Tobias Liebetrau

EU'S TEKNOLOGISKE SUVERÆNITET: MELLEM SIKKERHED, MARKED OG DIGITALISERING

Danmarks strategiske udfordringer

DJØF FORLAG
I SAMARBEJDE MED
CENTER FOR MILITÆRE STUDIER

EU's teknologiske suverænitet: mellem sikkerhed, marked og digitalisering

Danmarks strategiske udfordringer

Tobias Liebetrau

EU's teknologiske suverænitet: mellem sikkerhed, marked og digitalisering

Danmarks strategiske udfordringer

Djøf forlag
i samarbejde med
Center for Militære Studier
2022

Tobias Liebetrau
EU's teknologiske suverænitet:
mellem sikkerhed, marked og digitalisering
Danmarks strategiske udfordringer

Publikationen er fagfællebedømt

Omslag: Morten Lehmkuhl

Print: Ecograf

Printed in Denmark 2022

ISBN 978-87-574-5388-1

Djøf Forlag
Gothersgade 137
1123 København K

Telefon: 39 13 55 00
e-mail: forlag@djoef.dk
www. djoef-forlag.dk

Redaktørens forord

Denne udgivelsesrække indeholder ny forskning om forsvars- og sikkerhedspolitiske emner, som er relevant for især danske beslutningstagere og den danske offentlighed.

Udgivelsesrækken viderefører de studier, der hidtil har været udgivet som CMS-rapporter. Den udgør dermed en væsentlig del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet og de politiske partier bag forsvarsforliget. Center for Militære Studier er omfattet af Københavns Universitets retningslinjer for forskningsbaseret myndighedsbetjening, herunder forskningsfrihed og armslængdeprincippet. Analyserne er udført uafhængigt og er ikke udtryk for holdninger hos den danske regering, det danske forsvar eller andre myndigheder.

Rapporterne fokuserer på at tilvejebringe akademisk holdbar og anvendelsesorienteret viden. Udgivelsesrækkens analyser har gennemgået ekstern fagfællebedømmelse, og alle analyser afsluttes med anbefalinger til danske beslutningstagere. Det er mit håb, at vi med disse udgivelser både kan informere og styrke dansk politikformulering såvel som den demokratiske debat om forsvars- og sikkerhedspolitik i Danmark.

Center for Militære Studier er et forskningscenter på Institut for Statskundskab, Københavns Universitet. På centret forskes der i sikkerheds- og forsvarspolitik samt militær strategi. Læs mere om centret, dets aktiviteter og andre udgivelser på: https://cms.polsci.ku.dk/.

København, april 2022
Kristian Søby Kristensen

Indholdsfortegnelse

Oversigt over figurer og tekstbokse

Resumé og anbefalinger

Bevægelsen fra en relativt samarbejdende verdenspolitik præget af globalisering til en mere konkurrencepræget verdenspolitik præget af stormagtsrivalisering betyder, at teknologiens relative betydning i international politik er stigende. Teknologisk suverænitet er derfor blevet en afgørende strategisk parameter for verdens lande, og den påvirker den globale politiske og økonomiske konkurrence samt de indenrigspolitiske relationer mellem staten, virksomhederne og borgerne.

Rapporten viser, at teknologisk suverænitet er et strategisk kernespørgsmål for EU og Danmark, hvis problemfelt knytter sig til relationen mellem sikkerhed, marked og digitalisering. Gennem en analyse af EU's politik for cybersikkerhed og kunstig intelligens (AI) viser rapporten, hvordan EU's sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske handlerum bliver koblet sammen, når teknologisk suverænitet bliver gjort til et centralt strategisk element. En sammenkobling, der påvirker EU's globale rolle og de sikkerheds- og forsvarspolitiske autoritets- og ansvarsforhold mellem EU, medlemsstaterne, NATO og USA. EU's markante fokus på teknologisk suverænitet er således en del af en dybereliggende proces, hvor EU forsøger at tilpasse unionens selvopfattelse og plads i verden.

For Danmark repræsenterer EU's satsning på teknologisk suverænitet en accentuering af de strategiske konsekvenser, der følger af den intensiverede stormagtsrivalisering og teknologikonkurrence. De sikkerheds- og forsvarspolitiske konsekvenser af EU's fokus på teknologisk suverænitet indgår dermed i en bredere stillingtagen, hvor Danmark bør afveje, hvordan EU's målsætning om teknologisk suverænitet bedst bliver udfoldet, så danske hensyn til sikkerhed, forsvar, frihedsrettigheder, diplomati, erhvervsliv, industri og innovation bedst bliver vægtet og varetaget. Det kræver strategiske overvejelser over, hvad en national teknologipolitik bør fokusere på, hvordan sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske overlap, muligheder og udfordringer udspiller sig, og hvordan forholdet mellem Danmark, EU, NATO og USA bliver påvirket.

Rapporten identificerer en række anbefalinger, der fremover kan støtte dansk strategisk tænkning, politisk styring og offentlig debat om EU's teknologiske suverænitet og dansk teknologipolitik.

En kortlægning af eksisterende initiativer i Danmark og EU, der behandler civile og militære aspekter af teknologipolitik, vil give regeringen og forvaltningen et samlet overblik over de nuværende sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske snitflader, overlap, udfordringer og muligheder, der er forbundet med teknologipolitik og teknologikonkurrence. En vurdering af, **hvordan EU's rolle i teknologikonkurrencen påvirker de sikkerheds- og forsvarspolitiske konsekvenser af det danske forsvarsforbehold**, vil kunne bidrage positivt dertil. Et samlet overblik vil styrke regeringens mulighed for at fastsætte langsigtede strategiske mål og navigere efter dem samt søsætte konkrete tiltag for at opnå dem.

I forlængelse heraf kan regeringen overveje at få udarbejdet en **strategi for teknologikonkurrence**, der vil kunne danne ramme om samarbejde i snitfladerne mellem forsvaret, det digitale Danmark, EU og NATO, samt **en militær teknologistrategi**, der kan udstikke en overordnet ambition og retning for udvikling, indkøb og anvendelse af banebrydende militære teknologier.

Forvaltningen bør yderligere styrke sit arbejde med at **koordinere og harmonisere de strategiske indsatser i arbejdet med teknologipolitik**. Arbejdet kan inkludere udvikling af indikatorer til at afdække og overvåge Danmarks nuværende og fremtidige teknologiske afhængigheder, udviklingsstadier for disruptive teknologier samt det strategiske arbejde med teknologisk suverænitet i EU, toneangivende EU-medlemslande, USA og Kina. Desuden bør de offentlige myndigheder indlede en **bred dialog med styrelser, regioner og kommuner om, hvordan de forholder sig til sikkerheds- og forsvarspolitiske implikationer af teknologipolitik**.

Slutteligt kan Folketinget overveje, **hvorvidt de eksisterende udvalgsstrukturer understøtter den nødvendige diskussion af tværgående teknologipolitiske spørgsmål**. I forlængelse heraf kan Folketinget overveje nedsættelse af et teknologiudvalg eller en delegation for teknologi.

Abstract and recommendations

The intensified great-power rivalry has increased the relative importance of control and development of technology in international politics. Technological sovereignty has consequently become a crucial strategic parameter, affecting global political, economic, and military competition, as well as domestic political relations between the state, private companies, and citizens.

This report demonstrates that technological sovereignty is a core strategic matter for the EU and Denmark, and it shows how technological sovereignty is intimately linked to the changing relationship between security, market, and digitalisation. By analysing EU policy on cybersecurity and artificial intelligence (AI), the report shows how the EU's security and defence policies intersect with its industrial, business, and innovation policies when technological sovereignty is made a key strategic goal. This policy entanglement affects the global role of the EU and the distribution of security and defence policy authority and responsibility between the EU, its member states, NATO, and the US. The EU's significant strategic focus on technological sovereignty is thus part of a process in which the EU fundamentally seeks to adjust its self-perception and role in world politics.

Seen from a Danish perspective, the EU's pledge to technological sovereignty accentuates the strategic consequences that follow from intensified great-power rivalry and global technology competition. The EU's agenda on technological sovereignty requires Denmark to consider how EU technological sovereignty can be pursued and nurtured with a view to Danish considerations on security, defence, diplomacy, individual rights, business, and industry. This demands Danish strategic considerations regarding the scope and content of a national technology policy, the opportunities and challenges arising from the growing intersections between security and defence policies on the one hand, and industrial, business, and innovation policies on the other, and the effects on the relationship between Denmark, the EU, NATO, and the US.

The report identifies a number of recommendations that support further Danish strategic thinking, development of governance tools, and public debate addressing the EU's technological sovereignty and Danish technology policy.

Denmark can **focus on strengthening the ways in which the EU's market-based initiatives in the field of technology are translated into security and defence policy gains**. In doing so, Denmark should strive to ensure that the efforts are communicated, coordinated, and harmonised in a way that reinforces relations with NATO and the US. Relatedly, Denmark can **encourage the EU to develop further policies and processes to identify and monitor strategically important technologies, systems, and sectors**. In this context, Denmark should encourage the EU to direct particular focus on the convergence and interdependence of digital technologies and infrastructures. In continuation of this, Denmark can urge the EU to further clarify the relationship between general and military technologies, including dual and multiple use technologies. Moreover, Denmark can push the EU to establish mechanisms that ensure the incorporation of geopolitical and geo-economic perspectives in the EU's digital policies, strategies, and partnerships, including responsible use of technology in military applications that comply with the liberal, rule-based international order.

In general, Denmark can work to **ensure that EU efforts to achieve technological sovereignty do not undermine the liberal, rule-based international order and the transatlantic relationship**. Moreover, Denmark should **encourage further EU collaboration with NATO and the US, particularly in trying to reach mutual agreement on standards, rules, and regulations for digital technologies** such as AI and 5G.

TAK

Forfatteren vil gerne takke for de værdifulde kommentarer fra en anonym peer reviewer samt kollegerne fra CMS på et internt reviewseminar.

1

Teknologisk suverænitet som strategisk autonomi

I 2016 præsenterede daværende chef for EU's udenrigsanliggender, Federica Mogherini, EU's udenrigs- og sikkerhedspolitiske strategi, *Shared Vision, Common Action: A Stronger Europe*.[1] Strategien pustede nyt liv i EU's forsvars- og sikkerhedspolitik[2] og understregede betydningen af europæisk strategisk autonomi.[3] Betoningen af behovet for europæisk strategisk autonomi har traditionelt været forbundet med forsvarspolitik og forsvarssamarbejde,[4] men det er hverken blevet defineret eller besluttet i EU's politiske dokumenter, hvad EU's strategiske autonomi præcis består af, eller hvordan EU opnår den.[5] Strategisk autonomi er således et tvetydigt begreb. Debatten om EU's strategiske autonomi afspejler dermed den ambivalens, der omgærder EU's geopolitiske rolle i en verden, hvor stormagtsrivalisering igen er på dagsordenen.

1. European External Action Service, *Shared Vision, Common Action. A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy* (Luxembourg: Publications Office of The European Union, 2016).
2. Kristian Søby Kristensen og Niels Byrjalsen, *Aktiv afventning. Nordiske Perspektiver på forsvars- og sikkerhedspolitisk samarbejde* (København: Center for Militære Studier 2020).
3. European External Action Service, *Shared Vision, Common Action*, s. 16.
4. Finanskrisen (2009-2012) og flygtningekrisen (2015) er eksempler på to begivenheder, der har medført en diskussion om EU's strategiske autonomi, som rækker ud over traditionel forsvars- og sikkerhedspolitik.
5. Behovet for europæisk strategisk autonomi bliver i stigende grad understreget af EU og unionens medlemslande. Strategisk autonomi forbindes ofte med evnen til kollektivt og uafhængigt at tage ansvar for egen sikkerhed, men der er hverken enighed om, hvordan begrebet defineres, eller hvad det betyder i EU-kontekst. Se Christine Nissen og Jessica Larsen, *European strategic autonomy: from misconceived to useful concept what can we learn from the Northern outlook?* (DIIS Policy Brief, 2021).

Intensiveret stormagtsrivalisering og øget fokus på særligt den digitale udvikling medfører, at teknologisk suverænitet i dag er blevet et afgørende element i EU's bestræbelser på at opnå strategisk autonomi.[6] Teknologisk suverænitet indebærer ifølge forpersonen for Det Europæiske Råd, Charles Michel, at EU skal finde en europæisk vej mellem USA og Kina, så EU kan fastsætte globale standarder, være førende inden for digitale teknologier og blive strategisk uafhængigt.[7] Chefen for EU's udenrigsanliggender, Josep Borrell, har understreget, at "vi lever i en verden, hvor indbyrdes afhængighed bliver mere og mere konfliktfuld, og hvor blød magt er et våben: Handel, teknologi, data og information er nu instrumenter i politisk konkurrence".[8] Det betyder ifølge Borrell, at EU for "at undgå at ende som taber i dagens USA-Kina-konkurrencen skal [...] genlære magtens sprog og tænke på Europa som en geostrategisk aktør i topklasse".[9]

Kommissionsforperson Ursula von der Leyen gjorde det klart i sit politiske program fra 2019, at teknologisk udvikling og digitalisering er et gennemgående og højt prioriteret område for hendes geopolitiske kommission.[10] Det har hun gentagne gange slået fast siden. Senest i sin tale "Unionens tilstand 2021", hvor von der Leyen understregede nødvendigheden af "at investere i vores europæiske teknologiske suve-

6. Se f.eks. Det Europæiske Råd, "Digital sovereignty is central to European strategic autonomy," speech by President Charles Michel at "Masters of digital 2021" online event (Det Europæiske Råd, 3. februar 2021), https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/
7. Se f.eks. talerne: Det Europæiske Råd, "Strategic autonomy for Europe – the aim of our generation," speech by President Charles Michel to the Bruegel think tank, (Det Europæiske Råd, 28. september 2020), https://www.consilium.europa.eu/da/press/press-releases/2020/09/28/l-autonomie-strategique-europeenne-est-l-objectif-de-notre-generation-discours-du-president-charles-michel-au-groupe-de-reflexion-bruegel/; Det Europæiske Råd, "The Digital in a fractious world: Europe's way", speech by President Charles Michel at the "FT-ETNO Forum", (Det Europæiske Råd, 29. september 2020), https://www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum
8. Josep Borrell, "Embracing Europe's Power," *IPS Journal*, 2. marts 2020, https://www.ips-journal.eu/regions/europe/embracing-europes-power-4095/.
9. Josep Borrell, "Embracing Europe's Power," *IPS Journal*, 2. marts 2020, https://www.ips-journal.eu/regions/europe/embracing-europes-power-4095/.
10. Ursula von der Leyen, *A Union that strives for more. My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024* (Luxembourg: Publications Office of The European Union, 2019), https://op.europa.eu/en/publication-detail/-/publication/43a17056-ebf1-11e9-9c4e-01aa75ed71a1.

rænitet" og at "forme den digitale omstilling efter vores egne regler og værdier".[11] EU har desuden fremhævet betydningen af teknologisk suverænitet, digitalisering og cybersikkerhed ved at afsætte 7,5 milliarder euro til et målrettet digitalt program i unionens budget for 2021-2027,[12] mens mindst 20 % af corona-genopretningspakkens 672,5 milliarder euro skal gå til projekter, der relaterer sig til digital omstilling bredt set.[13]

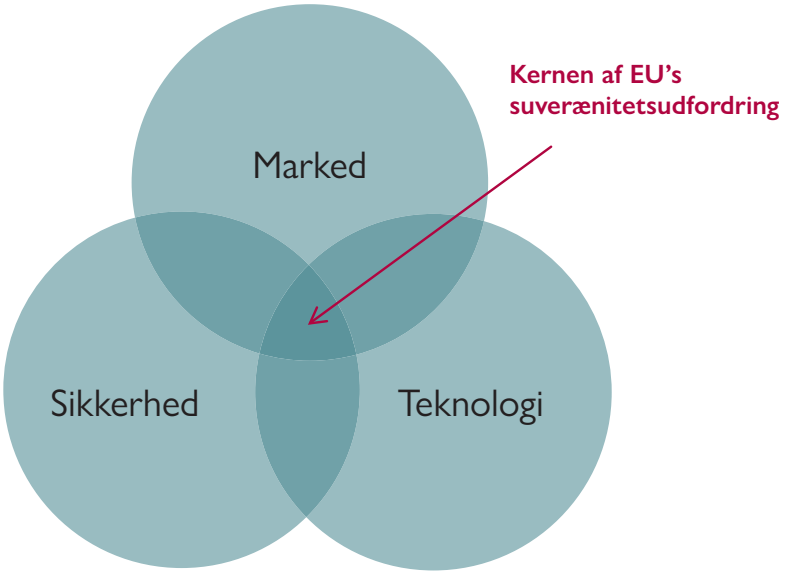
Udmeldingerne er nye toner fra et EU, der traditionelt har vendt det blinde øje til magt- og geopolitik.[14] Oprindeligt blev den tværnationale organisering af europæiske markeder og industrier betragtet som et middel til at sikre fred efter Anden Verdenskrig. I denne forståelse blev europæisk integration udtænkt og implementeret for at overvinde arven fra den magtpolitik, der alene i det 20. århundrede resulterede i to verdenskrige med udspring på kontinentet. Det europæiske samarbejde skulle fremme markedsintegration og indbyrdes afhængigheder, mens national sikkerhed forblev et eksklusivt privilegium for medlemsstaterne.[15]

Den arbejdsdeling er i dag udfordret af, at teknologiudvikling i stigende grad befinder sig i et spændingsfelt mellem sikkerheds- og forsvarspolitik på den ene side og industri-, erhvervs- og innovationspolitik på den anden. Når fortsat teknologiudvikling lover fremtidig velstand og vækst, er det et anliggende for EU's indre markeds-projekt. Når den samme teknologiudvikling samtidig er afgørende for den militærtekno-

11. Ursula von der Leyen, "Tale om Unionens tilstand," tale til Europa-Parlamentet, 15. september 2021, s. 6, https://ec.europa.eu/info/sites/default/files/soteu_2021_address_da_0.pdf.
12. EU-Kommisionen, "Digital Europe Programme: €7.5 billion of funding for 2021-2027," (EU-Kommissionen, 10. november 2021), https://digital-strategy.ec.europa.eu/en/library/digital-europe-programme-proposed-eu75-billion-funding-2021-2027. Ved præsentationen af det digitale budget understregede Thierry Breton, kommissær for det indre marked, at budgettet er "*essential to deliver on the twin digital and green transitions, to promote our technological sovereignty and strengthen our strategic digital capacities*". EU-Kommissionen, "Commission welcomes political agreement on €7.5 billion Digital Europe Programme," (EU-Kommissionen, 14. december 2020), https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2406.
13. Det Europæiske Råd, "A recovery plan for Europe," Det Europæiske Råd, tilgået 15. december 2021, https://www.consilium.europa.eu/en/policies/eu-recovery-plan/.
14. Sven Biscop, *European Strategy in the 21st Century: New Future for Old Powers*, (Abingdon, Oxon; New York, NY: Routledge, 2019), s. 8.
15. 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."

logiske udvikling og skaber flere sårbarheder og mere usikkerhed, bliver teknologipolitik til et fremtrædende nationalt sikkerhedsspørgsmål. EU's bestræbelser på at opnå yderligere strategisk autonomi gennem styrket teknologisk suverænitet udfordrer derfor den oprindelige fordeling af sikkerheds- og forsvarspolitisk autoritet og ansvar mellem EU, medlemsstaterne og NATO, da EU i stigende grad forsøger at fungere som en global magt, der handler strategisk ud fra overlappende sikkerheds-, forsvars-, industri-, erhvervs- og innovationspolitiske interesser og mål.

Figur 1. Teknolgisk suverænitet mellem sikkerhed, marked og teknologi



EU's vej mod at indfri målet om teknologisk suverænitet er imidlertid brolagt med udfordringer. Det skyldes primært, at EU's handlerum er begrænset af, at der ikke er enighed blandt medlemslandene om, hvad teknologisk suverænitet er, og hvordan det opnås, at afhængigheden af og presset fra USA og Kina er omfattende, og at den europæiske teknologiindustri langtfra er verdensførende på en række digitale kerneområder, hvor private virksomheder driver den teknologiske udvikling.

Det efterlader EU's ambition om teknologisk suverænitet med en række grundlæggende strategiske og politiske dilemmaer.

Ét dilemma angår forholdet mellem promovering af henholdsvis europæisk teknologisk uafhængighed på den ene side og interdependens på den anden side. Det dilemma er ikke blot centralt for EU, men berører selve kernen i den liberale vestlige globaliseringsdagsorden. Det er således et dilemma, der trækker tråde til den intensiverede strategiske konkurrence mellem USA og Kina, herunder den digitale handelskrig. Et andet dilemma er muligheden for reelt at opnå europæisk teknologisk suverænitet. Det gælder på områder som cloud, mikrochips og sociale medier, hvor EU allerede er dybt afhængig af tredjelande, og på områder som udvikling af AI og kvantecomputere, hvor EU står til at sakke agterud i fremtiden. Et tredje dilemma angår arbejdsdelingen mellem EU og NATO. Når EU styrker unionens teknologiske suverænitet – ved f.eks. at implementere Den Europæiske Forsvarsfond,[16] der gør EU til den tredje største investor i forsvarsforskning og -materiel i Europa – så rejser det sikkerheds- og forsvarspolitiske spørgsmål om en europæisk parallelstruktur til NATO-samarbejdet.

For Danmark repræsenterer EU's satsning på teknologisk suverænitet en accentuering af de strategiske konsekvenser, der følger af intensiveret stormagtsrivalisering og teknologikonkurrence. De sikkerheds- og forsvarspolitiske konsekvenser af EU's fokus på teknologisk suverænitet indgår dermed i en bredere stillingtagen, hvor Danmark bør afveje, hvordan EU's målsætning om teknologisk suverænitet bedst bliver udfoldet, så danske hensyn til sikkerhed, forsvar, frihedsrettigheder, diplomati, erhvervsliv, industri og innovation bedst bliver vægtet og varetaget. Det kræver strategiske overvejelser om, hvad en national teknologipolitik bør fokusere på, hvordan sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske overlap, muligheder og udfordringer udspiller sig, og hvordan forholdet mellem Danmark, EU, NATO og USA bliver påvirket.

Det er på den baggrund rapportens hovedformål at undersøge, hvordan EU har begrebsliggjort teknologisk suverænitet og omsat det til po-

16. EU-Forordning, "Regulation (EU) 2021/697 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092", *Official Journal of the European Union*, 12. maj 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0697&qid=1631263086142&from=EN.

litik og regulering inden for to vitale områder: cybersikkerhed og AI. Rapporten fokuserer særligt på, hvordan sikkerheds- og forsvarspolitik og industri-, erhvervs- og innovationspolitik smelter stadig mere sammen på det teknologiske område, hvordan EU's teknologiske suverænitet påvirker de sikkerheds- og forsvarspolitiske forhold mellem EU, medlemsstaterne og NATO, og hvad de strategiske implikationer er for Danmark.

1.1. Metode, afgrænsning og struktur

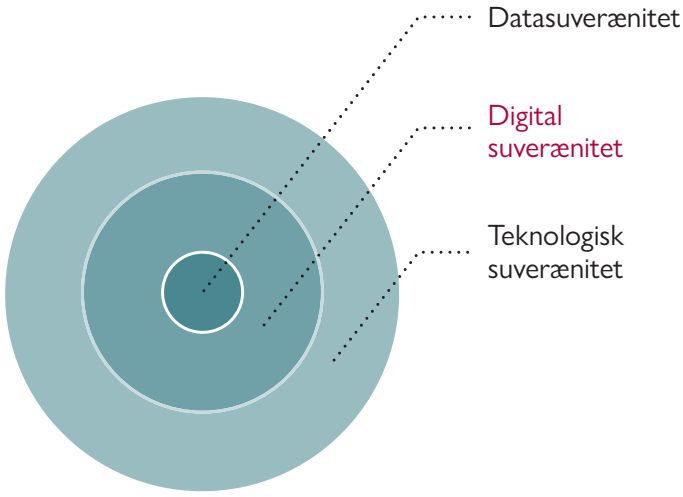
Rapporten er fundteret på samfundsvidenskabelig metode. Den bygger på et omfattende deskstudy af videnskabelige kilder, officielle EU-dokumenter og pressemateriale, der samlet set tegner et bredt billede af, hvordan teknologisk suverænitet bliver begrebsliggjort og omsat til strategi, politik og regulering i EU. Desuden trækker rapporten på ph.d.-afhandlingen *EU Cybersecurity Governance – Redefining the Role of the Internal Market*,[17] deltagelse i en række konferencer, seminarer og workshops samt uformelle samtaler og interviews med danske og europæiske embedsmænd og eksperter.

EU har ikke defineret, hvad teknologisk suverænitet er. Begrebet er blevet anvendt inden for en lang række områder, fra digitalisering over sundhed til klima. Rapporten fokuserer på, hvordan EU har begrebsliggjort teknologisk suverænitet og omsat det til politik og regulering på det digitale område, der, som det fremgår af indledningen, er et kerneområde for EU's bestræbelser på at opnå teknologisk suverænitet. Rapportens analyse placerer sig dermed mellem det snævre begreb "datasuverænitet" og det bredere begreb "teknologisk suverænitet".

Det gøres ved at analysere, hvordan EU har begrebsliggjort teknologisk suverænitet og omsat det til politik og regulering på to vitale digitale områder: cybersikkerhed og AI. De to indsatsområder er identificeret og udvalgt gennem studier af talrige EU-initiativer, deltagelse i offentlige konferencer og workshops samt uformelle samtaler med embedsmænd fra Danmark og EU. Cybersikkerhed er en del af dagligdagen for myn-

17. Tobias Liebetrau, *EU Cybersecurity Governance: Redefining the Role of the Internal Market* (ph.d.-afhandling, Københavns Universitet, Institut for Statskundskab, 2019).

Figur 2. Analysens placering



digheder, virksomheder og borgere i Europa.[18] Over det seneste tiår har cybersikkerhed udviklet sig til et væsentligt politikområde for EU – et område, hvor EU fører sikkerhedspolitik gennem sit indre markeds-mandat.[19] EU's fokus på cybersikkerhed indkapsler dermed, hvordan digitaliseringen er et janushovedfænomen, der rummer både muligheder og sårbarheder.[20] AI står centralt både i den globale teknologikonkurrence og i EU's ambition om teknologisk suverænitet. I løbet af de seneste fem år har EU således udviklet strategier og politikker for at fremme udvikling og regulering af AI.[21] I forbindelse med analysen af de to områder fokuserer rapporten på, hvordan de sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske tiltag og logikker placerer sig i

18. Tobias Liebetrau, *Dansk offensiv cybermagt mellem angreb, spionage og forsvar: En komparativ analyse på tværs af Europa* (København: Center for Militære Studier, maj 2020).
19. Liebetrau, *EU Cybersecurity Governance*.
20. Tobias Liebetrau, "Cybersikkerhed i Perspektiv – Temaredaktørens forord," Økonomi og Politik 93, nr. 3, s. 5–12.
21. Jeppe Teglskov Jacobsen og Tobias Liebetrau, "Kunstig intelligens, militær strategi og international konkurrence", i *Smart Krig – Militær anvendelse af kunstig intelligens*, red. Iben Yde, Thomas G Nielsen og Rasmus Dalhberg (København: Djøf Forlag, 2021).

et spændingsfelt mellem sikkerhed, marked og digitalisering, og hvordan det påvirker de sikkerhedspolitiske autoritets- og ansvarsforhold mellem EU, medlemsstaterne og NATO.

Rapporten er inddelt i tre kapitler foruden dette indledende. Kapitel 2 udfolder den globale teknologikonkurrence, der er rammesættende for EU's digitale teknologiske suverænitetsbestræbelser. I forlængelse heraf analyserer rapporten i kapitel 3, hvordan EU har begrebsliggjort teknologisk suverænitet og omsat det til politik og regulering på to vitale digitale områder: cybersikkerhed og AI. Kapitel 4 samler analysens resultater med henblik på at diskutere de strategiske implikationer i form af udfordringer og muligheder for henholdsvis EU og Danmark og identificerer desuden en række anbefalinger, der fremover kan støtte dansk strategisk tænkning, politisk styring og offentlig debat om EU's teknologiske suverænitet og dansk teknologipolitik.

2

Den globale teknologikonkurrence

Rapportens indledning viste, at EU i stigende grad retter opmærksomheden mod de globale geopolitiske og geoøkonomiske forskydninger, som de seneste år er blevet accentueret af USA's og Kinas tiltagende stormagtsrivalisering, herunder særligt af den intensiverede digitale teknologikonkurrence. For at kunne forstå EU's arbejde med teknologisk suverænitet og vurdere de strategiske konsekvenser for Danmark er det derfor nødvendigt at kaste et blik på den rammesættende globale teknologikonkurrence. En teknologikonkurrence, der er afgørende for den i indledningen fremhævede suverænitetsudfordring foruden sammensmeltningen mellem sikkerheds- og forsvarspolitik samt industri-, erhvervs- og innovationspolitik. Kapitlet falder i fire dele. Første del placerer teknologikonkurrencen i relation til den tiltagende stormagtsrivalisering. Anden del beskriver teknologikonkurrencens militære dimension. Tredje del zoomer ind på spændingsfeltet mellem stat og marked. Fjerde del konkluderer og relaterer til EU.

2.1. Stormagtsrivalisering og teknologikonkurrence

Bevægelsen fra en relativt samarbejdende verdenspolitik præget af globalisering til en mere konkurrencepræget verdenspolitik præget af stormagtsrivalisering betyder, at teknologiens relative betydning i international politik er stigende. Dertil kommer, at vi som samfund og individer bliver stadig mere afhængige af særligt digitale teknologier og infrastrukturer. Derfor vil de lande, der kontrollerer den teknologiske

udvikling, udrulning og integration i stigende grad kunne påvirke verdens politiske, økonomiske, sociale og militære udvikling. Teknologisk suverænitet bliver derfor i stigende grad fremhævet som en afgørende strategisk parameter, [22] der påvirker den globale stormagtsrivalisering samt de indenrigspolitiske relationer mellem stat, virksomheder og borgere. Det eksemplificerer de seneste års amerikansk-kinesiske digitale handelskrig om 5G-netværk, computerchips og mobilsoftware.

Allerede i 2012 advarede efterretningskomiteen i Repræsentanternes Hus om, at de kinesiske techgiganter Huawei og ZTE udgjorde en national sikkerhedstrussel. Siden har de kinesiske techgiganter været i Vestens søgelys. I dag er Huawei blevet udelukket fra at levere 5G-infrastruktur til en række vestlige lande, herunder USA, Australien og Sverige. I forlængelse af landets forbud mod implementering af Huawei 5G-infrastruktur præsenterede USA i august 2020 en strategi under navnet "The Clean Network". Planens grundlæggende mål er at forhindre kinesiske selskaber i at få adgang til følsomme data om amerikanere og amerikanske selskaber. Det skal planen sikre, ved at kinesiske techselskabers indflydelse i USA bliver minimeret på fem centrale digitale områder, herunder 5G, apps og cloud[23].

Hertil kommer, at blokering, filtrering og segmentering af internettet i en årrække er blevet brugt til at øge statslig kontrol med datastrømme og internetindhold og understøtte nationale industrier.[24] Det meste kendte eksempel herpå er den såkaldte kinesiske firewall, men også lande

22. Herunder en række relaterede begreber, der behandler suverænitet og digitalisering. Julia Pohle og Thorsten Thiel, "Digital sovereignty," *Internet Policy Review*, 9(4) (2020), https://doi.org/10.14763/2020.4.1532; Luciano Floridi, "The fight for digital sovereignty: What it is, and why it matters, especially for the EU," *Philosophy & Technology* 33, nr. 3 (2020): 369–378; Yu Hong and G. Thomas Goodnight, "How to think about cyber sovereignty: the case of China," *Chinese Journal of Communication* 13, nr. 1 (2020): 8-26; Milton L. Mueller, "Against sovereignty in cyberspace," *International Studies Review* 22. nr. 4 (2020): 779-801; Patrik Hummel et al., "Data sovereignty: A review," *Big Data & Society* 8, nr. 1 (2021).
23. Clean Carrier, Clean Store, Clean Apps, Clean Cloud og Clean Cable. "The Clean Network," U.S. Department of State, tilgået 15. december 2021, https://2017-2021.state.gov/the-clean-network/index.html.
24. Ronald J. Deibert "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium*, 32(3) 2003: 501-530; Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, (Cambridge; Malden, Polity Press, 2017); Sven Biscop, *European Strategy in the 21st Century: New Future for Old Powers*, (Abingdon, Oxon; New York, NY: Routledge, 2019), s. 8.

som Nordkorea,[25] Iran[26] og Rusland[27] har styrket den nationale kontrol med internettet. Derudover viste Edward Snowdens afsløring af NSA's globale spionageregime – via internetinfrastruktur som datakabler og datacentre samt samarbejde med teleudbydere og techgiganter – med tydelighed, at internettet ikke står uden for statslig magtudøvelse. Efter afsløringerne øgede både EU og BRIKS-landene deres fokus på de teknologier og infrastrukturer, der understøtter kontrol med internettet og dets datastrømme.[28]

Fragmenteringen af internettet, den amerikansk-kinesiske digitale handelskrig og EU's prioritering af teknologisk suverænitet understreger, at global digital teknologikonkurrence allerede er et centralt omdrejningspunkt for international politik. De senere års udvikling peger på, at den såkaldte fjerde industrielle revolution – hvor integration mellem den digitale og den fysiske verden accelerer yderligere med fortsat udvikling og udbredelsen af 5G- og 6G-netværk, tingenes internet, big data-analyse, AI, robotteknologi og kvantecomputere – er blevet et udtryk for, hvordan teknologisk-kommercielle spørgsmål og løsninger er en integreret del af den globale strategiske og sikkerhedspolitiske kampplads. Det dykker næste afsnit dybere ned i ved at se på den militære dimension af teknologikonkurrencen.

25. Seungahn Nah og Soomin Seo, "Talking With the Hermit Regime: North Korea, Media, and Communication: Introduction," *International Journal of Communication* 14 (2020): 1303–1307; Bernhard Seliger og Stefan Schmidt, "The Hermit Kingdom Goes Online... Information Technology, Internet Use and Communication Policy in North Korea," *North Korean Review* (2014): 71-88.
26. Jon Gambrell, "Iran deploys 'halal' internet in latest bid to rein in citizens' web freedoms," *Independent*, 29. januar 2019, https://www.independent.co.uk/news/world/middle-east/iran-halal-internet-national-information-network-web-freedoms-citizens-access-social-media-telegram-facebook-twitter-instagram-youtube-a8182841.html; Altug Yalcintas og Naseraddin Alizadeh, "Digital Protectionism and National Planning in the Age of the Internet: the Case of Iran," *Journal of Institutional Economics* 16, nr. 4 (2020): 519–536
27. Eva Claessen, "Reshaping the internet – the impact of the securitisation of internet infrastructure on approachesto internet governance: the case of Russia and the EU," *Journal of Cyber Policy*, 5:1 (2020): 140-157, DOI: 10.1080/23738871.2020.172835; Sergei Vedyashkin, "Russia Is 'Ready' to Disconnect from Global Internet, Medvedev Says," *Moscow Times*, 1. februar 2021, https://www.themoscowtimes.com/2021/02/01/russia-is-ready-to-disconnect-from-global-internet-medvedev-says-a72791.
28. Christian Bueger og Tobias Liebetrau, "Protecting hidden infrastructure: The security politics of the global submarine data cable network," *Contemporary Security Policy* 42, nr. 3 (2021): 391-413, DOI: 10.1080/13523260.2021.19071.

2.2. Teknologikonkurrencens militære dimension

En væsentlig del af stormagtsrivaliseringen og teknologikonkurrencen tager udgangspunkt i ideen om, at teknologier som AI, big data-analyse og kvanteteknologi besidder et potentiale til grundlæggende at forandre vores måde at forstå og føre krig på.[29] Hvordan teknologiske landvindinger kan og vil blive omsat til og anvendt i en militær kontekst, er afgørende for den globale teknologikonkurrence.

Spørgsmålet udgør grundelementet i den amerikanske såkaldte "Third Offset Strategy", som skal drive revolutionerende militære teknologier frem og sikre deres integration i de amerikanske væbnede styrker. USA arbejder dermed målrettet på at skabe (endnu) et amerikansk militært teknologiforspring. På den måde vil amerikanerne minimere betydningen af den globale digitale teknologispredning og fastholde USA's position som verdens førende militære magt. Trump-regeringen fortsatte de facto Third Offset-strategien og udgav i oktober 2020 en national strategi for disruptive teknologier.[30] NATO har ligeledes styrket sit fokus på disruptive teknologier, efter at alliancen i 2018 præsenterede sin strategi for at bevare sin teknologiske fordel.[31] Ved NATO Leaders Meeting i London i 2019 vedtog stats- og regeringscheferne således et *Emerging and Disruptive Technologies Roadmap*, i marts 2021 gav NATO-udenrigsministrene opbakning til en implementeringsstrategi med fokus på emergerende og disruptive teknologier,[32] og i oktober 2021 præsenterede NATO en strategi for AI.[33]

29. For en dybere beskrivelse af de enkelte teknologier og deres potentielle påvirkning af fremtidens krig se Henrik Breitenbauch og Tobias Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark* (København: Center for Militære Studier og Djøf Forlag, juni 2021).
30. The White House, *National strategy for critical and emerging technologies* (Washington, DC: White House Office, oktober 2020), https://www.hsdl.org/?view&did=845571.
31. NATO, *NATO Science & Technology Strategy Sustaining Technological Advantage*, tilgået 16. december 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20181107_180727-ST-strategy-eng.pdf. Se også "New focus on emerging and disruptive technologies helps prepare NATO for the future," NATO, 3. marts 2021, https://www.nato.int/cps/en/natohq/news_181901.htm.
32. NATO, "New Focus on Emerging and Disruptive Technologies Helps Prepare NATO for the Future"; North Atlantic Council, *London Declaration*, leader's meeting statement, Press Release 115, London 3-4 December 2019: "London Declaration," NATO, tilgået 16. december 2021. http://www.nato.int/cps/en/natohq/official_texts_171584.htm.
33. "NATO releases first-ever strategy for Artificial Intelligence," NATO, 22. oktober 2021, https://www.nato.int/cps/en/natohq/news_187934.htm.

Behovet for at udvikle strategier og politikker, der tager hånd om disruptive teknologiske landvindinger, ses også i Kina. Kina præsenterede allerede i 2015 en slags afkoblingsstrategi med landets "Made in China 2025"-strategi, der skal minimere afhængigheden af udenlandsk hardware og teknologi, gøre Kina til verdens førende inden for digital teknologisk innovation og dermed øge landets selvhjulpenhed.[34] Desuden har det kinesiske styre i en årrække prioriteret at sikre en langsigtet og velfinansieret militærteknologisk udvikling, hvis kerneformål er at nå op på siden af USA i det militærteknologiske kapløb. Denne kinesiske variant af den amerikanske offsetstrategi peger frem mod, at Kina sikkerhedspolitisk og militært satser på at blive en global militærmagt før 2050 – et mål, der fortolkes som at nå militær paritet med eller overhale USA's militære formåen.[35]

Det styrkede fokus på at forfine politikker og strategier for udvikling og håndtering af nye militære teknologier i USA, NATO og Kina understreger, hvordan konkrete forsvarspolitiske tiltag og investeringer skal levere løsninger på langsigtede sikkerhedspolitiske udfordringer, der rækker væsentligt ud over umiddelbar afskrækkelse og krigsdeltagelse.[36] For alle parter gælder det imidlertid, at det er privat, virksomhedsdrevet forskning og innovation, der skal lede den fremtidige digitale teknologiske udvikling – både civilt og militært – hvorfor private virksomheder er et centralt omdrejningspunkt i teknologikonkurrencen. Næste afsnit kaster yderligere lys over betydningen af relationen mellem stat og marked i den globale teknologikonkurrence.

34. "'Made in China 2025'. Plan Issued," The State Council of the People's Republic of China, 19. maj 2015, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm. Det kinesiske styres seneste femårsplan bekræfter den målsætning, se f.eks. Arjun Kharpal, "China spending on research and development to rise 7% per year in push for major tech breakthroughs", *CNBC*, (5. marts 2021), https://www.cnbc.com/2021/03/05/china-to-boost-research-and-development-spend-in-push-for-tech-breakthroughs.html; Arjun Kharpal, "In battle with U.S., China to focus on 7 'frontier' technologies from chips to brain-computer fusion," *CNBC*, (5 marts 2021), https://www.cnbc.com/2021/03/05/china-to-focus-on-frontier-tech-from-chips-to-quantum-computing.html.
35. Department of Defense of the United States of America, *Military and Security Developments Involving the People's Republic of China – Annual Report to Congress,* 2020, https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.
36. Breitenbauch og Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark*.

2.3. Techgiganter og teknologiudvikling

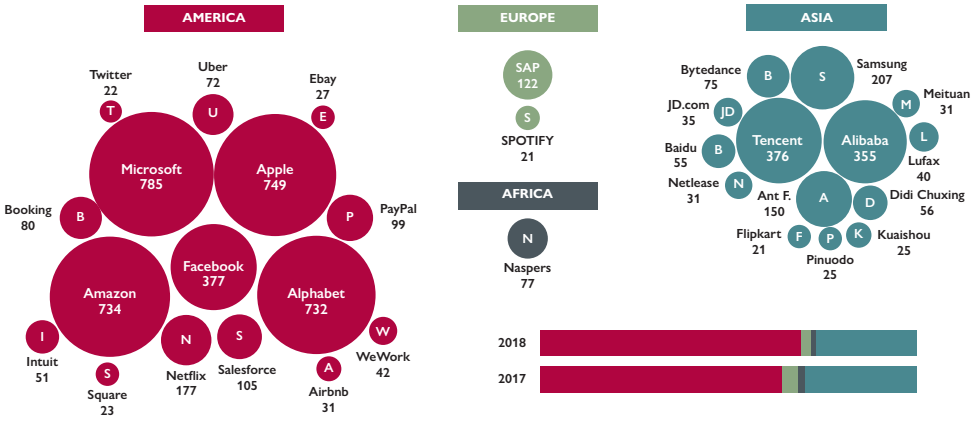
Den digitale, teknologiske udvikling og innovation er primært understøttet af investeringer i den private sektor, der normalt opererer på tværs af landegrænser og er afhængige af globale markeder og forsyningskæder. Teknologiudviklingens nationale og regionale betydning er således indlejret i den globale økonomi, der binder verdens lande sammen og skaber gensidige afhængigheder, men samtidig danner grobund for konkurrence og konflikt, som det er beskrevet ovenfor. Det skyldes ikke mindst, at relationerne mellem stat, marked og individ varierer på tværs af stormagter og regioner. Stormagterne er alle spundet ind i den globale økonomi, men deres perspektiv på den globale økonomiske og teknologiske konkurrence, markedsvilkår og borgerrettigheder er forskelligt.

I takt med at forskningen 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. Evne til og mulighed for at understøtte og overføre kommercielle teknologiske landvindinger, der er forbundet med den fjerde industrielle revolution, til økonomisk vækst, mindskning af klimaforandringer, forbedring af velfærd og udvikling af militæret kommer derfor til at spille en central rolle i fremtidens globale politik. Dermed bliver teknologipolitik – herunder på erhvervs- industri-, innovations- og forskningsområdet, og forsøg på at skabe synergi mellem marked og stat – til sikkerheds- og forsvarspolitik.[37]

Det er særligt iøjefaldende, at private virksomheder ejer, driver og udvikler langt størstedelen af verdens digitale teknologier og infrastrukturer. Digitalisering har dermed transformeret den globale økonomi og skabt en helt ny økonomisk sektor. Amerikanske Google/Alphabet, Apple, Facebook, Amazon og Microsoft og kinesiske Tencent og Alibaba er alle blandt verdens 10 mest værdifulde virksomheder.[38] Techgiganterne repræsenterer en platformsøkonomi, hvor virksomheder primært base-

37. Det er ikke i sig selv et nyt fænomen, men den globale digitale teknologikonkurrence og de private techvirksomheders position transformerer teknologipolitikkens betydning.
38. Statista, "The 100 largest companies in the world by market capitalization in 2021," Statista, tilgået 16. december 2021, https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/; "List of public corporations by market

Figur 3: Markedsværdi i milliarder dollar (2018)



UN, *Digital Economy Report 2019, Value Creation and Capture: Implications for Developing Countries*, (United Nations Publications, 2019), s. 10; Frances G. Burwell og Kenneth Propp, *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?* (Washington, DC: Atlantic Council, 2020), s. 6, https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf.

rer deres forretningsmodel på at indsamle og udnytte den eksponentielt stigende mængde brugerdata. En forretningsmodel, som professor Shoshana Zuboff har døbt "overvågningskapitalisme".[39] I Vesten bliver dataøkonomien og techgiganternes stigende magtposition i dag opfattet som en grundlæggende politisk og økonomisk udfordring, der kræver inddæmning, hvilket EU har sat sig i spidsen for.[40] Det sker, til trods for – eller måske netop på grund af – at kun én europæisk virksomhed er repræsenteret i top-20 på Forbes' liste over de mest betydningsfulde virksomheder inden for digitalisering.[41]

capitalization," Wikipedia, tilgået 16. decmber 2021, https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization.

39. Shoshana Zuboff, "Big other: Surveillance Capitalism and the Prospects of an Information Civilization", *Journal of Information Technology* 30(1) (2015):75–89; Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2019).
40. Digital Markets Act, Digital Services Act, GDPR etc.
41. Deutsche Telekom er nummer 19. I top-20 har USA 12, Kina 2, Japan 2 og Hong Kong, Sydkorea og Taiwan hver 1 virksomhed – https://www.forbes.com/top-digital-companies/list/#tab:rank.

Den globale teknologikonkurrence omfatter relationer mellem stat og marked og evnen til at koordinere og mobilisere samarbejde med henblik på at understøtte og udnytte innovation. Staternes generelle og militære teknologipolitikker bliver derfor til langsigtede sikkerheds- og forsvarspolitiske brikker.

2.4. Konklusion: Udfordringer og muligheder for EU

Den tiltagende stormagtsrivalisering og teknologiske kappestrid vil næppe erstatte globaliseringen, men den vil forandre den. Det gælder ikke mindst på det digitale område, hvor vi har set friktion inden for globale produktions- og værdikæder, der er særligt sikkerheds- og forsvarspolitisk relevante. Den globale teknologikonkurrence skaber både udfordringer og muligheder for EU. På den ene side er det en væsentlig udfordring for EU at skulle navigere i en teknologikonkurrence, som medlemslandene ser forskelligt på, hvor presset på USA og Kina er stort, hvor EU's teknologiindustri er bagud på en række kritiske digitale områder, hvor kompetencefordelingen mellem EU, medlemsstaterne og NATO bliver udfordret, og hvor private virksomheder spiller en stadig mere afgørende rolle. På den anden side tilskynder det EU til at markere sig som en global geopolitisk og geoøkonomisk spiller. Med udgangspunkt i unionens indre markedsmandat giver det EU en mulighed for at forsøge at handle strategisk ved at udpege sammenhængende europæiske sikkerheds-, forsvars, industri-, erhvervs- og innovationspolitiske interesser.

3

Indsatsområder for EU's teknologiske suverænitet

Rapportens hovedformål er at analysere EU's arbejde med teknologisk suverænitet og afdække de strategiske og sikkerhedspolitiske konsekvenser af arbejdet for Danmark, herunder særligt det forhold, at sikkerheds- og forsvarspolitik og industri-, erhvervs- og innovationspolitik smelter stadig mere sammen på det teknologiske område. Som det fremgik af indledningen og kapitel 2, har særligt den tiltagende digitalisering og udvikling af nye digitale teknologier katapulteret teknologisk suverænitet op i toppen af den EU-politiske dagsorden, hvor det er blevet kædet sammen med stormagtsrivalisering, cyberkonflikt, big tech og et tiltagende behov for europæisk strategisk autonomi.

Dette kapitel undersøger, hvordan teknologisk suverænitet er blevet begrebsliggjort og omsat til politik og regulering i EU på to vitale digitale områder: cybersikkerhed og AI. Analysen af de to områder fokuserer på, hvordan de sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske prioriteringer placerer sig i et spændingsfelt mellem sikkerhed, marked og digitalisering, og hvordan det påvirker de sikkerhedspolitiske autoritets- og ansvarsforhold mellem EU, medlemsstaterne og NATO.

Analysen behandler først cybersikkerhedsdimensionen, der i henved et årti har været en politisk topprioritet for EU,[42] som bliver knyttet stadig tættere og mere eksplicit til målet om teknologisk suverænitet. Dernæst koncentrerer analysen sig om AI, der primært knytter digital suverænitet til industri, erhverv og dataøkonomi. I løbet af de seneste

42. Liebetrau, "EU Cybersecurity Governance".

fem år har EU udviklet strategier og politikker til at fremme udvikling og regulering af AI, der står centralt både i den globale teknologikonkurrence og i EU's ambition om teknologisk suverænitet.

3.1. Cybersikkerhed

Cybersikkerhed har i snart et årti været et væsentligt prioritetsområde i EU.[43] I den periode er cybersikkerhedselementer blevet integreret i flere af EU's centrale og tværgående politikområder, og det er blevet koblet til teknologisk suverænitet. Analysen behandler udviklingen i EU's cybersikkerhedspolitik i fire dele. Den viser, hvordan EU's sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske tiltag på cybersikkerhedsområdet siden 2013 har placeret sig i et spændingsfelt mellem digitalisering, marked og sikkerhed. I forlængelse heraf slår den fast, at EU fører en væsentlig del af sin cybersikkerhedspolitik via sit indre markeds-mandat, hvilket skubber til det traditionelle sikkerhedspolitiske autoritetsforhold mellem EU og medlemsstaterne. Ydermere understreger analysen, at EU's cybersikkerhedspolitik i henved et årti har skabt grobund for unionens ambitioner om teknologisk suverænitet, men at sammenhængen mellem teknologisk suverænitet og cybersikkerhed for alvor blev ekspliciteret i EU's seneste cybersikkerhedsstrategi fra 2020.

3.1.1. Digitalisering, europæisk integration og cybersikkerhed

Digitaliseringen af de europæiske samfund har været en væsentlig drivkraft i den europæiske integration siden 1980'erne.[44] Et gennemgåede EU-argument har været, at digitalt europæisk samarbejde kunne skabe modvægt til først USA's og Japans digitale dominans og i dag USA's og Kinas. Samtidig er EU's fokus på 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 digitale indre marked.[45] Strategien understreger, at digitalisering

43. Analysen fokuserer på det centrale af EU's cybersikkerhedstiltag, der af EU bliver beskrevet som netværks- og informationssikkerhed.
44. Liebetrau, "EU Cybersecurity Governance".
45. EU-Kommissionen, *En strategi for et digitalt indre marked i EU*, 6. maj 2015, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

samt informations- og kommunikationsteknologi (IKT) danner et væsentligt grundlag for europæisk økonomisk udvikling samt for vores liv og samfund.

EU's politik på cybersikkerhedsområdet havde i 1990'erne ikke en klar strategisk retning, men bestod af løsrevne hensigtserklæringer, samarbejder og reguleringer. Først i 2001 præsenterede EU-Kommissionen en samlet policytilgang til netværks- og informationssikkerhed, der var drevet af unionens indre markeds-mandat. EU's cybersikkerhedspolitik forblev forholdsvis vag op gennem 00'erne. Dog blev EU i 2004 en institution rigere, da Den Europæiske Unions Agentur for Cybersikkerhed (ENISA) blev oprettet. Mod slutningen af 00'erne begyndte cybersikkerhed at få opmærksomhed i den brede offentlighed og den politiske debat. Ikke mindst som følge af cyberangrebene mod Estland i 2007 samt Stuxnet-cyberangrebet mod de iranske atomreaktorer i 2010. EU konsoliderede således sin tilgang til cybersikkerhed i 2010 i strategien for intern sikkerhed[46] og den digitale agenda for Europa.[47] Som næste afsnit vil vise, var det dog først i 2013, at cybersikkerhed blev et selvstændigt politikområde.

3.1.2. Cybersikkerhedsstrategi og harmoniserende lovgivning

I 2013 præsenterede EU-Kommissionen og EU-Udenrigstjenesten EU's første egentlige cybersikkerhedsstrategi.[48] Strategien fokuserede på fem overordnede mål: styrket cyberrobusthed, mindsket cyberkriminalitet, udvikling af cyberforsvarspolitik og -kapacitet, udvikling af industrielle og teknologiske cybersikkerhedsressourcer samt fastlæggelse af en international cyberspacepolitik tilpasset centrale EU-værdier. Strategien skabte en fælles tilgang til en række forskellige politikområder, herunder beskyttelse af kritisk infrastruktur, netværks- og informationssikkerhed og mod cyberkriminalitet, der tidligere var blevet behandlet hver for sig.

46. EU-Kommissionen, *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, 22. november 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF.
47. EU-Kommissionen, *A Digital Agenda for Europe*, 19. maj 2010, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.
48. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace*, 7. marts 2013, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52013JC0001&from=DA.

Strategien konsoliderede dermed EU's tilgang til cybersikkerhed, hvilket i vidt omfang var blevet muliggjort med afskaffelsen af søjlesystemet som følge af Lissabontraktatens implementering.[49]

Mest centralt i strategien står den første harmoniserende cybersikkerhedslovgivning – netværks- og informationssikkerhedsdirektivet (NIS-direktivet) – der blev vedtaget i 2016 og implementeret i maj 2018. Med direktivet søgte EU at sikre en minimal institutionel og harmoniseret kapacitet ved at forpligte medlemsstaterne til at vedtage nationale NIS-strategier og oprette centrale kontaktpunkter og enheder, der håndterer IT-sikkerhedshændelser (CSIRT'er). Desuden fastsætter direktivet sikkerheds- og underretningskrav til operatører af væsentlige tjenester i kritiske sektorer (energi-, transport, bank-, finans- og sundhedssektoren) og for udbydere af digitale tjenester. Vedtagelsen af direktivet afspejler en erkendelse af nødvendigheden af at udvikle et fælles europæisk minimumsniveau af cybersikkerhed for kritisk infrastruktur. Etableringen af en fælles cybertrussel mod Europa og et reguleret cybersikkerhedsansvar, der rækker ud over den enkelte medlemsstat og dennes grænser, var med til at gøre det muligt for EU at knytte digitalisering, fortsat integration af det indre marked og sikkerhedspolitik tættere sammen. Derved har direktivet været med til at skabe grobund for ændringer af det sikkerhedspolitiske forhold mellem EU og medlemsstaterne, sammenkædningen af industri-, erhvervs- og innovationspolitik med sikkerheds- og forsvarspolitik og det fremtidige fokus på teknologisk suverænitet.

Et andet af strategiens overordnede mål – udvikling af industrielle og teknologiske ressourcer til at fremme cybersikkerhed – har ligeledes været med til at så kimen til det, der senere er blevet kendt som teknologisk suverænitet. EU-Kommissionen slog fast allerede i 2013, at:

> *"[d]er er en risiko for, at Europa bliver for afhængig ikke kun af ikt, der produceres andre steder, men også af sikkerhedsløsninger, som udvikles uden for dets grænser. Det er vigtigt at sikre, at hardware- og softwarekomponenter, der produceres i EU og i tredjelande og anvendes i kritiske tjenester og infrastruktur samt også i stigende grad i mobile enheder, er pålidelige og sikre og garanterer, at personoplysninger beskyttes."*[50]

49. Til trods for ambitionen om konsistens og koordination fremstår strategiens tre fokusområder – kritisk beskyttelse af informationsinfrastruktur, cyberkriminalitet og cyberforsvar – fortsat forholdsvis adskilte.
50. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace*, s. 12.

Strategien nævner ikke eksplicit teknologisk suverænitet, men betoningen er ikke ulig den, der anvendes i dag. Som løsning på udfordringen foreslår EU-Kommissionen et styrket fokus på at fremme et indre EU-marked for cybersikkerhedsprodukter, at øge fokus på sikkerhed i alle led af værdikæden (hardware, software, tjenester etc.) og at fremme en fælles europæisk efterspørgsel efter sikre produkter, f.eks. gennem udvikling af standarder.[51] Desuden bliver det fremhævet i strategien, at investeringer i forskning og udvikling kan fremme en pålidelig europæisk IKT-industri, sætte skub i det indre marked og reducere Europas afhængighed af udenlandsk teknologi.[52] Igen ses det, at fortsat digitalisering, markedsintegration og industripolitik bliver vævet eksplicit sammen med europæisk autonomi og sikkerhed, om end de konkrete initiativer primært forbliver brede hensigtserklæringer.

2013-strategien og NIS-direktivet har været afgørende for at sætte EU's strategiske retning for arbejdet med cybersikkerhed, hvorved digitalisering samt udvikling og understøttelse af det indre marked blev knyttet yderligere sammen med sikkerhed.

3.1.3. Cybersikkerhed og strategisk autonomi

I 2017 præsenterede EU-Kommissionen og EU-Udenrigstjenesten en større cybersikkerhedspakke, der ajourførte 2013-strategien og foreslog yderligere en række initiativer til at udbygge og styrke EU's cybermodstandsdygtighed, afskrækkelse og forsvarsindsats. EU-Kommissionen fastslår, at cybersikkerhedspakken "vil skabe større robusthed og strategisk autonomi, hvilket vil styrke kapaciteten med hensyn til teknologier og færdigheder samt bidrage til at skabe et stærkt indre marked".[53] I 2017 er der altså kommet eksplicit fokus på sammenhængen mellem strategisk autonomi, indre marked og EU's teknologiske kapacitet.[54] I lyset af den iagttagelse og rapportens fokus er det bemærkelsesværdigt, at der i 2017

51. Ibid., s. 13.
52. Ibid., s. 14.
53. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *Modstandsdygtighed, afskrækkelse og forsvar: opbygning af en stærk cybersikkerhed for EU*, 13. september 2013, s. 3, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52017JC0450&from=DA.
54. "Det kræver også en mere omfattende, tværpolitisk tilgang til opbygning af cyberrobusthed og strategisk autonomi med et stærkt indre marked, betydelige fremskridt i EU's teknologiske kapacitet og et langt større antal kvalificerede eksperter", EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *Modstandsdygtighed, afskrækkelse og forsvar,* s. 4.

ingen omtale er af konkrete digitale teknologier eller infrastrukturer som 5G eller AI.

EU-Kommissionen understreger i strategien, at selvom medlemsstaterne fortsat har ansvaret for den nationale sikkerhed, så "er truslens omfang og grænseoverskridende karakter et stærkt argument for aktioner på EU-plan, der tilskynder til og støtter medlemsstaternes udvikling og opretholdelse af større og bedre national cybersikkerhedskapacitet, mens der samtidig opbygges kapacitet på EU-niveau".[55] Med cybersikkerhedsstrategien fra 2013, NIS-direktivet og cybersikkerhedspakken berører EU her kernen af national sikkerhedspolitik og udfordrer dermed den traditionelle fordeling af sikkerhedspolitisk autoritet og ansvar i Europa, samtidig med at EU legitimerer yderligere EU-indsatser på cybersikkerhedsområdet, hvilket rejser grundlæggende spørgsmål om, hvad der skal sikres af hvem og hvordan.

De konkrete initiativer i pakken omfatter et forslag om at udvide og gøre ENISA permanent samt et forslag til at etablere en ikke-obligatorisk europæisk certificeringsordning, der skal understøtte sikkerheden i forbindelse med IKT-produkter, -tjenester og -processer. De to forslag blev til en samlet forordning om ENISA og cybersikkerhedscertificering af IKT (EU Cybersecurity Act), der trådte i kraft i juni 2019. Certificeringsordningen er baseret på ideen om, at standarder og normer kan harmoniseres i EU og skabe en balance mellem behovene for henholdsvis forbrugerbeskyttelse og konkurrenceevne. Desuden kan udviklingen af et succesfuldt certificeringsprogram få global rækkevidde på grund af EU's markedsstørrelse, som det er set med GDPR.[56] Certificeringsordningen er dermed en vigtig strategisk brik i EU's udmøntning af unionens teknologiske suverænitet.

Det samme er cyberpakkens forslag om oprettelse af et europæisk industri-, teknologi- og forskningskompetencecenter for cybersikkerhed. I december 2020 nåede EU-Parlamentet og EU-Rådet til foreløbig enighed om at oprette det europæiske industri-, teknologi- og forskningskompetencecenter for cybersikkerhed i Bukarest. Centret vil blive understøttet af et netværk af nationale koordinationscentre.[57] Det skal

55. Ibid., s. 3.
56. Potentialet for regulering bliver udfoldet yderligere i afsnittet om AI.
57. EU-Rådet, "Nyt kompetencecenter og netværk for cybersikkerhed: uformel aftale med Europa-Parlamentet," EU-Rådet, 11. december 2020, https://www.consilium.europa.eu/da/

bidrage til styrke EU's konkurrenceevne, øge unionens autonomi på cybersikkerhedsområdet og sikre det digitale indre marked på områder som e-handel, intelligent mobilitet og tingenes internet.[58] Thierry Breton, kommissær for det indre marked, udtrykte klart centrets betydning for koblingen mellem marked, cybersikkerhed og strategisk autnomi: "It will help us reinforce our industrial and technological capacities in cybersecurity [...] it will enhance our strategic autonomy at a time when cybersecurity is more needed than ever".[59] Det blev fulgt op i april 2021, da rådet besluttede endeligt at godkende placeringen af centret. I den forbindelse understregede rådets portugisiske forperson ligeledes, at centret vil styrke EU's strategiske autonomi inden for cyberdomænet.[60]

3.1.4. Cybersikkerhed og teknologisk suverænitet i det digitale årti

I december 2020 fremlagde EU-Kommissionen og EU-Udenrigstjenesten en ny cybersikkerhedsstrategi, *EU's strategi for cybersikkerhed for det digitale årti*.[61] EU-Kommissionen fremhæver i strategien, at "truselsbilledet forværres af geopolitiske spændinger over det globale og åbne internet og over kontrollen med teknologier i hele forsyningskæden".[62] Chefen for EU's udenrigsanliggender, Josep Borrell, kæder ligeledes strategien sammen med EU's teknologiske suverænitet: "We need to enhance the security of our critical infrastructures, protect key technological sectors and strengthen our technological sovereignty."[63] Teknologisk suverænitet bliver også fremhævet blandt strategiens indsatsområder. Overordnet bygger strategien på regulerings-, investerings-

press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/.

58. EU-Rådet, "Nyt kompetencecenter og netværk for cybersikkerhed".
59. EU-Kommissionen, "Commission welcomes political agreement on the Cybersecurity Competence Centre and Network," EU-Kommissionen, 11. december 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384.
60. EU-Rådet, "Bucharest-based Cybersecurity Competence Centre gets green light from Council," EU-Rådet, 20. april 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/?utm_source=dsms-auto&utm_medium=email&utm_campaign=-Bucharest-based+Cybersecurity+Competence+Centre+gets+green+light+from+Council.
61. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *EU's strategi for cybersikkerhed for det digitale årti*, 16. december 2020, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52020JC0018&from=DA.
62. Ibid., s. 1.
63. Joseph Borrell, "Make cyberspace a safer place," *EEAS*, 17. december 2020, https://eeas.europa.eu/headquarters/headquarters-homepage_en/90747/Make%20cyberspace%20a%20safer%20place.

og policytiltag, der er målrettet tre indsatsområder: 1) modstandsdygtighed, teknologisk suverænitet og lederskab, 2) opbygning af operationel kapacitet til at forebygge, modvirke og reagere og 3) fremme af et globalt og åbent cyberspace.[64] Økonomisk understøttes strategien af de massive investeringer i digitalisering, der følger af EU's genopretningspakke og budget for 2021-2027. I budgettet er der således afsat 1,7 milliarder euro alene til at styrke europæisk cybersikkerhed.[65]

Flere af strategiens tiltag og delmål anskueliggør sammenhængen mellem cybersikkerhed, digitalisering og marked. Det bliver f.eks. understreget, at "cybersikkerhed skal integreres i alle disse digitale investeringer, navnlig centrale teknologier som AI, kryptering og kvantedatabehandling under anvendelse af incitamenter, forpligtelser og benchmarks. Dette kan stimulere væksten i den europæiske cybersikkerhedsindustri og skabe den sikkerhed, der er nødvendig for at lette udfasningen af eksisterende systemer."[66] I forlængelse heraf slår strategien – med implicit reference til teknologisk suverænitet – fast, at "det kommende årti er EU's mulighed for at blive førende i udviklingen af sikre teknologier i hele forsyningskæden. Sikring af robusthed og stærkere industriel og teknologisk kapacitet inden for cybersikkerhed bør mobilisere alle nødvendige regulerings-, investerings- og politikinstrumenter."[67]

Et af strategiens delmål er at styrke af EU's teknologiske forsyningskæde. Her fremhæver EU-Kommissionen, at de planlagte økonomiske investeringer i digital omstilling giver "EU en enestående mulighed for at samle sine aktiver og dermed fremme sin industristrategi og sit lederskab inden for digitale teknologier og cybersikkerhed i hele den digitale forsyningskæde (herunder data og cloud, næste generation af processorteknologier, ultrasikker konnektivitet og 6G-net) i overensstemmelse med EU's værdier og prioriteter".[68] Konkret ønsker EU-Kommissionen, at EU, medlemslandene og industrien skal investere i og udvide samarbejdet i det foreslåede industri-, teknologi- og forskningskompetencecenter

64. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *EU's strategi for cybersikkerhed for det digitale årti*, s. 4-5.
65. EU-Kommisionen, "Digital Europe Programme".
66. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *EU's strategi for cybersikkerhed for det digitale årti*, s. 5,
67. Ibid.
68. Ibid., s. 11.

for cybersikkerhed og netværket af koordinationscentre (CCCN). Disse "bør med input fra industrien og akademiske kredse spille en central rolle med hensyn til at udvikle EU's teknologiske suverænitet inden for cybersikkerhed, opbygge kapacitet til at sikre følsomme infrastrukturer såsom 5G og mindske afhængigheden af andre dele af verden for de mest afgørende teknologier".[69]

Strategien indeholder yderligere en række væsentlige tiltag, der indirekte og i mindre grad har relation til teknologisk suverænitet, herunder opdatering af netværks- og informationsdirektivet,[70] udvikling af en offentlig europæisk domænenavnstjeneste,[71] oprettelsen af en fælles cyberenhed, der skal udfylde den europæiske ramme for håndtering af cybersikkerhedskriser,[72] opbygning af et europæisk cybersikkerhedsskjold[73] og styrkelse af europæisk cyberafskrækkelse og -forsvar.[74] Samlet set udtrykker EU's seneste cybersikkerhedsstrategi et øget fokus på betydningen af teknologisk suverænitet for cybersikkerhed og europæisk autonomi. Samtidig udtrykker strategien, at cybersikkerhed, digital teknologiudvikling og markedsbaserede industri-, erhvervs- og innovationsindsatser ikke kan skilles, men er gensidigt afhængige.

Boks 1. 5G: Mellem cybersikkerhed og teknologisk suverænitet

En væsentlig del af EU's arbejde i spændingsfeltet mellem cybersikkerhed og teknologisk suverænitet har fokuseret på udrulningen af 5G-netværket. Udrulningen af 5G har vakt betydelig bekymring i Vesten. I centrum står en diskussion om, hvorvidt den kinesiske udbyder Huawei bør tildeles en central rolle i udrulningen af 5G. Debatten har primært drejet sig som om, at udrulning af 5G i flere lande bliver opfattet som et nationalt sikkerhedshensyn. Det har været den dominerende opfattelse i lande som USA, Australien og

69. Ibid., s. 12.
70. Ibid., s. 5-6.
71. Ibid., s. 11.
72. Ibid., s. 14-15.
73. Margaritis Schinas og Thierry Breton, "EU-kommissærer: Europa har brug for et cyberskjold," *Altinget*, 6. januar 2021, https://www.altinget.dk/digital/artikel/eu-kommissionen-europa-boer-indfoere-en-cyberdoktrin.
74. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *EU's strategi for cybersikkerhed for det digitale årti*, s. 17-19.

Japan, men er det nu også i store dele af Europa. Hvorvidt EU-landene formår at udvikle og implementere en fælles tilgang til 5G-sikkerhedsspørgsmålet, kan betragtes som en vigtig test for EU's teknologiske suverænitet og strategiske autonomi på det digitale område.

I kølvandet på debatten om Huawei og udrulning af 5G vedtog EU-Kommissionen i marts 2019 et forslag til en fælles EU-tilgang til sikring af 5G,[75] og i januar 2020 blev en EU-værktøjskasse med fokus på 5G-sikkerhed offentliggjort.[76] Af den seneste EU-cybersikkerhedsstrategi fremgår det, at EU opfordrer til, at tiltagene fra værktøjskassen er gennemført senest i andet kvartal af 2021. EU tilskynder desuden medlemsstaterne til fortsat at følge de fremskridt, der gøres, og sikre yderligere tilpasning af tilgangene. Strategien gør klart, at "på EU-plan vil tre hovedmål blive fulgt for at støtte denne proces: sikring af yderligere konvergens i tilgange til risikobegrænsning i hele EU, støtte til løbende udveksling af viden og kapacitetsopbygning og fremme af modstandsdygtighed i forsyningskæden og andre af EU's strategiske sikkerhedsmål".[77]

Spørgsmålet om udrulning af 5G og valg af leverandør er særligt interessant, da det viser, hvordan EU's dobbelte fokus på cybersikkerhed og teknologisk suverænitet gør, at det bliver særdeles vanskeligt at skille marked, sikkerhed og digitalisering. Til trods for – eller måske netop på grund af – bred europæisk konsensus om behovet for, at markedsfrihed, sikkerhed og beskyttelse af individuelle rettigheder er forbundet og balanceret i EU's politik og regulering, afspejler EU's og de nationale tilgange til 5G, at der fortsat ikke er enighed om, hvordan teknologisk suverænitet og teknologiske sikkerhedsstandarder kan forenes med EU's liberale markedslogik.[78]

75. EU-Kommissionen, "Kommissionens henstilling (EU) 2019/534 af 26. marts 2019, Cybersikkerheden i forbindelse med 5G-net" (*Den Europæiske Unions Tidende*, 29. marts 2019), https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32019H0534&from=DA.
76. EU-Kommissionen, *En EU-værktøjskasse til udrulning af sikre 5G-net i EU*, 29. januar 2020, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0050:FIN:DA:PDF; NIS Cooperation Group, *Cybersikkerhed i 5G-net: EU-værktøjskasse med risikobegrænsende foranstaltninger* (CG-publikation, januar 2020), https://cfcs.dk/globalassets/cfcs/dokumenter/telemyndighed/-cybersikkerhed-i-5g-net---eu-vaerktoejskasse-.pdf.
77. EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik, *EU's strategi for cybersikkerhed for det digitale årti*, s. 8-9.
78. For yderligere behandling af betydningen af 5G for EU's suverænitet, se f.eks. A. K. Jakobsson og M. Stolz, "Principled big tech: European pursuit of technological autonomy,"

3.1.5. Konklusion: Cybersikkerhed gennem det indre marked

I løbet af det seneste årti har EU etableret cybertruslen som en tværgående sikkerhedstrussel, der er uløseligt knyttet til den tiltagende digitalisering og kræver transnationale europæiske løsninger. Cybersikkerhed er derfor et væsentligt prioritetsområde for EU, der samtidig går på tværs af flere af unionens centrale økonomiske og markedspolitiske tiltag. Det betyder, at EU's cybersikkerhedspolitik placerer sig i et spændingsfelt mellem digitalisering, sikkerhed og marked. Dermed har EU's cybersikkerhedspolitik været med til at skabe grobund for unionens ambitioner om teknologisk suverænitet.

Samtidig er EU underlagt medlemsstaternes nationale sikkerhedspolitiske overmyndighed.[79] Det betyder, at EU's cybersikkerhedspolitiske ageren er begrænset. Medlemslandene er fortsat sig selv nærmest, når det f.eks. kommer til den militære og efterretningsmæssige del af cybersikkerhed. EU's cybersikkerhedspolitiske handlerum styrkes dog, når cybersikkerhed bliver kædet sammen teknologisk suverænitet og placeres eksplicit i et spændingsfelt mellem digitalisering, marked og sikkerhed. Cybersikkerhed bliver dermed både et middel for EU til at føre sikkerhedspolitik gennem sit indre markeds-mandat og en drivkraft for yderligere integration og harmonisering af det indre marked med økonomisk vækst for øje.

EU's sammenkædning af teknologisk suverænitet og cybersikkerhed integrerer sikkerheds- og forsvarspolitik og industri-, erhvervs- og innovationspolitik yderligere. Sammenkædningen af teknologisk suverænitet og cybersikkerhed styrker dermed et i forvejen eksisterende digitalt markeds-sikkerheds-neksus, der udfordrer den oprindelige fordeling af autoritet og ansvar mellem EU, dets medlemsstater og private virksomheder. Det er et dilemmafyldt neksus, som fordrer, at EU og dets medlemsstater gentænker og afvejer de sikkerhedspolitiske autoritets- og ansvarsforhold i lyset af sammensmeltningen af digitalisering, sikkerhed

i *Strategic autonomy and the transformation of the EU: New agendas for security, diplomacy, trade and technology*, red. N. Helwig, Finnish Institute of International Affairs (2021), bind 67, s. 105-130.

79. 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."

og marked samt sikkerheds- og forsvarspolitik og industri-, erhvervs- og innovationspolitik.

3.2. Kunstig intelligens

AI står centralt i den globale teknologikonkurrence. Udvikling og implementering af AI bliver ofte set som en afgørende parameter i den tiltagende stormagtsrivalisering mellem særligt USA og Kina.[80] EU har også meldt sig ind i kampen om at fremme udvikling og regulering af AI, der står centralt i unionens ambition om teknologisk suverænitet. EU har imidlertid været mere optaget af AI's økonomiske og sociale effekter end af de geopolitiske og militære.[81] I EU-regi bliver udvikling og regulering af AI – og dermed teknologisk suverænitet – primært kædet sammen med europæiske værdier. Et politisk udtryk, som særligt EU-Kommissionen bruger, hvorved den implicit henviser til de grundlæggende rettigheder og retsstatsprincipper, der er nedfældet i EU-traktaterne og EU-charteret om grundlæggende rettigheder.[82] Den linje er i tråd med EU-Kommissionens industri- og datastrategier,[83] der begge sætter kombinationen af regulering og fastholdelse af europæiske værdier og borgerrettigheder i centrum for EU's strategiske ageren i en verden præget af geopolitiske spændinger og intensiveret økonomisk konkurrence. Dette afsnit analyserer EU's politik for udvikling og regulering af AI, de udfordringer, EU står over for på AI-området, samt sikkerheds- og forsvarspolitiske dimensioner af EU's AI-politik.

80. Jacobsen og Liebetrau, "Kunstig intelligens, militær strategi og international konkurrence".
81. Ulrike Esther Franke, *Artificial Divide: How Europe and America Could Clash Over* AI, European Council on Foreign Relations, januar 2021, https://ecfr.eu/wp-content/uploads/Artificial-divide-How-Europe-and-America-could-clash-over-AI.pdf. Den franske AI-strategi er delvist en undtagelse, da den fokuserer eksplicit på farerne ved afhængighed af Kina og USA. Cédric Villani, "For A Meaningful Artificial Intelligence – Towards A French And Euopean Strategy," Mission assigned by the Prime Minister Édouard Philippe (marts 2018), https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.
82. Access Now, *Europe's Approach To Artificial Intelligence: How AI Strategy is Evolving*, december 2020, s. 4, https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf.
83. EU-Kommissionen, *En ny industristrategi for Europa 2020*, 10. marts 2020, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52020DC0102&from=DA; EU-Kommissionen, *EU's datastrategi 2020 – En europæisk strategi for data*, 19. februar 2020, https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

Boks 2. Hvad er kunstig intelligens?

AI er grundlæggende en muliggørende og understøttende teknologi, der benytter software, data og algoritmer til på forskellig måde at lære at træffe beslutninger og løse problemer i lighed med mennesker. I dag varetager AI primært specifikke opgaver på afgrænsede områder – til f.eks. kontrol, forudsigelse og vejledning (snæver AI). Særligt tre forhold og deres indbyrdes konvergens forventes at sætte yderligere skub i udviklingen og anvendelsen af AI: Eksponentiel vækst i computeres regnekraft og hukommelse. Udvikling af mere avancerede algoritmer. Eksplosion af data frembragt af blandt andet 5G-netværk og tingenes internet. Den forventede udvikling har medført diskussion af, hvorvidt vi en dag får AI, der kan måle sig med menneskelig intelligens (bred AI), men det er fortsat ikke muligt at sige med sikkerhed, hvornår – eller overhovedet om – vi når dertil, hvor AI opnår samme kompleksitet som den menneskelige intelligens.

Desuden er der en lang række udfordringer ved den potentielle anvendelse af AI, der gør det svært at forudsige, hvilken retning udviklingen og implementeringen af AI vil tage. Rent praktisk skal AI kunne anvendes i en række specifikke, komplekse, dynamiske og uforudsigelige kontekster. Dertil kommer teknik- og sikkerhedsudfordringer med hensyn til f.eks. manipulation med og bias i systemerne. Desuden er der politiske og sociale spørgsmål om, hvorvidt politikere, fagpersoner og befolkninger grundlæggende stoler på og har tillid til AI, etiske og moralske spørgsmål om at lade AI træffe væsentlige beslutning og juridiske spørgsmål om lovligheden af anvendelsen af AI.[84]

3.2.1. AI baseret på regulering og europæiske værdier

AI blev gjort til et særskilt politikområde under Jean-Claude Junckers formandskab for EU-Kommissionen.[85] Det skete i forbindelse med implementering af strategien for det digitale indre marked,[86] der banede vejen for en række konkrete EU-initiativer på AI-området. Dermed blev

84. Afsnittet bygger på Breitenbauch og Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark*.
85. Juncker var kommissionsforperson fra 2014-2019.
86. EU-Kommissionen, *En strategi for et digitalt indre marked i EU*.

AI en del af EU's bredere vision for digitalisering, der kan opsummeres i tre punkter: yderligere økonomiske integration, harmoniseret regulering af nye teknologier og fremme af europæiske værdier. Jean-Claude Juncker sammenfattede det således i sin state of the union-tale i 2018:

> *"Only a strong and united Europe can master the challenges of global digitisation. It is because of our single market – the largest in the world – that we can set standards for big data, artificial intelligence, and automation. And that we are able to uphold Europeans' values, rights and identities in doing so. But we can only do so if we stand united."*[87]

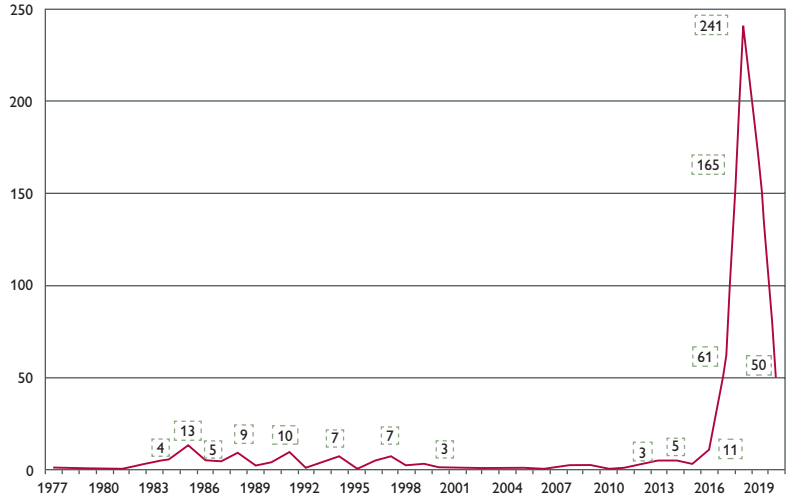
Talen fokuserede på europæisk suverænitet. Juncker understregede, at "den geopolitiske situation viser, at dette er Europas øjeblik: Det er nu, Europa må hævde sin suverænitet".[88] Han satte dermed en streg under, at et stærkt og forenet Europa bedst kan håndtere udfordringerne fra den verdensomspændende digitalisering. Det styrkede fokus på AI har de senere år været en væsentlig drivkraft bag EU's digitale ambitioner, herunder teknologisk suverænitet.

Som det fremgår af figur 4, er antallet af referencer til AI i EU's politik- og lovtekster eksploderet de seneste fem år.[89] EU-Kommissionens fokus på AI er således ikke afgrænset til den digitale sektor alene, men spænder over en række politikområder som sundhed, transport, klima, landbrug og erhverv.[90] Det illustrerer AI's tværgående karakter samt teknologiens mange muliggørende og understøttende potentialer. Desuden understreger det AI's strategiske betydning for EU's ambition om teknologisk suverænitet. EU-Kommissionens fokus på AI har også medvirket til at tilskynde medlemslandene til at udvikle nationale AI-strategier. Mellem 2018 og 2020 offentliggjorde ikke færre end 21 EU-lande natio-

87. Jean-Claude Juncker, "State of the Union 2018: The Hour of European Sovereignty," tale til Europa-Parlamentet, 2018, s. 5, https://ec.europa.eu/info/sites/info/files/soteu2018-speech_en_0.pdf.
88. Jean-Claude Juncker, "Unionens Tilstand 2018. Tiden er inde til et suverænt Europa," tale til Europa-Parlamentet, 2018, s. 5, https://ec.europa.eu/info/sites/info/files/soteu2018-speech_da_0.pdf.
89. Selvom EU's tilgang til AI som et særskilt politikområde er relativt ny, så er den delvist vokset ud af samarbejder inden for videnskabspolitik samt regulering af teknologier og marked.
90. Access Now, *Europe's Approach To Artificial Intelligence: How AI Strategy is Evolving*, s. 4.

nale AI-strategier,[91] herunder Danmark.[92] Senest har et studie sponsoreret af EU-Kommissionen og OECD konkluderet, at samtlige EU-medlemslande vil have fremlagt en national AI-strategi inden udgangen af 2021.[93]

Figur 4: Antal gange, AI er nævnt i forskellige EU-politik- og lovtekster[94]



EU-Kommissionens første samlede strategi for AI fra 2018 slår fast, at EU "bør have en koordineret tilgang for at få mest muligt ud af de muligheder, som AI giver, og for at løse de nye udfordringer, som AI medfører", og den slår fast, at "EU kan gå forrest i udviklingen og brugen af AI til det gode og for alle, på grundlag af Unionens værdier og styrker".[95]

91. Ulrike Esther Franke, *Artificial Divide*.
92. Regeringen, Finansministeriet og Erhvervsministeriet, *National strategi for kunstig intelligens,* marts 2019, s. 5, https://www.regeringen.dk/media/6537/ai-strategi_web.pdf.
93. Vincent V. Roy, Fiammetta Rossetti, Karine Perset og Laura Galindo-Romero, *AI-Watch – National strategies on Artificial Intelligence: A European perspective* (Luxembourg: Publications Office of the European Union, 2021), DOI: 10.2760/069178.
94. Oversigten er skabt ud fra Eurolex-databasen. Se Jędrzej Niklas and Lina Dencik (2020), *European Artificial Intelligence Policy: Mapping The Institutional Landscape*, Data Justice Lab, Cardiff University.
95. EU-Kommissionen, "Kunstig intelligens for Europa," *EU-Kommissionen* COM (2018) 237 Final. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:

Ved præsentationen af sit politiske program satte Ursula von der Leyen yderligere en streg under behovet for en koordineret europæisk tilgang for at sikre de menneskelige og etiske konsekvenser af udviklingen af AI.

> *"Digital technologies, especially Artificial Intelligence (AI), are transforming the world at an unprecedented speed [...] In my first 100 days in office, I will put forward legislation for a coordinated European approach on the human and ethical implications of Artificial Intelligence."*[96]

Målet om, at udvikling og anvendelse af AI skal ske i overensstemmelse med europæiske værdier,[97] står i dag som mantraet for EU's tilgang til AI. Det betyder, at etik, brugerrettigheder og sikkerhed udgør en central del af grundlaget for EU's strategiske fokus på AI-udvikling. EU-Kommissionen satser på, at gennemtænkt regulering og gennemsigtige standarder kan skabe et solidt grundlag for, at europæiske virksomheder kan udvikle og konkurrere med hensyn til AI-løsninger, som har indlejret europæiske værdier. Senest har EU-Kommissionen i foråret 2021 præsenteret et udkast til en forordning om regulering af AI. EU's grundlæggende argumenter for at indføre denne lovgivning er fortsat at sikre borgernes rettigheder og tillid samt styrke innovation og udvikling inden for AI. Det udtrykte Margrethe Vestager, Executive Vice-President for A Europe Fit for the Digital Age and Competition, klart ved lanceringen af udkastet:[98]

> *"On Artificial Intelligence, trust is a must, not a nice to have. With these landmark rules, the EU is spearheading the development of new global norms to make sure AI can be trusted. By setting the standards, we can pave the way to ethical technology worldwide and ensure that the EU remains competitive along the way. Future-proof and innovation-friendly, our rules will intervene where strictly needed: when the safety and fundamental rights of EU citizens are at stake."*

52018DC0237&from=DA.

96. Ursula von der Leyen, *A Union that strives for more,* s. 13.
97. Det henviser implicit til de retsstatsprincipper og grundlæggende rettigheder, som EU er bygget på.
98. EU-Kommissionen, "Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence", EU-Kommissionen, 21. april 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

EU-Kommissionens AI-tilgang er således i tråd med EU's overordnede industripolitiske tilgang. Det fremgår af EU's industristrategi fra 2020, at "det er vigtigere end nogensinde, at Europa gør sin indflydelse gældende, fastholder sine værdier og kæmper for lige konkurrencevilkår. Det handler om Europas suverænitet".[99] Desuden bliver det fremhævet i strategien, at "EU skal udnytte virkningen, størrelsen og integrationen af det indre marked til at fastsætte globale standarder. At være i stand til at skabe globale standarder af høj kvalitet, der er kendetegnende for Europas værdier og principper, vil kun styrke vores strategiske autonomi og den industrielle konkurrenceevne."[100]

EU-Kommissionens generelle industripolitik og specifikke AI-politik støtter sig således til unionens markeds- og lovgivningsmæssige indflydelse. EU-Kommissionen baserer sin AI-strategi på værdier, industristandarder, sikkerhed, juridisk klarhed og offentlig legitimitet. Ligesom GDPR har sat en høj standard for databeskyttelse, er det EU-Kommissionens mål, at EU's værdibaserede og regulerende tilgang til udvikling og anvendelse af AI vil blive efterstræbelsesværdig globalt. Læren fra GDPR tilsiger en vis optimisme. Med et stærkt fokus på governance og regulering af AI kan EU påvirke, hvilke typer AI der bliver udviklet, og hvordan de bliver anvendt. Som Nathalie Smuha har påpeget, "first-mover advantage that can be gained from setting the standards means the race to AI has also become a race to AI regulation".[101]

EU-Kommissionens strategi finder opbakning i professor Anu Bradfords bog *The Brussels Effect: How the European Union Rules the World*.[102] Her argumenterer Bradford for, at EU-regler ofte vedtages af resten af verden af alene på grund af markedskræfterne og uden nogen tvang. Grundlaget for denne unikke effekt er, at multinationale virksomheder, der ønsker at drive forretning i EU, ofte finder, det er mere praktisk at lade EU-reglerne styre deres globale operationer. Får EU succes med sin AI-strategi, kan EU på den måde skabe et globalt race-to-the-top med hensyn til regulering af AI. Det vil samtidig øge sandsynligheden for, at

99. EU-Kommissionen, *En ny industristrategi for Europa*, s. 1.
100. Ibid., s. 3.
101. Nathalie Smuha, "Europe's approach to AI governance: time for a vision," *Friends of Europe*, 2. april 2020, https://www.friendsofeurope.org/insights/europes-approach-to-ai-governance-time-for-a-vision/.
102. Anu Bredford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

EU's AI-politik kan fungere som modvægt til den militarisering af AI, som stormagtsrivaliseringen mellem USA og Kina risikerer at føre til.[103]

3.2.2. EU's AI-udfordringer

Kritikere har dog påpeget, at EU indtil videre har været mere interesseret i at skabe regler og regulering for AI-kapløbet end i at vinde det, hvorfor vendingen "dommere vinder ikke kampe" flittigt bliver brugt til at klandre EU-Kommissionen.[104] Eller som den tidligere svenske statsminister Carl Bildt har udtrykt det: "You simply can't regulate unicorns into existence."[105] Desuden bliver det ofte påpeget, at EU og europæiske virksomheder allerede halter langt efter USA og Kina, hvad angår AI-viden og investeringer.[106] En anden grundlæggende udfordring for EU angår indsamling og opbevaring af data, der udgør en meget væsentlig del af grundlaget for udvikling og anvendelse af AI. Udfordringen skyldes flere ting, herunder at offentlig dataindsamling og -anvendelse primært et nationalt anliggende i EU, de europæiske landes befolkningsstørrelser kontra USA's og Kinas og EU's restriktive databeskyttelseslovgivning. De kinesiske og amerikanske virksomheder drager fordel af store, homogene hjemmemarkeder, mens europæiske virksomheder kæmper på grund af deres fragmenterede markeder.

Desuden medfører EU's restriktive databeskyttelseslovgivning, at europæiske virksomheder og myndigheder – i sammenligning med USA's og Kinas – har relativt begrænset adgang til data. Som den tyske kansler, Angela Merkel, har bemærket: "I USA er kontrol over personoplysninger i stort omfang privatiseret. I Kina er det modsatte sandt: Staten

103. Jacobsen og Liebetrau, "Kunstig intelligens, militær strategi og international konkurrence".
104. Theodore Christakis, "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy," available at SSRN (2020); Guntram Wolff, "Europe may be the world's AI referee, but referees don't win," *Politico*, 17. februar 2020 https://www.politico.eu/article/europe-may-be-the-worlds-ai-referee-but-referees-dont-win-margrethe-vestager/; José Ignacio Torreblanca, "Referees don't win games: Europe and the digital great game," European Council on Foreign Relations, 9. februar 2021, https://ecfr.eu/article/referees-dont-win-games-europe-and-the-digital-great-game/.
105. Melissa Heikkilä, "The Achilles' heel of Europe's AI strategy," *Politico*, 13. marts 2020, https://www.politico.eu/article/europe-ai-strategy-weakness/.
106. Rapporten *Who Is Winning the AI Race: China, the EU, or the United States? – 2021 Update* giver et solidt overblik. Daniel Castro og Michael McLaughlin, *Who Is Winning the AI Race: China, the EU, or the United States? – 2021 Update* (Centre for Data Innovation, januar 2020), https://www2.datainnovation.org/2021-china-eu-us-ai.pdf.

har organiseret en overtagelse."[107] Merkel tilføjede, at det er mellem disse to poler, at Europa bliver nødt til at finde sin plads. I forlængelse heraf er EU-Kommissionens 2021-udkast til forordning om regulering af AI blevet mødt med en frygt for, at reguleringen af AI bliver en hæmsko for europæiske AI-virksomheder, hvilket vil sende Europe endnu længere tilbage i det globale AI-kapløb.[108] Samtidig er udspillet dog blevet kritiseret for at være både for upræcist og for snævert.[109]

Boks 3. Europæisk datastrategi[110] og cloud

EU blevet kritiseret for at halte efter USA og Kina, når det kommer til databrug bredt set. I februar 2020 fremlagde EU-Kommissionen imidlertid en "En europæisk strategi for data". Det fremgår af strategien, der er den første af sin art, at EU-Kommissionen forventer, at Europas dataøkonomi kan blive næsten tredoblet i perioden 2018-2025 ved at gå fra en værdi af 301 milliarder euro til en værdi af 829 milliarder euro, hvorfor EU skal styrke sin dataøkonomiske formåen. I strategien redegør EU-Kommissionen for "sin vision for, hvordan Europa kan bevare sin teknologiske og digitale suverænitet og være den globale digitale leder". Strategien er dermed væsentlig del af EU's strategiske satsning på at styrke unionens teknologiske suverænitet ved at frigøre og omsætte værdien af europæiske data.

Ifølge strategien har EU-Kommissionen til hensigt "at finansiere etableringen af fælles interoperable dataområder i hele EU inden for strategiske sektorer. Områderne har til formål at afhjælpe juridiske og tekniske hindringer for datadeling på tværs af organisati-

107. The Economist, "Can the EU Become Another AI Superpower?," *The Economist*, 22. september 2018, https://www.economist.com/business/2018/09/20/can-the-eu-become-another-ai-superpower.
108. Christakis, "European Digital Sovereignty"; Matthias Bauer og Fredrik Erixon, *Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls* (European Center for International Political Economy, 2020), https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf.
109. For en flersidig diskussion og kritik af udspillet, se denne temadebat i Altinget: Jarl Viktor Schultz, "Ny temadebat: Hvordan skal vi udnytte kunstig intelligens?," *Altinget*, 9. juni 2021, https://www.altinget.dk/digital/artikel/ny-temadebat-hvordan-skal-vi-udnytte-kunstig-intelligens.
110. Teksten i boksen, der behandler datastrategien og datarum, trækker på: EU-Kommissionen, *EU's datastrategi 2020*.

oner ved at kombinere de nødvendige værktøjer og infrastrukturer og afhjælpe problemer med hensyn til tillid, f.eks. ved hjælp af fælles regler, der er udviklet til området. Områderne skal omfatte: i) indførelsen af datadelingsværktøjer og -platforme, ii) oprettelsen af dataforvaltningsrammer og iii) en forbedring af datatilgængeligheden og dataenes kvalitet og interoperabilitet både i domænespecifik sammenhæng og på tværs af sektorer."

Europæisk cloud-infrastruktur: GAIA-X

I sammenhæng med diskussionerne om bedre europæisk dataudnyttelse og -beskyttelse har EU også rettet fokus mod etablering af en europæisk cloud-infrastruktur.[111] I dag er den europæiske brug af cloud-tjenester domineret af de amerikanske virksomheder Amazon, Microsoft, Google og IBM, men i 2019 erklærede Tyskland og Frankrig støtte til et fælles europæisk cloud-projekt, der skal sikre "oprettelse af en sikker og pålidelig datainfrastruktur for Europa".[112] I den fælles pressemeddelelse lagde både den tyske økonomiminister, Peter Altmaier, og hans franske modstykke Bruno Le Maire, vægt på, at projektet understøtter en genrejsning af europæisk digital suverænitet. Det blev i 2020 fulgt op af et fælles fransk-tysk positionspapir, støttet af både offentlige og private parter, der gør klart, at projektet GAIA-X skal "facilitate the creation of European data and AI driven ecosystems, to guarantee data sovereignty, and to ensure that value creation remains with the individual participants".[113]

Siden har EU-Kommissionen udtrykt støtte til projektet i den fælles europæiske datastrategi og senest i "2030 Digital Compass:

111. EU-Kommissionen, "Cloud computing," EU-Kommissionen, senest opdateret 23. september 2021, https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.
112. The German Federal Ministry for Economic Affairs and Energy og French Ministry of Economy and Finance, "Press Release on Franco-German common work on a secure and trustworthy data infrastructure," 29. oktober 2019, https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2019/20191029-press-release-on-franco-german-common-work-on-a-secure-and-trustworthy-data-infrastructure.html.
113. The German Federal Ministry for Economic Affairs and Energy and the French Ministry of Economy and Finance, "Franco-German Position on GAIA-X," 18. februar 2020, https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10.

the European way for the Digital Decade".[114] EU-landenes regeringer udtrykte også støtte til GAIA-X, da de i oktober 2020 underskrev en fælles deklaration, hvor de lover at investere op til 10 milliarder euro i projektet.[115] Regeringerne lægger vægt på, at:

"Cloud computing tilvejebringer den nødvendige databehandlingskapacitet for at muliggøre datadrevet innovation og dermed det presserende behov for at samarbejde for at fremme Europas teknologiske suverænitet og sikre, at vores virksomheder og den offentlige sektor har adgang til modstandsdygtig og konkurrencedygtig datalagrings- og behandlingskapacitet. Europas lederskab på dette område er afgørende for at muliggøre AI, tingenes internet og 5G/6G."[116]

Gaia-X-initiativet fremstår som et af EU's væsentligste bud på at sikre datasuverænitet og dataforvaltning. Dermed er GAIA-X også en afgørende del af EU's strategiske satsning på at styrke unionen samlede teknologiske suverænitet ved at skabe kontrol med samt opbevaring og beskyttelse af data. I følge Paul Timmers – tidligere direktør for EU-Kommissionens Generaldirektorat for Kommunikationsnet, Indhold og Teknologi (DG-Connect) og nu tilknyttet University of Oxford – er projektet en decideret lakmusprøve for EU's ide om teknologisk suverænitet.[117]

Kritikerne fremhæver desuden, at Europa halter efter både USA og Kina, når det kommer til uddannelse og fastholdelse af arbejdskraft med tilstrækkelige AI-færdigheder. Et emne, der bliver berørt i mange af de nationale europæiske AI-strategier.[118] Afhængighed af hardwarekomponen-

114. EU-Kommissionen, *Det digitale kompas 2030: Europas kurs i det digitale årti*, 9. marts 2021, https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0002.02/DOC_1&format=PDF.
115. EU-medlemslandene, *Declaration: Building the next generation cloud for businesses and the public sector in the EU,* 15. oktober 2020, https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe.
116. Ibid., s. 3.
117. Laurens Cerulus, "Europe's litmus test over cloud computing push," *Politico*, 28. juli 2020, https://www.politico.eu/article/shades-of-sovereignty-dent-european-cloud-dreams/.
118. Det gælder f.eks. for de tyske og de franske nationale AI-strategier; henholdsvis The Federal Government of Germany, *Artificial Intelligence Strategy of the German Federal Government,* ki-strategie-deutschlands.de (december 2020), https://www.ki-strategie-deutschland.de/fi-

ter samt risikoen for opkøb fra amerikanske og kinesiske techgiganter bliver fremhævet som yderligere udfordringer for, at EU kan indfri sine AI-mål. De europæiske befolkningers AI-skepsis bliver tillige fremført som et potentielt benspænd for Europas AI-udvikling. Befolkningerne i Europa har en tendens til at være skeptiske over for AI, hvorimod befolkningerne i USA og særligt Kina er markant mere optimistiske og teknologibegejstrede.[119]

Det er imidlertid for tidligt at afskrive et tættere transatlantisk samarbejde på AI-området, der vil kunne afbøde flere af EU's AI-udfordringer. I kølvandet på det amerikanske valg i november 2020 fremlagde EU-Kommissionen en ny ramme for de transatlantiske forbindelser: "A new EU-US agenda for global change".[120] Her fremhæver EU nødvendigheden af fælles handlen og foreslår udarbejdelse af en transatlantisk AI-aftale, der opstiller forslag til regionale og globale AI-standarder tilpasset fælles transatlantiske værdier. Desuden foreslår EU oprettelsen af et "EU-US Trade and Technology Council (TTC)", hvis formål vil være:

> *"to jointly maximise opportunities for market-driven transatlantic collaboration, strengthen our technological and industrial leadership and expand bilateral trade and investment. It will focus on reducing trade barriers, developing compatible standards and regulatory approaches for new technologies, ensuring critical supply chain security, deepening research collaboration and promoting innovation and fair competition".*[121]

Oprettelsen af TTC blev til virkelighed på EU-US-topmødet 15 juni 2021. Her blev det fremhævet, at TTC er et forum, hvor USA og EU kan "coordinate approaches to key global trade, economic, and technology issues and to deepen transatlantic trade and economic relations based on shared democratic values".[122] Under TTC vil der blive oprettet

---

les/downloads/Fortschreibung_KI-Strategie_engl.pdf; Villani, *For A Meaningful Artificial Intelligence*.

119. Ulrike Franke, *Harnessing Artificial Intelligence*, European Council on Foreign Relations, juni 2019, https://www.ecfr.eu/page/-/3_Harnessing_artificial_intelligence.pdf.
120. EU-Kommissionen, *A new EU-US agenda for global change*, 2. december 2020, https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf.
121. Ibid., s. 7.
122. EU-Kommissionen, "EU-US launch Trade and Technology Council to lead values-based global digital transformation," EU-Kommissionen, 15. juni 2021, https://ec.europa.eu/

en række arbejdsgrupper, der skal operationalisere og omsætte de overordnede politiske mål på områder som teknologisk standardsætning (inklusive AI og tingenes internet) og sikring af forsyningskæder (for f.eks. semikonduktorer). Oprettelsen af TTC taler ind i det voksende fokus på geopolitik og teknologikonkurrence i både EU og USA.[123] I denne sammenhæng har præsident Joe Biden foreslået en "alliance af liberale demokratier", der kan udgøre et økonomisk og politisk alternativ til Kina.[124] Udmøntningen af lovord og planer om styrket transatlantisk samarbejde om udvikling, regulering og handel med teknologier bliver afgørende for, hvordan EU's ambition om teknologisk suverænitet bliver ført ud i livet. Det er dog langtfra givet, hvordan det transatlantiske teknologiske samarbejde vil udmønte sig, da der er både overlappende og divergerende synspunkter på tværs af Atlanten, herunder på områder som persondatabeskyttelse, regulering af big tech-virksomheder og udrulning af 5G og 6G.

3.2.3. Krusninger i det sikkerheds- og forsvarspolitiske dødvande

Mens EU har styrket sit økonomiske og retlige AI-fokus og sin økonomiske og retlige AI-indsats de senere år, så har unionen – og dens medlemslande – samtidig været påpasselige med at fremstille udvikling og implementering af AI som en strategisk og geopolitisk konkurrence.[125] De globale sikkerheds- og forsvarspolitiske overvejelser vedrørende AI-udvikling fylder således ikke ret meget, hverken i EU[126] eller i medlemslandene,[127] herunder i Danmark. Her er de sikkerheds- og forsvarspolitiske dimensioner af AI-udviklingen stort set fraværende i den nationale strategi for kunstig intelligens, der primært fokuserer på

commission/presscorner/detail/en/IP_21_2990.

123. Breitenbauch og Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark*.
124. Joseph R. Biden, Jr., "Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump," *Foreign Affairs,* (marts/april 2020), https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again.
125. Franke, *Harnessing Artificial Intelligence*.
126. Eksempelvis undgår AI-hvidbogen fra 2020 enhver diskussion af udviklingen og brugen af AI til dual-use eller militære formål.
127. Ulrike Franke, *Artificial Intelligence diplomacy: Artificial Intelligence governance as a new European Union external policy tool*, Europa-Parlamentet, juni 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf.

AI's potentiale for at "skabe økonomisk vækst og velfærd for alle".[128] EU's medlemslandes manglende strategiske fokus på de globale magt-, sikkerheds- og forsvarspolitiske konsekvenser af AI -udvikling har fået den tyske forsker Ulrike Franke til at konkludere, at der mangler opmærksomhed på og sammenhæng i både EU's og de europæiske landes tilgang til udvikling og anvendelse af AI i sikkerheds- og forsvarspolitiske kontekster.[129]

Den hidtil manglende diskussion af synergieffekterne mellem civil og militær anvendelse af AI på EU-niveau knytter sig til flere faktorer, herunder at forsvars- og sikkerhedspolitik hovedsageligt er forankret i medlemsstaterne, og det militære samarbejde i EU er karakteriseret ved relativ uenighed om både omfang og retning. Desuden divergerer Frankrigs og Tysklands grundlæggende prioriteringer på AI-området. Frankrig ser AI som en væsentlig del af den globale geopolitiske og militære konkurrence, mens Tyskland i højere grad fokuserer på økonomiske og sociale aspekter af AI.[130] Den manglende europæiske koordination og fokus på koblingerne mellem civil og militær AI kan få den effekt, at flere EU-medlemslande – herunder Danmark – må formodes at hælde mod amerikanske militære AI-løsninger, når der skal investeres militært. Desuden kan udviklingen og implementeringen af AI-understøttede militære teknologier blive en udfordring med hensyn til interoperabilitet, da EU-medlemslandene og de NATO-allierede vil have forskellige tilgange til og forskellig brug af militær AI.[131]

Det Europæiske Forsvarsagentur (EDA) tog et skridt mod øget europæisk samarbejde og koordination, da det i december 2020 vedtog en handlingsplan for AI i forsvarssammenhæng, der identificerer muligheder for et styrket europæisk samarbejde om udvikling af militær AI. EDA vil supplere handlingsplanen med en strategisk forskningsagenda, der skal stimulere udviklingen af militær AI yderligere.[132] Det vil sand-

128. Regeringen, Finansministeriet og Erhvervsministeriet, *National strategi for kunstig intelligens*, s. 5.
129. Ulrike Esther Franke, *Not Smart Enough: The poverty of European Military Thinking on Artificial Intelligence*, European Council on Foreign Relations, december 2019, https://ecfr.eu/wp-content/uploads/Ulrike_Franke_not_smart_enough_AI.pdf; Franke, *Artificial Divide*; Franke, *Harnessing Artificial Intelligence*; Franke, *Artificial Intelligence diplomacy*.
130. Villani, "For a Meaningful Artificial Intelligence"; The Federal Government of Germany, "Artificial Intelligence Strategy"; Franke, *Not Smart Enough*.
131. Breitenbauch og Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark*.
132. European Defence Agency, *Annual Report 2020*, marts 2021, s. 14, https://eda.europa.eu/docs/default-source/eda-annual-reports/eda-annual-report-2020.pdf.

synligvis indebære målrettede investeringer i forskning og udvikling af AI-understøttede militære teknologier under Den Europæiske Forsvarsfond (EDF).[133] I februar 2021 vedtog EU-Kommissionen desuden en handlingsplan, der skal skabe synergi mellem civil-, forsvars- og rumindustrierne.[134] Ved præsentationen af handlingsplanen fremhævede Thierry Breton, at "ensuring strong synergies between defence, space and civil technologies will generate disruptive innovations and allow Europe to remain a global standard setter. It will also reduce our dependencies in critical technologies and boost the industrial leadership we need to recover from the crisis."[135] Handlingsplanens 11 initiativer understreger, at EU har rettet et strategisk blik mod muligheden for at styrke europæiske sikkerheds- og forsvarspolitik samt industri- og erhvervspolitik ved at øge koordinationen og samarbejdet på tværs af medlemslande, offentlig-private og civil-militære skel.

3.2.4. Konklusion: AI-politik domineret af økonomi og regulering

EU's AI-politik er baseret på to spor. Det første spor er grundlagt på offentlige investeringer og støtte til videnskab og innovation, der bliver udmøntet i diverse finansieringsprogrammer målrettet virksomheder, forskningsenheder, netværksskabelse m.m. Det andet spor er rettet mod styring, regulering og standardisering, herunder promovering af etiske principper og risikobaseret tilgang, som EU ser som en central styrke i det globale AI-kapløb. Drivkraften i EU's AI-politiske initiativer er dermed unionens markeds- og reguleringsmandat. Udvikling og implementering af AI bliver kædet sammen med yderligere økonomisk integration, harmoniseret regulering og fastholdelse af europæiske værdier, hvilket skal skabe grundlag for teknologisk suverænitet på AI-området.

133. Ifølge forordningen for Den Europæiske Forsvarsfond "skal op til 8 % af dens budget anvendes til at støtte disruptive teknologier, fremme ikke traditionelle forsvarsaktørers deltagelse og tiltrække nystartede virksomheder til forsvarsprojekter gennem åbne indkaldelser eller priser for innovative forsvarsapplikationer". EU-Kommissionen, *Action Plan on Synergies between Civil, Defence and Space Industries,* 22. februar 2021, s. 14, https://ec.europa.eu/info/sites/info/files/action_plan_on_synergies_en_1.pdf.
134. Ibid.
135. EU-Kommissionen, "EU industry: Commission takes action to improve synergies between civil, defence and space industries," EU-Kommissionen, 22. februar 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_651.

Hvor EU i et årti har arbejdet på at skabe et cybersikkerhedspolitisk rum til sig selv i spændingsfeltet mellem digitalisering, marked og sikkerhed, har unionen været tilbageholdende med at se udvikling og implementering af AI i et magt-, sikkerheds- og forsvarspolitisk lys. EU's sammenkædning af teknologisk suverænitet og AI har således endnu ikke medført samme grad af sammensmeltning af sikkerheds- og forsvarspolitik og industri-, erhvervs- og innovationspolitik, som det er sket på cybersikkerhedsområdet. De seneste års massive globale fokus på AI som afgørende for globale teknologikonkurrence og magtfordeling har imidlertid medført en stigende erkendelse af, at unionens og medlemslandenes digitale udsathed – særligt inden for AI – kan udvikle sig til en geopolitisk hæmsko og et sikkerhedsproblem, hvilket forstærkes af eksisterende europæiske afhængigheder i både den digitale sektor og forsvarssektoren. EU har derfor forsøgt at undgå, at der sker en yderligere adskillelse mellem medlemslandenes sikkerheds- og forsvarsdagspolitiske dagsorden og unionens teknologiske og videnskabelige formåen ved at øge koordinationen og samarbejdet på tværs af medlemslandene samt offentlig-private og civil-militære skel.

EU's sammenkædning af teknologisk suverænitet og AI har derfor potentiale til på sigt at styrke det eksisterende digitale markeds-sikkerheds-neksus, der udfordrer den oprindelige fordeling af sikkerheds- og forsvarspolitisk autoritet og ansvar mellem EU, dets medlemsstater, NATO og private virksomheder, men en række massive udfordringer består. Det er en udfordring for EU og medlemslandene, at størstedelen af AI-udviklingen udspringer af den private teknologisektor i USA og Kina, hvor også meget af verdens øvrige digitale infrastruktur er forankret. Desuden sætter medlemslandenes forskellige syn på AI-udvikling samt deres sikkerhedspolitiske overmyndighed grænser for EU's handlerum. Ydermere skal EU tage hensyn til NATO-samarbejdet, Nordamerika og Storbritannien, når det kommer til de sikkerheds- og forsvarspolitiske aspekter af AI.

4

Konklusion og anbefalinger

Rapporten viser, hvordan EU's fokus på teknologisk suverænitet knytter an til de internationale geopolitiske og geoøkonomiske forskydninger, som de seneste år er blevet accelereret som følge af den intensiverede stormagtsrivalisering og globale teknologikonkurrence. Analysen understreger, at EU's bestræbelser på at opnå teknologisk suverænitet på områderne cybersikkerhed og AI understøtter unionens målsætning om at blive en stærkere magt- og geopolitisk spiller i traditionel international politisk forstand. Det sker, efter at EU i årtier primært har været optaget af europæisk integration gennem medlemsudvidelser, indre markeds-tiltag, etablering af fælles valuta m.m.

Traditionelt har EU fokuseret på at fremme markedsintegration og indbyrdes økonomiske afhængigheder, mens national sikkerhed forblev et eksklusivt privilegium for medlemsstaterne og NATO. Analysen tydeliggør, at den arbejdsdeling i stigende grad bliver udfordret af, at cybersikkerhed og digital teknologiudvikling befinder sig i et spændingsfelt, hvor væsentlige dele af sikkerheds- og forsvarspolitikken overlapper med industri-, erhvervs- og innovationspolitikken. EU's begrebsliggørelse, politiske tiltag og juridiske regulering af den digitale teknologiske suverænitet giver teknologipolitik en ny betydning, samtidig med at grænserne for den traditionelle arbejdsdeling mellem EU og dets medlemsstater bliver udfordret.

Når teknologiudvikling i langt mindre omfang end tidligere er kontrolleret direkte eller indirekte af statslige aktører, men især finder sted i multinationale koncerner, der opererer på tværs af landegrænser, og som er afhængige af globale markeder og forsyningskæder, styrkes EU's mulighed for at føre sikkerheds- og forsvarspolitik gennem sit mandat for det indre marked. EU's prioritering af teknologisk suverænitet er således

med til at omformulere og genforhandle det sikkerhedspolitiske autoritets- og ansvarsforhold mellem EU, medlemsstaterne, NATO og private virksomheder. Det skyldes særligt, at den generelle teknologikonkurrence er vanskelig at adskille fra den militære. Det tiltagende fokus på teknologisk suverænitet kan derfor ikke adskilles fra forhandlinger om samt kampe med hensyn til, hvor grænserne for europæisk sikkerhedspolitisk autoritet og ansvar bliver trukket.

Analysen anskueliggør dermed, at EU's arbejde med teknologisk suverænitet er en del af en større genforhandling af EU's rolle i global politik, herunder særligt i forhold til medlemsstaterne, NATO, USA og private virksomheder. Det markante fokus på teknologisk suverænitet, der går på tværs af cybersikkerhed, AI og flere af EU's øvrige digitale politiske tiltag, er en del af en dybereliggende proces, hvor EU forsøger at tilpasse unionens selvopfattelse og plads i verden. En proces, hvor EU forsøger at fungere som en global magt, der handler strategisk ud fra sammenhængende og overlappende sikkerheds-, forsvars-, industri-, erhvervs- og innovationspolitiske interesser og mål.

Den proces er imidlertid langtfra gnidningsløs. Analysen peger på, at det er en fundamental politisk og strategisk udfordring for EU at skulle opfylde målsætningen om digital suverænitet på cybersikkerheds- og AI-området. På begge disse områder er EU underlagt medlemsstaternes nationale sikkerhedspolitiske overmyndighed. Det betyder, at EU's sikkerhedspolitiske ageren er begrænset. På cybersikkerhedsområdet er der ingen udsigt til, at medlemslandene ikke fortsætter med at være sig selv nærmest, når det kommer til den militære og efterretningsmæssige del af cybersikkerhed. På AI-området er udsigten til fortsat amerikansk og kinesisk dominans så massiv, at teknologisk suverænitet sandsynligvis vil fortsætte med primært at være et spørgsmål om EU-regulering. Hertil kommer spørgsmålet om, hvorvidt det er muligt for EU reelt at opnå europæisk teknologisk suverænitet på områder som cloud, mikrochips og sociale medier, hvor Europa allerede er dybt afhængigt af tredjelande, og hvordan den afhængighed spiller sammen udvikling og udrulning af f.eks. AI og tingenes internet.

Disse udfordringer skal ses i lyset af en række grundlæggende dilemmaer i EU's bestræbelser på at opnå teknologisk suverænitet. Et centralt dilemma er, at der ikke enighed blandt medlemslandene om, hvad teknologisk suverænitet er, og hvordan den bedst kan realiseres. Det er usandsynligt, at bred enighed skulle indfinde sig inden for den nærme-

ste årrække. Yderligere et afgørende dilemma angår forholdet mellem promovering af henholdsvis europæisk teknologisk uafhængighed og interdependens og samhandel. Det dilemma berører alliancepolitik, den globale teknologikonkurrence og kernen i den liberale vestlige globaliseringsdagsorden. Dilemmaet vil derfor være rammesættende for EU's fremtidige bestræbelser på at opnå teknologisk suverænitet. Et tredje dilemma angår arbejdsdelingen mellem EU og NATO. Når EU styrker unionens teknologiske suverænitet ved at knytte udvikling af det indre marked tættere sammen med sikkerheds- og forsvarspolitik, sætter det spørgsmålstegn ved arbejds- og kompetencedelingen mellem EU og NATO. F.eks. har EU allerede gennem EDF skabt nye europæiske rammer for teknologikonkurrencens militære aspekter af en størrelsesorden, som det er tvivlsomt, om NATO kommer til at matche uden en fornyet, stor transatlantisk aftale. EU's satsning på teknologisk suverænitet kan derfor accelerere de spændinger, der allerede eksisterer mellem EU, NATO og USA.[136] Rapporten understreger dermed teknologiens potentiale som politisk, økonomisk og militær *driver*, der kan skabe både fælles initiativer og adskillelse internt i EU og mellem EU, NATO og USA. Hvordan EU organiserer sig i forhold til medlemslandene, NATO og USA med hensyn til både den generelle og den militære teknologikonkurrence – og i forhold til Kina – er væsentlige faktorer i relation til spørgsmålet om, hvad EU's fremadrettede rolle i global politik bliver, og hvorvidt Vesten samlet set formår at agere systematisk i stormagtsrivaliseringen og teknologikonkurrencen.

4.1. Strategiske implikationer for Danmark

For Danmark repræsenterer EU's satsning på teknologisk suverænitet en betoning af en række af de politiske konsekvenser, der følger af den intensiverede stormagtsrivalisering og teknologikonkurrence. Det gælder ikke mindst, at sikkerheds- og forsvarspolitikken – med digitaliseringens mellemkomst – har fået nye snitflader i forhold til industri-, erhvervs- og innovationspolitikken. Det indebærer, at digitalisering og teknologiudvikling bedst bliver varetaget ved en bred dansk indsats, der adresserer

136. Breitenbauch og Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark*.

silo- og ressorttænkning samt de traditionelle skel mellem indenrigs og udenrigs, offentligt og privat samt civilt og militært. En indsats, der kræver målrettet og langsigtet planlægning.

Det betyder ikke, at ressortområder eller skillelinjer nødvendigvis skal overkommes eller ophæves. Snarere kræver det, at politikere og embedsmænd forholder sig til de politiske, økonomiske, strategiske og demokratiske konsekvenser af, at ressortområder og skillelinjer bliver udfordret, da det her er kernen i vores statsbygning, som er på spil. Danmarks bør derfor foretage en afvejning af, hvordan EU's målsætning om teknologisk suverænitet kan udfoldes, så danske hensyn til sikkerhed, forsvar, frihedsrettigheder, diplomati, erhvervsliv, industri og innovation bedst bliver vægtet og varetaget. Det kræver strategiske overvejelser om, hvad en national teknologipolitik bør fokusere på, hvordan sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske overlap, muligheder og udfordringer udspiller sig, og hvordan forholdet mellem Danmark, EU, NATO, USA og private virksomheder bliver bragt i spil og udfordret.

Desuden rejser det både strategiske og demokratiske udfordringer for Danmark at skulle navigere i en situation, hvor industri-, erhvervs- og innovationspolitikken med stor sandsynlighed fortsætter med at miste sine uskyld, som følge af at disse politikområder bliver spundet yderligere ind i sammen med sikkerheds- og forsvarspolitikken. Det er i den sammenhæng vigtigt, at de danske politikere og embedsmænd har for øje, at den tiltagende konvergens mellem EU's indre markedsmandat og danske sikkerheds- og forsvarspolitiske hensyn kan medføre, at EU-beslutninger får sikkerheds- og forsvarspolitiske konsekvenser for borgere, kommuner, regioner og statslige myndigheder, f.eks. når det gælder indkøb og brug af digitale tjenester, *devices* og infrastruktur.

Baseret på disse hovedkonklusioner slutter rapporten med en række anbefalinger, der fremover kan støtte dansk strategisk tænkning, politisk styring og offentlig debat om EU's teknologiske suverænitet og dansk teknologipolitik. Anbefalingerne kan dermed bidrage til at styrke Danmarks sikkerheds- og forsvarspolitik, der i stigende grad er betinget af den digitale udvikling og den globale teknologikonkurrence.

4.2. Anbefalinger

4.2.1. Strategisk rammesætning af teknologipolitiske indsatser

Danmarks fremtidige sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske handlerum er uløseligt knyttet til både den omsiggribende digitale teknologiudvikling og den tiltagende stormagtsrivalisering. De danske politiske beslutningstagere kan fremover påvirke handlerummet ved at opdyrke en strategisk tilgang til arbejdet med Danmarks teknologipolitik, så Danmark bliver bedre rustet til at træffe langsigtede og helhedsorienterede beslutninger på teknologiområdet. Beslutninger, der imødekommer både sociale og økonomiske muligheder samt nye trusler og nye forventninger og krav fra alliererede og partnere. Det indebærer en bredspektret politisk indsats, der ikke falder under et enkelt ministerområde eller lader sig indkapsle i et enkelt strategidokument. Den strategiske tilgang bør afspejle, at teknologipolitik omfatter både sikkerheds-, forsvars- og udenrigsområdet samt industri-, erhvervs-, og innovationsområdet, og at teknologipolitik ikke lader sig adskille af ministerielle ressort- og faggrænser.

- **Kortlægning af eksisterende indsatser**. Regeringen bør igangsætte en tværministeriel kortlægning af allerede igangsatte initiativer i Danmark og EU, der behandler civile og militære aspekter af teknologipolitik. Kortlægningen vil give regeringen og forvaltningen et samlet overblik over de nuværende sikkerheds- og forsvarspolitiske samt industri-, erhvervs- og innovationspolitiske snitflader, overlap, udfordringer og muligheder, der er forbundet med teknologipolitik og teknologikonkurrence. Et sådant overblik vil styrke regeringens mulighed for at udpege og navigere efter langsigtede strategiske mål samt søsætte konkrete tiltag for at opnå dem. Desuden vil overblikket kunne bruges til at undersøge, om de seneste års udvikling har åbnet nye og uudnyttede veje med hensyn til at varetage danske interesser. Samtidig kan det bruges til at iscenesætte Danmark i forhold til både EU's og NATO's teknologipolitiske prioriteter og sende et klart signal til vores allierede og partnere.

- **Vurdering af forsvarsforbeholdet**. Regeringen bør få foretaget en vurdering af, hvordan teknologikonkurrencen, herunder særligt EU's rolle, påvirker de sikkerheds- og forsvarspolitiske konsekvenserne af

det danske forsvarsforbehold. På den ene side kan EU's styrkede fokus på teknologisk suverænitet, herunder særligt sammenblandingen af sikkerheds- og forsvarspolitik på den ene side og industri-, erhvervs- og innovationspolitik på den anden medføre, at forsvarsforbeholdet bliver vanskeligere at forvalte. Samtidig kan forbeholdet bliver en begrænsning for Danmarks muligheder for at øve indflydelse på EU's teknologipolitiske udvikling. På den anden side kan Danmarks mulighed for at øve indflydelse på teknologipolitikken i EU blive styrket, hvis nye og disruptive teknologier primært bliver behandlet som industri-, erhvervs-, innovations-, og uddannelsespolitiske spørgsmål.[137]

- **Teknologikonkurrencestrategi**.[138] Regeringen bør overveje at igangsætte arbejdet med at fastlægge en egentlig teknologikonkurrencestrategi, som er forankret i Forsvarsministeriet, og som foruden Udenrigsministeriet inkluderer andre innovationsrelevante ministerier såsom Finansministeriet, Erhvervsministeriet og Uddannelses- og Forskningsministeriet. Strategien vil kunne danne ramme om samarbejde i snitfladerne mellem forsvaret, det digitale Danmark, EU og NATO, herunder forskning og udvikling samt konkrete projekter, som også kan få bredere samfundsøkonomiske effekter.

- **Militær teknologistrategi**. Regeringen bør overveje at igangsætte arbejdet med at fastlægge en militær teknologistrategi, der udstikker en overordnet ambition og retning for udvikling, indkøb og anvendelse af banebrydende militære teknologier. Strategien kan f.eks. sikre politisk opmærksomhed over for teknologiens rolle i udviklingen af det danske forsvar, være med til at rammesætte forsvarets kapacitetsudvikling samt sikre langsigtet fokus på samarbejde mellem forsvaret, det forsvarsindustrielle og digitale Danmark, EU og NATO.

137. Som det f.eks. er tilfældet med EU's Forsvarsfond, hvor Danmark kan engagere sig, da det juridiske grundlag ikke er forsvarssamarbejde, men industri og forskning. Christine Nissen, *Forsvarsfond uden forbehold*, Dansk Institut for Internationale Studier, 18. marts 2021, s. 3, https://pure.diis.dk/ws/files/4189700/DIIS_PB_MARTS_2021.pdf.
138. Anbefalingen er oprindeligt præsenteret i Breitenbauch og Liebetrau, *Teknologikonkurrencen og dens implikationer for Danmark*.

- **Folketinget**. Folketinget bør overveje, hvorvidt de eksisterende udvalgsstrukturer understøtter den nødvendige diskussion af tværgående teknologipolitiske spørgsmål. I forlængelse heraf kan Folketinget overveje nedsættelse af et teknologiudvalg eller en delegation for teknologi.

- **Fremadrettet koordinering og harmonisering**. Forvaltningen bør fremover koordinere og harmonisere de strategiske indsatser i arbejdet med teknologipolitik. Det bør som minimum inkludere Forsvarsministeriet, Udenrigsministeriet, Justitsministeriet, Erhvervsministeriet samt Uddannelses- og Forskningsministeriet og være funderet i en formel og fast samarbejdsform. Arbejdet kan inkludere udvikling af indikatorer til at afdække og overvåge Danmarks nuværende og fremtidige teknologiske afhængigheder, udviklingsstadier for disruptive teknologier samt det strategiske arbejde med teknologisk suverænitet i EU, toneangivende EU-medlemslande, USA og Kina. Desuden bør de offentlige myndigheder indlede en bred dialog med styrelser, regioner og kommuner om, hvordan de forholder sig til teknologipolitik, herunder til dens nationale sikkerheds- og forsvarspolitiske implikationer.

- **Formaliseret videndeling**. Regeringen og forvaltningen bør styrke opbygning og udveksling af viden på det digitalt-teknologiske område i et formaliseret samarbejde mellem staten, industrien og forskningsinstitutionerne. Et sådant samarbejde vil gavne Danmarks fremtidige sikkerheds- og forsvarspolitiske interesser samt kommercielle interesser.

4.2.2. Danmark, EU og det transatlantiske forhold

Danmark har mulighed for at påvirke, hvordan EU håndterer de fremtidige digitale muligheder og udfordringer, som følger af den intensiverede stormagtsrivalisering og teknologikonkurrence. I marts 2021 var den danske statsminister, Mette Frederiksen, eksempelvis medunderskriver af et brev til Ursula von der Leyen – sammen med de politiske ledere i Tyskland, Estland og Finland – der opfordrer EU til at reducere

strategiske digitale svagheder og undgå protektionisme.[139] Et budskab, som den danske techambassadør har gentaget.[140] Regeringen bør fortsat arbejde for, at EU styrker sin og medlemslandenes teknologiske suverænitet, men den bør styrke sit fokus på, hvordan det påvirker relationen mellem industri-, erhvervs-, og innovationspolitik og sikkerheds- og forsvarspolitik, herunder indvirkningen på båndene til NATO og USA. EU's stræben efter teknologisk suverænitet risikerer at grave grøfter mellem EU og NATO og USA. Samtidig er øget samarbejde mellem EU, NATO og USA afgørende for, at der bliver etableret globale regler og normer for teknologiudvikling og statsopførsel i det digitale rum.

- **Sikkerheds- og forsvarspolitiske gevinster**. Danmark bør arbejde for, at EU styrker sit fokus på, hvordan unionens markedsbaserede tiltag på teknologiområdet kan omsættes til sikkerheds- og forsvarspolitiske gevinster. I det arbejde bør Danmark bestræbe sig på, at indsatsen bliver kommunikeret, koordineret og harmoniseret på en måde, der styrker forholdet til NATO og USA.

- **Strategisk vigtige teknologier**. Danmark bør arbejde for, at EU styrker sin indsats med at udvikle en politik og en bredspektret proces for identifikation og monitorering af strategisk vigtige teknologier, systemer og sektorer. I det arbejde bør Danmark tilskynde, at EU ikke, som det primært er tilfældet i dag, behandler forskellige teknologier og infrastrukturer separat, men også fokuserer på, hvordan de spiller sammen og konvergerer. I forlængelse heraf bør Danmark arbejde for, at EU styrker sit arbejde med at klarlægge forholdet mellem generelle og militære teknologier, herunder for dual-use- og multiple-use-teknologier.

139. The Federal Chancellor of Germany, the Prime Minister of Denmark, the Prime Minister of Finland og the Prime Minister of Estonia, *Digital Sovereignty Letter,* 1. marts 2021, https://datasovereigntynow.org/wp-content/uploads/2021/03/Digital-sovereignty-letter3-copy.pdf.
140. Renaissance Numérique, *Digital Sovereignty: Which Strategy for Europe?,* juni 2021, https://www.renaissancenumerique.org/ckeditor_assets/attachments/634/renaissancenumerique_proceedings_digitalsovereignty.pdf

- **Geopolitiske og geoøkonomiske perspektiver.** Danmark bør arbejde for, at EU etablerer mekanismer, der sikrer indarbejdelse af geopolitiske og geoøkonomiske perspektiver i EU's digitale politikker, strategier og partnerskaber, herunder i tilgangene til cybersikkerhed, AI og 5G samt ansvarlig brug af teknologi i militære applikationer, der følger den regelbaserede internationale orden.

- **International orden og transatlantiske forhold**. Danmark bør arbejde for, at EU's tiltag for at opnå teknologisk suverænitet ikke underminerer den regelbaserede internationale orden og det transatlantiske forhold, samtidig med at den strategiske prioritering af teknologisk suverænitet ikke leder til et decideret brud med Kina. I forlængelse heraf bør Danmark arbejde for at sikre, at EU's forhold til den regelbaserede internationale orden samt USA og Kina kan rumme de forskellige – og til tider modsatrettede – krav og udfordringer, der følger af den tiltagende stormagtsrivalisering, teknologikonkurrence og hybridkonflikt.

- **Transatlantiske standarder og regler**. Danmark bør arbejde for, at EU i samarbejde med NATO og USA forsøger at nå til enighed om standarder og regler relateret til digitale teknologier som AI og 5G. Derved kan EU, NATO og USA udvise globalt lederskab baseret på grundlæggende frihedsrettigheder, demokratiske værdier og menneskerettigheder. Det vil styrke den regelbaserede internationale orden. Samtidig bør EU, NATO og USA fortsætte med at være aktive i multilaterale diskussioner, der vedrører de internationale digitale regler, standarder og normer.

- **Transatlantisk teknologisamarbejde**. Danmark bør arbejde for, at EU i samarbejde med NATO og USA udbygger og intensiverer det eksisterende forskningssamarbejde og øger den offentlige støtte til forskning i og udvikling af vitale nye digitale teknologier. EU bør stræbe efter at udvikle et innovativt transatlantisk marked for nye digitale teknologier, der involverer industrien, den akademiske verden og de statslige institutioner.

Litteraturliste

Access Now. *Europe's Approach To Artificial Intelligence: How AI Strategy is Evolving.* December 2020. https://www.accessnow.org/cms/assets/uploads/2020/12/Europes-approach-to-AI-strategy-is-evolving.pdf.

Bauer, Matthias og Fredrik Erixon. *Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls*. European Council for International Political Economy, 2020. https://ecipe.org/wp-content/uploads/2020/05/ECI_20_OccPaper_02_2020_Technology_LY02.pdf.

Biden, Jr., Joseph R. "Why America Must Lead Again: Rescuing U.S. Foreign Policy After Trump." *Foreign Affairs.* Tilgået 20. december 2021.
https://www.foreignaffairs.com/articles/united-states/2020-01-23/why-america-must-lead-again.

Biscop, Sven. *European Strategy in the 21st Century: New Future for Old Powers*. Abingdon, Oxon; New York, NY: Routledge, 2019.

Borrell, Josep. "Embracing Europe's Power." *IPS Journal,* 2. marts 2020. https://www.ips-journal.eu/regions/europe/embracing-europes-power-4095/.

Borrell, Josep. "Make cyberspace a safer place." *EEAS*, 17. december 2020. https://eeas.europa.eu/headquarters/headquarters-homepage_en/90747/Make%20cyberspace%20a%20safer%20place.

Bredford, Anu. *The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press, 2020.

Breitenbauch, Henrik og Tobias Liebetrau. *Teknologikonkurrencen og dens implikationer for Danmark*. København: Center for Militære Studier og Djøf Forlag, 2021.

Bueger, Christian og Tobias Liebetrau. "Protecting hidden infrastructure: The security politics of the global submarine data cable network." *Contemporary Security Policy* 42, nr. 3 (2021): 391-413. DOI: 10.1080/13523260.2021.19071.

Burwell, Frances G. og Kenneth Propp. *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?* Washington, DC: Atlantic Council, 2020. https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf.

Castro, Daniel og Michael McLaughlin. *Who Is Winning the AI Race: China, the EU, or the United States? – 2021 Update*. Centre for Data Innovation, januar 2020. https://www2.datainnovation.org/2021-china-eu-us-ai.pdf.

Cerulus, Laurens. "Europe's litmus test over cloud computing push." *Politico*, 28. juli 2020. https://www.politico.eu/article/shades-of-sovereignty-dent-european-cloud-dreams/.

Christakis, Theodore. "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy." *SSRN*, 7. december, 2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098.

Claessen, Eva. "Reshaping the internet – the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU." *Journal of Cyber Policy* 5:1 (2020): 140–157. DOI: 10.1080/23738871.2020.172835.

Deibert, Ronald J. "Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace," *Millennium*, 32(3) 2003: 501-530

Department of Defense of the United States of America. *Military and Security Developments Involving the People's Republic of China – Annual Report to Congress.* 2020. https://media.defense.gov/2021/Nov/03/2002885874/-1/-1/0/2021-CMPR-FINAL.PDF.

Det Europæiske Råd. "Strategic autonomy for Europe – the aim of our generation," *Speech by President Charles Michel to the Bruegel think tank*. 28. september, 2020. https://www.consilium.europa.eu/da/press/press-releases/2020/09/28/l-autonomie-strategique-europeenne-est-l-objectif-de-notre-generation-discours-du-president-charles-michel-au-groupe-de-reflexion-bruegel/.

Det Europæiske Råd. "The Digital in a fractious world: Europe's way," *Speech by President Charles Michel at the FT-ETNO Forum*. 29 september 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/09/29/the-digital-in-a-fractious-world-europe-s-way-speech-by-president-charles-michel-at-the-ft-etno-forum/.

Det Europæiske Råd. "Digital sovereignty is central to European strategic autonomy," *Speech by President Charles Michel at Masters of digital 2021 online event*. Det Europæiske Råd, 3. februar 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/.

Det Europæiske Råd. "A recovery plan for Europe." Det Europæiske Råd. Tilgået 15. december 2021. https://www.consilium.europa.eu/en/policies/eu-recovery-plan/.

EU-Forordning. "Regulation (EU) 2021/697 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092." *Official Journal of the European Union*, 12. maj 2021. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0697&qid=1631263086142&from=EN.

EU-Kommissionen. "Commission welcomes political agreement on €7.5 billion Digital Europe Programme." EU-Kommissionen, 14. december 2020.
https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2406.

EU-Kommissionen. "Digital Europe Programme: €7.5 billion of funding for 2021-2027." EU-Kommissionen. 10. november 2021. https://digital-strategy.ec.europa.eu/en/library/digital-europe-programme-proposed-eu75-billion-funding-2021-2027.

EU-Kommissionen. *En strategi for et digitalt indre marked i EU.* 6. maj 2015. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX-:52015DC0192&from=EN.

EU-Kommissionen. *The EU Internal Security Strategy in Action: Five steps towards a more secure Europe.* 22. november 2010. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF.

EU-Kommissionen. *A Digital Agenda for Europe*. 19. maj 2010. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik. *EU-strategi for cybersikkerhed: Et åbent, sikkert og beskyttet cyberspace.* 7. marts 2013. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52013JC0001&from=DA.

EU-Kommissionen. "Commission welcomes political agreement on the Cybersecurity Competence Centre and Network." 11. december 2020. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2384.

EU-Kommissionen. "Kommissionens henstilling (EU) 2019/534 af 26. marts 2019. Cybersikkerheden i forbindelse med 5G-net." *Den Europæiske Unions tidende*, 29. marts 2019. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32019H0534&from=DA.

EU-Kommissionen. *En EU-værktøjskasse til udrulning af sikre 5G-net i EU*. 29. januar 2020. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2020:0050:FIN:DA:PDF.

EU-Kommissionen. "Digital Europe Programme: €7.5 billion of funding for 2021-2027." 10. november 2021. https://digital-strategy.ec.europa.eu/en/library/digital-europe-programme-proposed-eu75-billion-funding-2021-2027.

EU-Kommissionen. *En ny industristrategi for Europa 2020.* 10. marts 2020. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX-:52020DC0102&from=DA.

EU-Kommissionen. *EU's datastrategi 2020 – En europæisk strategi for data*. 19. februar 2020. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

EU-Kommissionen. "Kunstig intelligens for Europa." *EU-Kommissionen* (2018). COM (2018) 237 Final. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52018DC0237&from=DA.

EU-Kommissionen. "Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence." EU-Kommissionen, 21. april 2021. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682.

EU-Kommissionen. "Cloud Computing." Senest opdateret 23. september 2021. https://digital-strategy.ec.europa.eu/en/policies/cloud-computing.

EU-Kommissionen. *Det digitale kompas 2030: Europas kurs i det digitale årti*. *9. marts* 2021. https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9 01aa75ed71a1.0002.02/DOC_1&format=PDF.

EU-Kommissionen. "EU-US launch Trade and Technology Council to lead values-based global digital trans-formation." 15. juni 2021. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990.

EU-Kommissionen. *A new EU-US agenda for global change.* 2. december 2020. https://ec.europa.eu/info/sites/info/files/joint-communication-eu-us-agenda_en.pdf.

EU-Kommissionen og Unionens Højtstående Repræsentant for Udenrigsanliggender og Sikkerhedspolitik. *EU's strategi for cybersikkerhed for det digitale årti*. 16. december 2020. https://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:52020JC0018&from=DA.

EU-Kommissionen, *Action Plan on Synergies between Civil, Defence and Space Industries*. 22. februar 2021.

https://ec.europa.eu/info/sites/info/files/action_plan_on_synergies_en_1.pdf.

EU-Kommissionen. "EU industry: Commission takes action to improve synergies between civil, defence and space industries," EU-Kommissionen. 22. februar 2021.

https://ec.europa.eu/commission/presscorner/detail/en/ip_21_651.

EU-medlemslandene. *Declaration: Building the next generation cloud for businesses and the public sector in the EU*. 15. oktober 2020. https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe.

EU-Rådet. "Nyt kompetencecenter og netværk for cybersikkerhed: uformel aftale med Europa-Parlamentet." 11. december 2020. https://www.consilium.europa.eu/da/press/press-releases/2020/12/11/new-cybersecurity-competence-centre-and-network-informal-agreement-with-the-european-parliament/.

EU-Rådet. "Bucharest-based Cybersecurity Competence Centre gets green light from Council." 20. April 2021. https://www.consilium.europa.eu/en/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/?utm_source=dsms-auto&utm_medium=e-mail&utm_campaign=Bucharest-based+Cybersecurity+Competence+Centre+gets+green+light+from+Council.

European Defence Agency, *Annual Report 2020*. Marts 2021. https://eda.europa.eu/docs/default-source/eda-annual-reports/eda-annual-report-2020.pdf.

European External Action Service. *Shared Vision, Common Action. A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy*. Luxembourg: Publications Office of The European Union, 2016.

Floridi, Luciano. "The fight for digital sovereignty: What it is, and why it matters, especially for the EU." *Philosophy & Technology* 33, nr. 3 (2020): 369–378.

Franke, Ulrike. *Artificial Intelligence diplomacy: Artificial Intelligence governance as a new European Union external policy tool*. Europa-Parlamentet, juni 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf.

Franke, Ulrike Esther. *Not Smart Enough: The poverty of European Military Thinking on Artificial Intelligence*. European Council on Foreign Affairs, decem-

ber 2019. https://ecfr.eu/wp-content/uploads/Ulrike_Franke_not_smart_enough_AI.pdf.

Franke, Ulrike Esther. *Artificial Divide: How Europe and America Could Clash Over AI*. European Council on Foreign Affairs, januar 2021. https://ecfr.eu/publication/artificial-divide-how-europe-and-america-could-clash-over-ai/.

Franke, Ulrike. *Harnessing Artificial Intelligence*. European Council on Foreign Affairs, juni 2019. https://www.ecfr.eu/page/-/3_Harnessing_artificial_intelligence.pdf.

Gambrell, Jon. "Iran deploys 'halal' internet in latest bid to rein in citizens' web freedoms." *Independent*, 29. januar 2019. https://www.independent.co.uk/news/world/middle-east/iran-halal-internet-national-information-network-web-freedoms-citizens-access-social-media-telegram-facebook-twitter-instagram-youtube-a8182841.html.

German Federal Ministry for Economic Affairs and Energy og French Ministry of Economy and Finance. "Press Release on Franco-German common work on a secure and trustworthy data infrastructure." 29. oktober 2019. https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2019/20191029-press-release-on-franco-german-common-work-on-a-secure-and-trustworthy-data-infrastructure.html.

German Federal Ministry for Economic Affairs and Energy og French Ministry of Economy and Finance. "Franco-German Position on GAIA-X." 18. februar 2020. https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=10.

Heikkilä, Melissa. "The Achilles' heel of Europe's AI strategy." *Politico*, 13. marts 2020. https://www.politico.eu/article/europe-ai-strategy-weakness/.

Hong, Yu og G. Thomas Goodnight. "How to think about cyber sovereignty: the case of China." *Chinese Journal of Communication* 13, nr. 1 (2020): 8–26.

Hummel, Patrik et al. "Data sovereignty: A review." *Big Data & Society* 8, nr. 1 (2021).

Jacobsen, Jeppe Teglskov og Tobias Liebetrau. "Kunstig intelligens, militær strategi og international konkurrence," I *Smart Krig – Militær anvendelse af kunstig intelligens*, red. Iben Yde, Thomas G Nielsen og Rasmus Dalhberg. København: Djøf Forlag, 2021.

Jakobsson, A. K. og M. Stolz. "Principled big tech: European pursuit of technological autonomy." I *Strategic autonomy and the transformation of the EU: New agendas for security, diplomacy, trade and technology*, red. N. Helwig, 105–130. Finnish Institute of International Affairs, 2021, bind 67.

Juncker, Jean-Claude, "State of the Union 2018: The Hour of European Sovereignty." *Tale til Europa-Parlamentet*, 2018. https://ec.europa.eu/info/sites/info/files/soteu2018-speech_en_0.pdf.

Juncker, Jean-Claude. "Unionens Tilstand 2018. Tiden er inde for et suverænt Europa." *Tale til Europa-Parlamentet*, 2018. https://ec.europa.eu/info/sites/info/files/soteu2018-speech_da_0.pdf.

Kharpal, Arjun. "China spending on research and development to rise 7% per year in push for major tech breakthroughs", *CNBC*, 5. marts 2021. https://www.cnbc.com/2021/03/05/china-to-boost-research-and-development-spend-in-push-for-tech-breakthroughs.html.

Kharpal, Arjun. "In battle with U.S., China to focus on 7 'frontier' technologies from chips to brain-computer fusion," *CNBC*, 5 marts, 2021. https://www.cnbc.com/2021/03/05/china-to-focus-on-frontier-tech-from-chips-to-quantum-computing.html.

Kristensen, Kristian Søby og Niels Byrjalsen. *Aktiv afventning. Nordiske Perspektiver på forsvars- og sikkerhedspolitisk samarbejde.* København: Center for Militære Studier, april 2020.

Liebetrau, Tobias. *EU Cybersecurity Governance: Redefining the Role of the Internal Market*. Ph.d.-afhandling, Københavns Universitet, Institut for Statskundskab, 2019.

Liebetrau, Tobias. *Dansk offensiv cybermagt mellem angreb, spionage og forsvar: En komparativ analyse på tværs af Europa*. København: Center for Militære Studier, maj 2020.

Liebetrau, Tobias. "Cybersikkerhed i Perspektiv – Temaredaktørens forord." *Økonomi og Politik* 93, nr. 3, 5–12.

Mueller, Milton L. *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, (Cambridge; Malden, Polity Press, 2017)

Mueller, Milton L. "Against sovereignty in cyberspace." *International Studies Review* 22, nr. 4 (2020): 779–801.

Nah, Seungahn og Soomin Seo. "Talking With the Hermit Regime: North Korea, Media, and Communication: Introduction." *International Journal of Communication* 14 (2020): 1303–1307.

NIS Cooperation Group. *Cybersikkerhed i 5G-net: EU-værktøjskasse med risikobegrænsende foranstaltninger.* CG-publikation, januar 2020. https://cfcs.dk/globalassets/cfcs/dokumenter/telemyndighed/-cybersikkerhed-i-5g-net---eu-vaerktoejskasse-.pdf.

Nissen, Christine. *Forsvarsfond uden forbehold*, Dansk Institut for Internationale Studier, 18. marts 2021. https://pure.diis.dk/ws/files/4189700/DIIS_PB_MARTS_2021.pdf.

North Atlantic Treaty Organization. "New Focus on Emerging and Disruptive Technologies Helps Prepare NATO for the Future." Tilgået 16. december 2021. https://www.nato.int/cps/en/natohq/news_181901.htm.

North Atlantic Treaty Organization. "London Declaration." Tilgået 17. december 2021. http://www.nato.int/cps/en/natohq/official_texts_171584.htm.

North Atlantic Treaty Organization. *NATO Science & Technology Strategy Sustaining Technological Advantage*. Tilgået 16. december 2021. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20181107_180727-ST-strategy-eng.pdf.

North Atlantic Treaty Organization. "NATO releases first-ever strategy for Artificial Intelligence." 22. oktober 2021. https://www.nato.int/cps/en/natohq/news_187934.htm.

Nissen, Christine og Jessica Larsen. *European strategic autonomy: from misconceived to useful concept what can we learn from the Northern outlook?* DIIS Policy Brief, 2021.

Pohle, Julia og Thorsten Thiel. Digital sovereignty. *Internet Policy Review*, 9(4), 2020, https://doi.org/10.14763/2020.4.1532.

Regeringen, Finansministeriet og Erhvervsministeriet. *National Strategi for kunstig intelligens*. Marts 2019. https://www.regeringen.dk/media/6537/ai-strategi_web.pdf.

Renaissance Numérique, *Digital Sovereignty: Which Strategy for Europe?*. Juni 2021, https://www.renaissancenumerique.org/ckeditor_assets/attachments/634/renaissancenumerique_proceedings_digitalsovereignty.pdf.

Roy, V. Vincent, Fiammetta Rossetti, Karine Perset og Laura Galindo-Romero. *AI-Watch – National strategies on Artificial Intelligence: A European perspective.* Luxembourg: Publications Office of the European Union, 2021. DOI: 10.2760/069178.

Schinas, Margaritis og Thierry Breton. "EU-kommissærer: Europa har brug for et cyberskjold." *Altinget*, 6. januar 2021. https://www.altinget.dk/digital/artikel/eu-kommissionen-europa-boer-indfoere-en-cyberdoktrin.

Schultz. Jarl Viktor. "Ny temadebat: Hvordan skal vi udnytte kunstig intelligens?" *Altinget*, 9. juni 2021. https://www.altinget.dk/digital/artikel/ny-temadebat-hvordan-skal-vi-udnytte-kunstig-intelligens.

Seliger, Bernhard og Stefan Schmidt. "The Hermit Kingdom Goes Online... Information Technology, Internet Use and Communication Policy in North Korea." *North Korean Review,* 2014: 71-88.

Smuha, Nathalie. "Europe's approach to AI governance: time for a vision." *Friends of Europe*, 2. april 2020. https://www.friendsofeurope.org/insights/europes-approach-to-ai-governance-time-for-a-vision/.

Statista. "The 100 largest companies in the world by market capitalization in 2021." *Tilgået 16. december 2021.* https://www.statista.com/statistics/263264/top-companies-in-the-world-by-market-capitalization/.

The Economist. "Can the EU Become Another AI Superpower?", *The Economist*, *22. september 2018.* https://www.economist.com/business/2018/09/20/can-the-eu-become-another-ai-superpower.

The Federal Government of Germany. "Artificial Intelligence Strategy of the German Federal Government," *ki-strategie-deutschlands.de,* december 2020. https://www.ki-strategie-deutschland.de/files/downloads/Fortschreibung_KI-Strategie_engl.pdf.

The Federal Chancellor of Germany, the Prime Minister of Denmark, the Prime Minister of Finland, and the Prime Minister of Estonia, *Digital Sovereignty Letter,* 1. marts 2021, https://datasovereigntynow.org/wp-content/uploads/2021/03/Digital-sovereignty-letter3-copy.pdf.

The State Council of the People's Republic of China. "'Made in China 2025'. Plan Issued". 19. maj 2021. http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

The U.S. Department of State. "The Clean Network". Tilgået 15. december 2021. https://2017-2021.state.gov/the-clean-network/index.html.

The White House. *National strategy for critical and emerging technologies.* Washington, DC: White House Office, oktober 2020. https://www.hsdl.org/?view&did=845571.

Torreblanca, José Ignacio. "Referees don't win games: Europe and the digital great game." European Council on Foreign Relations, 9. februar 2021. https://ecfr.eu/article/referees-dont-win-games-europe-and-the-digital-great-game/.

UN. *Digital Economy Report 2019, Value Creation and Capture: Implications for Developing Countries*. United Nations Publications, 2019.

Vedyashkin, Sergei. "Russia Is 'Ready' to Disconnect from Global Internet, Medvedev Says," *Moscow Times*, 1. februar 2021, https://www.themoscowtimes.com/2021/02/01/russia-is-ready-to-disconnect-from-global-internet-medvedev-says-a72791.

Villani, Cédric. "For A Meaningful Artificial Intelligence – Towards A French And Euopean Strategy," *Mission Assigned by the Prime Minister Édouard Philippe,* March, 2018. https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf.

von der Leyen, Ursula. "Tale om Unionens Tilstand." *Tale til Europa-Parlamentet*, 15. september 2021. https://ec.europa.eu/info/sites/default/files/soteu_2021_address_da_0.pdf.

von der Leyen, Ursula. *A Union that strives for more. My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024.* Luxembourg: Publications Office of The European Union, 2019. https://ec.europa.eu/info/sites/info/files/political-guidelines-next-commission_en_0.pdf.

Wikipedia. "List of public corporations by market capitalization." Tilgået 16. december 2021. https://en.wikipedia.org/wiki/List_of_public_corporations_by_market_capitalization.

Wolff, Guntram. "Europe may be the world's AI referee, but referees don't win," *Politico*, 17. februar 2020. https://www.politico.eu/article/europe-may-be-the-worlds-ai-referee-but-referees-dont-win-margrethe-vestager/

Yalcintas, Altug og Naseraddin Alizadeh. "Digital Protectionism and National Planning in the Age of the Internet: the Case of Iran," *Journal of Institutional Economics* 16, nr. 4 (2020): 519–536. DOI: 10.1017/S1744137420000077.

Zuboff Shoshana. "Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30(1) (2015): 75–89.

Zuboff Shoshana. *The Age of Surveillance Capitalism*. New York: Public Affairs, 2019.

OM FORFATTERNE

Tobias Liebetrau, ph.d., er postdoc ved Centre de Recherches Internationales, Sciences Po, Paris. Tobias forsker i politiske og strategiske aspekter af cybersikkerhed, digitalisering og teknologiudvikling.

9 788757 454406