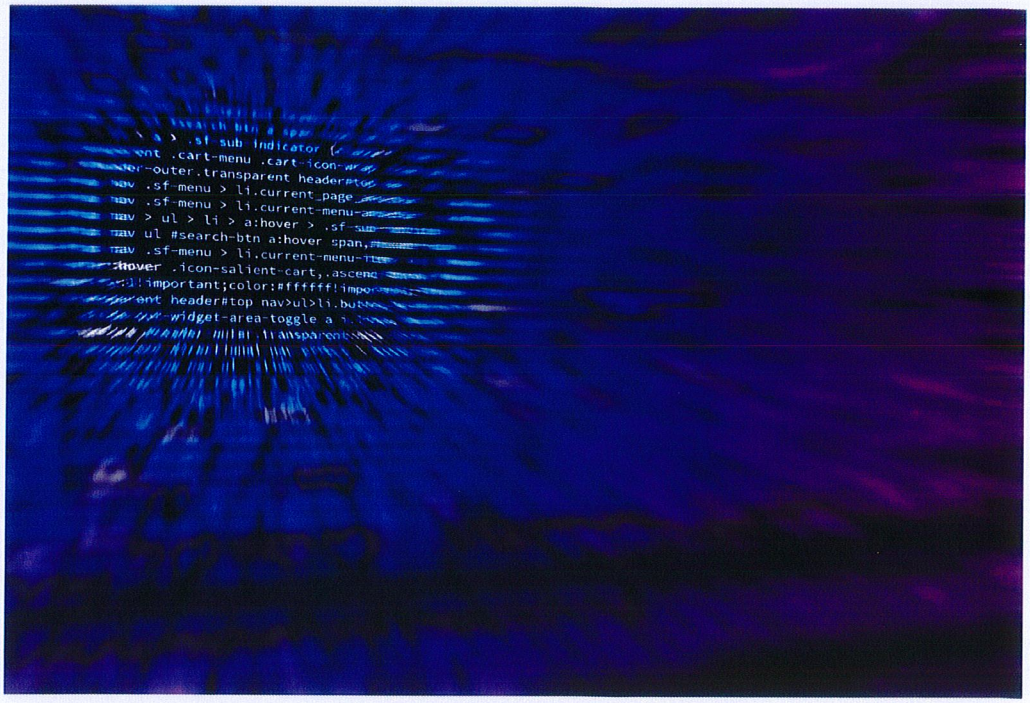

Kina og Russland prøver allerede å ta kontroll over «sitt» internett. Vil Vesten nå, etter USA-hackingen og foran vårens valg i Europa, følge etter?

Niels Nagelhus Schia

Publisert: 17.01.2017 - 15:39
Oppdatert: 18.01.2017 - 08:12

Lars Gjesvik

Presidentvalget i USA illustrerte hvordan hacking kan benyttes for å forstyrre og påvirke politiske valg i demokratiske land. Sensitiv informasjon ble stjålet og sluppet gjennom offentlige lekkasjesider som Wikileaks og DC Leaks, og mange mener Russland står bak. Selv om det ikke er sikkert at valgresultatet ville sett annerledes ut, ble amerikaneres oppfattelse av valget og derigjennom Donald Trumps hvetebrødsdager sterkt påvirket av hendelsene.

«Kina og Russland har forsøkt å beskytte seg ved å ta kontroll over "sitt" internett.»

I 2017 er det valg i Tyskland, Frankrike, Nederland og Norge. Vi bør være på vakt mot tilsvarende kampanjer i Europa, men når vi forsøker å beskytte oss mot lignende kampanjer er spørsmålet hva vi ofrer.

Vil Vesten følge Kina og Russland?

Kampanjer for å påvirke valg i andre land er ikke noe nytt. Under den kalde krigen blandet både Sovjetunionen og USA seg inn i andre lands valg. Utbredelsen av internett har imidlertid gitt en ny dimensjon til slike kampanjer.

Der utfordringen tidligere handlet om å innhente informasjon, er informasjonen nå i stor grad tilgjengelig. Utfordringen handler derfor mer om å kunne skille verdifull informasjonen fra verdiløs. Kombinasjonen av hacking og påvirkningskampanjer mot presidentvalget i USA har vist hvor slagkraftig denne cocktailen kan være når den treffer.

I Kina, og i økende grad Russland, har myndighetene forsøkt å beskytte seg ved å ta kontroll over "sitt" internett. Gjennom utstrakt bruk av sensur, brannmurer og kontroll innenfor egne landegrenser, håndheves det som ofte blir beskrevet som cybersuverentitet.

I en verden hvor internett stadig mer blir sett på som en trussel, og ikke en ressurs, er spørsmålet nå om Vesten vil følge etter.

Høstens hackerangrep i USA trenger imidlertid ikke å bety at vi må følge Kina og Russlands autoritære overvåkingssamfunn for å sikre oss mot dette. Mye kan gjøres gjennom bedre samarbeid på tvers av offentlig og privat sektor, gjennom økt bevissthet om problematikken og ved å gjøre cybersikkerhet til en større del av hverdagen til folk flest.

Hva vi vet om hackingen

I oktober 2016 gikk Barack Obama offisielt ut med anklagene om at Russland hadde stått bak hackingen av Demokratene. 6. januar i år fulgte amerikanske etterretningsorganisasjoner etter da de offentliggjorde en rapport som identifiserte Russland som den store syndebukken.

Rapporten og bevisene har imidlertid møtt kritikk for å være mangelfulle og for å inneholde lite ny informasjon. Mye av grunnen til det kan være at det som regel er vanskelig å bevise hvem som står bak hacking og cyberangrep. Klare digitale fingeravtrykk er sjeldne. Motiv og indisier som *peker* i en retning, er mye vanligere. Etterforskningen av innbruddet i Demokratenes epost-server pekte mot FSB og GRU, begge russiske etterretningsbyråer.

Allerede høsten 2015 ble DNC kontaktet av FBI, som anbefalte partiet om å gå gjennom nettverkene sine, men partiet fulgte ikke opp anbefalingen før i mai 2016. Da kontaktet de cybersikkerhetsselskapet CrowdStrike, som kunne bekrefte innbruddet og sporet det til to hackergrupper, Fancy Bear og Cozy Bear, og etter hvert

også til the Dukes og APT29, alle russiske hackergrupper.

«I stedet for å sette inn ressursene på å drive detektivarbeid på nett, vil det være mer hensiktsmessig å prioritere fortløpende evaluering og sikring av kritisk infrastruktur.»

14. juni publiserte The Washington Post nyheten om datainnbruddet, og samme dag slapp CrowdStrike en rapport som koblet hackergruppene til russisk etterretning. Hundrevis av anonyme hackere og entusiaster kastet seg over materialet. De pekte etter hvert ganske samstemt på særegenheter i kodingen man hadde sett fra andre operasjoner hvor man har antatt at Russland står bak.

Fortløpende evaluering og sikring

Selv om det meste tyder på at Russland sto bak angrepene, er det også noen som mener at bevisene kan være plantet. De trekker frem at enkelte dokumenter var blitt redigert med russiske språkinnstillinger. Redigeringen kan tyde på at noen har ønsket at det skulle se ut som om det var Russland som sto bak.

Men det viktigste er kanskje ikke å finne ut hvorvidt det var en russisk hackergruppe eller ikke som stod bak. I stedet for å sette inn ressursene på å drive detektivarbeid på nett, vil det være mer hensiktsmessig å prioritere fortløpende

evaluering og sikring av kritisk infrastruktur mot digitale trusler.

Selv om vi ikke vet hvorvidt hackingen faktisk bidro til å vippe valget i den ene eller den andre retningen, har den påfølgende påvirkningskampanjen preget både amerikansk og europeisk mediebilde og debatt. I den sammenheng kan det være lurt å ta ett skritt tilbake for å se på hvilke konsekvenser en slik retning på debatten kan få.

Et åpent internett

I Vesten har internett lenge vært forbundet med friske diskusjoner og en oppfatning om at "alt er lov". Årsaken finner man i måten internett ble utviklet og spredt på i USA på 70- og 80-tallet, hvor arbeidet var drevet av teknoutopisme og drømmen om et internett fritt for sensur, drevet fram av individer og organisasjoner som var løst forbundet med hverandre.

Oppbyggingen og forvaltningen av internett i dag gjenspeiler dette. Private selskaper og individer har fått en plass ved siden av stater, og selv om USA har hatt kontroll over mye av infrastrukturen som bærer internett, har landet i liten grad forsøkt å bruke denne posisjonen til å påtvinge regulering.

En annen grunn til at særlig USA har kjempet for et liberalt internett, har vært ideen om at det er i amerikansk interesse. Den arabiske våren ble løftet fram som beviset på hva internett og sosiale medier kan gjøre med undertrykkende regimer.

«Nøling, somling og misforståelser gjorde at angrepet fikk fortsette.»

Tanken var at autoritære og informasjonsundertrykkende regimer ville sprekke som troll i sola hvis man bare nådde gjennom med riktig informasjon. At de samme virkemidlene på et tidspunkt kunne bli snudd i motsatt retning, ble i liten grad vurdert.

Rapporten om russisk innblanding i den amerikanske valgkampen, avslører store problemer i måten land håndterer cyberangrep på. DNC tok ikke trusselen på alvor. Nøling, somling og misforståelser gjorde at angrepet fikk fortsette. Et kritisk spørsmål er hvilke tiltak stater må ta for å beskytte vitale interesser mot digitale trusler og påvirkningskampanjer.

Ironisk nok er Russland, og i enda større grad Kina, landene som har gått lengst i å beskytte seg mot denne typen politiske angrep, men man behøver ikke å innføre et autoritært kontrollregime for å beskytte seg mot phishing og hacking.

Cybersuverenitet i Kina

For myndighetene i Kina og Russland har internett alltid spredt farlig informasjon, vel så mye som virus og dataormer. Begge landene har i internasjonal politikk vært fanebærere for "cybersuverenitet", en ide om at alt som foregår i cyberspace innenfor et lands territorium, er et like internt anliggende som hva som foregår innenfor landegrensene ellers i samfunnet. For disse landene har

løsningen på feilinformasjon og falske nyheter vært tydelig lenge; stater må *selv* kunne kontrollere og sensurere *sitt* cyberspace.

Kinesiske myndigheter har ved hjelp av landets «Great Firewall» lenge kontrollert hvilke deler av internett og informasjon innbyggerne får tilgang til. I 2017 blir Kinas nye cybersikkerhetslov iverksatt. Den nye loven vil legge klare føringer for hvilke regler utenlandske selskap må følge, og hvilke nettsider som skal være tilgjengelige innenfor landets grenser. Det finnes allerede kinesiske varianter av de fleste ledende internettselskapene, som Facebook og Uber.

«Argumentet for mer kontroll vil kanskje møte større forståelse i Vesten i 2017 enn det gjorde i 2016.»

Kritikere peker på hvordan det muliggjør en streng statlig kontroll med alt som foregår på internett. Selskaper som ikke kontrollerer brukerne, kan bli kastet ut og miste tilgang på mer enn 700 millioner kunder.

Vesten tar grep for å beskytte seg

Etter hackingen av valget har USAs Department of Homeland Security tatt steg for å beskytte seg mot digitale angrep, men fokuset er fortsatt på den faktiske infrastrukturen, og mindre på påvirkningskampanjer og falske nyheter. Stadig flere amerikanske selskaper går nå til

staten for å få beskyttelse mot hacking og datainnbrudd. Europeiske land som Polen, Ungarn og Storbritannia har tatt skritt i samme retning. Argumentet for mer kontroll vil kanskje møte større forståelse i Vesten i 2017 enn det gjorde i 2016.

Det er likevel en høyst reell fare for at man nå overdriver risikoen. Snowden-avsløringene om den massive NSA-overvåkningen viser den stygge siden ved statlig kontroll over internett. Når Kina anklages for å pynte på undertrykking av dissidenter med sin påstand om cybersuverenitet, er det også legitim kritikk. Mulighetene for å misbruke argumentet om kontroll til å innføre streng overvåkning, er åpenbar. Påvirkningskampanjer av den typen USA nylig har vært gjennom, kan likevel få de kinesiske tiltakene til å virke visjonære.

Da er det viktig å huske at de beste tiltakene for bedre cybersikkerheten er "kjedelige" løsninger som enkle sikkerhetsrutiner, bedre samarbeid og større grad av bevissthet. Mye kan gjøres av hver enkelt uten at det behøver å gå utover kjerneverdier som personvern og det frie internett.

Må ikke gå utover det frie internettet

I 2017 er det som sagt valg i Norge, Tyskland, Frankrike og Nederland. Mange bekymrer seg nå for at valgene vil bli forsøkt påvirket gjennom hacking og kampanjer på samme måte som i USA.

«Noen særegenheter ved det amerikanske systemet gjør faren mindre akutt i Europa.»

For Vestens del er valgene i Tyskland og Frankrike særlige kritiske. Noen særegenheter ved det amerikanske systemet gjør faren mindre akutt i Europa. For eksempel bidro den lave tilliten til mediene i USA til at mange ignorerte advarslene. Men det er ingen grunn til å anta at lignende kampanjer ikke kan ha effekt også i Europa.

Hvordan vi skal regulere internett har gått fra et spørsmål for spesielt interesserte til et av de mest kritiske i vår tid. I en kongresshøring i høst uttalte en av de ledende cybersikkerhetsekspertene, Bruce Schneier, at «æraen hvor internett handlet om spill og moro er over, for internett har nå blitt farlig». Om den dystre spådommen blir sann eller ikke gjenstår å se, men mye vil bli avgjort av hvordan vi håndterer den type trusler som vi har sett gjennom høstens presidentvalg i USA.

Vi vil aldri kunne sikre samfunnene våre helt, men vi vil kunne gjøre ganske mye med små grep uten at det går utover personvern og det frie internettet.

cybersikkerhet hacking internett Kina Russland USA

Niels Nagelhus Schia

Schia er seniorforsker ved Norsk Utenrikspolitisk Institutt (NUPI) der han forsker på internasjonal politikk og cybersikkerhet. Han har en doktorgrad fra Universitetet i Oslo. Twitter: @nielsschia.

Lars Gjesvik

Gjesvik arbeider med cybersikkerhet som vitenskapelig assistent ved Norsk Utenrikspolitisk Institutt (NUPI).

FRA FORSIDEN

KOMMENTAR