5 PRINCIPLED BIG TECH: EUROPEAN PURSUIT OF TECHNOLOGICAL AUTONOMY

André Ken Jakobsson & Marcel Stolz

SUMMARY

- The European Union is pursuing technological autonomy from a position of relative weakness given the scarcity of European Big Tech companies, while American and Chinese giants occupy critical network nodes. Companies are able to leverage these nodes politically through 'weaponised interdependence'.
- This chapter argues that the answer to this situation is sought through the concept of 'Principled Big Tech'. The EU attempts to advance its own knowledge and industrial base while actively developing and using disruptive technologies in line with liberal political values.
- Implementing Chinese 5G technology poses a challenge for critical national infrastructure functions. The securitisation and ongoing decoupling of global supply chains in sensitive technologies is adding to the pressure for European cooperation on strategic assets.
- Leading EU member states, including France and Germany, have not yet found a coordinated agreement on action for advanced technologies such as Artificial Intelligence in order to ensure collaborative efforts.

RECOMMENDATIONS

- The EU should enhance its strategic technological capacities and safeguard past and future technological advancements by

streamlining national guidelines on critical assets (technologies, knowledge and data).

- The EU should intensify investment screening and export controls in order to minimise vulnerabilities to weaponised interdependence.
- The EU should maintain and expand its technical knowledge capacity by increasing research funding; collaboration among leading research institutions and industry leaders in and beyond Europe under the ethical framework of Principled Big Tech should be a key focus of EU and national research funding.
- Developing safe, secure and open standards and working towards economic diversification through modular and open designs, such as openRAN for telecommunications, should be identified as key elements of European strategic autonomy by the European Commission.
- The EU and its member states should allocate funds to multilateral standardisation bodies in order to reduce economic pressures related to vendor lock-in and dependence on foreign suppliers.

INTRODUCTION

Strategic dependencies in the field of advanced technology have forced European states to rethink the balance between national security and a globalised economy. This situation reflects European concerns over American abandonment, Russian aggression and Chinese assertiveness, and has ultimately led to the pursuit of strategic autonomy through technological autonomy. While the debate on strategic autonomy has a long pedigree in the military domain[229], it has expanded into a multi-domain deliberation in parallel with globalised trade,[230] facilitating an emerging multi-order world with inherent and growing tensions. Innovation, production, protection, and security of supply of advanced technology have become a highly competitive and contested pursuit as great-power competition is intensifying.

Global external dependencies have never been more entrenched than in the current tech sector.[231] The inevitable progression towards digitised

229 See N. Koenig, 'The EU as an autonomous defence actor', in N. Helwig, ed., The EU's ambition for Strategic Autonomy: early lessons and the way forward, (Helsinki: Finnish Institute of International Affairs)

230 See T. Gehrke, 'EU Strategic Autonomy in Trade and Investment policy', in N. Helwig, ed., The EU's ambition for Strategic Autonomy: early lessons and the way forward, (Helsinki: Finnish Institute of International Affairs)

231 J. Rogers, A. Foxall, M. Henderson, S. Armstrong, Breaking the China supply chain: how the 'five eyes' can decouple from strategic dependency, (London: The Henry Jackson Society, May 2020), https://henryjacksonsociety.org/wp-content/uploads/2020/05/Breaking-the-China-Chain.pdf, accessed 26 Feb. 2021

lives has inserted companies and the advanced technologies of foreign states directly into the everyday operations of critical sectors all over Europe. In response, the EU has come to view external influence and dependencies as a national security threat and is seeking to reclaim control over key critical technologies and infrastructures.[232] This is notably pursued in a principled way true to European values, attempting to place the EU as a global norm entrepreneur in disruptive and emerging tech – motivated in particular by China's rise and the risks posed by the implementation of China's *Made in China 2025* plan.

This chapter captures these EU aspirations within the concept of Principled Big Tech. It identifies the main drivers for the pursuit of European technological autonomy, situates vulnerabilities and threats within the dynamics of weaponised interdependence, analyses the critical case of implementation of next-generation wireless 5G technology and explores possibilities and pitfalls for European tech cooperation through the Franco-German debate on Artificial Intelligence. The chapter concludes by presenting policy perspectives and recommendations for *European Principled Big Tech*.

EUROPEAN VULNERABILITIES IN THE ADVANCED TECH SECTOR

The new security environment of great power competition[233] via advanced technology has come to dominate developments in security policies, business decisions and global knowledge flows. With technology colonising every aspect of the civilian sphere, it is impossible to contain this tech race within the realm of strategic competition and diplomatic affairs. One prominent example is the US 'Huawei ban' from 2019, which forced Google to withdraw its cooperation with Huawei thus leaving all next-generation Huawei devices without the Google suite of apps including YouTube, Gmail, Google Maps, Google Drive and the Google Play Store.[234] It is now quite a different experience for the private consumer buying a Huawei phone compared with before the ban. Everyday life is thus being shaped by the fast-moving ripples of international politics when market forces bend to the needs of national security and alliance politics.

232 E. S. Nicolás, 'EU five-year security plan to focus on critical infrastructure', EU Observer, 24 Jul. https://euobserver.com/justice/149030 accessed 15 Mar. 2021.

233 See V. Sinkkonen, E. Sikkonen, 'Setting the scene: A multi-dimensional view on US-China great-power competition', in N. Helwig, ed., The EU's ambition for Strategic Autonomy: early lessons and the way forward, (Helsinki: Finnish Institute of International Affairs)

234 C. Scott Brown, 'The Huawei ban explained: A complete timeline and everything you need to know', Android Authority, (7 Feb. 2021), https://www.androidauthority.com/huawei-google-android-ban-988382, accessed 26. Feb. 2021.

The driving actors, America and China, are quickly spiralling into a tech race and decoupling in highly sensitive areas of emerging and disruptive technologies. The dynamic involves other actors suffering collateral damage, as illustrated by US President Trump's 2018 blocking of the largest tech deal in history. When Singapore-based semiconductor and communications technology firm Broadcom attempted a takeover of the US-based mobile chip and wireless 5G giant Qualcomm, the Committee on Foreign Investment in the United States (CFIUS) saw a substantial national security threat relating to Qualcomm potentially losing out to Huawei in the 5G patent and standard-setting race.[235] Thus, a deal worth $117 billion collapsed. Conditioned by this rapid increase in what has been coined weaponised interdependence[236], European states must manoeuvre in a new world of securitised technologies in which battles are waged through economic coercion, infrastructure financing, foreign direct investments and espionage, to only name a few. The future of Europe's global role is at stake, and needs defining.

In response, President of the European Commission, Ursula von der Leyen, has announced the ambition to make the 2020s Europe's Digital Decade by focusing on principled approaches to research and development in data, technology and infrastructure. The political framework for achieving European technological autonomy is based on retaking and retaining control. According to von der Leyen, Europe's Digital Decade requires that "*we must have mastery and ownership of key technologies in Europe. These include quantum computing, artificial intelligence, blockchain, and critical chip technologies.*"[237] It is an ambitious vision that translates into Principled Big Tech and situates the EU as an actor in its own right – not just an actor to be acted upon by outside forces. The follow-through is, however, paved with conflicting interests among member states as will be exemplified by the issues involved in Franco-German cooperation on Artificial Intelligence.

Pursuing "*mastery and ownership*" confronts the changing landscape of weaponised interdependencies in networked relationships. Occupying critical global network nodes (e.g., routers, servers, online cloud services and also powerful roles in for example financial and political networks etc.) powered by advanced technology and knowledge is a

235 Depart of the Treasury, 'CFIUS CASE 18-036: Broadcom Limited (Singapore)/Qualcomm Incorporated', The Committee on Foreign Investments in the United States, (5 Mar. 2018), http://online.wsj.com/public/resources/documents/cfiusletter.pdf, accessed 26 Feb. 2021.

236 H. Farrell, A. L. Newman, 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', International Security, 44:1 (2019), 42-79, https://doi.org/10.1162/isec_a_00351

237 U. v.d. Leyen, 'Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme', (27 Nov. 2019), https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_6408, accessed 23. Feb. 2021.

primary objective in the global great power competition: node positions and network ties provide power and leverage.[238] Notably, this dynamic relates to and intertwines with the physical and the political world simultaneously. Controlling network chokepoints can mean gaining access to turning off physical telecommunications infrastructure as well as political access to deny specific actors' participation in, for example, a financial network such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT), as happened to Iran in 2012.[239]

Weaponising interdependence in the technology sector is at the abstract level particularly about controlling information infrastructure networks. This has forced many actors to recalibrate their perspectives on the consequences of technological dependencies, supply-chain links and international research partnerships.[240] It has also sparked a discussion on whether new technologies and their proliferation are infused with normative values. A critical challenge for the EU and its member states is to move from visions of Principled Big Tech to real political decisions. The potential of new technologies to compete with European values becomes evident in Chinese Artificial Intelligence and 5G technology, specifically given the dominance of companies such as Huawei that potentially undergird the global export of digital authoritarianism and the surveillance state.[241] A case in point is Huawei's 'Uighur alarm', which combines facial recognition with racial profiling to identify oppressed Uighur minorities and alert the Chinese police.[242] Europe's lacklustre performance in fostering Big Tech companies only accentuates this development, leaving both the EU bloc and individual European states vulnerable to external pressures and influence. These dynamics and challenges have spurred European introspection about the pursuit of technological autonomy and how it could affect the very nature of the European Union.

The quest for technological autonomy points back to the basic roots of the European Union providing and balancing freedom and security: the four fundamental freedoms of the common market allowing the free movement of goods, people, services and capital, and the security

238 Farrell et al., 'Weaponized Interdependence', 47

239 Farrell et al., 'Weaponized Interdependence', 67

240 R. Davies, 'Oxford places ban on donations and research grants from Huawei,The Guardian', (17 Jan. 2019), https://www.theguardian.com/technology/2019/jan/17/oxford-places-ban-on-donations-and-research-grants-from-huawei-chinese-national-security, accessed 27 Feb. 2021

241 P. Mozur, J. M. Kessel, M. Chan, 'Made in China, Exported to the World: The Surveillance State', New York Times, (24 Apr. 2019), https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html, accessed 27 Feb. 2021

242 D. Harwell, E. Dou, 'Huawei tested AI software that could recognize Uighur minorities and alert police, report says', Washington Post, (8 Dec. 2020), https://www.washingtonpost.com/technology/2020/12/08/huawei-tested-ai-software-that-could-recognize-uighur-minorities-alert-police-report-says, accessed 27 Feb. 2021

dimension expressed in the Common Foreign and Security Policy. The vision of a whole and free Europe as a model for the rest of the world[243] has increasingly been compromised due to a perceived lack of effectiveness of European common security. This clash between the free market ideology and security concerns has become evident through China's use of coercive diplomacy[244] in the 5G debate. For example, the Chinese ambassador to Germany publicly floated the idea of labelling German cars as unsafe, thereby cutting off valuable market access to China, if Germany were to exclude Huawei on security grounds.[245] In a recent response to critical voices, European Council President Charles Michel took issue with business concerns, in particular about trade-offs inherent in the European pursuit of strategic autonomy. He declared that "*autonomy is not protectionism. Quite the opposite!*"[246] This is, however, a difficult position to hold, in that autonomy in a world of weaponised interdependence requires, at a minimum, compartmentalised protectionism. This is also evidenced in the EU's tighter export controls and investment-screening measures, which are discussed more thoroughly later in the chapter.

The comparatively weak position of European high-tech can be inferred from the dominance of American, Chinese and Japanese companies in the technology sector of the Fortune Global 500 rankings.[247] Although German SAP (business software solutions), Irish Accenture (consulting) and Finnish Nokia (telecom) are represented, they are dwarfed by the extensive ecosystems and network node positions of non-European corporations. Gatekeepers that wield economic, social and political power and thus represent serious potential security risks are therefore targeted as platform providers. The aim is to regulate these gatekeepers in line with the Principled Big Tech approach of data protection, privacy and

243 G. Bush, 'A Europe Whole and Free', (31 May 1989), https://usa.usembassy.de/etexts/ga6-890531.htm, accessed 23. Feb. 2021.

244 F. Hanson, E. Currey, T. Beattie, 'The Chinese Communist Party's coercive diplomacy', Australian Strategic Policy Institute, (Policy Brief Report No. 36/2020), https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-08/The%20CCP%20coercive%20diplomacy_0.pdf?4M_JTUAd05Bjek_hvHt1NKKdcLts4kbY, accessed 27 Feb. 2021; See also N. Helwig, 'Strategic Autonomy and the EU as a diplomatic actor: a new leitmotiv in the era of international competition?', in N. Helwig, ed., The EU's ambition for Strategic Autonomy: early lessons and the way forward, (Helsinki: Finnish Institute of International Affairs)

245 K. Bennhold, J. Ewing, 'In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers', New York Times, (16 Jan. 2020), https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html, accessed 27 Feb. 2021; J. Petzinger. China threatens 'consequences' if Germany bans Huawei, Yahoo! News, (16 Dec. 2019), https://news.yahoo.com/china-huawei-ambassador-threat-germany-135600540.html, accessed 27 Feb. 2021

246 C. Michel, 'Strategic autonomy for Europe - the aim of our generation' - speech by President Charles Michel to the Bruegel think tank, (28 Sep. 2020), https://www.consilium.europa.eu/de/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, accessed 23 Feb. 2021.

247 Fortune, 'Global 500', https://fortune.com/global500/2020/search/?sector=Technology, accessed 23 Feb. 2021.

transparency, as well as to safeguard an efficient and open market.[248] It is noteworthy that the EU is under pressure from each side of the US–China great power competition. While the American Big Five tech companies Alphabet (Google), Amazon, Facebook, Apple and Microsoft leverage pressures and occupy market space from the West, the Chinese counterparts Baidu, Alibaba, Tencent and Xiaomi expand from the East. In addition, the global position on the 5G market of Chinese telecom behemoth Huawei, ByteDance's TikTok app and the Chinese state's GPS alternative BeiDou leave little room for European companies in the global Information and Communications Technology market.[249]

Technological ecosystems are ideal for weaponising interdependence in that they serve as underlying networks for the information space in all sectors ranging from business, health, finance and research to national resilience. It should nevertheless be kept in mind that European dependencies on US and Chinese network nodes do not carry similar types or levels of risk. This difference between being allies and non-allies is fundamentally formalised in NATO's collective security commitments with the US and Europe. Within this security relationship, network node positions are of prime importance as was evidenced by the Trump administration when it publicly contemplated scaling back intelligence sharing with partners choosing Huawei's 5G kits.[250]

Initial European steps towards reconciling freedom and security in this space lie, as mentioned, in the EU's attempts at Principled Big Tech. The main tools include regulating behaviour by taxing digital services[251], bringing antitrust cases against Google[252] and Amazon[253], and applying the General Data Protection Regulation (GDPR) for the protection of

248 Gatekeepers, according to the European Commission's proposed Digital Markets Act, are those providers of core platform services who: '(i) have a significant impact on the internal market, (ii) operate one or more important gateways to customers and (iii) enjoy or are expected to enjoy an entrenched and durable position in their operations.' The European Commission's embrace of the gatekeeping concept falls in line with the network nodes, ties and chokepoints approach of weaponised interdependence. See European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act), European Commission, (15 Dec. 2020), https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN, accessed 27 Feb. 2021

249 C. Yap, 'State Support Helped Fuel Huawei's Global Rise', Wall Street Journal (25 Dec. 2019), https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736, accessed 23 Feb. 2021

250 B. Pancevski, S. Germano, 'Drop Huawei or See Intelligence Sharing Pared Back, U.S. Tells Germany', (11 Mar. 2019), The Wall Street Journal, https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827, accessed 1 Mar. 2021

251 J. Vincent, 'Apple, Google, and Amazon respond to European tech taxes by passing on costs', The Verge (2 Sep. 2020), https://www.theverge.com/2020/9/2/21418114/european-uk-digital-tax-services-apple-google-amazon-raise-prices, accessed 23 Feb. 2021

252 J. Whalen, 'Europe fined Google nearly $10 billion for antitrust violations, but little has changed', Washington Post (10 Nov. 2020), https://www.washingtonpost.com/technology/2020/11/10/eu-antitrust-probe-google, accessed 23 Feb. 2021

253 N. Lomas, 'Europe lays out anititrust case against Amazon's use of big data', TechCrunch (10. Nov. 2020), https://techcrunch.com/2020/11/10/europe-lays-out-antitrust-case-against-amazons-use-of-big-data, accessed 23 Feb. 2021

personal data and the use and transfer thereof. Europe's Digital Decade has thus far been spearheaded by efforts at digital governance. Regulation, however, is neither mastery nor ownership of key technologies. All of these major cross-pressures on Europe's vulnerabilities in the field of advanced technologies have culminated in one critical case: Huawei in European 5G networks.

5G AS A CRITICAL CASE OF STRATEGIC TECHNOLOGICAL AUTONOMY

The emergence of the fifth generation of mobile technology, 5G, has brought to attention the importance of strategic technological autonomy. In this, it serves as a principal case of testing versus trusting. The 5G debate illustrates the continuously moving demarcation line between being confident in the ability of intelligence services to test and risk-assess advanced tech on the one hand and being forced by the opaqueness of complex tech to trust the supplier on the other. The current dominance of Huawei on the supplier market for 5G components has driven speculation about related risks, testing and trusting, and the influence of the Chinese government on strategic national assets.

The discussion on strategic risks related to Huawei was initiated by the Australian government [254] in 2018. The US government followed, banning Huawei as a supplier for its 5G networks and putting pressure on allied countries to do the same.[255] US intelligence services raised concerns about open backdoors for spying and sabotage on critical infrastructure [256], however, no technological or other evidence has been provided to the public.

Understanding the complexity of 5G supports a fact-based assessment of the risks involved concerning the technology and the reliance on vendors and their supply chains. Figure 1 illustrates the basic architecture of 5G components, based on the 3GPP technical specifications[257] and

254 Bryan-Low, C. et al. (2019) Hobbling Huawei: Inside the U.S. war on China's tech giant, Reuters. London. Available at: https://www.reuters.com/investigates/special-report/huawei-usa-campaign/, accessed 4 March 2021.

255 S. Woo, K. O'Keeffe (2018), 'Washington Asks Allies to Drop Huawei', The Wall Street Journal, 23 Nov., https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105?, accessed 15 Mar.2021.

256 Pancevski, B. (2020) 'U.S. Officials Say Huawei Can Covertly Access Telecom Networks - WSJ', The Wall Street Journal, 12 February. Available at: https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256, accessed 4 Mar. 2021.

257 3rd Generation Partnership Project, 3GPP Specification Set: 5G (no date), https://www.3gpp.org/dynareport/SpecList.htm?release=Rel-15&tech=4, accessed 2 March 2021.

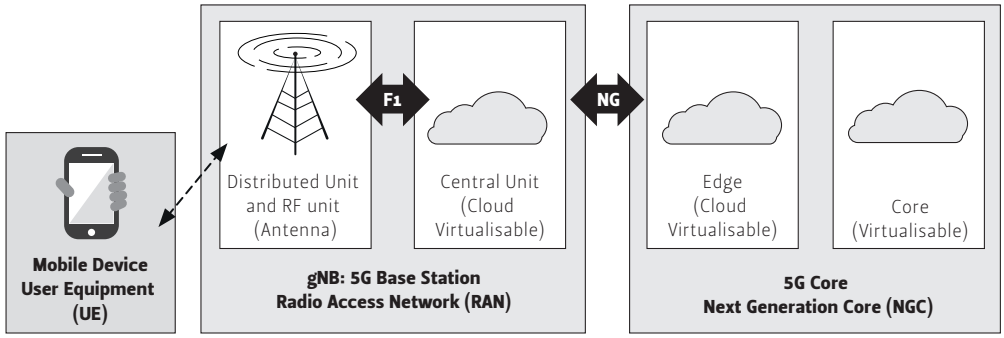

Figure 1: 5G Architecture components.

elaborations by Holma et al.[258] Typically, a mobile communication device is connected by radio signals to an antenna. Previously to 5G, the antenna had to be connected to and collocated with hardware components concerned with controlling the radio connection. The combination of these components and the antenna is known as the *Radio Access Network*, or RAN. The 5G specifications allow the virtualisation of former RAN hardware components. Virtualisation refers to the implementation of (former) hardware functionalities by means of software. Components that had to be bought as dedicated hardware can now be implemented and dynamically updated as software running on generic hardware, such as cloud server infrastructure. As Figure 1 shows, the RAN is connected to the Internet and other communication networks through the 5G Core network. Some Core network components have also become virtualisable since the introduction of 5G. This set-up enables the centralisation of RAN components for multiple antennas in a cloud infrastructure located in proximity, while decentralising 5G core components and moving them closer to the "edge" (the antennas).

5G specifies an open design of the interfaces connecting RAN and Core components (*F1* and *NG* in Figure 1). These features of 5G reduce the risk of vendor lock-in for RAN and the core network components, in other words it reduces reliance on one single vendor for a high number of components for reasons of compatibility. It has been claimed that this approach allows deployment of hardware components with a lower security risk, but this view is disputed.[259] The non-virtualisable RAN hardware components do not offer access to sensitive meta-data, since

258 H. Holma, A. Toskala and T. Nakamura, 5G technology: 3GPP new radio, John Wiley & Sons Ltd. Edited by H. Holma, A. Toskala, and T. Nakamura. John Wiley & Sons Ltd. (2020).

259 Y. Yang, What are the main security risks of using Huawei for 5G?, Financial Times (London: 2019), https://www.ft.com/content/8b48f460-50af-11e9-9c76-bf4a0ce37d49, accessed: 4 March 2021.

they are purely concerned with ensuring a stable radio connection. It is possible that these components might also become virtualisable through technological improvements.

Although the confidentiality risks in 5G RAN hardware components are low, malicious access to these components can potentially negatively affect the functioning of the whole 5G network by means of reducing or blocking radio-access capabilities. Backdoors or design errors of 5G RAN hardware components are not generally considered to enable straightforward attack vectors for spying or access to the core network. On the other hand, core components with built-in backdoors could facilitate malicious breaches of confidentiality.

Some governments have attempted to distinguish between vendor restrictions for higher-risk and low-risk components. However, experts (e.g., the UK's NCSC-led Huawei Oversight Board[260]) have accused Huawei of general malpractice in the secure design of its hardware components[261], which is not necessarily connected to any malicious intent and could be attributable to low-quality engineering.

As mentioned above, the discussion on risks in Huawei components was initiated by the Australian government and US intelligence services. A technical distinction between RAN and Core components, as outlined above, was not made. Claims were made that 5G networks depend on "*software updates pushed out by equipment suppliers - and that access to the 5G network* [...] *could be used to deploy malicious code*"[262], which seems plausible with regard to virtualised components running on cloud infrastructure. Hardware components of the 5G RAN architecture, however, do not fall into this category, although they might pose other risks, as outlined earlier. Moreover, Chinese national security laws force businesses such as Huawei to hand over data and information in cases of conflict.[263] This has been claimed to pose potential for malicious activities.

In terms of managing vendor risk, the UK government first released a differentiated assessment after its National Cyber Security Centre (NCSC) had assessed the risk to be *manageable*[264] in 2019. The NCSC

260 D. Bond, 'UK cyber security chief says Huawei risk can be managed', Financial Times (20 Feb. 2019), https://www.ft.com/content/4c2b6fa0-350d-11e9-bd3a-8b2a211d90d5, accessed 4 March 2021.

261 N. Lomas, 'UK Report Blasts Huawei for Network Security Incompetence', Tech Crunch (28 Mar. 2019), https://techcrunch.com/2019/03/28/uk-report-blasts-huawei-for-network-security-incompetence accessed 4 March 2021.

262 C. Bryan-Low, et al., 'Hobbling Huawei: Inside the U.S. war on China's tech giant', Reuters (London, 2019), https://www.reuters.com/investigates/special-report/huawei-usa-campaign/ accessed 4 March 2021.

263 A. Kharpal, 'Huawei would have to give data to China government if asked: experts', CNBC (Cliffs, New Jersey, 2019), https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html accessed 4 March 2021.

264 D. Bond, 'UK cyber security chief says Huawei risk can be managed', Financial Times (20 Feb. 2019), https://www.ft.com/content/4c2b6fa0-350d-11e9-bd3a-8b2a211d90d5 accessed 4 March 2021.

recommendation also analysed Huawei's software, i.e., software that runs on cloud components and virtualises RAN components. While backdoors in software are possible, they can be controlled and analysed more effectively, as done by the NCSC Huawei Oversight Board. It would be essential, however, that the hardware of the cloud infrastructure is not provided by the same vendor. If it were it, this would allow built-in hardware backdoors, which are more challenging to discover: cloud hardware components could then be used to access software backdoors from the same vendor.

The NCSC's recommendation on Huawei changed in 2020, and a plan has been published that eventually bans the use of any Huawei equipment on the UK's telecommunication networks by 2027.[265] This decision was based on concerns about supply-chain and further risks related to Huawei components under US sanctions against Huawei.[266] Although some supply-chain risks might be connected to US sanctions, there is an important case to be made about the risk connected with the location of production facilities in China and south-east Asia.

The UK's initial differentiated approach provides interesting policy considerations. The technical analysis of security-relevant parts of the network architecture, as well as the analysis conducted by the security oversight board analysing proprietary source-code and design documents in a confidential environment, provided an independent decision base. Strategic supply-chain considerations and collaboration with the UK's strategic partners, most prominently the US, seem to have had a significant impact on the reconsideration of the NCSC's recommendation.

The main competitors of Huawei for 5G components are Nokia and Ericsson. Both are headquartered in Europe, and their technological expertise on the architecture and design of mobile communication networks and components is an important European strategic asset in the 5G debate. Nevertheless, their hardware relies on components manufactured and assembled in Asia. This reliance on components from foreign vendors and the location of production facilities represent an important risk relevant for the assessment of strategic risks. Further risks arise from the practicalities of shipping: some of the Snowden revelations uncovered how simple it is for intelligence services to intercept and tamper with components delivered through standard channels, such as Cisco routers.[267] Even

265 H. Gold, 'UK bans Huawei from its 5G network in rapid about-face', Reuters (London, 2020), https://www.reuters.com/article/us-britain-huawei-reaction-instantview-idUSKCN24F1JL, accessed 4 March 2021.

266 NCSC UK, 'Summary of the NCSC analysis of May 2020 US sanction' (2020), https://www.ncsc.gov.uk/report/summary-of-ncsc-analysis-of-us-may-2020-sanction, accessed 4 March 2021.

267 B. Snyder, 'Snowden: The NSA planted backdoors in Cisco products', Infoworld, (15 May 2014), https://www.infoworld.com/article/2608141/snowden--the-nsa-planted-backdoors-in-cisco-products.html, accessed 4 March 2021.

more sophisticated supply-chain risks were brought to public attention in 2018 and 2021[268]: Components developed by Super Micro Computer, a US vendor, were allegedly altered in their Chinese manufacturing facilities before being shipped to customers. The hardware alterations enabled the attacker to connect to the components.

The Cisco and Super Micro examples underline the relevance of supply-chain risks for hardware components and that hardware components from high-risk suppliers only should be deployed if the risk of altered or added components has no or little influence on the overall risk assessment. This might be the case for Huawei 5G RAN hardware components when considering confidentiality risks. As mentioned, risks to network availability cannot be fully mitigated. It is up to national risk assessment procedures to consider the impact of this strategic risk and to balance it with economic factors. The EU has identified some of the risks outlined above in its *Cybersecurity of 5G networks EU Toolbox.*[269]

Furthermore, it has been claimed that relying on the Nokia-Ericsson duopoly would be economically unhealthy and strategically unwise in the long term[270], and that the modularisation of components in 5G and the standardisation of their interoperability enables a diversification towards smaller suppliers as a reasonable option. The aim behind the openRAN[271] initiative is to further develop interoperability of mobile network components from different vendors and thereby reduce the risk of "vendor lock-in". A diversification of vendors is further supported by technological security considerations. The 'Swiss Cheese Model of Accident Causation', a framework illustrating how a series of failures contribute to the breakdown of complex systems,[272] is commonly used for the mitigation of cybersecurity risks. It outlines how system failures, in this case strategic security incidents, arise from consecutive failures of defences in multiple layers. Each of these layers is illustrated as a slice of Swiss cheese, where security incidents are possible if the security holes in each layer align. Applied to the complexity of 5G, this means that systematic failures could be reduced if each network component (i.e., Swiss cheese layer) was provided by independent vendors, it being less likely that the

268 B. Snyder, 'Snowden: The NSA planted backdoors in Cisco products', Infoworld (15 May 2014), https://www.infoworld.com/article/2608141/snowden--the-nsa-planted-backdoors-in-cisco-products.html, accessed 4 March 2021.

269 NIS Cooperation Group, 'Report on Member States Progress in Implementing the EU Toolbox on 5G Cybersecurity July 2020' (2020), https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity, accessed 4 March 2021.

270 S. Häberli, 'Open RAN: Eine Alternative zu Nokia, Ericsson und Huawei', NZZ Pro Global (7 December 2020), https://www.nzz.ch/technologie/open-ran-eine-alternative-zu-nokia-ericsson-und-huawei-ld.1567348, accessed 4 March 2021.

271 O-RAN Alliance, O-RAN ALLIANCE (no date), https://www.o-ran.org/, accessed 4 March 2021.

272 J. Reason, 'The Contribution of Latent Human Failures to the Breakdown of Complex Systems'. Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences, 327(1241), (1990), 475-484.

security holes of differently sourced components would align. This is a strong argument in favour of vendor diversification and interoperability standards, as supported by the openRAN initiative.

The useful measures and steps suggested in the EU 5G Toolbox should be complemented by the recommendations in this chapter. A study launched by the European Commission in June 2020 currently analyses the potential of openRAN and global 5G supply-chain market trends.[273] These steps are in line with the idea of Principled Big Tech: they encourage economic diversification, reducing reliance on potentially high-risk oligopolist companies such as Huawei, while supporting the evolvement of smaller companies producing 5G components in Europe and beyond. A diversification of vendors for strategic technologies, reduces the risk of single-points-of-failure and cluster risks and supports the economic development of smaller vendors, enabling dynamic risk management in response to changes in the risk landscape.

TECH AS A NATIONAL SECURITY THREAT PUSHING EUROPEAN AMBITIONS

Securitisation of emerging and disruptive technologies are likely to follow the precedent set by the 5G debate, intensifying arguments about trust and testing. Unless the EU manages to deliver on Europe's Digital Decade, European vulnerabilities will be exacerbated through an accelerating pace of development and deployment of these technologies by non-EU actors. In response, political ambitions have been bolstered to such a degree that the EU's new Cybersecurity Strategy proposal calls for technological sovereignty–not just autonomy–and leadership through an '*unprecedented level of investment in the EU's digital transition*'.[274] The EU is budgeting for a proposed funding of €7.5 billion for the *Digital Europe Programme* in 2021-2027, also targeting research and development in AI (€2.1 billion).[275] To put these numbers into perspective, the US National Security Commission on Artificial Intelligence recently recommended increased federal funding for AI research to reach €26.5 billion per year

273 The Directorate General for Communications Networks Content and Technology. European Commission launches study on 5G supply markets and Open RAN. European Commission (24 July 2020), https://ec.europa.eu/digital-single-market/en/news/european-commission-launches-study-5g-supply-markets-and-open-ran

274 European Commission, 'The Cybersecurity Strategy', European Commission (16 Dec. 2020), https://ec.europa.eu/digital-singlae-market/en/cybersecurity-strategy, accessed 23 Feb. 2021.

275 European Commission, 'Europe investing in digital: the Digital Europe Programme', European Commission, (n.d.), https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme, accessed 28 Feb. 2021

by 2026.[276] Looking at China, it is difficult[277] to estimate Chinese state funding of AI research and development, but it is general practice to rank the US first and China second in the global AI race with Europe coming in third place.[278]

The European intention to develop technological or digital sovereignty through regulation and an increase in local innovation and knowledge capacity must be distinguished from alternative and competing visions of sovereignty. This is where EU technological sovereignty through Principled Big Tech differs from the example of China's vision of attempting to re-establish territoriality and information control on the Internet through the restriction of information flow and services.[279] This vision is fundamentally opposed to the technological structure of the current Internet, as well as to the politically liberal idea of a free and open Internet that has shaped the Western approach to Internet regulation.[280] Russia[281] and other countries, such as Iran[282], follow a similar approach of establishing information control on the Internet, ultimately leading to a 'splinternet' in that the global character of cyberspace would be destroyed.[283] European Principled Big Tech would be the technological antidote to this: it does not aim to censor political content and puts a stronger emphasis on freedom, while acknowledging and further developing the global nature of cyberspace services and the Internet. These developments are taking place within a geopolitical dynamic similar to the long-standing debates

276 National Security Commission on Artificial Intelligence, 'Draft Final Report', National Security Commission on Artificial Intelligence, (Jan. 2021), 90, https://www.nscai.gov/wp-content/uploads/2021/01/NSCAI-Draft-Final-Report-1.19.21.pdf, accessed 28 Feb. 2021.

277 T. J. Colvin, I. Liu, T. F. Babou, G. J. Wong, 'A Brief Examination of Chinese Government Expenditures on Artificial Intelligence R&D', (Feb. 2020), (Washington: IDA SCIENCE & TECHNOLOGY POLICY INSTITUTE), iv, https://www.ida.org/-/media/feature/publications/a/ab/a-brief-examination-of-chinese-government-expenditures-on-artificial-intelligence-r-and-d/d-12068.ashx, accessed 1 Mar. 2021

278 D. Castro, M. McLaughlin, 'Who is winning the AI race: China, the EU, or the United States? 2021 update', (Jan. 2021), Center for Data Innovation, https://www2.datainnovation.org/2021-china-eu-us-ai.pdf, accessed 28 Feb. 2021; European Commission, 'USA-China-EU plans for AI: where do we stand?', (Jan. 2018), Digital Transformation Monitor, https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_AI%20USA-China-EU%20plans%20for%20AI%20v5.pdf, accessed 1 Mar. 2021.

279 A. Segal, 'China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace', in N. Rolland, ed., An Emerging China-centric Order. China's Vision for a New World Order in Practice, NBR Special Report no. 87, (25 Aug. 2020), (Washington: The National Bureau of Asian Research), https://www.nbr.org/wp-content/uploads/pdfs/publications/sr87_aug2020.pdf, accessed 1 Mar. 2021.

280 J. P. Barlow, 'A Declaration of the Independence of Cyberspace', (8 Feb. 1996), Electronic Frontier Foundation, https://www.eff.org/cyberspace-independence, accessed 1 Mar. 2021.

281 N. Tsydenova, 'Russia plans 'sovereign internet' tests to combat external threats', (19 Dec. 2019), Reuters, https://www.reuters.com/article/us-russia-putin-internet/russia-plans-sovereign-internet-tests-to-combat-external-threats-idUSKBN1YN23Z, accessed 1 Mar. 2021.

282 M. Burgess, 'Iran's total internet shutdown is a blueprint for breaking the web', (7 Oct. 2020), Wired, https://www.wired.co.uk/article/iran-news-internet-shutdown, accessed 1 Mar. 2021.

283 M. Murgia, A. Gross, 'Inside China's controversial mission to reinvent the internet', (27 Mar. 2020), Financial Times Magazine, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f, accessed 1 Mar. 2021.

on strategic autonomy in the military domain, which are expanding into the digital technology sector.

In recent years, the French ambitions to develop an autonomous European military capability without depending on American capacities have received renewed political backing in the light of Russian aggression, American retrenchment and the exit of the United Kingdom from the EU. German chancellor Angela Merkel reacted to these fundamental changes in the threat and alliance landscape in 2017, declaring that '*[t]he era in which we could fully rely on others is over to some extent*', concluding '*[w]e Europeans truly have to take our fate into our own hands*'.[284] In the pursuit of technological autonomy, this sentiment can by now be considered as widely adopted amongst EU leaders, but with one critical sectorial addition: the primary driver for Europe is China's technological rise. Simultaneously, the American Trump administration's forceful 5G-Huawei campaign also brought European technological concerns to the attention of the EU and its member states.

China's native and global tech ambitions have been outlined and pursued since at least 2006 when the 15-year 'Medium- to Long-term Plan for the Development of Science and Technology' was launched.[285] In continuation hereof, China's current push to lead and pursue self-sufficiency in 10 core industries has been formalised since the 2015 launch of the *Made in China 2025* plan. The plan's focus is on leading global innovation and production in 10 highly specialised sectors such as New materials, Next-generation IT as well as High-end computerised machines and robots.[286] Early on, the European Union Chamber of Commerce in China criticised the plan for being '*a large-scale import substitution plan aimed at nationalizing key industries*'[287] and the German MERICS think-tank has pointed out the primary aim of large-scale technology transfer to China.[288] This approach lines up with capacity building to be able to simultaneously avoid and exert weaponised interdependence by conquering central network nodes and ties. Although this challenge from China is not new, the global ambitions, intensity of impact and

284 G. Paravicini, 'Angela Merkel: Europe must take 'our fate' into own hands', Politico (28 May 2017), https://www.politico.eu/article/angela-merkel-europe-cdu-must-take-its-fate-into-its-own-hands-elections-2017, accessed 23 Feb. 2021

285 C. Cao, R. P. Suttmeir, D. F. Simon, 'China's 15-year science and technology plan', Physics Today (Dec. 2006), 38, https://china-us.uoregon.edu/pdf/final%20print%20version.pdf, accessed 23 Feb. 2021.

286 M. J. Zenglein, A. Holzmann, Evolving Made in China 2025 - China's industrial policy in the quest for global tech leadership, (Berlin: MERICS, Jul 2019), 20, https://merics.org/sites/default/files/2020-04/MPOC_8_MadeinChina_2025_final_3.pdf

287 J. McDonald, 'Business group: China tech plan threat to foreign firms', Associated Press (7 Mar. 2017), https://apnews.com/article/8451ec21c5e543bda2e41cc81fae31f0, accessed 23 Feb. 2021

288 J. Wübbeke, M. Meissner, M. J. Zenglein, J. Ives, B. Conrad, Made in China 2025 - The making of a high-tech superpower and consequences for industrial countries, (Berlin: Rhodium Group/MERICS, Dec. 2016), 8, https://merics.org/sites/default/files/2020-04/Made%20in%20China%202025.pdf

US-Sino confrontation add novel attributes and ask of Europe to give greater weight to security implications of global tech interdependencies.

An acceleration of potential and actual weaponised interdependence in the tech sector has taken place since the 2007-08 global financial crisis. The crisis emboldened Chinese elites to abandon their '*strategic patience*', waiting for China to finally assume its quietly developed great power status. As confidence in the US-led economic order faltered, it simultaneously reinforced Chinese elite views of US decline and the potency of a Chinese alternative.[289] In the wake of the financial crisis, Chinese foreign direct investments in the EU skyrocketed from 700 million dollars in 2008 to its peak at 37.3 billion dollars in 2016,[290] with many acquisitions of advanced technology in support of China's technology transfer strategy. These enormous shifts are taking place in the context of China's overarching Military-Civil-Fusion strategy that, according to the US-China Economic and Security Review Commission, aims at '*leveraging the fruits of civilian innovation for China's defense sector.*'[291] This is an immense national security challenge in that civilian rather than traditionally dual-use advanced technology from Europe risks being exploited, frequently by state-owned companies or private companies under the control of the Chinese military, in a high-tech military arms race.[292]

These concerns have built political momentum, converging in a changed European perception of China that made its debut in the EU's strategic outlook, famously labelling China '*an economic competitor in the pursuit of technological leadership, and a systemic rival promoting alternative models of governance.*'[293] French president Emmanuel Macron has assumed an albeit ambivalent[294] but leading role in this policy process to guard the EU through his 'protective' Europe agenda.[295] Con-

289 J. Blanchette, 'The Case of Xi Jinping', The Asan Forum (20 Jan. 2020), http://www.theasanforum.org/the-case-of-xi-jinping/#a6, accessed 23 Feb. 2021

290 A. Kratz, M. Huotari, T. Hanemann, R. Arcesati, Chinese FDI in Europe: 2019 Update - Special Topic: Research Collaborations, (Berlin: MERICS, Apr. 2020), 9, accessed 23 Feb. 2021, https://merics.org/sites/default/files/2020-05/MERICSRhodium%20GroupCOFDIUpdate2020.pdf, accessed 23 Feb. 2021.

291 U.S.-China Economic and Security Review Commission, 2019 Report to Congress of the U.S.-China Economic and Security Review Commission, (2019), 205, https://www.uscc.gov/sites/default/files/2019-11/Chapter%203%20Section%202%20-%20Emerging%20Technologies%20and%20Military-Civil%20Fusion%20-%20Artificial%20Intelligence,%20New%20Materials,%20and%20New%20Energy.pdf, accessed 23 Feb. 2021

292 G. Levesque, 'Military-Civil Fusion: Beijing's "Guns AND Butter" Strategy to Become a Technological Superpower', China Brief, Volume: 19 Issue: 18, (Oct. 2019), https://jamestown.org/program/military-civil-fusion-beijings-guns-and-butter-strategy-to-become-a-technological-superpower, accessed 23 Feb. 2021

293 European Commission, 'EU-China - A strategic outlook', European Commission, (12 Mar. 2019), 1, https://ec.europa.eu/info/sites/info/files/communication-eu-china-a-strategic-outlook.pdf, accessed 28 Feb. 2021.

294 F. Nicolas, 'France's incoherent China policy confuses partners', East Asia Forum, (22 Oct. 2020), https://www.eastasiaforum.org/2020/10/22/frances-incoherent-china-policy-confuses-partners, accessed 28 Feb. 2021

295 R. Emmott, M. Rose, 'At EU summit, Macron pleads for limits to foreign takeovers', Reuters, (22 Jun. 2017), https://www.reuters.com/article/us-eu-summit-macron-idUKKBN19D2HY?edition-redirect=uk, accessed 28 Feb. 2021

sequentially, president Macron, with the support of Chancellor Merkel, introduced the EU-wide investment-screening mechanism already in 2017. Its aim was to vet and potentially block foreign take-overs of key European industries and it initially encountered resistance from a host of pro-trade EU member states.[296] However, as a testament to the fast pace of change, this screening framework was in place in March 2019.[297] However, the effectiveness of the mechanism depends fully on national intelligence agencies and governments activating it, even when faced with a potential backlash. In light of the coronavirus pandemic's negative economic effects at the beginning of 2020, the European Commission activated the framework and issued guidelines to protect critical European assets and technology from being sold off. It is thus clear that the bolstering of European tech ambitions requires strategic risk-aware regulation of market access to foreign entities. This is an overly complex matter involving a host of vested interests and actors for whom national security is not necessarily on top of their agenda.[298]

EUROPEAN CONSTRAINTS ON TECHNOLOGICAL AUTONOMY

European momentum usually requires Franco-German leadership. This logic also applies to the pursuit of technological autonomy. One such prominent venture and bellwether for future pathways is the GAIA-X project that aims to achieve European cloud computing independence from US and Chinese data ecosystems, while under the protection of EU data laws. It will therefore facilitate synergies across industries and services.[299] These ambitious aims underscore the massive impact of successful Franco-German tech cooperation. Nevertheless, even as Macron and Merkel have reached political agreement on boosting the European industrial base to develop 5G, Artificial Intelligence and cloud infrastructure,[300]

296 A. Beesley, A. Chassany, J. Brunsden, D. Robinson, 'EU free-traders water down Macron's plan to vet foreign takeovers', Financial Times, (23 Jun. 2017), https://www.ft.com/content/e72b6342-582e-11e7-9fed-c19e2700005f, accessed 28 Feb. 2021

297 European Union, 'REGULATION (EU) 2019/452 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union', European Union, (19 Mar. 2019), https://eur-lex.europa.eu/legal-content/ENG/TXT/HTML/?uri=CELEX%3A32019R0452, accessed 28 Feb. 2021.

298 M. Karnitschnig, 'How Germany opened the door to China — and threw away the key', (10 Sep. 2020), Politico, https://www.politico.eu/article/germany-china-economy-business-technology-industry-trade-security, accessed 1 Mar. 2021

299 O. Hughes, 'What is Gaia-X? A guide to Europe's cloud computing fight-back plan', (10 Jun. 2020), Tech Republic, https://www.techrepublic.com/article/what-is-gaia-x-a-guide-to-europes-cloud-computing-fight-back-plan, accessed 28 Feb. 2021.

300 Élysée, 'Dialogue franco-allemand sur la Technologie.', (13 Oct. 2020), Élysée, https://www.elysee.fr/emmanuel-macron/2020/10/13/dialogue-franco-allemand-sur-la-technologie, accessed 28 Feb. 2021.

challenges still await in intra-European debates on use cases, economic commitments and profitability.

The lack of consensus on how technological autonomy should be defined and achieved puts serious limits to cooperative projects at the EU level and furthers uncertainties about member states' national policies and external relations.[301] This is particularly evident in efforts to develop Artificial Intelligence as a strategic necessity for the data-driven future. As one of the most disruptive emerging technologies, AI will be decisive in terms of which actors provide and occupy critical network nodes and ties.[302] French[303] and German[304] national AI strategies exemplify some of the main constraints holding back overall European progress. The French strategy stresses Europe's dire situation as a cyber colony in many aspects,[305] and in addition, France has expanded on the use case of AI by publishing a military AI strategy.[306] The German AI strategy, on the other hand, defers foreign policy and defence-related AI matters to the Ministry of Defence and focuses narrowly on AI as a largely economic concern.[307] The general German AI sentiment is one of moral scepticism towards the Big Data gathering and analysis that drives AI development.[308]

EU-level cooperation on technological autonomy also faces constraints through smaller states' fears of Franco-German industrial dominance given that global tech titans will likely rise from the largest EU members and therefore drive out competition.[309] Yet another constraint regards the contentious nexus of technological autonomy and trade policies as highlighted by the EU investment-screening mechanism. Here, too, the

301 P. Tamma, 'Europe wants 'strategic autonomy' — it just has to decide what that means', Politico, (15 Oct. 2020), https://www.politico.eu/article/europe-trade-wants-strategic-autonomy-decide-what-means, accessed 28 Feb. 2021.

302 J. Vincent, 'Putin says the nation that leads in AI 'will be the ruler of the world', (4 Sep. 2017), The Verge, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world, accessed 28 Feb. 2021.

303 C. Villani, 'For a meaningful Artificial Intelligence - Towards a French and European Strategy', AI for humanity, (Mar. 2018), https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf, accessed 28 Feb. 2021.

304 Bundesregierung, 'Strategie Künstliche Intelligenz der Bundesregierung', (Nov. 2018), Bundesregierung, https://www.bmbf.de/files/Nationale_KI-Strategie.pdf, accessed 28 Feb. 2021.

305 C. Villani, 'For a meaningful Artificial Intelligence - Towards a French and European Strategy', 6.

306 Ministère des Armées, 'Report of the AI Task Force September 2019', (Sep. 2019), Ministère des Armées, https://www.defense.gouv.fr/english/content/download/573877/9834690/Strat%C3%A9gie%20de%20l%27IA-UK_9%201%202020.pdf, accessed 28 Feb. 2021.

307 U. Franke, 'Not smart enough: The poverty of European military thinking on artificial intelligence', European Council on Foreign Relations, (18 Dec. 2019), https://ecfr.eu/publication/not_smart_enough_poverty_european_military_thinking_artificial_intelligence, accessed 28 Feb. 2021.

308 S. Kinkartz, 'Skeptical Germany lags behind on artificial intelligence', Deutsche Welle (29 Dec. 2019), https://www.dw.com/en/skeptical-germany-lags-behind-on-artificial-intelligence/a-51828604, accessed 28 Feb. 2021.

309 P. Tamma, 'Europe wants 'strategic autonomy' — it just has to decide what that means', Politico (15 Oct. 2020), https://www.politico.eu/article/europe-trade-wants-strategic-autonomy-decide-what-means/ accessed 28 Feb. 2021.

EU suffers from strategic ambivalence in that the proposed EU–China Comprehensive Agreement on Investment[310] will increase external dependencies by opening up the Chinese market to more European activity while simultaneously driving a wedge between the European and American strategies.[311] The Franco–German locomotive therefore still needs to get all its parts assembled to gain European momentum.

CONCLUSION: THE PATH TO EUROPEAN PRINCIPLED BIG TECH

The pursuit of European technological autonomy through a principled path of political values and judicial regulations puts the EU in the position of a potential universal norm entrepreneur. Attempting to shape global tech standards by turning the coming years into Europe's Digital Decade is, however, an enormous task. Two major and interlinked questions remain to be answered. Will the EU have to accelerate its development of advanced technology to succeed as a global norm entrepreneur? And will the EU be able to catch up in the Big Tech race following its own principled path?

The EU has already shown itself successful in promoting the GDPR rule set as a global data-protection standard. It has done this through leveraging its own economic network nodes and ties by linking free-trade agreements to the adoption of privacy standards similar to the GDPR.[312] The process takes place through adequacy decisions allowing personal data flows from the EU to approved countries. In spite of 12 such approvals so far, there is still a momentous distance from the Faroe Islands and Switzerland to Iran or China. Moreover, the EU's networked leverage in this matter (single market access) is not specifically technological in nature, which would likely be required in order to shape standards adopted by illiberal or authoritarian states. It is thus assessed to be an improbable outcome for the EU to succeed as a norm entrepreneur on advanced tech without having globally competitive companies, ecosystems and industrial bases. Lessons learned from the 5G debate attest to the need for the EU to overcome its internal constraints to strategically pursue technological autonomy in a direct race with leading global actors. Pursuing it along

310 European Commission, 'Key elements of the EU–China Comprehensive Agreement on Investment', (30 Dec. 2020), European Commission, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2542, accessed 28 Feb. 2021.

311 T. Colson, 'China is playing divide-and-rule between the United States and Europe and it's working', Business Insider (9 Jan. 2021), https://www.businessinsider.com/china-divide-and-rule-tactics-divide-bidens-us-and-europe-2021-1?r=US&IR=T, accessed 28 Feb. 2021.

312 M. Scott, L. Cerulus, 'Europe's new data protection rules export privacy standards worldwide', Politico (31 Jan. 2018), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation, accessed 28 Feb. 2021.

the path of Principled Big Tech may, however, turn out to be difficult. A number of recommendations can support this ambition.

Two mutually reinforcing approaches place the following recommendations within already established and developing political frameworks. With regard to the protection of strategic assets the aim is to safeguard past and future technological advancements by intensifying investment screening and export controls. In terms of investment in strategic assets, the aim is to boost the EU's credibility and leverage as a norm entrepreneur through innovation and transparency.

Protection of strategic assets should focus on streamlining national guidelines on critical infrastructure to also include critical technologies, knowledge and data to advance the principled use of the EU investment-screening mechanism. Likewise, EU export-control regulations on dual-use technologies should take the concept of weaponised interdependence seriously and consider broadening its scope, especially in light of the Chinese Military-Civil-Fusion strategy. The recently added 'human security' dimension related to cyber-surveillance in particular is a step in the right direction,[313] calling for the adoption of general technical and ethical standards by suppliers in sensitive tech sectors. This change should be implemented through transatlantic agreement to leverage the full potential of US-EU network nodes and ties. Finally, funding of independent security-assessment centres should be prioritised in collaboration with technology companies to ensure the confidential assessment and review of proprietary technologies, software and hardware designs.

Investment in strategic assets requires the building and expansion of technical knowledge capacity at the EU level. This should be executed by means of increased funding for research in critical technologies, and exchange and collaboration between research institutions and industrial leaders in and beyond Europe while respecting EU standards for ethical scientific conduct. This further requires strategic EU-level funding for trans-disciplinary research and education to bridge the exponentially important knowledge gap between political and technological dynamics. Fundamental to this initiative is synergizing insights from cyber-security research, industry innovations and intelligence on vulnerabilities and future threat environments.[314] Most critically, EU knowledge capacity should be applied in order to ensure the development of safe, secure and open standards. The resulting economic diversification combined

313 European Commission, Commission welcomes agreement on the modernisation of EU export controls, European Commission (9 Nov. 2020), https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2045, accessed 1 Mar. 2021.

314 Such an effort could find inspiration from the UK initiative CyberInvest; National Cyber Security Center, 'CyberInvest', National Cyber Security Center, https://www.ncsc.gov.uk/information/cyber-invest, accessed 1 Mar. 2021.

with funding for standardisation bodies will enable the EU to reduce the foreign-supplier risk and to act as a global influencer on key digital technologies.