

# Nyckelaktörerna för rysk cyberstrategi: 2000–2020



Carolina Vendil Pallin  
Stockholm: Totalförsvarets forskningsinstitut  
2020  
Rapportnr. FOI-R--5025--SE  
100 sider. ISSN: 16501942

Omtalt av **Bjørn Svenungsen** [høyskolelektor og leder for Cyberprogrammet ved Institutt for Forsvarsstudier/Forsvarets Høyskole, bsvenungsen@mil.no]

Russiske cyberoperasjoner har av gode grunner blitt mye omtalt de siste 10 årene. Som Andy Greenberg beskriver i *Sandworm* – en bok Vendil Pallin også viser til – har avanserte og vedvarende russiske cyberangrep ikke bare hatt etterretning som formål, men også ført til fysisk ødeleggelse og hatt betydelige økonomiske konsekvenser. I den grad angrepene har blitt tilskrevet bestemte gjerningsmenn, har vestlige myndigheter som regel pekt på enheter innenfor russiske sikkerhetstjenester som GRU og FSB.

Samtidig har Russland det siste tiåret gjennom diplomati aktivt søkt å påvirke det internasjonale samfunn i retning av «suverene» internett og økt statlig kontroll over den globale internettforvaltningen. Videre vet vi, gjennom blant annet bøkene til Andrej Soldatov og Irina Borogan – også de blant Vendil Pallins kilder, at russiske myndigheter anså internett som en trussel og et verktøy for amerikansk hegemoni da det for alvor gjorde seg gjeldende på 1990-tallet.

Således er det ikke til å undres over at internett for russiske myndigheter har vært krevende å forholde seg til. På den ene siden har de ønsket å utnytte internettets muligheter for økonomisk vekst, utvikling og teknologisk fremgang. På den andre siden har de vært livredde for den trusselen og det potensialet for destabilisering og

uro som internett representerer gjennom fri flyt av ytringer, kriminalitet og ondsinnede handlinger.

Alt dette og mye mer berøres i Vendil Pallins grundige rapport. Mye av dette er det forsket på tidligere, også av Vendil Pallin selv. I denne rapporten hever imidlertid forfatteren blikket og ser forskjellige utviklingstrekk i sammenheng. Ved å ta for seg nøkkelaktørene i russisk cyberpolitikk gjennom en periode på tyve år, fra 2000 til 2020, viser hun hvordan russiske myndigheters overordnede holdninger til internett og cyberspace gradvis har endret seg, noe som igjen har ført til endringer i russiske cyberstrategier. Det har også påvirket hvordan vanlige russere og russisk næringsliv, og da særlig tech-industrien, forholder seg til internett.

Det er ingen lystig lesning. Med et tørt, nøkternt, etterrettelig og saklig akademisk språk beskriver Vendil Pallin en utvikling som får det til å gå kaldt nedover ryggen selv på en erfaren diplomat og forsker. Hun deler perioden inn i tre. I første periode, 2000–2011, er Russland fortsatt et fritt land hva gjelder bruk av internett. En rekke private og offentlige initiativ for å fremme innovasjon og økonomi støttes av myndighetene. I andre periode, 2011–2013, strammes skruen til og sikkerhetsmyndighetene får en stadig mer dominerende rolle versus de myndigheter som fremmer teknologi, innovasjon og økonomi. Den tredje perioden starter i 2014, hvor annekteringen av Krim er avgjørende for hvordan sikkerhetsmyndighetene og kontrollivrige aktørers tilnærming til internett blir tilnærmet enerådende. Det er altså de myndighetene som først og fremst anser internett som en trussel, ikke som en mulighet, som styrer utviklingen. Den perioden strekker seg til 2019. Forfatteren indikerer at Russland etter 2019 går inn i en fjerde periode som ennå ikke er avklart, men hvor kunstig intelligens (AI) og behovet for store mengder data vil spille en betydelig rolle for fremtidige cyberstrategier.

Gjennom rapporten ser vi hvordan utviklingen av en stadig mer autoritær stat gjenspeiles i internettpolitikken. Stikkord er omfattende overvåkning, kontroll, blokkering av websider, nye lover og lovforslag, undergraving av organisasjoner og bedrifter som ikke støtter eller har nære bånd til Kreml, en offensiv utenrikspolitikk som søker allierte i Russlands syn på hvordan internett skal styres globalt, og hyppige russiske cyberangrep. Rapporten kulminerer på sett og vis med Dumaens vedtak av loven om et suverent internett i 2019. Paradokset ved et «suverent» internett (som strengt tatt ikke lenger er internett), behandles ikke, men dette er heller ikke et savn. Vendil Pallins ambisjon er å analysere de mange aktører som har bidratt til å forme russiske cyberinteresser og cyberstrategier, og det lykkes hun godt med.

Vi får en forståelse av de mange dragkamper som må ha funnet sted mellom ulike russiske myndigheter, mellom næringslivet og myndighetene, og i parlamentet, hvor haukene har vunnet og duene har tapt, hver gang. I alle fall etter 2014. Rapporten viser også at oppfatningen om at president Vladimir Putin er enerådende og bestemmer alt, i beste fall bør nyanseres, i alle fall på cyberområdet.

Kort fortalt tok det litt tid før russiske myndigheter fikk summet seg. Da de først gjorde det, ble internett og cyberspace i all hovedsak behandlet som et verktøy

for myndighetene, både sivilt og militært. I praksis betød det at sikkerhet og kontroll trumfet innovasjon, utvikling og økonomi.

Ambisjoner om å fremme en innovativ og teknologisk avansert privat sektor i Russland har i stor grad falt på stengrunn, først og fremst fordi maktapparatet i Kreml gjennom kameraderi, eierskap og et ekstremt behov for kontroll har undergravd tilliten til russisk teknologi utenfor Russland. I dag er det noen få selskap, de Vendil Pallin kaller «de tre store» (MTS, Megafon, og Vypelkom) som kontrollerer det meste av den private internett- og IT-teknologiutviklingen i Russland. Alle har svært tette bånd til Kreml. Ingen av dem nyter særlig tillit utenfor Russland. Mindre selskap som forsøker å slå seg opp må pent føye seg inn i rekkene, eller ta konsekvensene. Det betyr ofte å få nye eiere eller å flytte utenlands. Den slags praksis fremmer ikke innovasjon. Et godt eksempel i rapporten er cybersikkerhetsselskapet Kaspersky Lab. Bare ryktet om at de er koblet til Kreml er nok til at markedsandelen for dette tidligere høyt anerkjente firmaet faller, og deres internasjonale marked forvitrer.

Vendil Pallins rapport er nedslående, men viktig. Den fikk meg til å tenke på pågående diskusjoner i Norge og Vesten, om sikkerhetsmyndigheters legitime behov for å kunne overvåke internettets infrastruktur og innhold. Vi balanserer i all hovedsak fortsatt på den tynne eggen mellom frihet og sikkerhet på internett; mellom trusler og muligheter; mellom statlig kontroll og privat innovasjon. Vendil Pallin viser oss hvordan Russland har mistet denne balansen.