestemmes af modstanderen.

Det går ud over fleksibilitet, når cybervåben anvendes og genbruges. En sabotageaktion som Stuxnet krævede eksempelvis års udvikling og test, før den var perfektioneret til at opnå den ønskede effekt på det iranske atomanlæg. Selvom dele af Stuxnet senere har fundet vej til flere cyberspionageoperationer (Kello, 2017, s. 170–1), mistede våbnet sin evne til fortsat at ødelægge de iranske centrifuger, da det blev opdaget. Vigtigt er det imidlertid, at USA ikke ønskede, at Stuxnet blev opdaget. Er hemmeligholdelse ikke afgørende nødvendigt i fremtidige operationer, vil cybervåben ofte kunne udvikles og anvendes hurtigere.

Udviklingen af cybervåben må derfor nødvendigvis ofte gå forud for udviklingen af en militær konfrontation. Medlemsstater, der ønsker at levere en cybereffekt i en NATO-operation, må selv i fredstid tilegne sig adgang til en potentiel fremtidig fjendes kritiske netværk og udnytte it-sårbarheder i disse netværk. Ellers er der ikke tid til at udvikle de mest sofistikerede malware. Tidlig forberedelse og udvikling af cybervåben gør sig især gældende, hvis en cybereffekt ønskes leveret i de indledende stadier af en væbnet konflikt. NATO-medlemslande må alternativt sikre sig adgang til så mange generelle teknikker ("exploits") til udnyttelse af it-sårbarheder i kommercielle produkter som muligt (eventuelt via firmaer, der sælger denne service). Derefter må medlemsstater håbe på hurtigt at kunne tilegne sig et overblik over fjendens it-infrastruktur.

Selvom en NATO-medlemsstat udvikler sofistikerede, målrettede cybervåben imod en stat, som NATO kunne komme i konflikt med i fremtiden, eller ligefrem gemmer generelle "exploits" af kommercielle produkter, er det ikke sikkert, at en cybereffekt kan opnås i det øjeblik, den efterspørges. Det skyldes, at de it-sårbarheder, som et cyberangreb ofte er afhængig af, ikke eksisterer for evigt. Cyberspace er et dynamisk domæne: It-systemer opdateres, opgraderes eller erstattes, og fejl og dårlige praksisser opdages og rettes. Det betyder, at cybervåben aldrig blot kan "lægges i værktøjskassen", når de er udviklet. I stedet skal medlemsstater hele tiden sikre sig, at cybervåbnene fortsat fungerer, hvilket ofte kræver små tilpasninger, når eksempelvis opdateringer finder sted. Ergo, jo flere "exploits" og cybervåben en stat råder over, jo flere teknikere skal der bruges til at vedligeholde disse cybervåben.

Cyberspaces dynamiske karakter gør ikke blot, at NATOs medlemsstater skal forudsige, hvor den næste konflikt opstår måneder eller år i forvejen, samt udvikle og vedligeholde cybervåben rettet mod denne (måske) fremtidige fjende. Det resulterer også i, at virkningen af en cybereffekt langt fra kan garanteres, når den endelig efterspørges.

Vurdering af effekt

Hvad er sandsynligheden for at opnå en efterspurgt cybereffekt? Både i planlægningen af OCO og i evalueringen af effekten er svaret ikke altid entydigt. Det skyldes

ikke udelukkende, at nye sårbarheder hele tiden opstår og rettes. Det skyldes også den kompleksitet, som stater skal navigere i i cyberspace, når de skal vurdere effekt og mulige sideeffekter. Rekognosceringen af de it-netværk, der skal påvirkes, er afgørende for et cyberangrebs succes. Men rekognosceringsarbejdet i cyberspace er vanskeligere og mindre entydigt end almindelig rekognoscering.

Når en aktør forsøger at påvirke et netværk, kan det være tilkoblet andre netværk på måder, man ikke har forudset. Derfor kan cyberangreb være svære at inddæmme. Et eksempel herpå er Ruslands forsøg på at forstyrre kritisk infrastruktur i Ukraine ved at kryptere computere i 2017. Angrebet spredte sig globalt og endte med at påvirke store virksomheder som Mærsk, WPP og FedEx.

Utilsigtede konsekvenser er en alvorlig begrænsning for NATO. Alliancen bryster sig af at følge principperne fra international ret om eksempelvis proportionalitet, hvorfor forstyrrelse af civile servere eller generiske cyberangreb, der risikerer at sprede sig vidt og bredt, sandsynligvis ikke vil blive foretrukket. Det amerikanske militær kæmpede eksempelvis med at sikre sig, at dette ikke var tilfældet i cyberangrebene mod ISIS (Nakashima & Ryan, 2016).

En beslægtet problemstilling er videre, at det kan være svært at vide, om det cyberforsvar, en (cyber)angribende aktør er oppe imod, holder øje med en og vildleder en til at tro, at man kan sætte systemet ud af kraft. Cyberforsvar har således udviklet sig til ikke blot at handle om at smide fremmed aktivitet ud, når den bliver opdaget i et netværk. (Aktivt) cyberforsvar handler i stigende grad om at følge en fremmed aktivitet, identificere de teknikker, der bruges, og vildlede dem til at tro, at de ser ting, de ikke gør. Risikoen for vildledning gør det ligeledes vanskeligt at vurdere og verificere effekten af et cyberangreb.

Det er således ikke sikkert, at en medlemsstat uden videre vil stå klar med cybereffekter, hvis NATO kommer til at stå over for en aktør med betydelige defensive cyberkapabiliteter. Det gør sig især gældende, hvis operationel succes er afhængig af den cybereffekt, der efterspørges. Men det skyldes ikke blot, at en stat ikke nødvendigvis har haft tid nok til at udvikle det målrettede cybervåben. Det kan også skyldes, at en medlemsstat alene står med ansvaret for at sikre (og verificere), at den ønskede effekt faktisk opnås, samt at cyberangrebet inddæmmes på en sådan måde, at det ikke medfører indirekte skader på civile.

Selvom en medlemsstat skulle føle sig tilstrækkeligt overbevist om, at en cybereffekt er mulig i det øjeblik, effekten efterspørges, skal denne medlemsstat *også* være overbevist om, at det kan lade sig gøre på det specifikke tidspunkt ude i fremtiden, hvor effekten skal leveres. Det angribende NATO-medlemsland skal have en stærk tro på egne offensive evner, hvis det skal love en specifik cybereffekt på et bestemt tidspunkt i fremtiden. Det bliver kun vanskeligere at stole på egne evner mod fremtidige cyberforsvar, der i højere grad end eksempelvis ISIS har øje på behovet for og har kompetencerne til at identificere og udbedre egne it-sårbarheder samt vildlede modstandere i deres (ofte komplekse) netværk. Som Ben Buchanan (2017) påpeger, er den æra, hvor USA finder, udnytter og gemmer it-sårbarheder, som ingen andre

har adgang til, på vej mod sin afslutning. Det vil med tiden øge tvivlen hos medlemsstater, der forud for en militær operation skal kunne garantere en cybereffekt på et specifikt tidspunkt.

Vanskelighederne ved at vurdere effekten af et cyberangreb gør, at en cybereffekt påført af en medlemsstat i operationel NATO-kontekst er mest sandsynlig mod mål, der ikke er afgørende for en specifik operations succes, hvor konventionelle våben har svært ved at nå, og hvor der efterspørges reversible effekter. Cybereffekter bliver derfor hovedsageligt til irritationsmomenter, der eksisterer sideløbende med de konventionelle militære operationer: Konstante servernedbrud, miskommunikation, dræning af fjendens ressourcer. Disse effekter kan være en værdifuld støtte til de strategiske mål.

Washington Posts rapportering om *Operation GLOWING SYMPHONY* – US Cyber Commands "cyberbombning" af ISIS med henblik på at forstyrre organisationens kommunikation – understreger imidlertid, at selv denne brug af cyberangreb er politisk kontroversiel, da det ofte involverer nedtagning af servere i tredjeland, nogle gange hos allierede (Martelle, 2018). Foregår en operation i en NATO-kontekst, bliver forstyrrende cyberangreb endnu mere problematiske. Påvirkning af servere i tredjelande knytter an til den tredje udfordring for integrationen af cyberoperationer i NATO, kollisioner.

Kollisioner

At allierede koordinerer, så der ikke er tidsmæssigt sammenfald mellem for eksempel en luftoperation og en specialstyrkeoperation i det samme område, er en central aktivitet for enhver militær koalition. Cyberangreb vanskeliggør imidlertid muligheden for at undgå kollisioner. Udvikling af cybervåben og planlægning af cybereffekter er forbundet med et nødvendigt hemmelighedskræmmeri. Fortæller en cybermilitær enhed omverdenen, hvilke it-sårbarheder de udnytter, kan disse sårbarheder rettes, og cybereffekten kan ikke længere opnås (Gartzke, 2013). Store overlap mellem cyberangreb og cyberspionage gør endvidere, at de sårbarheder, der kan udnyttes i et angreb, også kan bruges til indhentning af vigtige efterretninger.

Grunden til, at NATO har indført en forespørgselsdreven og effektbaseret tilgang til cyberoperationer, er, at medlemsstaterne på tværs af alliancen ikke ønsker at dele deres viden om it-sårbarheder og "exploits". Denne tilbageholdenhed øger risikoen for, at den cybereffekt, en medlemsstat stiller til rådighed, har en negativ effekt på andre medlemsstaters indhentningsarbejde og måske endda for allieredes generelle netværkssikkerhed. Det skyldes, at de militære enheder, der påfører en cybereffekt i en operationel kontekst, sjældent interesserer sig for at bibeholde adgang til de påvirkede netværk, efter effekten er påført. Det handler om effekt, ikke spionage. Selvom teknikkerne ofte slører, hvilke sårbarheder der udnyttes, er det vanskeligt fuldstændig at sikre, at sårbarhederne ikke vil blive kendt af andre efter et cyberangreb. En medlemsstats brug af cyberangreb vil således ofte indeholde en nervøsitet

og afvejning af risikoen for, at andre interessenter (allierede, virksomheder, fjendtlige stater, kriminelle) kan forsøge at rette, forsvare sig imod eller selv udnytte samme sårbarheder og "exploits".

På denne baggrund kan der opstå en interessekonflikt mellem cyberindhentning, cyberforsvar og cyberangreb. US Cyber Commands ønske om at blive udskilt fra National Security Agency (NSA) er blandt andet et forsøg på at opnå en stærkere position, så de ikke altid bliver domineret af NSA's ønske om at indhente fremfor at påføre en "højlydt" militær cybereffekt (Bing, 2016). Den amerikanske regering har følte sig nødsaget til at oprette en intern procedure for at vurdere, hvorvidt de fejl og sårbarheder, som NSA og US Cyber Command identificerer, skal deles bredt med eksempelvis virksomheder, så de kan udbedres og den generelle it-sikkerhed højnes (Otto, 2017). Lignende procedurer eksisterer ikke i NATO, hvilket givetvis skyldes medlemsstaterne forskellige syn på, hvordan indhentning, forsvar og angreb bør vægtes i cyberspace. Det betyder, at hvis Danmark eksempelvis tilbyder at bidrage med en cybereffekt, kan en "højlydt" effekt meget vel føre til, at de it-sårbarheder, der bliver offentlige (og rettet), ikke længere kan bruges i fx de britiske eller amerikanske indhentningsoperationer, der udnytter samme sårbarheder (Jacobsen, 2017). Samtidig kan offentligt kendskab til sårbarheder i et it-system, fx i et kommercielt produkt, give kriminelle eller fjendtligt indstillede aktører mulighed for at udnytte de samme sårbarheder i andre sammenhænge mod private eller offentlige systemer, som ikke har nået at forsvare sig imod de teknikker, der nu er blevet offentligt kendt. WannaCry og NotPetya var eksempler på de negative effekter, der kan opstå, hvis en efterretningstjenestes it-sårbarheder bliver offentligt kendte (Jacobsen, 2018).

Det store overlap mellem indhentning og angreb – samt den manglende åbenhed omkring cybervåben, som dette overlap medfører – understreger, at der eksisterer et kollisionspotentiale både internt i en stat (mellem efterretningstjenesten og militæret) og allierede partnere imellem. Dette potentiale kan meget vel påvirke medlemsstaters villighed til at bidrage med cybereffekter til NATO.

NATOs igangværende arbejde med at overkomme de ovenstående udfordringer for integrationen af cybereffekter i den militære planlægning vidner imidlertid om, at NATO ikke for alvor har formået at tilpasse sig til cyberdomænet. NATO har ikke fundet en måde, hvorpå alliancen kan bevæge sig videre end det rendyrket militære fundament, som NATO i sin tid blev oprettet på. Cyberspace har vist sig specielt brugbart som et (efterretnings)redskab i de igangværende geopolitiske spændinger, der *ikke* har karakter af en væbnet konflikt. Men NATO har ikke på nuværende tidspunkt et sprog og en struktur, der muliggør en anerkendelse af en brug af cyberspace under tærsklen for væbnet konflikt. Det betyder, at NATO paradoksalt nok risikerer at bidrage til en underminering af den efterretningsnorm, der indtil nu har kendetegnet interaktionen i cyberspace – en efterretningsnorm, hvor statslige aktiviteter i fremmed netværk ikke bliver set som eskalerende. Denne pointe uddybes i det følgende.

Kultursammenstød

Overlappet mellem indhentning og angreb i cyberspace gør det vanskeligt at sende klare signaler til potentielle fjender, både vedrørende kapaciteter og intentioner, når man bevæger sig rundt i fremmed netværk: Er det en del af en begyndende NATO-operation? Er det almindelig rekognoscering? Er det cyberspionage? Eller er det aktivt forsvar? Vanskelighederne ved at besvare disse spørgsmål har skabt nervøsitet for eskalation i cyberspace.

Manglende eskalation kan meget vel skyldes, at de statslige efterretningstjenester – som indtil nu for de fleste staters vedkommende har domineret cyberspace – er omfattet af et specifikt sæt normer. Den etablerede efterretningsnorm knytter sig ikke i nævneværdig grad til militære begreber som eskalation og behovet for afskrækkelse. På efterretningstjenesternes kampplads har der altid været kontakt mellem fjendens spioner og egne spioner. Der er altid risici, og der arbejdes ofte i juridiske gråzoner, hvor distinktion ikke er et bærende juridisk princip, og hvor muligheder for at irritere og bedrage hinanden tages, når de opstår. Spionage og kontraspionage passer ikke til en tung operationel planlægning, som militære operationer i for eksempel NATO er karakteriseret ved. Efterretningsoperationer passer derimod glimrende til cyberdomænet. Såfremt stater omfavner cyberspace som et domæne, hvor efterretningsnormer dominerer, vil statslige efterretningstjenester kun tilbyde en bredere vifte af værktøjer, der ikke blot relaterer sig til militære operationer i en væbnet konflikt.

US Cyber Command ser ud til at vende sig i denne retning med deres 2018-vision, der netop har fokus på at agere hurtigt og tæt på fjenden i et domæne, hvor konstant kontakt ses som et grundlæggende princip (USCYBERCOM, 2018). Denne anerkendelse anses for nødvendig hvis USA skal gøre sig håb om ikke blot at levere militære cybereffekter, men også generelt at opnå overlegenhed i cyberspace og i højere grad udnytte domænets potentiale til bredere sikkerhedspolitiske mål. Selvom en sådan bredere brug af cyberspace er vanskelig at tilpasse en militæralliance som NATO, vil en anerkendelse af og åbning imod disse gavne NATOs forsøg på at signalere, at cyberspace tages seriøst. Hvis en sådan anerkendelse ikke finder sted, vil NATO, sit Cyber Operation Centre til trods, fortsat fremstå som værende et skridt bagefter og allerede forældet. Det sender ikke et stærkt signal til Rusland.

Anerkender vi forskellen på en militær- og en efterretningstænkning i cyberspace, bliver det også tydeligt, at eskalationsrisikoen i cyberspace hovedsageligt eksisterer, når den militærstrategiske kultur ikke har øje for, at en efterretningsnorm fortsat dominerer cyberspace. Ignorerer vi efterretningsnormen, er der større risiko for, at statslige militæranalytikere mistolker konstant kontakt i cyberspace som begyndende angreb. NATO risikerer samtidig at underminere normen om, at indtrængen i netværk og småirritationer ikke er eskalerende, hvis alliancen insisterer på at tilpasse cyberspace til en militær tænkning, som kun i begrænset grad lader sig gøre. I stedet for burde NATO forsøge at klargøre, hvordan efterretningstænkning og militærtænkning bør sameksistere.

Selvfølgelig er omfavnelse af efterretningsnormen, som USA's militære enhed US Cyber Command ansporer, ikke uproblematisk. Jason Healey (2018) peger eksempelvis på, at det kan føre til mere udnyttelse af it-sårbarheder, der ultimativt kan underminere USA's ønske om et åbent, frit og sikkert internet for alle. Men en diskussion af de forskellige normer, der allerede eksisterer i cyberspace, er vigtig både i USA og mellem allierede. For NATO, der ønsker at fremstå relevant i cyberspace, er det således naturligt at påtage sig opgaven og forsøge at forstå og adressere de "kulturforskelle", der er mellem en militær- og en efterretningstænkning blandt medlemslandene og internt i organisationen samt frem for alt hos de potentielle modstandere, man i øjeblikket konstant interagerer med i cyberspace.

Konklusion

Selvom cyberangreb ved første øjekast fremstår som en kapabilitet med stort potentiale, argumenterer denne artikel for, at offensive cyberspaceoperationer i en NATO-kontekst står over for en række udfordringer, som vanskeliggør integrationen af cybereffekter som militær støttefunktion i NATOs operationelle planlægning. I et komplekst og evigt foranderligt cyberspace forbliver det vanskeligt hurtigt at udvikle målrettede cybervåben, der yder direkte støtte til militære operationer, samt at forudse og verificere effekter, herunder også de mulige indirekte effekter mod civile, som OCO medfører. NATO bør således fokusere sit integrationsarbejde mod cybereffekter, så de hovedsageligt tænkes som irritationsmomenter, der ikke er har direkte strategisk effekt, men forstyrrer og dræner fjendens ressourcer sideløbende med de konventionelle militære operationer.

Ydermere indeholder OCO i NATO et forhøjet kollisionspotentiale, da "højlydte" cyberangreb afslører de sårbarheder og "exploits", som bliver brugt, hvilket både kan underminere allieredes cyberindhentning og kan øge risikoen for cyberangreb mod egne og allieredes utilstrækkeligt beskyttede private og offentlige netværk.

Sidst argumenterer artiklen for, at NATOs primære fokus på integration af cybereffekter som støttefunktion i militære operationer får alliancen til at fremstå forældet og ude af trit med den efterretningstænkning, som indtil nu har domineret cyberspace. Netop den militære tænkning er ikke gearet til at adressere den palet af sikkerhedspolitiske muligheder, som den herskende efterretningsnorm i cyberspace kan tilbyde. Ønsker NATO at sende et stærkt signal om, at alliancen mestrer domænet, kan de passende starte med internt at drøfte, hvordan man forholder sig til de aktiviteter, der ikke blot knytter sig til cybereffekter som støttefunktion i væbnet konflikt, som cyberspace også – og primært – tilbyder.

Om forfatteren

Jeppe Teglskov Jacobsen er adjunkt på Institut for Militær Teknologi, Forsvarsakademiet i Danmark.

Litteratur

Ali, R. (2017, 7. desember). NATO's little noticed but important new aggressive stance on cyber weapons. *Foreign Policy*. Hentet fra https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/

Bing, C. (2016, 30. august). U.S. cyber command director: We want 'loud,' offensive cyber tools. *Fedscoop*. Hentet fra https://www.fedscoop.com/us-cyber-command-offensive-cybersecurity-nsa-august-2016/

Bond, D. (2018, 4. desember). UK reveals Isis target of first military cyber attack. *Financial Times*. Hentet fra https://www.ft.com/content/cea9d608-3e3f-11e8-b7e0-52972418fec4

Buchanan, B. (2017). Nobody but us. The rise and fall of the golden age of signals intelligence. A Hoover Institute Essay. Aegis Series Paper No. 1708.

Carter, A. B. (2017). *A lasting defeat: The campaign to destroy ISIS*. Rapport fra Belfer Center for Science and International Affairs, Harvard Kennedy School. Hentet 17.10.2018 fra https://www.belfercenter.org/publication/lasting-defeat-campaign-destroy-isis

Gartzke, E. (2013). The myth of cyber war. *International Security, 38*(2), 41–73.

Healey, J. (2018, 1. april). Triggering the new forever war, in cyberspace. *The Cipher Brief*. Hentet fra https://www.thecipherbrief.com/triggering-new-forever-war-cyberspace

Jacobsen, J. T. (2017, 26. april). Europe is developing offensive cyber capabilities. The United States should pay attention. Hentet fra https://www.cfr.org/blog/europe-developing-offensive-cyber-capabilities-united-states-should-pay-attention

Jacobsen, J. T. (2018). En "digital Genèvekonvention" er ikke i Danmarks interesse. *Internasjonal Politikk*, *76*(2), 73–88.

Jacobsen, J. T. & Ringsmose, J. (2017). Cyber-bombing ISIS. Why disclose what is better kept secret? *Global Affairs*, *3*(2), 125–137.

Kello, L. (2017). *The virtual weapon and international order*. New Haven, CT og London: Yale University Press.

Libicki, M. (2016). *Cyberspace in war and peace*. Annapolis, MD: Naval Institute Press.

Lynn III, W. J. (2010). Defending a new domain: The Pentagon's cyberstrategy. *Foreign Affairs*, *89*(5), 97–108.

Martelle, M. (2018, 13. august). Joint task force ARES and operation GLOWING SYMPHONY: Cyber command's internet aar against ISIL. Hentet fra https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil

Moore, D. & Smeets, M. (2018). Why we are unconvinced NATO's cyber policy is more aggressive, and that's a good thing. Hentet fra https://www.cfr.org/blog/why-we-are-unconvinced-natos-cyber-policy-more-aggressive-and-thats-good-thing

Nakashima, E. & Ryan, M. (2016, 15. juli). U.S. military has launched a new digital war against the Islamic State. *The Washington Post*. Hentet fra https://www.washingtonpost.com/world/national-security/us-militarys-digital-war-against-the-islamic-state-is-off-to-a-slow-start/2016/07/15/76a3fe82-3da3-11e6-a66f-aa6c1883b6b1_story.html?utm_term=.a8a50fdbf7a5

Otto, G. (2017, 15. november). White House unveils process behind disclosing software vulnerabilities. *CyberScoop*. Hentet fra https://www.cyberscoop.com/vulnerabilities-equities-process-vep-charter-white-house-rob-joyce/

Sanger, D. E. (2018). *The perfect weapon. War, sabotage and fear in the cyber age*. New York, NY: Crown.

Smeets, M. (2017). A matter of time: On the transitory nature of cyber weapons. *Journal of Strategic Studies*, *41*(1–2), 6–32.

Smeets, M. (2018). The strategic promise of offensive cyber operations. *Strategic Studies Quarterly*, *12*(3), 90–113.

Stoltenberg, J. (2017, 8. november). Press conference. Hentet fra https://www.nato.int/cps/en/natohq/opinions_148417.htm

USCYBERCOM (2018). Achieve and maintain cyberspace superiority. Command vision for US cyber command. Hentet fra https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

Abstract in English

For the past decade, NATO has prioritised a strengthened cyber defence. However, at the end of 2017, the alliance made it clear that future operational planning will include the possibility of offensive cyberspace operations (OCO). The integration of OCO will happen through an effect-based model where the NATO commander – through the new NATO Cyber Operations Centre – requests a specific effect from member states. This article assesses the risks and opportunities of this model. It argues that even though OCO holds much potential for constant disruptions of an adversary's networks, OCO comes with several limitations and pitfalls when integrated through a request- and effect-based model. These include the risk of confliction and the difficulty of containing and assessing cyber effects. Such limitations weaken the ability to signal that NATO has the capacity to master this new domain. If NATO wants a to send a clear signal to adversaries, then the alliance needs to start discussing how it can utilise the possibilities below the threshold of armed conflict, which cyberspace primarily offers.

Keywords: cyber warfare · cyber attack · NATO operational planning · integration