Cybersikkerhed omdefinerer EU's indre marked

Af **Tobias Liebetrau**

EU's cybersikkerhedspolitik skal styrke det indre marked. Samtidig er den en betydelig drivkraft for yderligere europæisk integration. Fra at markedet var et middel til at skabe fred og sikkerhed, er sikkerhed i stigende grad blevet et middel til at beskytte og udvide det nu digitale indre marked.

Siden Anden Verdenskrig har sikkerhed primært været forbundet med national sikkerhed, nødvendighed og *raison d'état*. Det europæiske samarbejde er grundlagt på denne logik. Oprindeligt blev den tværnationale organisering af europæiske markeder og industrier betragtet som et middel til at sikre fred efter Anden Verdenskrig. Dette foreskrev en klar deling af arbejdsområder, ansvar og autoritet. Sikkerhed var et privilegium for medlemsstaterne, mens det europæiske samarbejde skulle fremme markedsintegration og indbyrdes afhængighed. Artikel 4, stk. 2, i traktaten om Den Europæiske Union bestemmer klart, at national sikkerhed er et medlemsstatsprivilegium:

"Den [EU] respekterer deres [medlemsstaternes] centrale statslige funktioner, herunder sikring af statens territoriale integritet, opretholdelse af lov og orden samt beskyttelse af den nationale sikkerhed. Navnlig forbliver den nationale sikkerhed den enkelte medlemsstats eneansvar."

Traktatteksten har imidlertid ikke forhindret EU i at engagere sig i cybersikkerhedspolitik. Den dobbeltsidede digitale udvikling har nemlig ændret den traditionelle europæiske sikkerhedsgeografi og -logik.

"Europa er endnu ikke godt rustet, når det kommer til cyberangreb. Cyberangreb kan være farligere for demokratiers og økonomiers stabilitet end våben og kampvogne. Alene sidste år var der flere end 4.000

Tobias Liebetrau er postdoc ved Center for Militære Studier, Institut for Statskundskab, Københavns Universitet. Han forsker i dansk og europæisk cybersikkerhed.

'*ransomware*'-angreb om dagen, og 80 procent af europæiske virksomheder oplevede mindst én utilsigtet hændelse relateret til cybersikkerhed. Cyberangreb kender inden grænser, og ingen er immune (oversat fra engelsk, red.)"

Ordene er Jean-Claude Junckers. De stammer fra den nu tidligere kommissionsformands State of the Union-tale fra 2017. I talen understregede Juncker behovet for bedre beskyttelse af europæere i den digitale tidsalder og gjorde cybersikkerhed til et prioriteret indsatsområde for unionen. Junckers bemærkning er især bemærkelsesværdig af to grunde. For det første sætter den spørgsmålstegn ved de traditionelle rumlige og funktionelle betingelser for europæisk sikkerhedspolitik, når cybersikkerhedstrusler ingen grænser har og ingen er immune. For det andet placerer Juncker cybertruslen i en eksistentiel ramme, når han fremhæver, at cyberangreb kan være mere farlig for stabiliteten af demokratier og økonomier end pistoler og tanks. Det åbner et potentielt et rum for og legitimerer yderligere EU-indsats på cybersikkerhedsområdet. Junckers bemærkning rejser grundlæggende spørgsmål om, hvad der skal sikres af hvem og hvordan. Talen berører dermed kernen af europæisk sikkerhedspolitik og udfordrer den traditionelle fordeling af sikkerhedspolitisk autoritet og ansvar i Europa.

EU har siden 1980'erne beskrevet digitaliseringen af de europæiske samfund som uundgåelig. Samtidig er digitaliseringen blevet akkompagneret af lovord, der kredser om fortsat velstand, vækst og grænseoverskridende samarbejde. Med udviklingen følger imidlertid et dilemma:

Et af mest løfterige samfundsudviklingstræk – øget digitalisering og teknologisk udvikling – bliver nemlig tillige betragtet som én af de største sikkerhedstrusler mod vores samfund og levevis. Digitalisering er altså et janushovedfænomen. Introduktionen af nye digitale teknologier er på den ene side ledsaget af politiske, sociale og økonomiske muligheder og på den anden af usikkerheder og sårbarheder.

Digitaliseringen af de europæiske samfund har været en væsentlig drivkraft i den europæiske integration siden 1980'erne.

Mulighedsrummet for europæisk sikkerhedspolitik er blevet ændret som følge af den tiltagende digitalisering. Gennem sammenkædning af digitalisering, marked og sikkerhed kan EU drage fordel af disse ændringer. EU har med succes formået at konstruere digitalisering og cybersikkerhed som centrale elementer i unionens funktion og kompetence inden for det indre marked.

Det, vi ser i dag, er et EU, der fører cybersikkerhedspolitik gennem sit indre markedsmandat. Det betyder, at autoriteten og ansvaret for europæisk cybersikkerhedspolitik bliver markedsliggjort, privatiseret og pluraliseret. EU's cybersikkerhedspolitik er således med til at omformulere og genforhandle de t sikkerhedspolitiske autoritets- og ansvarsforhold mellem EU, medlemsstater og private virksomheder. I EU-sammenhæng er cy-

bersikkerhedspolitik derfor uadskillelig fra forhandlinger om samt kampe over, hvad cybersikkerhed er, og hvor den europæiske sikkerhedspolitiske autoritet og ansvar bør være placeret.

Marked versus sikkerhed

Digitalisering bliver ofte fremhævet som ét af de mest lovende økonomiske og sociale udviklingstræk ved moderne samfund, når der bliver holdt politiske skåltaler og udgivet strategier og visionspapirer på glittet papir. Det gør sig også gældende i EU-regi.

Digitaliseringen af de europæiske samfund har været en væsentlig drivkraft i den europæiske integration siden 1980'erne. EU har slået på, at digitalt europæisk samarbejde kunne skabe modvægt til først USA's og Japans digitale dominans og i dag USA's og Kinas ditto. Samtidig har løftet om europæisk digitalisering gået hånd i hånd med et løfte om øget økonomisk vækst og flere arbejdspladser. En udvikling, der kulminerende med, at EU i 2015 præsenterede sin strategi for det fremtrædende digitale indre marked.

Cybersikkerhed er i dag blandt EU's politiske kerneprioriteter.

Strategien understreger, at digitalisering samt informations- og kommunikationsteknologi (IKT) danner et væsentligt grundlag for europæisk økonomisk udvikling og transformerer vores liv og samfund. Senest har den nye kommissionsforperson Ursula von der Leyen slået fast, at digitalisering er et gennemgående og højt prioriteret område for hele Kommissionen.

Samtidig er det i dag en indiskutabel og indlysende sandhed, at cybersikkerhed er fremherskende på de sikkerhedspolitiske dagsordener og i de militærbudgetterne verden over. Den massive spredning af IKT gør os sårbare, hvorfor den digitale udvikling påvirker trusselsbilledet negativt. Fremvæksten og spredningen af digitale teknologier udfordrer endvidere de traditionelle grænser for statens sikkerhedspolitiske autoritet og ansvar som følge af deres grænseoverskridende, komplekse og dynamiske karakter.

Cybersikkerhed er uløseligt forbundet med en stribe forskelligartede aktører, da fleste digitale teknologier, platforme og infrastrukturer er privatejede, -drevne og -udviklede. EU's politik på området for digital sikkerhed havde ikke en klar strategisk retning i 1990'erne, men bestod af løsrevne hensigtserklæringer, samarbejder og reguleringer. Først i 2001 spillede Kommissionen ud med en samlet policy-tilgang til netværks- og informationssikkerhed, der var drevet af unionens mandat på det indre marked.

EU's digitale sikkerhedspolitik forblev spagfærdig i 00'erne, men udviklede sig dog op gennem årtiet. Tiltag på området for netværks- og informationssikkerhed blev blandt andet kædet sammen med initiativer inden for beskyttelse af kritisk infrastruktur, der oplevede et boom i kølvandet på 11. september 2001, samt bomberne i Madrid (2004) og London (2005). Desuden blev EU i 2004 en institution rigere, da det europæiske agentur for netværks- og informationssikkerhed (ENISA) blev oprettet. ENISA blev født som en "første

søjle"-institution (fællesskabssøjlen), hvorfor ENISAs mandat og mission er grundlagt på det indre marked. Mod slutningen af 00'erne begyndte cybersikkerhed at få opmærksomhed i den brede offentlighed og politiske debat. Ikke mindst som følge af cyberangrebene mod Estland i 2007 samt Stuxnet-cyberangrebet mod de iranske atomreaktorer i 2010. Dermed blev det digitale sikkerhedsdilemma sat på spidsen.

Cybersikkerhed som kerneprioritet

I 2013 præsenterede EU sin første egentlige cybersikkerhedsstrategi. Strategien blev fulgt op af den første harmoniserende cybersikkerhedslovgivning, da netværks- og informationssikkerhedsdirektivet (NIS-direktivet) blev vedtaget i 2016. Strategien skabte en fælles tilgang til en række forskellige politikområder, herunder beskyttelse af kritisk infrastruktur, netværks- og informationsikkerhed samt cyberkriminalitet, der tidligere var blevet behandlet hver for sig. Strategien konsoliderede dermed EU's tilgang til cybersikkerhed.

EU og dets medlemsstater må gentænke og afveje en række forhold vedrørende politik, sikkerhed og marked.

Det skyldes ikke mindst, at strategien var et resultatet af en kombineret indsats, der inkluderede daværende kommissær for indenrigsanliggender Cecilia Malmström, EU's repræsentant for den fælles udenrigs- og sikkerhedspolitik Catherine Ashton og kommissær for digitale anliggender Neelie Kroes samt input fra kommissæren for retlige anliggender og EU-borgerskab Viviane Reding. Et samarbejde og en koordinering, der i vidt omfang var blevet muliggjort af afskaffelsen af søjlesystemet som følge af Lissabontraktatens vedtagelse. Til trods for ambitionen om konsistens og koordination fremstår strategiens tre søjler – kritisk beskyttelse af informationsinfrastruktur, cyberkriminalitet og cyberforsvar – fortsat forholdsvis adskilte.

Det ændrer dog ikke på, at strategien har været afgørende for at knytte digitalisering samt udvikling og understøttelse af det indre marked yderligere sammen med sikkerhed. Etableringen af en sikkerhedstrussel og et cybersikkerhedsansvar, der rækker ud over den enkelte medlemsstat og dennes grænser, var med til at gøre det muligt for EU at knytte integration af det indre marked endnu tættere til cybersikkerhed. En udvikling, der senere er blevet fulgt op i Europa-Kommissionens cybersikkerhedspakke fra 2017, som præsenterede en række nye initiativer til yderligere at udbygge og styrke EU's cyber-modstandsdygtighed, afskrækkelse og forsvarsindsats, samt von der Leyens foreløbige politiske udmeldinger. Det understreger, at cybersikkerhed i dag er blandt EU's politiske kerneprioriteter. Det skyldes ikke mindst, at cybersikkerhedselementer er blevet integreret på tværs af andre EU-politikker. Cybersikkerhed optræder i særdeleshed som en uundværlig del af etableringen af det digitale indre markedsprojekt, som Europa-Kommissionen beskrev i 2015. Det blev eksempelvis

EU har derimod været nødt til - og er i vidt omfang lykkedes med - at placere sig oven på og ved siden af sine medlemslande.

understreget i EU's midtvejsrevision af strategien for det digitale indre marked i maj 2017, hvor Kommissionen identificerede håndtering af cybersikkerhedstrusler som ét af de tre vigtigste indsatsområder for unionen de kommende år. EU's opprioritering af cybersikkerhedsområdet er imidlertid ikke uden knaster.

En paradoksal balance

Uløseligt knyttet sammen med den tiltagende digitalisering har EU etableret cybersikkerhed som et europæisk problem, der kræver transnationale europæiske løsninger. Det, vi ser i dag, er et EU, der i stigende grad fører cybersikkerhedspolitik gennem sit indre markedsmandat. Kort sagt plejede det indre marked at være et middel til at skabe fred. I dag er cybersikkerhed blevet et middel til at beskytte og udvide markedet. Cybersikkerhed er blevet en drivkraft for yderligere integration og harmonisering af det indre marked med økonomisk vækst for øje.

Traditionelt har nye politiske enheder og autoriteter fortrængt tidligere herskere. EU har derimod været nødt til – og er i vidt omfang lykkedes med – at placere sig oven på og ved siden af sine medlemslande. Navigerer omhyggeligt mellem dem. EU er altså en innovation inden for sikkerhedspolitik i den forstand, at unionen sameksisterer med sine forgængere – medlemslandene. EU skal dog tolerere og understøtte den nationale sikkerhedspolitiske overmyndighed. Også når unionen praktiserer cybersikkerhed gennem det indre marked. Det betyder, at EU's cybersikkerhedspolitiske ageren er begrænset. Medlemslandene er fortsat sig selv nærmest, når det kommer til for eksempel den militære og efterretningsmæssige del cybersikkerhedsarbejdet.

Ovenstående taler direkte ind i det beskrevne dilemma vedrørende sammenhængen mellem forsat digitalisering og usikkerhed. Når fortsat digitalisering lover fremtidig velstand og vækst, så bliver det et anliggende for EU's indre markedsprojekt. Når fortsat digitalisering samtidig skaber flere sårbarheder og usikkerheder, så bliver cybersikkerhed et af de mest fremtrædende nationale sikkerhedsspørgsmål. Det skaber et digitalt indre marked-sikkerhedsnexus, som udfordrer den oprindelige fordeling af arbejde, autoritet og ansvar mellem EU, dets medlemsstater og private virksomheder.

Det er et dilemmafyldt nexus, som tvinger EU og dets medlemsstater til at gentænke og afveje en række forhold vedrørende politik, sikkerhed og marked. Forhold, der på paradoksalvis indeholder løfter om både politiske, økonomiske og demokratiske udfordringer og muligheder. Digitalisering er et centralt omdrejningspunkt for Ursula von der Leyens kommission. Fremtiden vil vise, hvordan det påvirker forholdet mellem politik, sikkerhed og marked under hende.