TEMAREDAKTØRENS FORORD

Cybersikkerhed i perspektiv

TOBIAS LIEBETRAU
post.doc., Center for Militære Studier, Institut for Statskundskab, Københavns Universitet,
tobias.liebetrau@ifs.ku.dk

Digitaliseringen er et janushoved

Verden over gennemsyres samfund og hverdagsliv af informations- og kommunikationsteknologi. Den digitale udrulning og indrullering er normalt akkompagneret af løfter om øget vækst, velstand og velfærd. Den forjættende digitalisering går imidlertid hånd i hånd med nye risici og usikkerheder.

Det skyldes, at anvendelsen af informations- og kommunikationsteknologi er kompleks, dynamisk og diffus. Grænserne mellem det digitale og det fysiske opblødes, udviskes og forvitrer. Geografisk og tidslig bundethed omkalfatres. Desuden er størstedelen af den digitale infrastruktur privat udviklet, ejet og drevet. Ydermere indeholder den software, der understøtter digitaliseringen sårbarheder, som fjendtlige sindede aktører kan finde og udnytte. Det kan medføre, at en angriber overtager kontrollen med sårbare systemer, manipulerer data eller sætter softwaren ude af stand til at fungere efter hensigten. Derudover kan den fremtidige brug og videreudvikling af eksisterende digitale teknologier ikke sættes på formel, men forbliver åben og uforudsigelig.

> Introduktionen af nye digitale teknologier er på den ene side ledsaget af politiske, sociale og økonomiske muligheder og på den anden af nye usikkerheder og sårbarheder

Digitaliseringen af vores samfund og vores liv er derfor et janushovedet fænomen. Introduktionen af nye digitale teknologier er på den ene side ledsaget af politiske, sociale og økonomiske muligheder og på den anden af nye usikkerheder og sårbarheder. Derfor bliver cybertruslen i dag regnet for en af de – hvis ikke den – absolut største sikkerhedstrussel. Det gælder i et nationalt sikkerhedspolitisk perspektiv såvel som i erhvervslivet.

Det er karakteristisk for cybertruslen, at den både udvider og sammenkæder de sikkerhedspolitiske risici og antallet af potentielle mål – fra stater over private virksomheder til individuelle brugere. Cybertruslen og håndteringen af den udfordrer en række af de traditionelle skillelinjer, som vi normalt bruger til at indrette vores samfund og sikkerhedspolitiske tænkning efter, herunder skellene mellem nationalt og internationalt, offentligt og privat, politisk og teknologisk samt krig og fred.

Den uforudsigelighed og usikkerhed, der er forbundet med den fortsatte udvikling i og brug af informations- og kommunikationsteknologi, samt den

private sektors mellemkomst gør traditionel sikkerhedspolitisk styring, organisering og lovgivning vanskelig. Cybertruslen udfordrer dermed statens historiske monopol på at bedrive sikkerhedspolitik. Ydermere forplumrer den statslige håndtering af cybertruslen i stadigt stigende grad det klassiske skel mellem national sikkerhedshåndtering og kriminalitetsbekæmpelse, mellem intrastatslige politiopgaver og interstatslig forsvarsopgaver og mellem offentligt sikkerhedsansvar og privat sikkerhedsansvar. Vi er således vidner til et opbrud i grænserne mellem statens ansvar for nationens sikkerhed og borgerens ret til beskyttelse.

Det er derfor ikke overraskende, at cybersikkerhed er et omstridt og anfægtet begreb. Hvad der bliver kategoriseret som cybersikkerhed, og hvem der har ansvaret for at håndtere cybersikkerhed, er ikke statiske størrelser. Der findes militær-strategiske, politiske, juridiske og tekniske definitioner af cybersikkerhed, men begrebet er kontinuerligt til forhandling. Begrebsliggørelsen af cybersikkerhed konstitueres gensidigt af, hvilke typer af cybersikkerhedsudfordringer, -viden og -løsninger der vinder frem, herunder i forskningsverdenen.

I den resterende del af dette forord vil jeg derfor først præsentere et grundrids af den eksisterende cybersikkerhedslitteratur inden for forskningsfeltet International Politik. Jeg inddeler således cybersikkerhedslitteraturen i tre delvist overlappende kategorier. Derefter introducerer jeg de fem artikler, der indgår i temanummeret. De fem artikler præsenterer forskellige vinkler på cybersikkerhed. De tydeliggør, at cybersikkerhed er mangetydigt både begrebsligt og empirisk. De fem artikler tager afsat i forskellige fagdiscipliner og præsenterer en vifte af metodologiske udgangspunkter, konceptuelle tilgange og empirisk fokusområder.

Cybersikkerhedsforskningens tre ansigter

Vi kan ikke forstå vores undersøgelsesobjekter uden en forståelse for de akademiske discipliner og teorier, der konstituerer dem som sådan. En introduktion til cybersikkerhed kræver en forståelse for cybersikkerhedsforskningens historie og position inden for forskellige forskningsdipliner. I det følgende afsnit vil jeg derfor præsentere et grundrids af cybersikkerhedslitteraturen inden for International Politik og sikkerhedsstudier, herunder dens kontekst, udvikling og fortsatte forgreninger. Jeg rubricerer cybersikkerhedslitteraturen i tre kategorier: strategiske studier, governance-studier og kritiske sikkerhedsstudier.

> Jeg rubricerer cybersikkerhedslitteraturen i tre kategorier: strategiske studier, governance-studier og kritiske sikkerhedsstudier

Sondringen mellem de tre litteraturer henviser primært til forskellige teoretiske og metodologiske udgangspunkter. At fremhæve dette skel skal ikke ses som en essentialisering af de tre forskningsgrene. Snarere er der tale om forskellige videnskabelige diskurser, der har udviklet sig sideløbende, adskilt og

overlappende. Grænserne mellem dem er flydende, og de samme empiriske fænomener er ofte genstand for forskningen i alle tre litteraturer. De forskellige teoretiske og metodologiske udgangspunkter betyder imidlertid, at det er analytisk værdifuldt at behandle de tre litteraturer hver for sig.

Strategiske studier: Fra dommedagsscenarier over cyberkrig til gråzonekonflikt

Den akademiske litteratur om cybersikkerhed har sit udspring i USA. I denne litteratur bliver cyberspace betragtet som et femte militær- og krigsdomæne. Litteraturen anvender og tilpasser begreber og metodologiske tilgange, der har rod i realistisk International Politik og strategiske studier, til at foretage analyser af cyberkrig, -konflikt samt militære cybersikkerhedsstrategier (Cavelty og Wenger, 2019; Warner, 2012). Mere specifikt søger den at forstå, hvordan digitale teknologier transformerer krig og konfliktdynamikker og dermed påvirker sikkerhed og magtbalance i det internationale system. Denne tænkning trækker på og understøtter grundlæggende et neorealistisk syn på interstatslig sikkerhed og konflikt i et anarkisk system, hvor stater er black-boxes (de kan alle behandles som kompatible enheder), og det er magtbalancen, der tvinger dem til at handle på bestemte måder.

Den cybersikkerhedslitteratur, der blev udviklet i 1990'ernes og 00'ernes USA, var præget af hyperbolske dommedagsscenarier (Lawson, 2013). I forlængelse heraf opstod der i slutningen af 00'erne en konceptuel og teoretisk diskussion om anvendeligheden af cyberkrigsbegrebet (Libicki, 2007; 2009; Liff, 2012; Ridd, 2012, 2013; Stone, 2013). Thomas Ridds (2013) bog med titlen "Cyber War Will Not Take Place" er symptomatisk for denne debat. Sideløbende med den teoretiske og begrebslige litteratur om cyberkrig udviklede der sig en mere policy-orienteret diskussion om de strategiske, politiske og juridiske implikationer af brugen af militær cybermagt (Farwell og Rohozinski, 2011, 2012).

Det seneste tiår er forskning i cybersikkerhed for alvor blevet rodfæstet i den bredere realistiske og strategiske sikkerhedsdebat. Traditionel konfliktforskning er begyndt at anvende kvantitative metoder til se på effekten af digitale teknologier som værktøjer i udenrigspolitik og konfliktstyring (Valeriano og Maness, 2014; Valeriano et al., 2019). Andre har engageret sig i, hvordan og i hvilken grad cyberspace som krigsdomæne påvirker international orden (Buchanan, 2016; Kello, 2017), afskrækkelse (Godmann, 2010; Fischerkeller og Harknett, 2017; Nye, 2017; Stevens, 2012), offensiv-defensiv-balancen (Garfinkel og Dafoe, 2019; Gartzke og Lindsay, 2015; Slayton, 2017; Smeets, 2019) og tvang (Lindsay og Gartzke, 2018; Valeriano et al., 2018; Sharp, 2017).

Senest har litteraturen kastet sig over cyberangreb, der ikke enkeltstående lever op til de gængse definitioner af krig og væbnet konflikt. De udgør snarere et nyt konfliktrum, der har kilet sig ind mellem krig og fred. Her forsøger særligt stormagter som Rusland og Kina at føre en subtil form for magt- og geopolitik ved konstant at udfordre og overskride eksisterende internationale normer og regler (Breitenbauch og Byrjalsen, 2019; Harknett og Smeets, 2020; Jensen et al., 2019; Liebetrau, 2020).

Governance: Cybersikkerhedens hvem, hvad, hvor

Traditionelt har militæret, efterretningstjenester og andre nationale sikkerhedsinstitutioner været ansvarlige for national sikkerhed. På den måde har man forsøgt at bygge bro over spændingen mellem (ekstraordinær) national sikkerhedspolitik og (normal) demokratisk politik. Når cyberhændelser, der går på tværs af territorielle grænser med stor hastighed, bliver mere almindelige, så bliver de traditionelle statsbundne sikkerhedsstrukturer udfordret. Det er problematisk, da de ikke blot skal sikre samfundet og individet, men også transparens i og demokratisk kontrol med den sikkerhedspolitiske beslutningstagning. Cybersikkerhed tvinger os derfor til at genbesøge grundlæggende politiske og demokratiske spørgsmål om, hvem der skal holdes ansvarlig for hvad og af hvem.

En række forskere har derfor kastet sig over cybersikkerheds-governance det seneste årti. Det dominerende perspektiv undersøger forholdet mellem stater og virksomheder. Ofte gennem begrebet offentlige-private partnerskaber (Carr, 2016; Cavelty og Suter, 2009; Christensen og Petersen, 2017). Som følge af privatiseringen og dereguleringen af mange dele af den offentlige sektor siden 1980'erne befinder store dele af den kritiske (informations-) infrastruktur sig i dag på private hænder. Samlet set fokuserer disse studier på udfordringerne ved, at vi i stigende grad er tvunget til at fæstne lid til, at markedsdynamikker kan definere og understøtte et tilstrækkeligt højt niveau af national cybersikkerhed. Det gælder ikke kun, når vi snakker beskyttelse af kritisk infrastruktur, men også persondatabeskyttelse og beskyttelse mod cyberkriminalitet. Udgangspunktet i litteraturen er, at en grundlæggende forskel mellem økonomiske og politiske sikkerhedsinteresser hindrer de offentlige-private partnerskabers succes.

En anden del af governance-litteraturen undersøger og konceptualiserer den intrastatslige organisering af cybersikkerhedsenheder og –institutioner (Boeke, 2017; Weiss og Jankauskas, 2018). Ydermere kaster en del af litteraturen lys over private it- og cybersikkerhedsfirmaers rolle i relation til specifikke cybersikkerhedshændelser som Stuxnet (Stevens, 2019) og WannaCry (Christensen og Liebetrau, 2019).

Kritisk sikkerhedsteori: Den flygtige og flertydige cybersikkerhed

Den første bølge af forskning i cybersikkerhed inden for kritiske sikkerhedsstudier red på ryggen af sikkerhedsliggørelsesteori (Ericsson, 2001; Cavelty, 2007, 2008; Hansen og Nissenbaum, 2009). Her blev den diskursive indramning af cybersikkerhed samt brugen af metaforer og analogier studeret (Betz og Stevens, 2013; Cavelty, 2013). Første bølge af litteraturen skabte en væsentlig platform for at forstå og diskutere, hvordan forbindelser mellem cybersikkerhed og national sikkerhed bliver skabt samt en indsigt i de sikkerhedspolitiske virkninger af specifikke trusselsrepræsentationer. Som fremhævet af (Liebetrau og Christensen, 2020: 4), så er denne del af litteraturen dog begrænset af, at cybersikkerhed nemt bliver fastlåst som et spørgsmål om

national sikkerhed. Desuden bliver teknologiers politiske rolle indordnet og underlagt det diskursive udgangspunkt.

De seneste år har forskningen i cybersikkerhed inden for kritiske sikkerhedsstudier udviklet sig markant. Med inspiration fra teorier og begreber hentet i videnskabs- og teknologistudier (Cavelty, 2018; Liebetrau og Christensen, 2020: 4), Aktør-Netværk-Teori (Balzacq og Cavelty, 2016), psykoanalyse (Jacobsen, 2020a) og assemblage-teori (Collier, 2018; Stevens, 2019) har andenbølge-litteraturen rettet opmærksomhed mod, hvordan cybersikkerhed og digitalisering udfordrer og (re)konfigurerer tidslige (Stevens, 2016) rumlige (Balzacq og Cavelty, 2016), funktionelle (Christensen og Liebetrau, 2019; Jacobsen 2020; Tanzer 2019) og aktørmæssige (Liebetrau og Christensen, 2020: 4) aspekter af sikkerhed og politik.

Disse studier har bidraget til overvejelser over det epistemologiske og ontologiske grundlag for cybersikkerhed og studiet heraf. Studierne viser, at cybersikkerhed er flertydigt. At cybersikkerhed og cybersikkerhedspolitiske spørgsmål og svar bliver skabt i relationer mellem mennesker, teknologier, devices og infrastrukturer, der samtidig fastholder, unddrager og udfordrer det traditionelle nationalstatslige sikkerhedspolitiske udgangspunkt. Disse tilgange medfører en ontologisk åbenhed, idet de søger at tage højde for de foreløbige og historisk betingede forhold mellem heterogene elementer (Cavelty, 2018; Balzacq og Cavelty, 2016; Liebetrau og Christensen, under udgivelse). Det kræver en "analytisk sensibilitet for den dynamiske, heterogene og forbigående assemblage af cybersikkerhed" og understreger "behovet for situerede og kontekstuelle analyser" (Liebetrau og Christensen, 2020: 4).

Temanummerets bidrag til cybersikkerhedsforskningen

Temanummerets fem artikler tydeliggør, at cybersikkerhed er mangetydigt både begrebsligt og empirisk. De fem artikler tager afsat i forskellige fagdiscipliner og præsenterer en vifte af metodologiske udgangspunkter, konceptuelle tilgange og empirisk fokusområder.

I den første artikel undersøger Mikkel Storm Jensen muligheden for, at cybervåben giver småstater nye strategiske muligheder. Jensen gennemgår en række generelle karakteristika for cybervåben og beskriver, hvad de betyder for småstater generelt og Danmark specifikt. Han konkluderer, at cybervåben delvist ændrer balancen mellem småstater og stormagter i småstaternes favør. Han anfører dog, at der er grænser for de muligheder, våbnene åbner. Særligt for småstater, der som Danmark knytter deres sikkerhedspolitik snævert til medlemskab af en militær alliance som NATO.

Karsten Friis kaster i sin artikel lys over staters mulighed for at forsvare sig og gå til modangreb, når de bliver udsat for skadelige cyberoperationer i fredstid. Artiklen placerer sig dermed i et skæringspunkt mellem sikkerhedspolitik og folkeret. Med udgangspunkt i international ret og internationale normer undersøger Friis, hvordan toneangivende lande agerer, og han diskuterer de

sikkerhedspolitiske konsekvenser af øget brug af offensive cyberoperationer. Empirisk fokuserer artiklen på USA's nye cyberstrategi, der er baseret på vedvarende engagement og fremadrettet forsvar. Desuden undersøger Friis Norges anvendelse af offensive cyberoperationer som forsvarsmiddel, og han argumenterer for, at "Responsibility of States of International Wrongful Acts" er det mest relevante lovværk, når det kommer til offensive cyberoperationer, der falder under grænsen for væbnet konflikt.

I den tredje artikel stiller Jeppe Teglskov Jacobsen skarpt på den aktuelle status for international cybernormdannelse. Han spørger, hvorfor de internationale normforhandlinger er strandet, og hvorfor den vestlige koalitions normstrategi er fejlet? Og hvorvidt en småstat som Danmark kan være normentreprenøren, der skubber den vestlige cybernormdagsorden fremad? Jacobsens svar tager afsæt i, at kampen om internationale cybernormer er karakteriseret ved gensidige beskyldninger om hykleri og manglende anerkendelse af den efterretningsnorm, der dominerer i cyberspace. Han påpeger, at en begyndende vestlig åbenhed om og nuancering af statslig brug af cyberkapaciteter giver mulighed for, at Danmark kan blive et foregangsland, der udvikler de nødvendige politiske afklaringer og deler best practices og derved bidrager med de vigtige referencepunkter, som andre stater kan finde tiltrængt inspiration i.

I sit bidrag undersøger Ole Willers ved hjælp af professions- og ekspertsociologi, hvem cybereksperten egentlig er. Han spørger, hvad der karakteriserer cybereksperten, og hvordan cyberekspertrollen har udviklet sig over tid? Baseret på et nyt dataset omhandlende ekspertprofiler i danske offentlige og private cybersikkerhedsråd og -udvalg argumenterer Willers for, at cybersikkerhedseksperter har bevæget sig væk fra et rent teknisk fokus og hen mod en procesorientering, som både er bredere i fokus og placeret tættere på beslutningstagere. Han argumenterer for, at denne udvikling kan styrke ekspertmagten, som nu er begrænset til få hybride aktører, der formår at bygge bro mellem tekniske, organisatoriske og økonomiske rationaliteter. Han påpeger, at en sådan udvikling kan være demokratisk betænkeligt. Samtidig understreger han, at en mindre teknifiseret cyber-diskurs åbner mulighed for at re-politisere cybersikkerhedsområdet og dermed en inklusion af langt flere aktører i den offentlige debat.

I temanummerets femte og sidste artikel zoomer Lene Wacher Lentz og Jens Myrup Pedersen ind på hacking. De peger på, at hacking både bliver forstået som en forbrydelse og en it-sikkerhedskompetence. Det kan skabe forvirring, da ikke alt er tilladt for at optimere eller teste sikkerheden ved it-systemer f.eks. gennem hacking. Lentz og Pedersen klarlægger, hvornår der bliver straffet for "hacking" efter straffeloven. Desuden undersøger de, om en it-sikkerhedsaktør må bruge "hacking" som et forsvar, når it-systemer bliver angrebet af en fjendtlig "hacker". Dermed illustrerer de, at det kan være vanskeligt at forudsige, hvor grænserne for strafansvar går for den, der vil optimere sikkerheden ved sine systemer.

Litteratur

Balzacq, Thierry og Myriam Dunn Cavelty (2016), "A theory of actor-network for cyber-security", *European Journal of International Security*, 1(2): 176-98.

Betz, David J. og Tim Stevens (2013), "Analogical Reasoning and Cybersecurity", *Security Dialogue* 44(2): 147-64.

Boeke, Sergei (2017), "National cyber crisis management: Different European approaches", *Governance*, 31(3): 449-64.

Borghard, Erica D. og Shawn W. Lonergan (2017), "The Logic of Coercion in Cyberspace", *Security Studies*, 26(3): 452-81.

Breitenbauch, Henrik og Niels Byrjalsen (2019), "Subversion, Statecraft and Liberal Democracy", *Survival*, 61(4): 31-41.

Buchanan, Ben (2016), *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, New York: Oxford University Press.

Carr, Madeline Public-private partnerships in national cyber-security strategies, *International Affairs*, 92:1

Cavelty, D. Myriam (2007) Cyber-terror: Looming threat or phantom menace? The framing of the US cyber-threat debate, *Journal of Information Technology & Politics*, 4:1. 19–36

Cavelty, D. Myriam (2008) C*yber-Security and Threat Politics: US Efforts to Secure the Information Age*. London. Routledge.

Cavelty, D. Myriam (2018), "Cybersecurity Research Meets Science and Technology Studies", *Politics and Governance*, 6(2): 22-30.

Cavelty, D. Myriam & Andreas Wenger (2020) Cyber security meets security politics: Complex technology, fragmented politics, and networked science, *Contemporary Security Policy*, 41:1, 5-32

Cavelty, D. Myriam og Florian J. Egloff (2019), "The Politics of Cybersecurity: Balancing Different Roles of the State", *St Antony's International Review*, 15(1): 37-57.

Cavelty, D. Myriam (2013), "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse", *International Studies Review*, 15(1): 105-22.

Christensen, K. Kristoffer og Tobias Liebetrau (2019), "A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry", *Intelligence and National Security*, 34(3): 395-408.

Christensen, K. Kristoffer & Karen L. Petersen, Public-private partnerships on cyber security: A practice of loyalty, *International Affairs*, 93:6. 1435–52.

Collier, Jamie (2018) Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision, *Politics and Governance*, 6:2. 13-21

Cormac, Rory og Richard J. Aldrich (2018), "Grey is the new black: covert action and implausible deniability", *International Affairs*, 94(3): 477–94.

Eriksson, Johan (2001) Cyberplagues, IT, and security: Threat politics in the information age, *Journal of Contingencies and Crisis Management*, 9:4. 200–10

Farwell, P. James og Rafal Rohozinksi (2011), "Stuxnet and the Future of Cyber War", *Survival,* 53(1): 23–40.

Farwell, P. James og Rafal Rohozinksi (2012), "The New Reality of Cyber War", S*urvival*, 54(4): 107–20.

Fischerkeller, Michael P. & Richard J. Harknett (2017) Deterrence is Not a Credible Strategy for Cyberspace. *Orbis*, 61: 381-393.

Garfinkel, Ben og Allan Dafoe (2019), "How does the offense-defense balance scale"?, *Journal of Strategic Studies*, 42(6): 736-63.

Gartzke, Erik Jon R. Lindsay (2015), "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace", *Security Studies*, 24(2): 316-48.

Hansen, Lene og Helen Nissenbaum (2009), "Digital Disaster, Cyber-Security, and the Copenhagen School", *International Studies Quarterly*, 53(4): 1155-75.

Harknett, J. Richard & Max Smeets (2020) Cyber campaigns and strategic outcomes, *Journal of Strategic Studies*.

Healey Jason, red. (2013), *A fierce domain: conflict in cyberspace, 1986 to 2012*, Arlington, VA: Cyber Conflict Studies Association.

Jacobsen, J.T. (2020), "Lacan in the US cyber defence: Between public discourse and transgressive practice", *Review of International Studies*, first view 20. marts, 1–19.

Jensen, Benjamin, Brandon Valeriano og Ryan Maness (2019), "Fancy bears and digital trolls: Cyber strategy with a Russian twist", *Journal of Strategic Studies*, 42(2): 212-34.

Kello, Lucas (2017), *The Virtual Weapon and International Order*, New Haven and London: Yale University Pres.

Lawson, Sean (2013), "Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats", *Journal of Information Technology & Politics*, 10(1): 86-103.

Libicki, Martin C (2007), *Conquest in Cyberspace, National Security and Information Warfare*, Cambridge: Cambridge University Press.

Libicki, Martin C (2009), *Cyberdeterrence and Cyberwar*, Santa Monica: Rand Corporation.

Liebetrau, Tobias (2020), "Dansk offensiv cybermagt mellem angreb, spionage og forsvar: En komparativ analyse på tværs af Europa", Københavns Universitet: Center for Militære Studier, 50.

Liebetrau, Tobias og Kristoffer K. Christensen (2020), "The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces, *European Journal of International Security*.

Liff, Adam P (2012), "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War", *Journal of Strategic Studies* 35(3): 401-28.

Lin, Herbet og Amy Zegart (2018), "Introduction", i Herbert Lin og Amy Zegart, red., *Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations*, Washington D.C: Brookings Institution Press.

Lindsay, Jon R. og Erik Gartzke (2018), "Coercion Through Cyberspace: The Stability-Instability Paradox Revisited', i Kelly M. Greenhill og Peter Krause, red., *Coercion: The Power to Hurt in International Politics*, New York. Oxford University Press.

Nye, Jr., Joseph S. (2016/2017) Deterrence and Dissuasion in Cyberspace. *International Security* 41.3: 44-71.

Rid, Thomas (2012), "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 35(1): 5–32.

Rid, Thomas (2013), *Cyber War Will Not Take Place*, London: Hurst.

Sharp, Travis (2017), "Theorizing cyber coercion: The 2014 North Korean operation against Sony", *Journal of Strategic Studies*, 40(7): 898-926

Slayton, Rebecca (2017) What is the Cyber Offense-Defense Balance? Conceptions, Causes and Assessment. *International Security* 41(3): 72-109

Smeets, Max (2019), "The Strategic Promise of Offensive Cyber Operations", *Strategic Studies Quarterly*, 12(3): 90-113.

Stevens, C.L. (2019). Assembling cybersecurity: The politics andmateriality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*.

Stevens, Tim (2016) *Cyber Security and the Politics of Time*. Cambridge. Cambridge University Press.

Stevens, Tim, Global cybersecurity: New directions in theory and methods, *Politics and Governance*, 6:2. 1-4

Stone, John (2013) Cyber War Will Take Place!, *Journal of Strategic Studies*, 36:1, 101-108

Tanczer, M. Leonie (2019) 50 shades of hacking: How IT and cybersecurity industry actors perceive good, bad, and former hackers, *Contemporary Security Policy*.

Valeriano, Brandon & Ryan Maness (2018). How We Stopped Worrying About Cyber Doom and Started Collecting Data. *Politics and Governance*. 6(2): 49-60

Valeriano, Brandon og Ryan C. Maness (2014), "The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11,' *Journal of Peace Research*, 51(3): 347–60.

Warner, Michael (2012), "Cybersecurity: A Pre-history", *Intelligence and National Security*, 27(5): 781-99.

Weiss, Moritz and Vytautas Jankauskas (2018) Securing cyberspace: How states design governance arrangements. *Governance*.