Essay

Den digitale sårbarhed: Teknologivirksomheder, geopolitik og magtforskydninger

Af Tobias Liebetrau, Forsker,
Institut for Statskundskab, Københavns Universitet

Rebecca Adler-Nissen, Professor,
Institut for Statskundskab, Københavns Universitet

Magtudredningen 2.0

Intensiveret stormagtskonkurrence mellem USA og Kina, krig i Europa, pres på den liberale verdensorden, klimaforandringer, globale økonomiske forskydninger og strategisk udnyttelse af forsyningskæder og handelspolitik betyder, at Danmarks sikkerhedspolitiske virkelighed er blevet grundlæggende forandret de seneste år (Den sikkerhedspolitiske analysegruppe 2022; Regeringen 2023).

Den nye virkelighed er stærkt påvirket af den rivende udvikling og anvendelse af nye teknologier og infrastrukturer til både civile og militære formål. Teknologiudvikling er de seneste år gået fra at foregå i et relativt samarbejdende og globaliseret marked til i dag at være et centralt omdrejningspunkt i en mere konfliktpræget og rivaliserende verdenspolitik (Breitenbauch og Liebetrau 2021). Det gælder ikke mindst på det digitale område med den fjerde industrielle revolution – integrationen af vores digitale og fysiske verden via udbredelse af 5G- og 6G-netværk, tingenes internet, big data-analyse, kunstig intelligens, robotteknologi og kvanteteknologi. Den har medvirket til at digitale teknologier er gået fra primært at være et markedsspørgsmål knyttet til private virksomheders udvikling af kommercielle løsninger til at blive en global økonomisk, værdimæssig og sikkerhedspolitisk kampplads (Udenrigsministeriet 2024). I dag er evnen til at udnytte og kontrollere digitale teknologier og infrastrukturer blevet en afgørende strategisk faktor i international politik. Den digitale teknologiudvikling er en del af den politiske, militære og økonomiske rivalisering mellem lande og påvirker relationer mellem stat, marked og civilsamfund i hvert enkelt land. Digitale teknologiers tiltagende internationale politiske betydning medfører, at sikkerheds- og forsvarspolitik bliver filtret stadigt tættere sammen med økonomi-, industri-, erhvervs-, innovations- og forskningspolitik og vice-versa.

I enhver analyse af geopolitiske forskydninger i det 21. århundrede er den digitale teknologiske udvikling derfor fundamental. I dette essay kaster vi lys over, hvordan den digitale teknologiske udvikling påvirker globale geopolitiske forskydninger, Danmarks sikkerhedspolitiske positionering og magtbalancen mellem danske institutioner og internationale aktører. Det gør vi ved at undersøge, hvordan digitaliseringen af Danmark både er en sårbarhed og en styrke.

Essayet falder i fem dele. Vi starter med at udfolde, hvad vi kalder et det digitale sårbarhedsparadoks. Derefter undersøger vi paradoksets konsekvenser ved at præsentere tre hypoteser om den geopolitiske betydning af digitalisering:

- **Hypotese 1:** Digitale teknologier er et tveægget svær for den liberale verdensorden.
- **Hypotese 2:** Digital teknologi er afgørende for fremtidens sikkerhed og militære kampplads.
- **Hypotese 3:** Teknologivirksomheder har overtaget store dele af statens rolle og opgaver.

Slutteligt behandler vi konsekvenser for Danmarks sikkerhedspolitiske positionering og magtbalancen mellem danske institutioner og regionale og internationale aktører, herunder særligt på det digitale teknologiområde. Undersøgelsen af det digitale sårbarhedsparadoks kobler sig dermed direkte til to af magtudredningens centrale temaer om sikkerhedspolitiske forskydninger i det 21. århundrede og tech-giganternes magt og indflydelse på det danske demokrati. Essayet tydeliggør, hvordan de to temaer griber ind i og påvirker hinanden.

Det digitale sårbarhedsparadoks

Digitalisering er i årtier blevet opfattet som en uundgåelig udvikling, der i Danmark primært har kredset om ord som vækst, velstand og velfærd. I de senere år er opmærksomheden på digitaliseringens skyggesider imidlertid taget til (Regeringens ekspertgruppe om tech-giganter 2023). I kontekst af dette essay fokuserer vi på det, vi kalder det digitale sårbarhedsparadoks.

En af de mest løfterige samfundsudviklinger – øget digitalisering og digital teknologisk udvikling – bliver i stigende grad betragtet som en af de største sikkerhedstrusler mod vores samfund og levevis. Cybertruslen bliver i dag regnet for en af de absolut største sikkerhedstrusler. Det gælder i et nationalt sikkerhedspolitisk perspektiv, i erhvervslivet såvel som for den enkelte borger (Jacobsen og Liebetrau 2022). Udnyttelse af digitale teknologier bliver set som en garant for sikkerhed og økonomisk fremskridt i Danmark og i Vesten, men samtidig udgør den en af de største sårbarbarheder i vores samfund

(Adler-Nissen & Eggeling 2024; Bradford 2023; Farrel and Newman 2019, 2023; Liebetrau 2023). Det kommer til udtryk f.eks. ved striden om kinesiske Huaweis involvering i udrulningen af 5G-netværk i Vesten, kampen om produktionen og anvendelsen af mikrochips og kapløbet om udvikling af kunstig intelligens til brug for civile og militære formål.

Digitalisering kan derfor betragtes som et tosidet fænomen. Introduktionen af nye digitale teknologier er på den ene side ledsaget af politiske, sociale og økonomiske styrker og muligheder og på den anden af usikkerheder, sårbarheder og risici. De danske myndigheder, virksomheder og borgere er alle underlagt det digitale sårbarhedsparadoks. Det er ikke kun Danmark, der oplever denne tosidede udvikling, det gør langt de fleste lande i verden.

Digitale teknologier er blevet et tveægget sværd for den liberale verdensorden

Den geopolitiske betydning af digitalisering og digital teknologisk udvikling kan ikke forstås uden blik for den globale kontekst. På den internationale politiske scene har digital teknologiudvikling det seneste årti bevæget sig fra at blive opfattet som et fænomen, der primært var forbundet økonomisk vækst, globalisering og en styrket liberal verdensorden – og en styrkelse af liberale demokratier – til i stigende grad at blive opfattet som en afgørende strategisk konkurrenceparameter, der ikke bare påvirker den internationale politiske, militære og økonomiske konkurrence og de indenrigspolitiske relationer mellem staten, virksomhederne og borgerne, men som også udfordrer selve ideen om globalisering, interdependens og liberal verdensorden. Det har f.eks. vist sig, at digitale teknologier og platforme er særdeles effektive værktøjer for autoritære stater både hjemme og ude ift. systematisk overvågning af individer og kontrol af den offentlige debat (Ghodes 2024).

Med skiftet fra en relativt samarbejdende verdenspolitik præget af globalisering som økonomisk integration til en relativt konkurrencepræget verdenspolitik med øget fokus på uafhængighed i forsynings- og produktionskæder er investeringer i og kontrol med fremtidens digitale teknologier blevet kædet samme med et markant statsligt fokus på statslig rivalisering og digital suverænitet. Her skiller det digitale teknologikapløb

mellem Kina og USA, der kredser om, hvem der leder udviklingen af en række kritiske digitale teknologier som kvanteteknologi, kunstig intelligens og mikrochips, sig ud. Den digitale teknologiske rivalisering mellem USA og Kina er blevet kaldt en teknologikrig, hvis ultimative mål er global digital teknologisk dominans. Men USA og Kina er ikke alene om at fokusere på digitale teknologier.

De seneste år har EU styrket sit fokus på at mindske unionens og medlemslandenes sårbarheder og afhængigheder relateret til udenlandske tech-giganter (Adler-Nissen & Eggeling 2024; Liebetrau 2022). Problematikkerne med digitale teknologier er i sagens natur grænse- overskridende. Skal regulering have reel effekt, er det på den internationale spillebane, de store slag skal slås. For Danmark og danske politikere er EU det primære sted at udvikle fælles spilleregler og håndhæve den lovgivning, der allerede er på plads. EU er i dag en global standardsætter, når det gælder regler, der sætter hegnspæle for den digitale teknologi og beskytter menneskerettigheder og den demokratiske offentlighed. Således er tech-giganter allerede i dag underlagt EU-regulering på en række områder, herunder inden for databeskyttelses, og der er flere EU-krav på vej. Kunstig intelligens og digitale tjenester reguleres dels gennem kunstig intelligens-forordningen, dels gennem Digital Services Act, Digital Markets Act og GDPR. De enorme bøder, som Europa-Kommissionen har udstedt til en række teknologivirksomheder såsom Google og Apple, vidner om, at EU også har musklerne til at håndhæve lovgivningen, hvis viljen er der (Regeringens ekspertgruppe om tech-giganter 2023).

USA, Kina og EU har øget deres investeringer i forskning og innovation relateret til udvikling af digitale teknologier og infrastrukturer med det formål at skabe forudsætninger for yderligere økonomisk vækst, større uafhængighed og styrket kontrol med digital teknologiudvikling og anvendelse. Et tydeligt eksempel på den udvikling er konkurrencen om produktion af og adgang til mikrochips. Konkurrencen om at sikre sig tilstrækkelig forsyning af de små halvledere, der er afgørende for både økonomisk og militær sikkerhed, har igangsat et veritabelt statsstøttekapløb mellem USA og Kina suppleret af EU, Japan, Sydkorea, Taiwan og Indien. Senest oprettede Kina sin tredje statsstøttede investeringsfond for at styrke landets halvlederindustri. Fonden er registreret med en startkapital på 344 milliarder yuan eller 47,5 mia. dollar

(Reuters 2024). I 2023 trådte forordningen om europæiske mikrochips i kraft. Den vil mobilisere 43 mia. euro til at støtte forskning og udvikling inden for mikrochipsektoren i EU, kanalisere statsstøtte og private investeringer til virksomheder og udvikle et overvågnings- og krisestyringssystem, der kan pålægge mikrochipvirksomheder at reservere dele af deres produktion til EU-virksomheder med akut behov. Kommissionen lancerede i 2023 desuden Critical Raw Materials Act, som skal sikre EU's adgang til en sikker, økonomisk overkommelig og bæredygtig forsyning af kritiske råstoffer. Endelig ser vi i stigende grad, at investeringsscreeninger og eksportkontrol bliver brugt verden over til at sikre forsyningskæder og kritisk infrastruktur på den ene side og stække andre staters udvikling og anvendelse af digitale teknologier på den anden.

Det er derfor vores hypotese, at vi befinder os i en situation, hvor udviklingen af og konkurrencen om digitale teknologier er blevet et tveægget sværd for den liberale verdensorden. Konkurrencen om udvikling og anvendelse af digitale teknologier vil i stigende grad udfordre økonomisk integration, bekæmpelse af klimaforandringer, sundhedssamarbejde, kulturel udveksling og andre globale dagsordener, der fortsat er hjørnesten i verdenspolitikken.

Digital teknologi er afgørende for fremtidens sikkerhed og militære kampplads

Konkurrence om udviklingen af militærteknologi har altid været et væsentligt aspekt af international sikkerhedspolitik. Teknologiske fremskridt er længe blevet opfattet som afgørende for militær slagkraft og dominans på kamppladsen. Vender vi blikket mod krigen i Ukraine, så har den vist, hvordan digital innovation og transformation har været kampafgørende, herunder ved brug af droner, kunstig intelligens og satellitter. For at forstå den geopolitiske betydning af digitalisering er det derfor afgørende at zoome ind på den dominerende ide, at teknologier som kunstig intelligens, big data-analyse og kvanteteknologi har potentiale til grundlæggende at forandre vores måde at forstå og føre krig, herunder hvordan digitale teknologiske landvindinger bliver omsat til og anvendt i en militær kontekst.

Disse spørgsmål udgør grundelementet i den amerikanske Third Offset Strategy (2016), der skal drive revolutionerende militære teknologier frem og sikre deres integration i det amerikanske militær. Med strategien sigter amerikanerne på at minimere betydningen af global teknologispredning og fastholde USA's position som verdens førende militære magt. Senest har Biden-regeringens strategier for national sikkerhed (2022), forsvar (2022), forsvarsindustri (2023), nationalt forsvar, videnskab og teknologi (2023) og internationalt cyberspace og digital policy (2024) på forskellig vis understreget vigtigheden af at fastholde en dominerende teknologiposition. NATO og EU har ligeledes styrket deres fokus på disruptive, digitale teknologier. NATO har blandt andet etableret Defence Innovation Accelerator for the North Atlantic (DIANA) og NATO Innovation Fund (NIF). EU har etableret European Defence Fund (EDF) og European Defence Innovation Scheme (EUDIS).

USA, NATO og EU er ikke alene om at udvikle strategier og politikker, der tager hånd om digitale teknologiske landvindingers militære komponent. Sideløbende med arbejdet på at blive et globalt kraftcenter for højteknologisk udvikling har det kinesiske styre prioriteret at sikre en langsigtet og velfinansieret militærteknologisk udvikling, hvis sigte er at nå op på siden af USA i det militærteknologiske kapløb. Visionen for indsatsen er integreret samarbejde mellem militære myndigheder, civile virksomheder og forskningsmiljøer i en 'civil-militær fusion'.

Det styrkede fokus på nationale politikker og strategier for udvikling og håndtering af nye militære teknologier understreger, hvordan konkrete forsvarspolitiske tiltag og investeringer skal levere løsninger på langsigtede sikkerhedspolitiske udfordringer, der rækker væsentligt ud over umiddelbar afskrækkelse og krigsdeltagelse (Breitenbauch og Liebetrau 2021). Det gælder også for Danmark, hvor Forsvaret står over for et omfattende arbejde med og vanskelige beslutninger knyttet til monitorering, indkøb og implementering af væsensforskellige nye særligt digitale teknologier med stort forandringspotentiale for Forsvarets organisering, opgaveløsning og partnerskaber.

Det skaber en dobbelt sårbarhed. Den første angår spørgsmålet om, hvilke firmaer, der skal levere digitale teknologier, devices og infrastrukturer til det danske forsvar, som Forsvaret derved gør sig afhængige af. Valget af leverandører er også afgørende i

forhold til spørgsmål om skalérbarhed, integration, interoperabilitet, vedligeholdelse, redundans og opdateringsmuligheder, der alle er svært forudsigelige størrelser, når de bliver koblet med en så dynamisk teknologisk udvikling. Den anden angår det faktum, at digitalisering åbner en flanke af nye sårbarheder, der skal forsvares imod, hvilket skaber nye afhængigheder og dermed yderligere sårbarheder. Det rejser samlet et spørgsmål om, hvordan Danmark ønsker at digitalisere sit forsvar og sin kampkraft sammenholdt med de afhængigheder og sårbarheder, der nødvendigvis følger.

Teknologivirksomheder har overtaget store dele af statens rolle og opgaver

Samtidig gælder det i både Vesten og Kina, at det er privat virksomhedsdrevet forskning og innovation, der skal lede den digitale teknologiske udvikling – både civilt og militært – hvorfor private virksomheder er et centralt omdrejningspunkt for at forstå, hvordan digitalisering og digital teknologiudvikling påvirker geopolitiske udviklinger. I takt med at forskningen i og udviklingen af digitale teknologier i stigende grad overlades til private aktører, bliver staterne afhængige af samarbejdet med den private sektor. Det medfører i sig selv et tab af statslig kontrol, og det stiller krav om udvikling af nye former for offentlig-privat samarbejde. Derfor er private virksomheder og relationen mellem stat og marked et centralt omdrejningspunkt for at forstå Danmarks digitale sårbarhedsparadoks.

Den statslige styring og kontrol med den digitale teknologiudvikling er mindre i dag end i de sidste mange århundreder. Staternes mulighed for at styre, mobilisere og samarbejde med private, digitale teknologivirksomheder vil i stigende grad påvirke det geopolitiske landskab. Samtidig vil private virksomheders digitale teknologiudvikling få stadig større relevans for staters sikkerhedspolitik, forsvarsplanlægning og militærteknologisk innovation. Det gælder særligt på det digitale område, hvor private virksomheder i både USA, Kina og Europa driver den teknologiske udvikling og innovation. Igen ser vi, hvordan den geopolitiske betydning af digitalisering og private virksomheders nye rolle udvikler sig i et spændingsfelt mellem sikkerheds- og forsvarspolitik på den ene side og økonomi-, industri-, erhvervs-, innovations- og forskningspolitik på den anden side.

Politologen Ian Bremmer argumenterer for, at vi lever i en technopolar tid. Det vil sige en tid, hvor de store teknologivirksomheder konkurrerer med både hinanden og stater om geopolitisk indflydelse. Det er teknologivirksomhederne i stand til, da de kontrollerer store dele af samfundets digitale infrastruktur. De er simpelthen blivet en forudsætning for store dele af samfundets sammenhængskraft, økonomi og sikkerhed. Senest har Ruslands invasion af Ukraine sat en tyk streg under Ukraines dybe afhængighed af tech-giganter som Microsoft, Google, Amazon og Starlink. Desuden har krigen gjort det klart, at de store tech-virksomheder er blevet sikkerheds- og forsvarspolitiske aktører i egen ret, som også Danmark er dybt afhængig af - også i tilfælde af konflikt eller krig. Det er imidlertid usikkert, hvordan klassiske politiske og juridiske spørgsmål om kontrol, ansvar og gennemsigtighed tager sig ud, når store teknologivirksomheder står i forreste geled.

Konsekvenser for Danmark

Konkurrencen om udvikling og anvendelse af digitale teknologier vil være en væsentlig faktor i international, national og lokalpolitik i de kommende årtier. Digitalisering vil derfor vedblive at være en væsentlig prisme for at forstå geopolitiske udviklinger, hvad end de relaterer sig til den liberale verdensorden, stormagtskonkurrence, suverænitet, relationen mellem USA og Europa, fremtidens kampplads eller private teknologivirksomheders rolle. Danmarks fremtidige sikkerheds- og forsvarspolitiske samt økonomi-, industri-, erhvervs-, innovations- og forskningspolitiske handlerum er derfor uløseligt knyttet til den omsiggribende digitale teknologiudvikling. En digital teknologiudvikling vi i Danmark ikke har den store kontrol over. Det betyder, at det digitale sårbarhedsparadoks med stor sandsynlighed vil fortsætte med at vokse. Det understreger vigtigheden af, at diskussionen om digitale teknologiers geopolitiske betydning og betydning for dansk sikkerheds- og forsvarspolitik ikke bliver frakoblet den bredere samfundsmæssige debat om techgiganter og digitaliseringen.

Da der er en høj grad af usikkerhed forbundet med den digitale teknologiudvikling, er det umuligt at fastlægge de præcise muligheder og udfordringer, der følger af den. Det gælder således for det digitale teknologiområde, som det gælder for

sikkerhedspolitisk planlægning i øvrigt, at der skal tages hensyn til spørgsmålet om usikkerhed og risici. Men netop vores forventninger til digitale teknologier får betydelige konsekvenser for, hvordan vi indretter sikkerheds- og forsvarspolitikken. Danske sikkerheds- og forsvarspolitiske beslutningstagere, eksperter og medier skal være sig deres medproducerende rolle bevidst, når det kommer til de forudsigelser om fremtiden, som vi indretter vores sikkerheds- og forsvarspolitik efter.

En særlig udfordring i den forbindelse er, at emnet kan fremstå enten hyperspekulativt eller teknisk komplekst. Det skyldes ikke mindst magtforskydningen fra stater til globale teknologivirksomheder, som også indebærer en ekstrem videns-asymmetri: teknologivirksomheder, både danske og udenlandske, har langt højere udviklings- og forskningsbudgetter, er beskyttet af forretningshemmeligheder, fortrolighed og dygtige advokater og har monopol eller delt markedet mellem sig. Danske myndigheder har derfor svært ved at få pålidelig og solid viden om teknologierne og tiltrække og fastholde talent, der kan matche de private aktører. Det placerer de folkevalgte i kommunerne, regionerne og Folketinget og offentligheden som sådan i en underlegen situation, der gør det svært at sætte en selvstændig dagsorden eller overvåge retningen for udrulningen af digitale teknologier, herunder inden for sikkerheds- og forsvarspolitikken. Afhængigheden af virksomhedernes viden og innovation betyder, at der er begrænset demokratisk overblik og kontrol med digitale teknologier. Det er således primært i EU-regi, at folkevalgte har været i stand til at bruge EU's position som attraktivt marked til at stille reelle krav til virksomhederne og udfordre deres dominans.

Litteratur

Adler-Nissen, Rebecca og Eggeling, Kristin. A. (2024) The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X. *JCMS: Journal of Common Market Studies*, 62, 993–1011

Bradford, Anu (2023). Digital Empires: The Global Battle to Regulate Technology. New York. Oxford University Press.

Breitenbauch, Henrik og Liebetrau, Tobias (2021). Teknologikonkurrencen og dens implikationer for Danmark. DJØF Forlag og Center for Militære Studier.

Den Sikkerhedspolitiske Analysegruppe (2022). Dansk sikkerhed og forsvar frem mod 2035. København. Udenrigsministeriet.

Ghode, Anita (2024). Repression in the digital age. CPH Tech Policy Brief #8. The Queen Mary's Centre, Copenhagen Center for Social Data Science and Department of Political Science, University of Copenhagen.

Henry Farrell og Newman, Abraham L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security*, 44:1, 42–79.

Jacobsen, Jeppe Teglskov og Liebetrau, Tobias (2022). Cybertrusler – Det digitale samfunds skyggeside. København. DJØF Forlag.

Liebetrau, Tobias (2022). EU's teknologiske suverænitet: Mellem sikkerhed, marked og digitalisering. København. DJØF Forlag og Center for Militære Studier.

Liebetrau, Tobias (2023). Problematising EU Cybersecurity: Exploring How the Single Market Functions as a Security Practice. *JCMS: Journal of Common Market Studies*, 62, 705–724.

Regeringen (2023). Udenrigs- og sikkerhedspolitisk strategi 2023. København. Udenrigsministeriet.

Regeringens ekspertgruppe om tech-giganter (2023) Demokratisk kontrol med tech-giganternes forretningsmodeller. København. Erhvervsministeriet.

Regeringens ekspertgruppe om tech-giganter (2024). Grænser for tech-giganternes udvikling og anvendelse af kunstig intelligens. København. Erhvervsministeriet.

Reuters (2024). China sets up third fund with $47.5 bln to boost semiconductor sector. Beijing. May 27, 2024.

Udenrigsministeriet (2024). Udenrigsministeriets strategi for teknologisk diplomati. København. Udenrigsministeriet.

Magtudredningen 2.0: Essay-serien

En central del af Magtudredningen 2.0 er en bred inddragelse af forskere, hvis forskning kredser om et eller flere af magtudredningens temaer. Som led i projektet blev der i foråret 2024 afholdt 15 forskerworkshops, hvor oplægsholdere efterfølgende blev inviteret til at omarbejde deres oplæg til et essay. Essay-serien er forfatternes perspektiver på centrale tematikker for en dansk magtudredning og har forfatterne som afsender.

Dette essays er en del af tema 7.2 i Magtudredningen 2.0's forskningsplan: "Hvilke sikkerhedspolitiske forskydninger har der været i det 21. århundrede?"

Dette tema undersøger magtforskydninger mellem internationale aktører og det danske demokrati. Et første spørgsmål er på hvilke måder Danmarks beslutningsrum udvides og begrænses af forholdet til EU? Implementeringen af EU-beslutninger kan begrænse råderummet, men samtidigt kan EU-reguleringer udvide beslutningsrummet til at omfatte områder, hvor Danmark ellers ville stå med begrænset beslutningskompetence. Et andet spørgsmål er, hvordan de geopolitiske forskydninger påvirker Danmarks sikkerhedspolitiske orientering? Det gælder både generelle globaliseringstendenser og nye geopolitiske spændinger relateret til eksempelvis krigen i Ukraine, ressourcer i Arktis og Kinas stigende magt.