Redaktionelt forord

MARTIN MARCUSSEN
Ansvarshavende redaktør

Center for Cybersecurity, der er placeret hos Forsvarets Efterretningstjeneste, lægger i deres årlige trusselvurdering ikke fingrene imellem: "Truslen fra cyberkriminalitet er **MEGET HØJ**", slås fast med versaler i fed skrift. Cyberkriminalitet er en samlebetegnelse for handlinger, hvor hackere bruger cyberangreb til at begå kriminalitet, der er motiveret af et ønske om økonomisk berigelse. Også truslen fra cyberspionage er **MEGET HØJ**, konkluderer centeret. Det betyder konkret, at det er meget sandsynligt, at danske myndigheder og virksomheder vil blive udsat for forsøg på cyberspionage inden for de næste to år. Truslen er især rettet mod myndigheder, som arbejder med udenrigs- og sikkerhedspolitik samt virksomheder, der besidder en viden, som andre stater har en interesse i. Helt konkret meddeler udenrigstjenesterne i Østrig, Tyskland, Italien, Kroatien og Belgien, at de har været udsat for omfattende cyberangreb på det seneste, og at statslige aktører kan have stået bag disse angreb. Særlig Rusland og Kina er således kommet i søgelyset som stater, der i særlig stor udstrækning benytter sig af cyberspionage.

Trusselsvurderingen konkluderer samtidig, at sandsynligheden for, at Danmark udsættes for destruktive cyberangreb – det vil sige angreb, der fører til omfattende datadestruktion, fysisk ødelæggelse eller ligefrem dødsfald - er **LAV**. Sådanne angreb har godt nok fundet sted i vore nærområder – på hospitaler i Storbritannien, Tv-stationer i Georgien og elselskaber i Ukraine – og godt nok måtte A.P. Møller-Mærsk tage et tab på mellem 1,6 og 1,9 milliarder kroner i 2017 og Demant et tab på op mod kr. 650 millioner i 2019 som et resultatet af destruktive cyberangreb – men alligevel identificerer Forsvarets Efterretningstjeneste kun en lav risiko på den front.

Det samme gør sig gældende for den såkaldte cyberaktivisme, hvor formålet er at gribe ind i en politisk proces eller at gøre opmærksom på en enkeltsag. Også her er trusselsvurderingen **LAV**. Cyberaktivisme kan eksempelvis tage form af kampagner, hvor der spredes falsk information og propaganda. I vore nabolande, som eksempelvis Litauen, kæmper man løbende med russiske påvirkningskampagner, der har til formål at skabe splittelse mellem befolkningsgrupper i landet og til Litauens allierede. Mest kendt er selvfølgelig den læk af informationer, bl.a. e-mails, som Demokraternes Nationale Komité blev udsat for forud for det amerikanske præsidentvalg i 2016. Men heller ikke dette synes at bekymre Center for Cybersecurity. Herhjemme blev Udenrigsministeriet udsat for en slags cyberaktivisme i 2017 da en såkaldt pro-tyrkisk gruppe

valgte at oversvømme ministeriets hjemmeside med trafik i forlængelse af endnu en debat om muhammedtegninger.

Selvom trusselsvurderingen siger tingene ligeud, er der også forhold i relation til cybersikkerhed, der ikke diskuteres så eksplicit. Dette temanummer af Økonomi & Politik, der er redigeret af Tobias Liebetrau ved Center for Militære Studier, Københavns Universitet, ønsker at kaste lys på nogle af de forhold i relation til cybersikkerhedsfænomenet, som vi enten ikke har den store viden om, eller som danske offentlige myndigheder ikke kan tale åbent om. For eksempel taler vi ofte om, at Kina og Rusland meget aktivt engagerer sig i alle former for aggressiv adfærd på cyberområdet. Vi taler knap så ofte om, at vore allertætteste allierede – som eksempelvis USA og Storbritannien – også er helt fremme på området. I både USA og Storbritannien fremfører man det synspunkt, at deres cyberadfærd har et præventivt formål og at deres gentagne forsøg på at forhindre lande som Iran, Rusland og Kina i at begå cyberspionage, -kriminalitet og –angreb kan retfærdiggøre, at man også samtidig helt eksplicit træder andre landes suverænitet under fode. Det er netop et forhold som dette, der gør, at de vestlige lande ikke virker troværdige i deres forsøg på at udvikle et fælles internationalt normsæt på området.

Vi taler også en del om, at vi som et lille land er særdeles sårbare i forhold til andre landes cyberadfærd, men vi taler ikke så meget om, at selv vore nærmeste allierede angiveligt deltager i cyberspionage på dansk grund, og da slet ikke om, at vi selv anvender cyberspionage som en del af vores generelle informationsindhentning i udlandet. Faktisk kan man sige, at cyberdomænet giver små stater som Danmark flere nye muligheder i udenrigs- og sikkerhedspolitikken. Cyberaktivitet kræver nemlig som udgangspunkt ikke dyrt materiel og koster typisk ikke menneskeliv. I dag tilbyder både universiteter og det danske forsvar unge mennesker en uddannelse i hacking – i nationens tjeneste.

Endelig gemmer der sig en vigtig diskussion, der vedrører spørgsmålet om, hvorvidt vore politikere og den brede befolkning nogensinde kan opnå en bare tilnærmelsesvis tilstrækkelig indsigt i et felt, hvor den teknologiske udvikling er kolossal hurtig med kvanteteknologien og kunstig intelligens som det næste udviklingstrin, og hvor der helt rutinemæssigt tales om ransomware-angreb, phishing-mails, VPN-løsninger og DDoS-angreb. På globalt plan er der en betydelig efterspørgsel efter eksperter, der kan hitte rede i de muligheder og gennemgribende udfordringer, der er forbundet med cybersikkerhedsfeltet. Det er eksperternes paradis – især fordi der på området endnu ikke eksisterer nogle professionsstandarder, der præciserer, hvad der er god henholdsvis dårlig praksis. I den situation er det utrygt at vide, at det er disse såkaldte eksperter, der grundlæggende definerer de præmisser som vore politikkere handler på grundlag af. Der er **MEGET HØJ** risiko for, at der styres i blinde.