Cyberdomænet i Ukrainekrigen
et udvidet kamprum med proxyaktører, eskalationsstiger og fjendemærkater

Jakobsson, André Ken; Nielsen, Liv

Published in:
Politica

DOI:
10.7146/politica.v55i1.135827

Publication date:
2023

Document version:
Forlagets udgivne version

Document license:
Ikke-specificeret

Citation for pulished version (APA):
Jakobsson, A. K., & Nielsen, L. (2023). Cyberdomænet i Ukrainekrigen: et udvidet kamprum med proxyaktører, eskalationsstiger og fjendemærkater. *Politica*, *55*(1), 60-73. https://doi.org/10.7146/politica.v55i1.135827

politica, 55. årg., nr. 1 2023, 60-73

André Ken Jakobsson og Liv Nielsen

Cyberdomænet i Ukrainekrigen: et udvidet kamprum med proxyaktører, eskalationsstiger og fjendemærkater

Ruslands invasion af Ukraine indvarsler en ny æra af konflikt mellem teknologisk avancerede stater, hvor det fysiske domænes konventionelle krig smelter sammen med krigsførelse i cyberdomænet. Ukrainekrigens unikke karakter er kendetegnet ved et udvidet kamprum, hvor den militære logik trænger ind i den civile sfære og skaber nye konfliktrelationer på tværs af offentlige og private skillelinjer. På denne baggrund udforsker artiklen, hvordan Ukrainekrigens udvikling informerer tre af cyberdomænets kernespørgsmål. Første spørgsmål handler om relationen mellem staten og ikkestatslige aktører med et fokus på brugen af cyberproxyer i krigen under inddragelse af Ukraines it-hær. Andet spørgsmål handler om afskrækkelse og eskalering af konflikten gennem cyberdomænets eskalationsstiger og -tærskler, der angår strategisk signalering og udvides med eskalationsgitteret. Tredje spørgsmål omhandler attribuering, der er en politisk højspændt affære, hvor aktøren bag cyberoperationer påsættes et fjendemærkat. Artiklen konkluderer på, hvordan de hidtidige erfaringer fra krigen kan informere brugen af cyberdomænet i fremtidens konflikter.

Nøgleord: Ukrainekrigen, cyberdomænet, it-hær, eskalationsgitter, attribuering

Et udvidet kamprum

Krigen i Ukraine og den rolle, som cyberdomænet spiller, er den hidtidige kulmination på et kamprum, der har udvidet sig voldsomt over de seneste årtier. En udvidelse, der er sket gennem en evolution i tænkningen om krigsvindende strategier, og som har bevæget sig i konceptuelle og doktrinære ryk. Disse ændringer i strategisk tænkning finder traditionelt sted ved at kombinere historiske erfaringer fra tidligere konflikter med nye organisatoriske principper og teknologiske fremskridt i militære kapaciteter. Eksempelvis var en dominerende tænkning under Anden Verdenskrig idéen om at drage fordel af luftdomænet baseret på erfaringerne fra det forholdsvis nye flyvevåben under Første Verdenskrig. Det førte ultimativt til idéen om tæppebombning af store byområder som en krigsvindende strategi. Og tusindvis af dræbte civile. Bombningerne af London og ødelæggelsen af Dresden står som eksempler på strategiens konsekvenser i praksis. Litteraturen om strategisk tænkning har siden født en række

konkurrerende koncepter, der ofte hviler på teknologiske landvindinger. Et gennemgående træk fra 1980'erne og frem er idéen om netværksbaseret krigsførelse. Registrerende sensorer til dataindsamling, computere til databehandling og koordinerende kommunikation mellem enheder og våbensystemer udstyret med præcisionsvåben er siden da blevet set som afgørende for succes. Den netværksbaserede amerikanske sejr i Golfkrigen mod Irak i starten af 90'erne blev af mange tolket som et skelsættende bevis herpå (Renz og Smith, 2016). Siden har avanceret teknologi, der bliver opfundet, produceret og driftet af private aktører, indtaget en voksende rolle i moderne krigsførelse, der særligt via cyberdomænet trænger ind i ellers traditionelt set civile rum.

Et nyt domæne

Da det amerikanske forsvarsministerium, Pentagon, i 2011 officielt anerkendte cyber som et operationelt kampdomæne på linje med de fire fysiske domæner land, vand, luft og rummet, skete det samtidig med en erkendelse af, at forsvaret af dette domæne i høj grad afhænger af offentligt-private partnerskaber (DoD, 2011). Cyberdomænets særlige natur, der består af både fysiske og virtuelle lag samt fungerer som civil kritisk infrastruktur, har således det militære kamprums ekspansion indbygget i sig. Krigsførelse i cyberdomænet og ekspansionen ind i den civile sfære bliver forsøgt fanget gennem den strategiske tænkning indeholdt i hybrid krigsførelse. Her er fokus ultimativt på en *whole-of-society* tilgang, der forsøger at bringe alle relevante instrumenter og angrebsvektorer i spil. Og heri består det hybride element, altså inddragelsen af især ikkemilitære instrumenter til at opnå strategisk succes. Det hybride angreb mod en anden stat vil derfor udgøres af "den synkroniserede brug af flere magtinstrumenter, der er skræddersyet til specifikke sårbarheder på tværs af hele spektret af samfundsfunktioner for at opnå synergieffekter" (Cullen og Reichborn-Kjennerud, 2017). Disse magtinstrumenter kan antage mange former såsom det militære (soldater, våben, doktrin), det økonomiske (lån, investeringer, eksport), det politiske (diplomati, infiltrering, korruption), informationsinstrumentet (mediestyring, påvirkningsoperationer, desinformation) og så videre. Cyberdomænets særegne natur gør, at det i varierende udstrækning løber på tværs af, samt faciliterer og samtidig udgør en svaghed for, alle disse instrumenter. Handlinger i det udvidede kamprum finder således i stigende grad sted i den svært gennemskuelige gråzone mellem krig og fred (Jakobsson, 2019).

Ukrainekrigens cyberdimension

Invasionen af Ukraine tog reelt set sin begyndelse i cyberdomænet, da russiske angreb mod den engelsksprogede avis, *Kyiv Post*, og Viasat (KA-SAT) satel-

litnetværket blev iværksat, en time før Ruslands konventionelle styrker rullede ind over de ukrainske grænser den 24. februar (Przetacznik og Tarpova, 2022: 2). Det amerikanske Viasat-netværk blev brugt af Ukraines militær til kommunikation med landets fronttropper, og cyberangrebet var dermed et centralt element i invasionsplanen (Miller, Scott og Bender, 2022). Ruslands praktisering af hybrid krigsførelse har tiltrukket sig opmærksomhed siden den ulovlige annektering af Krim i 2014, hvor de berygtede små grønne mænd i militæruniformer uden insignier overraskede Ukraines forsvar og resten af verden. Siden da har den russiske generalstabschef Gerasimovs analyse af vestlig krigsførelse i det 21. århundrede været et centralt tema i debatten om strategisk tænkning. Især fordi Gerasimov fra sin russiske synsvinkel ser Vesten udnytte et hybridt udvidet kamprum. Gerasimov ser derfor en ny tilstand, hvor krig ikke længere erklæres, og hvor "[s]elve "krigens regler" har ændret sig. Rollen, som ikke-militære midler spiller for at opnå politiske og strategiske mål, er vokset, og i mange tilfælde har de overskredet kraften af våbenmagt i deres effektivitet" (Gerasimov, 2016: 16). Vurderingen er derfor, at det ofte er mere effektivt at anvende andre magtinstrumenter end det militære. Og selvom Ruslands krig mod Ukraine naturligvis er domineret af konventionel krigsførelse og har et stort fokus på de sikkerhedspolitiske aspekter af Vestens våbenleverancer, så må betydningen af cyberdomænet ikke forsømmes. I det udvidede kamprum smelter den konventionelle krigs netværksbaserede krigsførelse sammen med cyberdomænets hybride muligheder. Det er opsigtsvækkende, at Storbritanniens Nationale Center for Cybersikkerhed (NCSC) vurderer, at krigens cyberdimension kan være uden historisk sidestykke. Direktøren, Lindy Cameron, pointerede syv måneder efter invasionens start, at "det, vi har set, er en meget betydelig konflikt i cyberspace – sandsynligvis den mest vedvarende og intensive cyberkampagne nogensinde" (Palmer, 2022).

Den vurdering finder ammunition hos amerikanske Microsoft, der tager del i det ukrainske cyberforsvar. Microsoft har i den rolle fra december 2021 til marts 2022 observeret hundredvis af cyberhændelser fra russiske statsaffilierede grupper rettet mod Ukraine, hvoraf en del er destruktive angreb samt bredspektrede efterretningsaktiviteter. I tilgift har Microsoft i løbet af krigens første seks uger observeret tydelige sammenhænge mellem høj kinetisk aktivitet og høj cyberaktivitet målrettet de samme sektorer eller geografiske steder. Rusland har altså som forventet forfulgt en synkronisering mellem militære aktiviteter i de traditionelle domæner og cyberdomænet som led i krigen (Microsoft, 2022: 9–10). En synkronisering, som Rusland dog har haft svært ved at levere de ønskede effekter af og derfor den 10. og 11. oktober 2022 satte de første store missilangreb mod kritisk ukrainsk energiinfrastruktur ind – og ramte cirka 30

pct. af denne med store udfald og restriktioner til følge (Voitovych og Hardie, 2022).

Til trods for den russiske cybermagts mange angreb, så har den hidtil rapporterede destruktive effekt altså været relativt begrænset, hvilket understreger værdien af et velorganiseret cyberforsvar samt den koordinerede indsats fra store vestlige firmaer. Men dette hidtidige udfald kan også sætte spørgsmålstegn ved nytten af offensive cyberkapabiliteter (Lewis, 2022). Her er det vigtigt at huske på, at cyberdimensionen af konventionel krig også dækker spionage, forberedelse af kampplads, angreb på udenlandske aktører samt påvirkningsoperationer i informationsrummet. Cyberdomænet trives i det udvidede kamprum, hvor det menneskelige sind også er genstand for krigsførelse. Russiske påvirkningsaktiviteter gennem eksempelvis *hack-and-leak* af fortrolig eller falsk information, der fører til et sammenbrud af transatlantisk solidaritet med Ukraine og dermed underminering af våbenleverancer, vil potentielt være et stærkere våben mod det ukrainske militær end nok så mange russiske krydsermissiler.

Proxyaktører

Det første af cyberdomænets tre kernespørgsmål angår, hvem der er domænets centrale aktører. Et entydigt svar herpå bliver kompliceret af domænets demokratisering, der karakteriseres af meget lave *entry-costs* i modsætning til krigsførelsens andre domæner, hvor adgangen oftest kræver højt specialiseret uddannelse og træning samt dyrt materiel, der er underlagt strenge restriktioner for anskaffelse og brug. Cyberdomænets centrale aktører skal findes i et bredt spektrum fra leverandører og programmører over efterretningstjenester og militærenheder til organiserede cyberkriminelle og frivillige hacktivister. Ruslands krig mod Ukraine kan derfor fungere som en linse, hvorigennem spektret relativt set kan indsnævres ved at fokusere på det rum, der udstrækkes mellem statslige og ikke-statslige aktører, der aktivt deltager i krigens cyberoperationer. For en mere dybdegående analyse af især private markedsaktørers rolle og status henvises til Karen Lund Pedersens artikel i dette temanummer. For nuværende rettes fokus her mod en særlig aktør.

Ukraines it-hær

Fra den ukrainske side blev ét svar på invasionen den hastigt etablerede gruppe IT army of Ukraine. Gruppens eksistens illustrerer demokratiseringen af cyberdomænet gennem *crowd-sourced* deltagelse af frivillige. It-hæren bliver dermed en case, der gør det muligt at udforske en stats bevæggrunde for mobiliseringen af denne type aktør, samt hvilke udfordringer der kendetegner denne cyberproxyrelation. Et analytisk rammeværktøj må centreres om brugen af proxyaktører

i cyberdomænet, der i en eller anden udstrækning arbejder for samt forfølger statens målsætninger. Til brug herfor identificerer Tim Maurer to typer *shaping*-praksisser, hvor en stat enten forsøger at forme andre staters relation til deres proxyer eller forsøger at forme statens eget forhold til statens egne cyberproxyer (Maurer, 2018: 138). Sidstnævnte er af særlig interesse for det statusspil om anerkendelse og tilknytning til eller afvisning fra staten, som cyberproxyer i denne krig indgår i. Relationerne mellem en stat og cyberproxyer falder i tre overordnede kategorier, der handler om delegation, orkestrering og sanktionering. Hvor de to første kategorier beskriver statens relation til aktøren forud for og under en proxyaktørs offensive cyberoperationer, beskriver den sidste kategori statens relation til proxyer, *efter* en given operation har fundet sted (Maurer, 2018: 125–128). Hver kategori skal betragtes som et kontinuum, inden for hvilket relationen styrkes eller svækkes, alt efter graden af statens indflydelse samt kontrol over proxyens handlinger (Maurer, 2018: 125).

I de tidligste faser af cyberkonflikten mellem Rusland og Ukraine efter den russiske hybride besættelse af Krim i 2014, formåede Ukraine, mod forventning, ikke i tilstrækkelig grad at mobilisere og udnytte landets offensive cyberkapabiliteter i form af frivillige samt mere organiserede proxyaktører (Maurer, 2015: 88). En statslig strategi og kapacitet var fraværende. I kølvandet på Ruslands invasion i 2022 er der i midlertidig opstået en ny situation, kendetegnet ved en nærmest eksplosiv mobilisering af aktører, der flokkes om at understøtte Ukraines defensive og offensive cyberoperationer. Mobiliseringen af Ukraines it-hær opstod delvist på baggrund af et tweet fra den Ukrainske vicepremiereminister, Mykhailo Fedorov, den 26. februar 2022. I tweetet bekendtgjorde Fedorov, at Ukraine søgte frivillige til en it-hær, og at oplysninger om aktuelle mål for offensive operationer ville blive delt på chattjenesten Telegram (Soesanto, 2022: 6). Trods massiv mediebevågenhed rettet mod it-hæren er det endnu uklart, *hvem* der udgør it-hæren, samt hvilken relation staten konkret har til gruppen. Disse udestående svar er vigtige, da relationen rejser udfordringer for grundlæggende forhold som kontrol, autoritet og statsligt ansvar. Foreløbige oplysninger indikerer, at it-hæren overordnet kan inddeles i to grupperinger; en "global" it-hær bestående af frivillige samt en intern "kerne" sammensat af højtkvalificerede it-specialister (Delcker, 2022; Soesanto, 2022).

Den "globale" it-hær

Den "globale" it-hær er sammensat af en række vidt forskellige aktører, herunder enkelte individer, løsere grupperinger som hackerkollektivet *Anonymous* eller dele heraf (Soesanto, 2022: 25) samt en række ukrainske techvirksomheder (Cerulus, 2022). It-hærens relation til den ukrainske stat kan anskues ud fra

statens *orkestrering* af it-hærens aktiviteter. For eksempel beskriver Ukraines viceminister for digital omstilling, Oleksandr Bornyakov, hvordan hans team udsender specifikke instrukser til it-hæren via Telegram (Labott, 2022). Relationen fremstår ikke som præget af kontrol, men bygger i stedet på antagelsen om, at stat og it-hær deler nogle fælles mål, der danner grundlag for samarbejdet. For eksempel beskriver en dansk frivillig, hvordan russiske krigsforbrydelser har motiveret ham til dagligt at iværksætte koordinerede DDoS angreb (Delcker, 2022). Ligeledes beskriver CEO for cybersikkerhedsvirksomheden *Hackem,* Dmytro Budorin, hvordan han i fællesskabet med øvrige aktører oplever, at det ukrainske tech-samfund er "forenet som aldrig før" (Cerulus, 2022). It-hærens diversificerede organisation gør den ifølge viceminister Bornyakov til et magtfuldt redskab for staten og han beskriver, hvordan gruppen i sin natur er svær at forstyrre og nær umulig at nedbryde (Labott, 2022).

"Kernen" af Ukraines it-hær

Hvor den "globale" it-hær agerer på baggrund af informationer, der deles på Telegram, indikerer analyser af en række cyberoperationer og efterfølgende deling af informationer, at der ud over den "globale" it-hær eksisterer en "intern" gruppering, sammensat af højtspecialiserede aktører, der lader til at operere i tæt samarbejde med ukrainske forsvars- og efterretningsmyndigheder (Soesanto, 2022: 20). Techentreprenøren Yegor Aushev beskriver, hvordan han, efter forespørgsel fra staten, har iværksat en mobilisering af højtuddannede og verificerede it-specialister, der bidrager til statens indsatser (Delcker, 2022). Samarbejdet er endnu ikke bekræftet af de ukrainske myndigheder, men Bornyakov fremhæver eksempelvis, at staten gennem de seneste år har investeret betydelige ressourcer i at udvikle landets techindustri. Resultatet er, at Ukraine i dag kan trække på betydelige kapaciteter fra sektoren, der dels kan fungere som substitut for en begrænset offensiv cyberkapacitet i militæret, dels kan bidrage til beskyttelsen af landets kritiske infrastruktur (Voo, Hemani og Cassidy, 2022: 12).

Specifikke krav til aktørernes kompetencer og verificering indikerer, at relationen bygger på en grad af kontrol, hvor staten *delegerer* autoritet til en organiseret cyberproxy, men bevarer en grad af indflydelse, navnlig ved at deltage i planlægning og supervision (Maurer, 2015: 127). Alligevel viser udtalelser fra medlemmer af "kernen", at proxyaktørerne grundlæggende agerer ud fra en idé om, at de deler et fælles mål med staten. Dette indikerer, at relationen bevæger sig i et spektrum mellem *orkestrering,* hvor staten udsteder specifikke instruktioner på baggrund af fælles interesser, og *delegation,* hvor staten fortsat bevarer en tilstrækkelig grad af kontrol over aktørens handlinger. Dette er klassisk brug

af det udvidede kamprum gennem cyberproxyer, der friholder staten til kunne påberåbe sig plausibel benægtelse og dermed fraskrive sig ansvaret.

Eskalationsstiger

Artiklens andet kernespørgsmål angår, hvordan stater håndterer afskrækkelse og eskalation i cyberdomænet. I 2014 erklærede NATO, at cyberangreb kan udløse et artikel 5-svar på linje med konventionelle angreb mod en medlemsstat (Prucková, 2022). Dermed er grundudfordringen på overfladen ens for de traditionelle domæner og cyberdomænet, hvor afskrækkelse og eskalation hviler på, hvilke defensive eller offensive handlinger aktørerne foretager sig, hvilke signaler de ønsker at sende, samt hvordan handlinger og signaler bliver modtaget. Strategisk signalering er derfor et bærende element. Og i parallel med hvordan aktører, der fører hybrid krigsførelse generelt sigter efter at holde deres handlinger under tærsklen for, hvornår den angrebne part kan eller vil svare igen eller eskalere, så efterstræber operationer i cyberdomænet som hovedregel det samme. Forskellen fra de fire traditionelle domæner er imidlertid, at mens litteraturen om strategisk tænkning har udviklet avancerede strategier for både konventionel og nuklear afskrækkelse, så mangler der en fælles anerkendelse af, hvordan eskalationsstigerne i cyberdomænet virker (Shea, 2017: 27). Besvarer man fx proportionelt den potentielle skade, en afværget offensiv cyberoperation kunne udøve, eller besvarer man den faktiske skadevirkning? Og hvordan udmåler man et proportionelt svar – måske endda mod en aktør, der ikke vedkender sig angrebet? Disse er kun de mest fundamentale spørgsmål, hvis svar tilsammen er afgørende for, hvor langt en aktør bevæger sig op eller ned ad cyberdomænets eskalationsstige. Frygten er, naturligvis, at den ene eskalerende handling medfører den næste op ad trinene.

Et eskalationsgitter

Eskalationsstigen er universalt brugt i strategisk tænkning som en metafor for udviklingen i en konflikts intensitet. Men i cyberdomænets udvidede kamprum vil stigen ofte repræsentere et problematisk endimensionelt analyseapparat, da fjendtlige handlinger i det udvidede kamprum netop søger tvetydigheden som en strategi for risikohåndtering. Stigen er, i kontrast hertil, begrænset af kun at have et vertikalt eskalationsrum til rådighed. Den horisontale eskalation, hvor fjendtlige handlinger udvides gennem brug af nye magtinstrumenter eller nye angrebsflader, kan være umulige at indplacere på stigens vertikale trappetrin. Eksempler fra offensive cyberoperationer i Ukrainekrigen kan belyse denne problemstilling. Ruslands historisk set enormt effektive offensive cyberoperationer udført af Sandworm-gruppen mod Ukraines energiforsyning i de

kolde decembermåneder i 2015 og 2016 resulterede i begge tilfælde i blackouts for tusindvis af ukrainske borgere (Park og Walstrom, 2017). Og som led i Ruslands invasion i 2022, har Sandworm, der antages at være tilknyttet det russiske militær, udført lignende operationer mod Ukraine for at udløse et tredje blackout. Denne gang var angrebene dog langtfra lige så succesfulde, og effekten blev minimeret. Men angrebet var både velforberedt og sofistikeret og kunne potentielt have lukket for strømmen til 2 mio. mennesker (Conger, 2022). I alle tre tilfælde kunne strømmen reetableres, og ingen har officielt taget ejerskab for operationerne, men uanset denne tvetydighed er der tale om alvorlige suverænitetskrænkelser. Et modsvar på invasionen blev fra den ukrainske side den ovenfor nævnte ukrainske it-hær, der i de første dage af invasionen udarbejdede en offentlig liste på 31 russiske mål, der siden er vokset over tid. De tidligste mål inkluderede russiske myndigheder, tre banker og store infrastrukturvirksomheder samt søgemaskinen og mailudbyderen Yandex (Abrams, 2022). Også i Ukraines tilfælde er konsekvenserne af disse cyberoperationer svære at vurdere, og vigtigst af alt: Hvor på eskalationsstigen skal de to parters handlinger indplaceres? Usikkerheder, der forøges af en mængde aktører, der kan handle på egen hånden uden for statens magt. Disse eksempler peger på behovet for et mere avanceret analytisk værktøj end eskalationsstigen. Her kommer eskalationsgitteret til sin ret. Gitteret som en tredimensionel struktur (tænk på skelettet til et højhus) gør det muligt at planlægge egne samt forstå modstanderens træk som horisontale bevægelser – og dermed ikke kun som den voldsommere eskalation, næste stigetrin ville være udtryk for.

Gittermetaforen hjælper også til en nuanceret forståelse af cyberdomænets forskellige operationstyper. En trusselsanalyse, der benytter eskalationsgitteret, kan i højere grad skelne mellem de tre overordnede Computer Network Operations: forsvar (defense), efterretning (exploitation) og angreb (attack) (DoD, 2018: 40-41). Forsvar handler om at detektere og neutralisere specifikke trusler, efterretning forsøger at indhente data eller forberede fremtidige operationer, og angreb handler om at skabe nægtelseseffekter såsom nedbrydning eller ødelæggelse af systemer eller fysiske elementer. Der kan være stor forskel i trusselsniveauet fra disse operationer, hvilket illustreres af udviklingen i cyberoperationer rettet mod den danske energisektor. I 2018 advarede både Forsvarets Efterretningstjeneste og energibranchen om, at sektoren var udsat for hacking, der på daværende tidspunkt blev set som spionageaktiviteter og dermed faldt i efterretningskategorien. Dog stadig i den alvorlige ende, da USA advarede om en koordineret kampagne, der skulle lamme den europæiske energiforsyning før en mulig konflikt (Kongstad og Seidelin, 2018). Siden den russiske invasion begyndte, har den danske energisektor oplevet et væsentligt forvær-

ret trusselsniveau, hvor alene angreb mod fjernvarmeforsyningen er femdoblet, særligt målrettet den operationelle driftsteknologi. Alle tegn peger på russiske aktører (Eriksen, 2022). Den kronologiske udvikling i cyberoperationer mod dansk energiforsyning har således udviklet sig fra en horisontal eskalering af efterretningstypen til vertikal eskalering af angrebstypen. Yderligere træk har fundet sted gennem det udvidede kamprums hybride metoder, hvor sabotagen af gasrørsledningerne Nord Stream 1 og 2 tæt på Bornholm i september 2022 formodentlig er del af samme koordinerede kampagne (Mortensen, 2022), der i kombination med truslen fra uidentificerede droneoverflyvninger ved skandinaviske olie- og gasfelter skal udnytte danske og europæiske energisårbarheder (Bugge, 2022).

Attribuering

Cyberdomænets tredje centrale spørgsmål angår, hvordan stater håndterer attribuering af cyberoperationer, altså hvordan man tilskriver ansvaret til en bestemt aktør. Dette kan foregå på forskellige niveauer internt i statens efterretningsmyndigheder, der rapporterer til det politiske niveau baseret på hændelsens karakter. Spørgsmålet om at foretage en offentlig attribuering bliver imidlertid politisk følsomt, da en sådan åben tilskrivelse bevæger sig ind i eskalationsgitterets dynamikker. Derfor bliver cyberoperationer, uanset om typen er forsvar, efterretning eller angreb, i overvejende grad ikke meddelt offentligheden og slet ikke attribueret. Denne stiltiende accept skyldes også, at både offentlige og private aktører er tilbageholdende med at offentliggøre succesfulde angreb mod deres systemer af frygt for at miste legitimitet eller kunder. Der er således overbevisende argumenter for ikke at foretage en offentlig attribuering, der ultimativt placerer et fjendemærkat på (proxy)aktøren og den eventuelt bagvedliggende stat.

Det udvidede kamprums tvetydighed vanskeliggør også efterforskningen, da man ofte er nødt til at arbejde med sandsynligheder og motiver, når de konkrete beviser ikke er tilstrækkelige. En teknisk attribuering vil eksempelvis tage udgangspunkt i, hvilke sårbarheder udnyttes, og hvilke offensive værktøjer der bliver brugt, da disse ofte kan knyttes til bestemte aktører som et teknisk fingeraftryk. Nogle af de seneste års største cyberoperationer understreger dog kompleksiteten heri. EternalBlue, et værktøj udviklet af den amerikanske efterretningstjeneste, National Security Agency (NSA), til at udnytte sårbarheder i Windows styresystemet, blev i 2017 lækket af Shadow Brokers gruppen. Det førte til brugen af EternalBlue i blandt andet den globale WannaCry ransomware operation få måneder efter og igen i det destruktive NotPetya angreb rettet mod Ukraine, men med global spredning til Mærsk-koncernen og det

britiske sygehusvæsen (Hern, 2017). Der er således mange bevægelige dele i spil, men alligevel resulterede disse operationer i offentlig stat-til-stat attribuering, hvor en række lande med Amerika og Storbritannien i spidsen tilskrev WannaCry til Nordkorea og, med Danmark som medunderskriver, tilskrev NotPetya til Rusland (Tsagourias og Farrell, 2020: 4). Og det er ikke kun brugen af andres værktøjer, der komplicerer attribuering, men også brugen af andre staters operative infrastruktur som eksempelvis den russiske gruppe Turla, der ifølge Storbritannien infiltrerede den iranske gruppe APT34 og udførte cyberoperationer herigennem hovedsageligt i Mellemøsten. Med den overlagte risiko for at disse fejlagtigt blev tilskrevet Iran i stedet for Rusland (Stubss og Bing, 2019). Selv med disse udfordringer in mente bliver visse offensive cyberoperationer alligevel offentligt attribueret, og dermed består det centrale spørgsmål: Hvordan kan stater håndtere denne beslutning?

Et offentligt attribueringsframework

Ruslands konventionelle krigshandlinger mod Ukraine har i voldsom grad øget opmærksomheden på cyberdomænet og i forlængelse heraf øget villigheden fra både stater og private firmaer til offentligt at attribuere russiske cyberoperationer. Og ifølge Florian J. Egloff og Max Smeets' *Public Attribution Framework* gør beslutningstagere klogt i at anskue spørgsmålet gennem en "strategisk, koordineret pragmatisme", hvor man holder sig målet med attribuering for øje og samtidig vurderer potentielle negative konsekvenser fra sag til sag (Egloff og Smeets, 2021: 2). Det strategiske mål med offentlig attribuering handler fundamentalt om at afskrække yderligere cyberoperationer ved fx at delegitimere gennem *naming-and-shaming*, true med straffeaktioner, sætte normer for adfærd i cyberdomænet, opbygge et fælles trusselbillede eller alternativt at retfærdiggøre nationale efterretningsmyndigheders ressourcetræk (Egloff og Smeets, 2021: 7-8). Frameworkets fire kategorier guider og vurderer, om beslutningen fremmer eller begrænser muligheden for at forfølge det strategiske mål. Disse hjælper også den udenforstående iagttager. Første kategori, efterretning, vurderer styrken af beviser for den mulige attribuering, og om målet helliger eventuel afsløring af metoder og viden. Anden kategori, hændelsens alvorlighed, vurderer cyberoperationens type og formål samt aktørens motivationer og identitet, der kan være afgørende for, hvilket mål det er muligt at forfølge gennem offentlig attribuering, da nogle aktører kan være svære at udskamme eller straffe. Tredje kategori, geopolitisk kontekst, vurderer tidsmæssige aspekter samt relationen til angriberen, da offentlig attribuering af en allieret stats spionage kan være kontraproduktivt, mens det kan forholde sig omvendt med en fjendtlig stat. Fjerde kategori, handlingsrummet efter attribuering, vurderer de ressourcer,

der er nødvendige for at følge op på tilskrivningen samt de negative effekter, der kan opstå, såsom øget interesse fra fjendtlige aktører rettet mod et strategisk vigtigt aktiv (Egloff and Smeets, 2021: 8-16). Det helt fundamentale spørgsmål, som både private og offentlige aktører skal forholde sig struktureret til, er: Vil forfølgelse af det strategiske mål overskride omkostningerne ved den form for attribuering, der er mulig? Ukrainekrigen og erfaringerne herfra har allerede ændret kalkulerne for frameworkets fire kategorier og kommer utvivlsomt til at være normskabende fremadrettet, hvor Rusland i Vesten utvetydigt opfattes som en fjendtlig cybermagt.

Konklusion: Ukrainekrigen kræver handling

Svar på cyberdomænets tre kernespørgsmål om aktører, eskalation og attribuering har kun fået yderligere relevans i lyset af Ruslands krig mod Ukraine. En intensiverende brug af det udvidede kamprum kræver hurtig læring og tilpasning, der kan sikre større afskrækkelsespotentiale. Analysen peger således i retning af tre svar. For det første må især vestlige stater fundamentalt gentænke forholdet til private cyberaktører, herunder cyberproxyer. Ukraines succesfulde inddragelse af ikkestatslige aktører samt det internationale samarbejde med vestlige techgiganter understreger, at cyberforsvar er både muligt og effektivt. Den strategiske tænkning om netværksbaseret krigsførelse udvider derigennem sin logik til den civile sfære, men introducerer også udfordrende relationer, der kræver nye styringsmekanismer. For det andet må den strategiske forståelse af eskalation gennem cyberdomænet nuanceres yderligere i takt med, at forskellen mellem operationstyper sløres, mens angrebsvektorer og aktivitetsniveauer øges. Eskalationsstigen som analytisk værktøj kan derfor med fordel udbygges til eskalationsgitteret, der bedre kan håndtere den horisontale eskalation, hvor flere og forskelligartede (cyber)magtinstrumenter tages i brug og synkroniseres. For det tredje tyder meget på, at offentlig attribuering af cyberoperationer vil spille en større rolle i at informere staternes egne cyberforsvar gennem opmærksomhed om trusselsniveauet, men også som forsøg på at samle internationale alliancer og søge normdannelse for cyberdomænet. Derfor kræver offentlig tilskrivning af cyberoperationer fremadrettet endnu større strategiske overvejelser og bør altid afklare attribueringens strategiske mål samt inddrage strukturerede vurderinger af effekt og opfyldelse. Det tilnærmelsesvise kollektive sikkerhedssvar fra Vesten i form af hjælp til Ukraine kan danne præcedens for cyberdomænet på tværs af en lang række aktører, der med sikkerhedsdimensionen i centrum må genoverveje samarbejdsrelationer. Både internt i staten og globalt.

Litteratur

Abrams, Lawrence (2022). Ukraine recruits "IT army" to hack Russian entities, lists 31 targets. *BleepingComputer*, 26. februar. https://www.bleepingcomputer.com/news/security/ukraine-recruits-it-army-to-hack-russian-entities-lists-31-targets/

Bugge, Mathilde (2022). Eksperter kalder mystisk droneaktivitet "påfaldende" efter Nord Stream-eksplosion. DR, 30. september 2022 https://www.dr.dk/nyheder/indland/eksperter-kalder-mystisk-droneaktivitet-paafaldende-efter-nord-stream-eksplosion

Cerulus, Laurens (2022). Kyiv's hackers seize their wartime moment. *POLITICO*, 10. marts. https://www.politico.eu/article/kyiv-cyber-firm-state-backed-hacking-group/

Conger, Kate (2022). Ukraine says it thwarted a sophisticated Russian cyberattack on its power grid. *The New York Times*, 12. april. https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html

Cullen, Patrick J. og Erik Reichborn-Kjennerud (2017). MCDC countering hybrid warfare project: Understanding hybrid warfare. *Multinational Capability Development Campaign*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Delcker, Janosch (2022). Ukraine's IT army: Who are the cyber guerrillas hacking Russia? *Deutsche Welle*. https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527

DoD (2011). *Department of Defense strategy for operating in cyberspace*. United States Department of Defense. https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf

DoD (2018). *Joint publication 3-12: Cyberspace operations 9 June 2018*. United States Department of Defense. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Egloff, Florian J. og Max Smeets (2021). Publicly attributing cyber attacks: a framework. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2021.1895117

Eriksen, Freja Celine (2022). Cyberangreb mod fjernvarmen er femdoblet siden Ukraine-invasion. *Energiwatch.dk*, 24. marts. https://energiwatch.dk/Energinyt/Politik___Markeder/article13851044.ece

Gerasimov, Valery (2016). The value of science is in the foresight. *Military Review*, January-February. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

Hern, Alex (2017). WannaCry, Petya, NotPetya: How ransomware hit the big time in 2017. *The Guardian*, 30. december. https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

Jakobsson, André Ken (2019). *Når Hydra angriber: Hybrid afskrækkelse i gråzonen mellem krig og fred*. Center for Militære Studier, Københavns Universitet. https://cms.

polsci.ku.dk/publikationer/naar-hydra-angriber-hybrid-afskraekkelse-i-graazonen-mellem-krig-og-fred/download-cms-rapport/CMS_Rapport_2019__2_-_N_r_hydra_angriber_-_hybrid_afskr_kkelse_i_gr_zonen_mellem_krig_og_fred.pdf.

Kongstad, Jesper og Matias Seidelin (2018). Hvad lavede hackerne i det danske elnet? Ifølge USA ønsker Rusland at lamme den europæiske energiforsyning før en mulig konflikt. *Jyllands-Posten,* 17. juli. https://jyllands-posten.dk/indland/ECE10705311/da-hackerne-brugte-en-schweizerkniv-mod-det-danske-elnet/

Labott, Elise (2022). "We are the first in the world to introduce this new warfare": Ukraine's digital battle against Russia. *POLITICO,* 3. august. https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880

Lewis, James A. (2022) Cyber war and Ukraine. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash

Maurer, Tim (2015). Cyber proxies and the crisis in Ukraine, pp. 79-86 i Kenneth Geers (red.), *Cyber war in perspective: Russian aggression against Ukraine*. Tallinn, Estonia: CCDCOE, NATO Cooperative Cyber Defence Centre of Excellence.

Maurer, Tim (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge: Cambridge University Press.

Microsoft (2022). *Special report Ukraine: An overview of Russia's cyberattack activity in Ukraine*. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Miller, Christopher, Mark Scott og Bryan Bender (2022) UkraineX: How Elon Musk's space satellites changed the war on the ground. *POLITICO,* 8. juni. https://www.politico.eu/article/elon-musk-ukraine-starlink/

Mortensen, Mikkel Walentin (2022) Ekspert advarer: Stor risiko for angreb mod energisektoren. TV 2 Nyhederne, 26. oktober. https://nyheder.tv2.dk/business/2022-10-24-ekspert-advarer-stor-risiko-for-angreb-mod-energisektoren

Palmer, Danny (2022) Russian hackers' lack of success against Ukraine shows that strong cyber defences work, says cybersecurity chief. *ZDNET*, 29. september. https://www.zdnet.com/article/russian-hackers-lack-of-success-against-ukraine-shows-strong-cyber-defences-work-says-cybersecurity-chief/

Park, Donghui og Michael Walstrom (2017). Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks. The Henry M. Jackson School of International Studies, 11. oktober. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

Prucková, Michaela (2022). *Cyber attacks and Article 5: A note on a blurry but consistent position of NATO*. The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/library/publications/cyber-attacks-and-article-5-a-note-on-a-blurry-but-consistent-position-of-nato/

Przetacznik, Jakub og Simona Tarpova (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Renz, Bettina og Hanna Smith (2016). Russia and hybrid warfare: Going beyond the label. *Aleksanteri Papers*. https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf

Shea, Jamie (2017). How is NATO meeting the challenge of cyberspace? *PRISM* 7 (2): 11. https://cco.ndu.edu/PRISM-7-2/Article/1401835/how-is-nato-meeting-the-challenge-of-cyberspace/

Soesanto, Stefan (2022). *The IT army of Ukraine: Structure, tasking, and ecosystem*. Center for Security Studies, ETH Zürich. http://hdl.handle.net/20.500.11850/552293

Stubss, Jack og Christopher Bing (2019). Hacking the hackers: Russian group hijacked Iranian spying operation, officials say. *Reuters*, 21. oktober. https://www.reuters.com/article/uk-russia-cyber-idUKKBN1X00AX

Tsagourias, Nicholas og Michael Farrell (2020). Cyber attribution: Technical and legal approaches and challenges. *European Journal of International Law* 31 (3): 941–967. https://doi.org/10.1093/ejil/chaa057

Voitovych, Olga og Alex Hardie (2022). Ukrainian PM calls for 25% cut in electricity use during peak hours to avoid outages. *CNN*, 12. oktober. https://www.cnn.com/2022/10/12/europe/ukraine-electricity-outages-intl/index.html

Voo, Julia, Irfan Hemani, og Daniel Cassidy (2022). *National cyber power index 2022*. BELFER Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf