Nationalstatens overlevelse er blevet afhængig af techgiganterne

Amerikanske techfirmaer som Microsoft, Google og Amazon har kæmpet på Ukraines side i en usynlig cyberkrig mod Rusland. Magtbalancen mellem stater og virksomheder er blevet forrykket.

Af Michael Jarlner

Der var næppe mange, der på forhånd havde set IT-milliardæren Oleg Roginskyj som en nøglebrik i forsvaret af Ukraine imod russisk aggression. Men den unge ukrainer havde noget ganske særligt: Han havde kontakter. Og han havde vel at mærke kontakter til en techindustri, der med krigen i Ukraine er trådt frem som en central aktør i forsvaret af det 21. århundredes nationalstat.

Oleg Roginskyj kom således til at spille sin første rolle i dagene omkring den russiske invasion i februar, da folk i og omkring den ukrainske regering blev urolige over Google Maps, der i realtid viste billeder fra ukrainske byer og veje: Tænk, hvad russisk militær dog ikke kunne bruge den viden til, tænkte de. Så Oleg Roginskyj, der har opbygget en formue i det californiske IT-mekka, Silicon Valley, blev kontaktet og bedt om at bruge alle de kontakter, han havde i den amerikanske techindustri, til at få slukket for det.

Og operationen lykkedes, fortalte han, da han i foråret deltog i et udsat årsmøde i World Economic Forum i den schweiziske alpeby Davos: Google slukkede for sin live-transmission, og russisk militær mistede en digital udkigspost. Snart efter var Oleg Roginskyj i færd med at hjælpe en anden IT-milliardær, Tesla- og SpaceX-stifteren, Elon Musk, der forsynede ukrainerne med tusindvis af såkaldte Starlink-satellitter, så russerne ikke kunne fratage dem deres adgang til internettet.

De første skud

Men bag kulisserne foregik der meget mere. Amerikanske techgiganter som Google, Amazon og Microsoft var også dybt engagerede i forsvaret af den ukrainske stat mod russiske cyberangreb. Og de begyndte allerede dagen før den russiske invasion 24. februar i år.

”De første skud blev faktisk affyret i timerne inden, mens kalenderen stadig viste 23. februar,” fortalte Microsoft-præsidenten Brad Smith i Davos.

Han uddybede det i juni, da Microsoft offentliggjorde en foreløbig statusrapport om den cyberkrig, der er foregået som en usynlig

parallelkrig til den fysiske krig – eller 'kinetiske krig', om man vil – i Ukraine.

I rapporten fortæller Brad Smith, hvordan Rusland gik til angreb med såkaldte Foxblade-cybervåben, der skulle nedlægge store dele af Ukraines offentlige og halvoffentlige computere og computernetværk, hvorved den ukrainske stat ville være lammet som en slags digital 'failed state', når russisk militær rykkede ind. Hvis det altså var lykkedes. Men det gjorde det ikke. Og det var der flere grunde til.

For det første havde den ukrainske regering i al hast fået vedtaget en lov, der tillod den at overføre kritiske statslige data fra fysiske servere i Ukraine til den såkaldte sky – et digitalt lager af data ude i cyberspace – og placere dem i datacentre rundt om i Europa. Det skete 17. februar, blot en uge før Ruslands invasion. Man fornemmer næsten en svedperle eller to i Brad Smiths fremstilling af sagen i rapporten:

"En uge før den russiske invasion kørte den ukrainske stat udelukkende på servere, der var placeret i offentlige bygninger, der var sårbare over for missilangreb og bombardementer."

For det andet var de amerikanske techgiganter dybt involveret i forsvaret af Ukraine mod cyberangreb. Cyberangrebene 23. februar var ifølge Microsoft kun den første skudsalve. Der er siden da registreret otte forskellige former for cyberangreb mod mindst 48 ukrainske ministerier og virksomheder, herunder forsyningsvirksomheder.

"Russisk militær har ved flere lejligheder forbundet deres cyberangreb med brugen af konventionelle våben mod de samme mål," skriver Microsoft i sin rapport:

"Ligesom man ved en invasion fra havet kombinerer brugen af flåde- og landstyrker, så har krigen i Ukraine vist en russisk brug af cyberangreb til at uskadeliggøre et bestemt måls computernetværk, hvorved man har forsøgt at overraske det med landstyrker, luft- eller missilangreb."

Et par eksempler – og stadig ifølge Microsofts fremstilling af sagen: 2. marts opdagede Microsofts såkaldte *Threat Intelligence Center* et cyberangreb mod en ukrainsk atomkraftvirksomheds computernetværk. Og dagen efter angreb og besatte russisk militær virksomhedens største atomkraftværk.

"Russisk militær kombinerede brugen af cybervåben og konventionelle våben i angrebet på et atomkraftværk," konstaterer Microsoft.

I samme uge gik russiske cyberkrigere angiveligt til angreb på byen Vinnytsjas computernetværk, hvorefter byens lufthavn blev angrebet med otte krydsermissiler to dage efter.

"En række senere destruktive cyberangreb blev koordineret med missilangreb og rettet mod Ukraines jernbaner og transportsystemer, der bruges til transport af våben og militære forsyninger," hedder det videre:

"Da russiske missiler for eksempel slog ned på flere jernbanestationer i Lviv 3. maj – et logistisk knudepunkt for transport af militær og humanitær hjælp – var den militære Iridium-gruppe allerede aktive på deres digitale netværk."

Cyberkrigen: Stor eller lille?

Man kan diskutere, hvor meget disse cyberangreb reelt har fyldt i Ukraine, lige som man blandt andet gør det i militærforskerne Jeppe Jacobsen og Tobias Liebetraus nye bog *Cybertrusler – det digitale samfunds skyggeside* fra Djøf's Forlag.

Der er dem, som mener, at cyberkrigen i høj grad har stået i skyggen af et fortsat russisk fokus på såkaldt kinetisk – fysisk – krigsførelse, mens andre advarer mod at underdrive cybertruslen, blot fordi man ikke kan se dens skader med det blotte øje, som man kan efter brugen af krudt og bomber.

"Den begrænsede opmærksomhed på de russiske militære cyberspaceoperationer skal ikke nødvendigvis forstås på den måde, at cyberspaceoperationernes muligheder har været overfortolkede," påpeger militæreksperten Lasse Kronborg fra Forsvarsakademiet i et af bogens eksterne bidrag:

"Svaret kan i lige så høj grad være, at det var Ruslands doktrin og manglende modenhed inden for multidomæneoperationer, der har hæmmet Ruslands evne til at udnytte cyberspaceoperationens fulde potentiale."

Foto: M Zakiyuddin Munziri / Unsplash

Foto: Levi Meir Clancy / Unsplash

Eller … Måske har vi ikke opdaget nogle af de digitale lureminer eller fjernstyrede cyberbomber, der er placeret rundt om i USA's eller Europas mere eller mindre beskyttede systemer, hvor de blot venter på at blive udløst. For knap to år siden viste det omfattende Solar Winds-angreb, hvor avancerede cybervåben Rusland råder over. Måske er grunden til de hidtidige cyberangrebs begrænsede effekt slet og ret, at brugen af avanceret kunstig intelligens har ført til, at cyberforsvaret indtil videre har været stærkere end cyberangrebene. Husk i den sammenhæng på, at Rusland kæmper alene mod nogle af verdens mest avancerede økonomier og techgiganter.

"Denne krig har ikke alene stillet Rusland, en cyberstormagt, over for en alliance af lande. Cyberforsvaret af Ukraine hviler i afgørende grad på en koalition af både lande, virksomheder og NGO'er," påpeger Brad Smith.

Technopolar verden

Den internationalt berømmede analytiker, amerikaneren Ian Bremmer, taler direkte om fremkomsten af en technopolar verden, hvor netop techvirksomheder er afgørende for forsvaret af nationalstaterne.

Techgiganter som Microsoft, Google og Amazon har såmænd allerede hver især modtaget en officiel ukrainsk frihedspris, fordi de har været afgørende for den ukrainske stats muligheder for at afværge russiske cyberangreb og dermed sikre dens mulighed for fortsat at fungere.

Tænk, hvor meget kaos det ville have udløst, hvis Ukraines pengesystem, elforsyning eller sundhedsvæsen var brudt sammen. Det kunne måske ligefrem have ført til præcis den ustabilitet, der skulle til for at nå et af Ruslands første primære krigsmål: at vælte præsident Zelenskyj og hans regering.

Da dagbladet Politiken i foråret mødte chefen for Det Europæiske Forsvarsagentur (EDA), Jiri Sedivy, i Davos, kunne han godt forestille sig, at krige i fremtiden vil blive udkæmpet som rene cyberkrige. Altså helt uden brug af bomber, kampvogne og krudt.

"Hvis man som Claus von Clausewitz (berømt preussisk militærteoretiker fra 1800-tallet, *red.*) opfatter krige som et middel til at påtvinge andre stater sin vilje, så vil man formentlig i fremtiden kunne gøre det ved en cyberkrig," sagde han:

"Tænk, hvis Rusland med et cyberangreb havde haft så meget held til at lamme den ukrainske regering og stat, at det havde banet vej for et kaos, der ville fremtvinge et regimeskifte i retning af en prorussisk præsident".

I takt med at privatejede – og profitdrevne – techgiganter i dag er så afgørende for forsvaret af det 21. århundredes nationalstat, ser vi også en forrykkelse af magtbalancen mellem offentlig og privat. Men hvor Vestens nationalstater anføres af demokratisk valgte ledere, der står til ansvar over for deres befolkninger, så står techgiganternes topchefer primært til ansvar over for deres aktionærer og ejere.

Så hvilke værdier driver dem? Hvad er det for et regnestykke, der har fået Microsoft til at poste 239 millioner dollar – langt over en milliard danske kroner – til at melde sig ind på den ene side af en storkrig?

Og hvad er det egentlig for en udvikling, der drives frem, når techgiganter på den måde gør sig til krigsførende virksomheder? Hvad hvis Kinas techgiganter gør det samme? Når man spørger techgiganterne, taler de i reglen rundt om spørgsmålene: Det afhænger af situationen. De stiller sig på 'det sikre internets' side. De bekender sig til kampen mod den misinformation, der er en anden del af cyberkrigens våbenarsenal. Ikke mindst i Rusland har den tidligere sovjetiske efterretningstjeneste KGB (i dag FSB) mange års erfaring med påvirkningskampagner, som den nu kombinerer med sociale medier som Twitter, Facebook og TikTok.

Men risikoen ved 'krigsførende' techgiganter, der melder sig ind på den ene side af militære konflikter, er, at vi ender et sted, hvor mange ikke ville være: I en situation, hvor techgiganterne opgiver at være globale virksomheder, men i stedet opbygger hver deres digitale parallelverden. Én i Kina, én i USA og én i… ja, det må tiden vise.

Føromtalte Ian Bremmer stillede det for nylig således op: "Hvis det digitale rum bliver den vigtigste arena for stormagtsrivalisering,

Foto: Artem Kniaz / Unsplash

og hvis statens magt i forhold til techvirksomhederne eroderer, lige som det er sket i de seneste ti år, så vil den digitale verdensorden i sig selv blive den nye dominerende globale verdensorden".

Den slags ting spekulerede Oleg Roginskyj næppe over, da han en dag i februar blev bedt om at mobilisere sit netværk for at hjælpe sit hjemland. Indimellem foregår den globale udvikling helt som filosoffen Søren Kierkegaard har beskrevet livet: Det skal leves forlæns, men må forstås baglæns.

Michael Jarlner er international kommentator og techredaktør ved dagbladet Politiken samt medlem af Det Udenrigspolitiske Selskabs bestyrelse.