STRATEGIC AUTONOMY TECH ALLIANCES

POLITICAL-INDUSTRIAL COLLABORATION IN STRATEGIC TECHNOLOGIES

SUMMARY

The EU has embarked on the road to more strategic autonomy, notably in digital technologies. A significant number of digital technologies are essential for our economy, society and democracy. It is not feasible, nor is it desirable, for the EU to become self-sufficient in each of these. The name of the game is therefore to work in partnerships or alliances, either with likeminded countries or globally.

But to do that, Europe needs to bring together political support and industrial ecosystems in key technology areas and to build strategic autonomy tech alliances. This will allow the EU to build and sustain the necessary capabilities, capacities and control in technology areas that are considered key for the EU's economic and democratic future, that is, for sovereignty in the EU.

This policy brief reviews the landscape and concludes that strategic autonomy tech alliances can only be said to be in place for semiconductors and cloud. Although even in these areas, there are strategic choices to be made. In addition, several strategic autonomy tech alliances should be and could be launched, notably in the areas of cybersecurity, quantum tech, secure 5G/6G, and supercomputing. Finally, there are areas, like artificial intelligence and the Internet of Things, where these should be launched but first more careful political, industrial and technological reflections must be undertaken.

AUTHOR

PROF. DR PAUL TIMMERS
Research Associate,
University of Oxford

IN PARTNERSHIP WITH

FRIEDRICH EBERT STIFTUNG

Fondation Jean Jaurès

STRATEGIC AUTONOMY SERIES
pathways to progressive action

TABLE OF CONTENTS

1. Introduction

Pervasive and disruptive digital developments, rising geopolitical tensions and global challenges including cyber-threats force the EU to address strategic autonomy across economy, society and democracy. In this, digital technologies are special as they have become foundational for our economy, society and democracy. Strategic autonomy is about control of those capabilities and capacities (**C3**) that are necessary to safeguard sovereignty. Strategic autonomy is therefore a means to an end, namely to sovereignty.

The strategic autonomy label used to be associated with defence and military but in recent years has been affixed to many topics, such as, for example, finance, health, materials, energy, digital and technology in general (Timmers 2019). In this policy brief we focus on digital technologies.[1] The C3 of essential capabilities (knowledge, skills), the necessary capacity (amount of resources) and the required degree of control concerns, from an industrial perspective: R&D; standards; digital infrastructures; design tools; applications/use; case knowledge; investment; and production capacity.

However, strategic autonomy also requires policymaking and institutional capability and capacity. In this respect legislation can be a strategic autonomy capability and capacity (for example, EU law is a resource that can be used internationally, in other words the 'Brussels effect' [Bradford 2020]); at the same time, there are limits to what unilateral law-making can achieve in these areas (see Renda 2022). In the quest for increased strategic autonomy, there is a recent and growing political interest in the EU in industrial collaboration on strategic technologies, notably in the digital domain. That is, the interest is growing for **strategic autonomy technology alliances** (SATAs). These address a critical technology, involve an industry ecosystem and government, and have a political motivation in strategic autonomy.

This policy brief explains that for a collaboration to be a strategic autonomy technology alliance, it will need adequate political, industrial[2] and technology anchoring. The policy brief addresses actual and potential alliances that can provide control over strategic digital technologies and their production system, and thereby contribute to EU strategic autonomy. The brief concludes with policy recommendations.

2. Routes to strategic autonomy

Let us first consider the full spectrum of approaches to realise strategic autonomy through public policy. One approach would be self-sufficiency or autarky. For the EU this is generally neither feasible nor desirable.[3] Rather, a common approach is to rely on **risk management**, that is, ensuring resilience to

threats according to the 'state of the art'. Risk management requires having capabilities and capacities for resilience such as intelligence, analysis, response, recovery, insurance, sharing and crisis exercises. Past EU policy for critical infrastructures such as electricity, water, transport, hospitals and telecommunications

---

1   Somewhat confusingly, strategic autonomy in digital technologies is also called 'digital sovereignty'.
2   The term 'industrial' here means the whole value chain, from research to production to market.
3   Except in a very limited number of cases (eg, hardware security modules as discussed below).

has mostly been based on a risk-management approach. However, while resilience is necessary it is not sufficient for sovereignty. Worse, the past risk-management approach has not always delivered the desired sovereignty. An illustration is that past risk management for mobile telecommunications led to strong dependency on Chinese 5G suppliers, which in turn raised fears for national security, that is, for sovereignty.

A more explicit approach to pursuing strategic autonomy involves **strategic partnerships** of likeminded partners. These partners share provision and control of capabilities and capacities in key areas. Importantly, such partnerships can still be complemented by strategic interdependency arrangements with non-likeminded parties, on issues for which both sides would lose more than they would win by foregoing co-operation. Consider for example the dependency of the US and EU on China for rare earth metals in semiconductors at the same time as China's dependency on the US and EU for the design of chips and for the equipment to manufacture them.[4] Ideally such interdependency creates a strategic equilibrium and is reasonably stable so that it does not escalate into trade war or worse.[5] Where strategic interdependency cannot be achieved or maintained, diversification of suppliers may sometimes be an alternative.

Finally, strategic autonomy can in specific instances also be realised by wide international collaboration on **global common goods**. That is, by promoting globally shared

interests rather than state-centricity through globally shared assets, distributed control, open access arrangements, precautionary norms and international agreements. A well-known example is the so-called public core of the Internet (Broeders 2017), which includes the joint management and protection of the Internet Domain Name System by ICANN (Internet Corporation for Assigned Names and Numbers) and of Internet protocols by the IETF (Internet Engineering Task Force).[6]

It seems natural that the strategic partnership approach results in creating strategic autonomy tech alliances. But it is important to keep an open mind about the fact that SATAs can also result from a risk-management approach, or, more likely, from global collaboration on common goods. Some potential examples of the latter will be discussed below.

Strategic autonomy does not come for free. Substantial budgets have already been earmarked for Europe to take part in the global race on semiconductors, quantum technologies and high-performance computing. Are these budgets adequate? Is strategic autonomy pursued in the most cost-effective way? It is hard at this stage to answer these questions. Nevertheless, as stated, self-sufficiency is generally not even financially an option for the EU. Let's illustrate that with the case of semiconductors. Table 1 compares cost savings between the extremes of global open markets and self-sufficiency (BCG and Semiconductor Industry Association 2021). Global open markets would reduce investment

---

4   The Trans-Atlantic Trade and Technology Council's Inaugural Statement (Pittsburgh, September 2021) states that the EU and US '[…] have some important respective strengths as well as ongoing significant mutual dependencies, and common external dependencies.' See 'EU-US Trade and Technology Council Inaugural Joint Statement', Text, European Commission - European Commission, accessed 21 March 2022, https://ec.europa.eu/commission/presscorner/detail/en/statement_21_4951.

5   The Russian aggression against Ukraine has destabilised strategic interdependencies between Russia and the EU/US in energy, finance and materials.

6   Resp. Internet Corporation for Assigned Names and Numbers and Internet Engineering Task Force.

costs, bring cost efficiencies and result in lower semiconductor prices, to the tune of trillions of dollars. This does not even factor in the benefits of bringing innovation to the market faster. Other studies suggest an investment gap of €65-125 billion annually, if Europe were to catch up in all digital areas with the US and China (Codagnone et al 2021).

Benefits of using global open markets	Cost savings compared to fully local 'self-sufficient' supply chains
Avoidance of upfront investment	0.9-1.2 trillion USD
Increase in annual cost efficiencies	45-125 billion USD
Resulting reduction in semiconductor prices	35-65 percent

Table 1: Semiconductor cost savings,
global open market vs 'self-sufficient' supply chains.
Source: see text.

However, Europe has not pursued self-sufficiency but rather an open market and risk-management approach. As argued, this did not sufficiently safeguard sovereignty. The middle ground, namely tech alliances of likeminded or global collaborations, has only been explored to a limited extent. For instance, as suggested by the transatlantic Trade and Technology Council (TTC), an alliance between likeminded parties may increase innovation and rein in the temptation for subsidies to home-grown incumbents and 'national champions'.

Above all, however, there are the important and even essential non-financial benefits to strategic autonomy and sovereignty. The value of sovereignty cannot be expressed in financial terms only: what is the value of autonomy and self-determination? We certainly look at these questions differently than in the past, from the perspective of the Russian aggression against Ukraine and the millions of deaths from COVID-19.

Therefore, sharing or reducing the burden through collaboration in partnerships or alliances is the name of the game. The most important route to strategic autonomy that is considered here is alliances of likeminded parties. 'Likemindedness' is not strictly defined but broadly speaking is when countries share, to an acceptable degree, a common outlook on individual rights, economic governance and democracy. As mentioned above, these can be complemented by strategic interdependency with non-likeminded parties.

3. Characteristics of strategic autonomy tech alliances

A huge range of partnerships or alliances are called 'strategic'. They vary from solemn government-to-government declarations to large-scale industrial R&D projects and global multistakeholder organisations. But where lies the motivation to call such alliances strategic? What are intent, objectives, participants and organisation?

Let us first consider this from the perspective of *international relations* (IR). Even though IR scholarship on strategic alliances is rich, it is also inconclusive when it comes to providing us with an explanation for why and how such alliances emerge, and how effective they are (Tyushka and Czechowska 2019). However, it is clear, and perhaps trivial to point out, that international strategic alliances must have strategic intent, have a long-term perspective and always have a national security dimension. That is, sovereignty always plays a role, explicitly or implicitly, and often with room for ambiguity (Holslag 2011). The emphasis in IR tends to be on government-to-government alliances.

Another perspective can be found in national competitiveness literature, where the focus is on the industrial ecosystems in a specific domain (for example semiconductors) that contribute to long-term *national competitiveness*.[7] These ecosystems not only involve the industries that are directly in the domain but also government in its role as regulator *and* buyer, input factors such as skills and capital, related industries, and buyers or markets. Authoritative in this field is Michael Porter's Diamond Model (Porter 1990).[8]

National competitiveness is a contributor to strategic autonomy, but the pursuit of sovereignty/strategic autonomy is rarely invoked in such analyses.[9] The literature is rich in addressing public-policy interventions that impact competitiveness (Lane 2020). These can be market-creating, market-facilitating, market-modifying, market-proscribing and market-substituting (Aggarwal and Reddie 2018). From the perspective of national competitiveness theory, strategic alliances are collaborations within such industrial ecosystems. They can be industry alliances or private-public collaborations.

Finally, business alliances have also been studied extensively from the perspectives of *business strategy and industrial economics*. Research shows that companies engage in business alliances to reduce transaction costs, or gain access to resources, markets or innovation. These commercial motivations will play a role also when companies take part in a strategic autonomy-driven alliance. Table 2 shows the link between sovereignty-thinking and these three perspectives on alliances.

The main insight we can gain from the literature is on the key characteristics of strategic autonomy tech alliances. The literature does not provide ample evidence that SATAs actually deliver the aimed-for C3 (capabilities, capacities, control) of strategic autonomy. This is understandable as the debate on strategic autonomy in the wide sense (that is, beyond defence and military) is fairly recent.

---

7   Eg, such as measured by the World Economic Forum Competitiveness Index.
8   Porter's Diamond Model is extensively used, such as by the OECD to analyse the national competitiveness of Finland and Mexico.
9   Unless the defence industry is a component in the ecosystem and even then, with the warning that a focus on national defensc can become a barrier to success in global markets.

The main characteristic of strategic autonomy tech alliances is that they are anchored in three types of driver: technological; industrial; and political (see Figure 1).

- **Technological anchoring** is present by definition, because the focus is on critical/essential technologies for strategic autonomy.

- **Industrial anchoring** is needed because only the industrial ecosystem including its

supply-side and/or demand-side actors can provide the necessary strategic autonomy capabilities and capacities for the selected technology.

- **Political anchoring** is to be present because of the strategic autonomy or sovereignty intent which of course is political par excellence. A political anchor consists of a number of political actors (typically governments) with an expression of shared political interest and related public policy.

Perspectives on alliances	Sovereignty concern
Politics and international relations	**Yes:** national security
National competitiveness and industry ecosystem	**Somewhat**: long-term competitiveness
Business strategy and industrial economics	**No:** commercial motivations

Table 2: Three perspectives on alliances .

These three anchors can be more or less strong and change over time. Consequently, strategic autonomy tech alliances can range from strong to weak, and be in different stages of maturity, from emergent to established to declining.

A strategic autonomy tech alliance has **shared strategic intent**, based on long-term, major, common interests. However, even if parties inside the alliance have shared intent, they may still also have their own agenda. In particular, in strategic autonomy tech alliances, national interests will be at stake and national security (or EU security), whether or not explicit. National

security interests will not be identical for each party. Some ambiguity in the way shared intent is formulated can be useful as a diplomatic way to soften conflicts over values or ideologies. However, ambiguity can become destructive if it leads to mistrust about ulterior motives.[10]

Furthermore, strategic autonomy tech alliances set out to deliver practical progress in the development of and control over essential technologies. They must have a **strategic plan** which specifies time, milestones, tasks, roles and resources as a broad framework for action. Strategic planning reflects that parties need

---

10   The TTC Pittsburgh statement has several examples of this balancing act, eg '[...] effectively addressing shared concerns, while respecting the full regulatory autonomy of the European Union and the United States.'

each other, that there is mutual **dependency**, that is, a necessary complementarity. There are **incentives** to favour collaboration. The practical (tactical) level may be only loosely coupled to the strategic level as this permits flexibility in terms of allocation of tasks and responsibilities. For example, practical efforts may be distributed to national rather than transnational consortia, whereas the strategic plan continues to be a joint effort. The strategic plan is likely not of contractual nature as it may be hard to enforce dispute resolution, while practical collaboration more likely is contractual.

In summary, the primary condition for an actual or potential strategic autonomy tech alliance is its political, industrial and technological anchoring. As argued, however, more will be needed for success, such as a strategic plan with sufficient resources. Collaborations will also carry risks that need to be clearly understood.

Finally, most collaborations are highly contingent on circumstances such as geopolitics and stage of technology development. Most will have a high path-dependency. Consequently, timing is of the essence. It can very well be too early or too late to launch a strategic autonomy alliance.
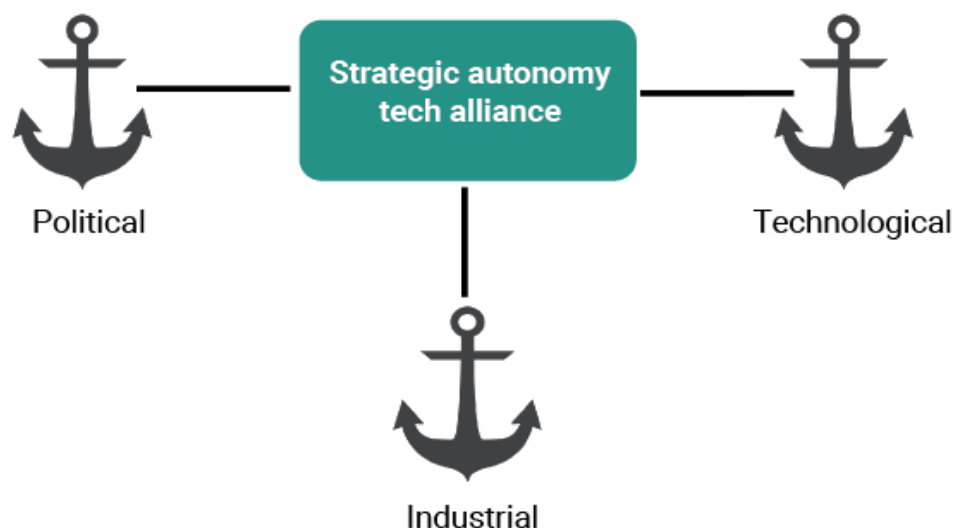

Figure 1: The three anchors of a strategic autonomy tech alliance.

Strategic autonomy tech alliances: some examples

The EU Chips Act, proposed in February 2022, creates the basis for the European Semiconductor or Chips for Europe Initiative, a strategic autonomy tech alliance. The political anchoring is the Chips Act itself and preceding declarations by the EU Council. Industrially, it has an extensive anchoring in the European Industrial Alliance on Processors and Semiconductor Technologies (which has restrictive participation), the Key Digital Technologies Joint Undertaking, itself building on the Electronic Components and Systems for European Leadership Joint Undertaking (ECSEL), an EU semiconductor R&D Joint Undertaking running since 2014, and an Important Project of Common European Interest (IPCEI). Its technological anchor is in a focus on selected types of semiconductor and advanced design and manufacturing. Terms of reference impose close collaboration between industry, academia and governments and include clear strategic planning.

A potential strategic autonomy tech alliance could emerge from EU-US collaboration on security in the ICT supply chain (this is the ICT used above all by critical services and infrastructures, for example finance, energy, transport). Given recent incidents such as SolarWinds and Kaseya,[11] supply chain security is now considered a case of strategic autonomy.

Politically, the US can anchor this in Biden's software supply chain security initiative.[12] For the EU the political anchoring could be in the NIS2 and DORA Directives,[13] although these did not take strategic autonomy or sovereignty or national security as their starting point (contrary to the Biden initiative). Industrial anchoring would be through involving software supply chain companies on both sides of the Atlantic.[14] However, both for industrial and technological anchoring a selection of priorities will be needed since the software supply chain is huge in technologies and companies. For example, the priority could be trustworthy software updating and related technologies such as blockchain.[15] Another focus could be open-source software vulnerability.[16]

---

11   SolarWinds was a hack of software used to manage IT systems; Kaseya was a hack of software used by managed service providers.
12   https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity
13   NIS2 is the revision of the EU Network and Information Security Directive; DORA is the EI Digital Operational Resilience Act (Directive) for the financial sector.
14   Both NIST (US) and ENISA (EU) have work ongoing with industry on supply-chain security.
15   Blockchain-based 'locking' of software versions already exists for industrial control systems (SCADA system), eg https://www.ft.com/content/fe6930cc-8c29-11e8-bf9e-8771d5404543
16   EC's DG DIGIT already provides limited support, with reference to 'digital autonomy', for open-source vulnerability discovery (European Commission, 2020).

Risks for strategic autonomy tech alliances

Strategic autonomy tech alliances can be vulnerable. Risks can also combine and influence each other.[17] Some of the risks to which tech alliances can be exposed are as follows:

Fair returns (juste retour): coalitions of the willing may be facilitated by enhanced co-operation[18] and IPCEIs.[19] Yet if not all EU countries are involved and EU funding needs to be mobilised, there may be a claim for fair compensation by the outsider countries.

Competition concerns: alliances may invite collusion,[20] or run into mergers and acquisitions (M&A) and market-dominance issues.[21]

Subsidy race: in the TTC both the EU and US warn against triggering a subsidy race.

Crowding out 'the market': private initiative and investment may become crowded out by public involvement and investment (to some extent this may also be an ideological concern).

Lack of focus: in a partnership there may be a tendency to gloss over differences by including a multitude of different objectives, resulting in dilution of resources and tasks that risk to under-deliver.

Short-termism: given the political anchor of tech alliances a risk is that short-termism of election cycles derails and demotes such initiatives.

Policy myopia: incomplete mobilisation and integration of policies or lack of interdepartmental co-operation (Renda et al 2021).

Normative-instrumental tensions: differences or confusions about desirable ends and whether the means fit with the ends.

---

17   Politico recorded as risks to the GAIA-X initiative a combination of confusion about ends and means, lack of focus, and short-termism.
18   TEU Art 20 and TFEU Art 326 to 334.
19   TFEU Art 107.
20   See for an example the very extensive warnings against anti-competitive behaviour in the Declaration of the Industrial Alliance for Processors and Semiconductor Technologies.
21   Such as in the Thales/Gemalto takeover in 2017. Competition authorities imposed divestment of Thales' HSM division nShield, which got ultimately acquired by US-based Entrust Datacard (see HSM section).

4. Actual and potential strategic autonomy tech alliances

There are several ways to identify actual and potential strategic autonomy alliances. We could make an inventory of all collaborations that could provide a political or industrial anchor and which have, or might be given, a specific focus on a critical technology for strategic autonomy. However, rather than starting from all potential collaborations, this policy brief will start from the critical digital technologies. Here, we identify existing (or the lack of) political and industrial collaborations and to what extent they can form the basis of a strategic autonomy alliance. In addition, the brief will restrict the analysis to the two most important international collaborations, namely between the EU and US, or between EU member states (or a subset of them).

To identify critical technologies, we can use a stack diagram (Figure 3). For each layer in the stack the question is: what are the technologies that are critical for sovereignty? That is, for which technologies should Europe seek adequate control, capabilities and capacities to safeguard sovereignty? Figure 3 is a technology-centric diagram and does not seek to be complete.
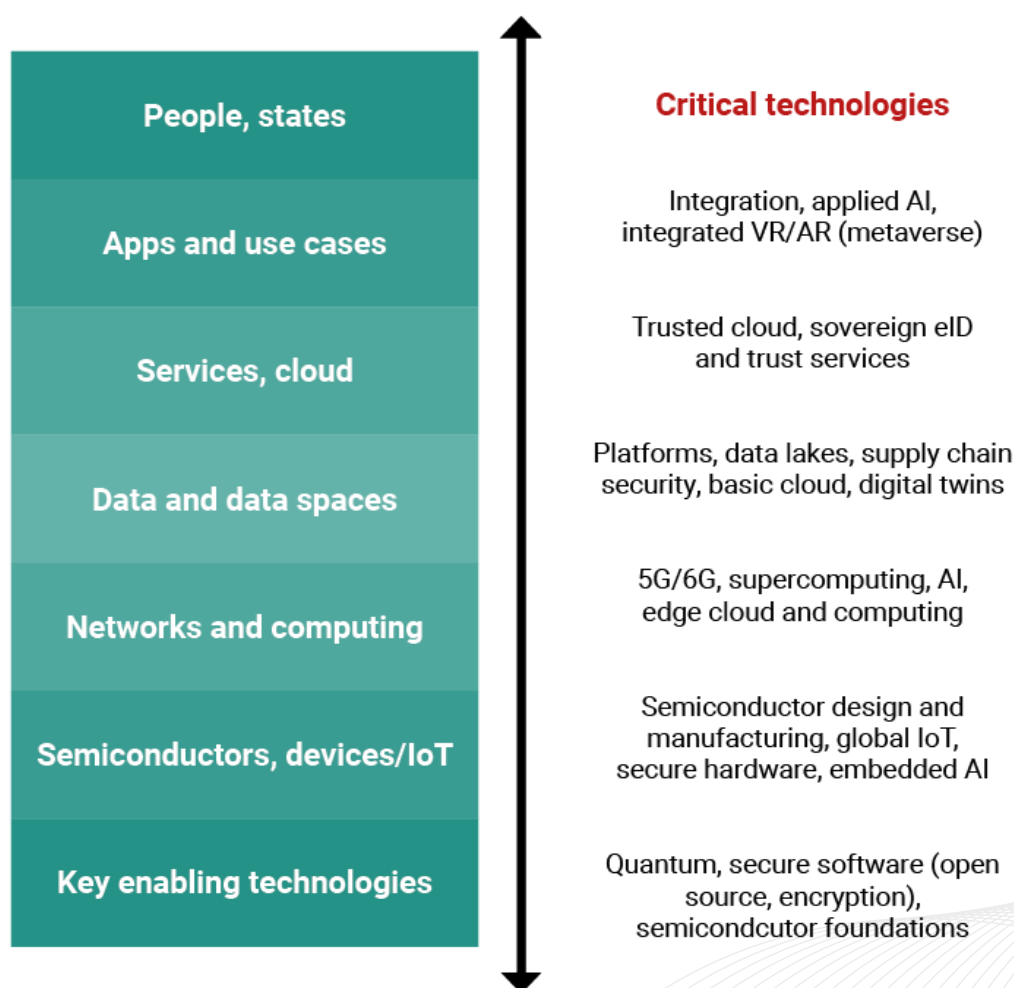

Figure 3: Stack of critical technologies.
Source: author.

Nevertheless, it can bridge to the national maps of critical and emerging technologies that all major states are developing. The US has such a map and added their strategic autonomy approaches.[22] China has a Made in China 2025 plan.[23] Here we then select the most important strategic autonomy technologies, largely common to the national critical technology plans of the US, China, the UK and Germany, and frequently mentioned in EU policy. Further digital technologies could be analysed for the opportunity and need for a strategic autonomy tech alliance, such as robotics, photonics, electronic ID (eID) and other trust services, or social media and metaverse.

4.1 Quantum technologies

Quantum technologies represent a new fundamental technology paradigm, based on quantum entanglement. In principle this enables many simultaneous calculations, going far beyond the capabilities of traditional technology. Quantum technologies form a wide field, including quantum computing, simulation, sensing, communications, algorithms and cryptography. Opinions are widely different as to when quantum computers will become at scale to the market, but it is not imminent. Currently there is rush of risk capital investment in this field. The significant interest from US investors for European quantum start-ups is a potential threat for EU strategic autonomy in the long term.

At EU level, a quantum R&D strategy is in place and supported by funding from the EU's Horizon programme.[24] The EU Quantum Flagship is an R&D collaboration involving research institutions, academia, industry, enterprises and policymakers. It addresses in principle the full range of quantum technologies through research. It provides a strong technological reference, that is, technological anchoring is evolving in a solid way. It does not build up a quantum industrial ecosystem in the EU, let alone provide quantum supply chains.

For a quantum communications infrastructure (QCI), EuroQCI, a collaboration of the 27 EU member states, is a political alliance that is being operationalised through projects that address research, deployment and operations. With this political anchoring, its clear technological anchoring, and existing industrial and governmental collaboration, EuroQCI gets close to being a true strategic autonomy tech alliance in QCI. However, with its focus on providing a key infrastructure, it is still missing other industrial policy elements (such as risk capital investment and a possible golden share participation of governments in key companies) that would build up and would keep the full industrial ecosystem under the level of democratic control that is necessary for strategic autonomy.

Post-quantum cryptography is another important development. With the arrival of quantum computing, the encryption of today can be broken. Even if we may not have quantum computers for another 10 years, today's encrypted information is stored and could become decrypted in 10 years' time. This would be a huge risk for sovereignty. The solution is to develop post-quantum crypto (PQC) algorithms and make it possible to replace today's encryption with PQC, which allows encryption to be hardened with PQC as soon as it becomes

22   White House, 'National Strategy for Critical and Emerging Technologies', October 2020.
23   China State Council, 'Made in China 2025', 2015, http://english.www.gov.cn/2016special/madeinchina2025/.
24   For an amount of €1 billion . Though a significant amount, the gap in funding to geo-competitors is considerable, however, for instance China may be spending 5-10 times this amount.

available. While PQC can be largely an open standard/open-source development, Europe needs to retain a say in this – to be convinced that national security is indeed protected – and sustain its excellent academic crypto expertise in order to develop its own EU PQC industry. PQC is in a 'sweet spot'[25] with cyber-, quantum- and public-sector markets. That is, in PQC strong drivers come together: the public interest and government as a market can join up with cyber-industry interest and with a strategic, emerging technological domain where Europe can still play a role.

The USA and China are moving fast in PQC. It is therefore time to prepare a fully fledged **strategic autonomy tech alliance on post-quantum cryptography of the EU and likeminded partners**. The global open-source standards development will facilitate wider participation by likeminded countries.

At national level, policies and plans have been developed that go beyond R&D and are thereby moving closer to industrial ecosystem policy (even if parts are still missing, such as risk capital). For a well-developed example, see the Netherlands' plan (Quantum Delta Nederland, 2019). France and the Netherlands recently agreed to quantum tech collaboration (explicitly formulated as contribution to strategic autonomy) as did the US and the UK. Still, overall the focus is on science and technology research rather than on the full industrial ecosystem.

In summary, quantum is a wide field. For some aspects (QCI, PQC) the time is ripe to launch a full-scale quantum strategic autonomy tech alliance as political, industrial and technological anchors are starting to be put into place, even if important elements still need to be addressed (such as public procurement, risk capital and

key shareholding). While more fundamental research is suited to transatlantic and global co-operation, in quantum communications an alliance would preferably be EU-only, given its highly strategic nature. Political anchoring could be stronger by articulating a shared strategic intent of 'quantum for strategic autonomy in Europe'. It is reasonable to expect that strategic planning can be secured on the basis of the existing EU collaboration of governments, industry and academia.

4.2 Semiconductors/chips

Semiconductors, or chips, are the little engines that power all of the digital world. The semiconductor world talks of nodes, which are the smallest components inside the chips that can be manufactured. Ever smaller nodes in the same volume means ever more computing power. In the coming years node sizes as low as 2nm (nanometres) are coming on-stream.

Semiconductors have complex value chains, from research to design, materials to fabrication plants (fabs) and packaging to customers (Kleinhans 2021). Europe's control in several of these areas is weak (BCG and Semiconductor Industry Association 2021). In particular, Europe has fallen behind in fabs (wafer-manufacturing plants) and in chips design (Baisakova and Kleinhans 2020) (see Figure 4).

The EU and the US worry about their lack of strategic autonomy in semiconductors. The US has adopted a CHIPS Act funded with $52 billion and is considering a FABS Act with tax credit support. The European Chips Act of February 2022 is a strategy to reduce EU dependencies, increase market share and build a sustainable technological and industrial base in selected

---

25   A 'sweet spot' means that public interest, markets, industrial and technological capability can be joined up.

types of semiconductor. It comes with an investment plan to the tune of €43 billion, an industrial-technological collaboration plan, and a regulatory toolbox to address semiconductor supply-shortage risks.

The collaboration (involving government, industry and research labs) includes a Chips Joint Undertaking, established by law, and links to the European Industrial Alliance on Processors and Semiconductor Technologies (IA-PST) as well as an existing and a forthcoming IPCEI on micro-electronics.

The collaboration of industry and governments is to address the reinforcement of the European electronics design ecosystem and establishment of the necessary manufacturing capacity, from 16nm to 10nm node size and from 5nm to 2nm and below. Members can be organisations in processor and semiconductor technologies, including end-user companies, associations and research and technology organisations. As they start to join, the industrial ecosystem anchor will become ever firmer.
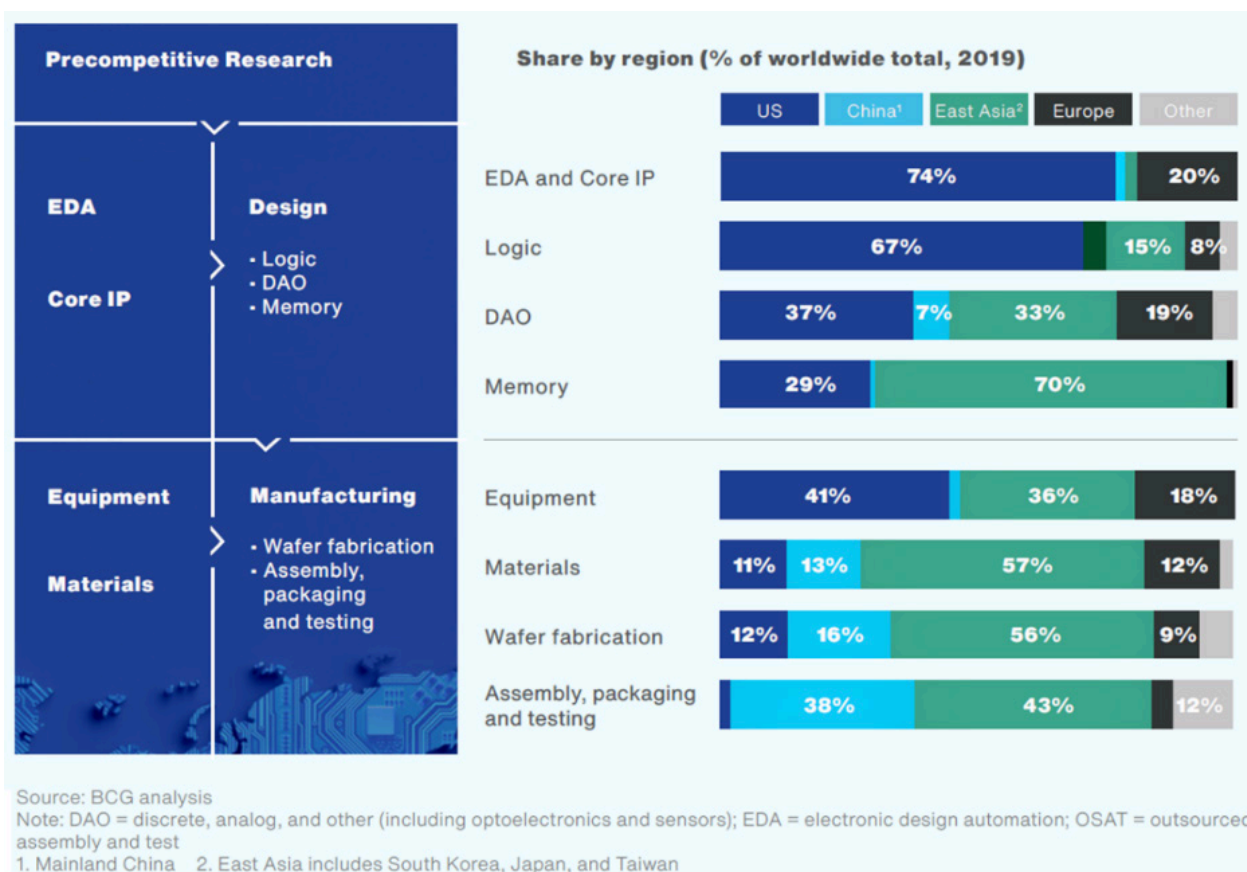
Figure 4: Share by region of semiconductor supply chain.[26]

26   BCG and Semiconductor Industry Association, 'Strengthening the global semiconductor supply chain in an uncertain era', 2021.

Strategic intent is explicit in the Chips Act: 'Given the central role that chips play in the digital economy, their geopolitical dimension […] the Union has to urgently reinforce its semiconductor ecosystem, increasing […] security of supply and reducing its external dependencies.' Strategic planning is explicit in the Chips Act, with a broad outline of activities, from the short term to the long term, and formulated in terms of building specific capabilities in design and fabs, mobilising investments and joining up actors.

In conclusion, the Chips Act fits the bill for an **EU strategic autonomy tech alliance** on semiconductors, even though it is not yet fully up and running. For further development of EU strategic autonomy in semiconductors, the EU has to consider:

1. **The focus in terms of node size**: strategic autonomy in sub-2nm is considered a necessary but long-term target. Leading edge today is 5-10nm. Mature are semiconductors with a node size of 10nm or larger. They are today essential for telecoms edge computing, specialised chips in hardware security modules and automotive.[27] Analysts consider the EC's target of doubling the market share to 20 percent a very ambitious (Codagnone et al 2021) but necessary target though only achievable with strong government support and global partnering (Kearney 2021).

2. **Reinforcement**: by seeking synergies with other strategic autonomy tech developments, coupled with strong private-sector demand and public procurement. There is an interesting opportunity in linking the edge and cloud initiative (see below) with 5G/6G demand, as suggested in the diagram.
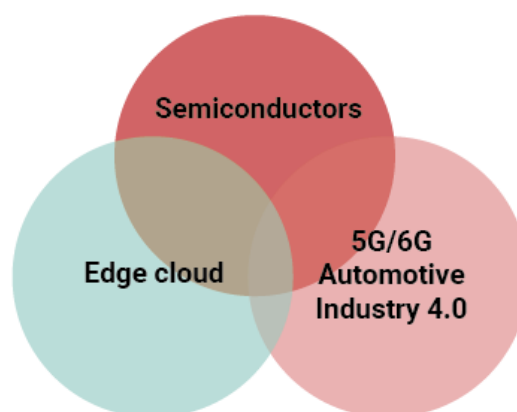
Synergies: chips and cloud

3. **EU-US co-operation**: the TTC provides a strong link for a transatlantic approach.[28] Nevertheless, it also reveals sources of potential conflict. This is captured by TTC language such as 'this partnership should be balanced and of equal interest for both sides' and 'we share the aim of avoiding a subsidy race and the risk of crowding out private investments that would themselves contribute to our security and resilience'. Interestingly, the terms of membership of the IA-PST seem more restrictive than that

---

27 Intel's Core i7 uses 10-14 nm node sizes and currently considered to deliver adequate performance for edge computing, whereas FPGAs for the high-end market are a growth market with the rise of edge computing. 10 nm chips for 5G and AI and are now appearing; for HSMs node size are also above 10nm, eg for FPGAs for automotive, HSMs are based on TSMC's 16nm process. In future this may change, and there are several criteria that determine the application area: computing power, weight, power consumption.

28 The 2021 TTC Pittsburgh launch statement said: 'The European Union and the United States reaffirm our commitment to building a partnership on the rebalancing of global supply chains in semiconductors with a view to enhancing respective security of supply as well as their respective capacity to design and produce semiconductors, especially, but not limited to, those with leading-edge capabilities. This partnership should be balanced and of equal interest for both sides. We underline the importance of working together to identify gaps in the semiconductor value chain, and strengthening our domestic semiconductor ecosystems.'

of the Chips Act itself (restrictions are clearly related to security and strategic autonomy such as evidence of no control by a third country and security clearance of personnel). Nevertheless, the recent and welcomed investment by Intel in semiconductors in the EU, including a fab in Magdeburg, makes clear that EU-US co-operation is seen as essential in this strategic autonomy tech alliance

4. **Budget**: the Chips Act is rather opaque about the budget calculation, where a relatively limited amount of EU funding (of which part is re-allocated existing budget) should leverage much more industry and member state funding. Analysts have raised concerns about the budget but an encouraging sign of leveraging should be the €17 billion Intel investment. Even if the leveraging materialises there may still be a significant funding gap relative to budgets foreseen in Taiwan, South Korea and China (ASML 2022).

5. **Dependency on non-likeminded countries**: this will persist given the complex and geographically dispersed value chains. A strategy is still missing to move towards more stable strategic interdependency, a likely EU interest. On the contrary, the US push for decoupling from China, increasing tensions between China and Taiwan, the main location of the advanced fabs, and Chinese self-sufficiency goals only escalate the semiconductor race (European Chamber of Commerce in China 2021).

4.3 Mobile telecommunications, 5G/6G, Open-RAN

In mobile telecommunications the attention is focused on 5G, 6G and Open-RAN. The latter is about the opening up of the radio-equipment part of the mobile networks. This can bring more competitors to the equipment leaders Huawei (China), Ericsson (EU), Nokia (EU) and Samsung (South Korea).

Network management is increasingly in the cloud, with cloud services that can be bought from the big cloud providers. These in turn could become competitors to both telecoms operators and equipment suppliers. Together with their growing assets in long-distance cables, private networks and off-net servers (Stocker, Knieps and Dietzel 2021), and duplication of the DNS system (Voelsen 2019), they control ever more of the communications and Internet infrastructure. Another important development is edge computing, bringing network and data processing close to the customer for low latency, as well as AI for network management (European Commission 2021).

Mobile telecoms standardisation largely happens in 3GPP[29] and is industry-driven. Over the years two concerns have arisen: about 5G security which could not readily be technically isolated; and about opaque influence of the Chinese state through participation of state-influenced industry in standardisation work in 3GPP. Chinese presence in telecoms standardisation has rapidly risen, though traditional incumbent stakeholder categories and Western nationals still occupy an outsized proportion of leadership positions (Baron and Whitaker 2021). Some analysts advise to financially support US companies in telecoms

---

29   3GPP is a partnership of standardisation organisations and business organisations in mobile communications. 3GPP produces technical specifications that become global standards. Much of the work in 3GPP is done by telecommunications companies (through the partners).

standardisation but warn against increasing geopolitical pressure on 3GPP.

It could be argued that the issue of 5G security came up as an afterthought precisely because governments did not stay close enough to standards development. Corrective action ranges from excluding certain companies as suppliers (notably in the US) to certification of security (the EU's 5G Security Toolbox). 5G security concerns spill over into 6G and may lead to a fragmented future telecoms standards landscape (Timmers 2020). In 6G much R&D is co-funded by the EU. The US is keen on getting control over 5G and 6G (Beattie 2021).

In conclusion, there is a substantial – but not complete – **basis for a strategic autonomy tech alliance** in secure 5G/6G with wide participation. The EU has already set out to strengthen its presence in industry-led standardisation (European Commission 2022). A more coherent political-strategic view needs to be developed to engage with likeminded partners, notably the US and Japan on Open-RAN but also with Korea on equipment, on India and possibly also African partners on markets and infrastructure. An EU-US-only partnership could fall victim to commercial capture disguised as national security (Lee-Makiyama and Forsthuber 2020). The ambition level should be to achieve clearer technical security than has been realised in the past and wide international market presence. This should leave space for collaboration between European and Chinese companies on other aspects of 5G/6G than security. Ideally, parts of 5G/6G are raised to a global multi-stakeholder platform, such as a transparent 3GPP with balanced government-industry presence. Some lessons can be learned from SWIFT (see the information box) as well as from collaboration on parts of the Internet such as the DNS in ICANN and Internet protocols in IETF.

4.4 Supercomputing

Europe recognised in 2016 that it was falling behind in supercomputing. There were no European supercomputers in the top league, while China and the US and to some extent Japan were forging ahead. The fear was that with lack of supercomputing capacity on European soil, data and researchers would also move abroad.

The EuroHPC, an R&D joint collaboration of

member states, the European Commission, industry and research institutes, was then launched in 2018 to advance supercomputing capability in Europe. Private partners in EuroHPC are represented through two associations, resp. on technology for high-performance computing and on big data. These associations include next to European also American and Chinese companies.

Supercomputing is undoubtedly a strategic autonomy technology, but the actions taken in this area in Europe preceded the debate on strategic autonomy. Probably this is the reason why membership criteria are not as strict as those of the more recent alliances on semiconductors or edge cloud.

Collaboration in Europe on supercomputing may therefore be confronted at some stage to spin off a more restricted (EU-centric or likeminded) tech alliance. Notably, this may be the case once Europe develops stronger own industrial capability and manufacturing capacity in supercomputing and becomes less dependent on procurement from foreign suppliers.

In short, it would be a stretch to argue that all of political, industrial and technological anchoring is in place for a supercomputing strategic autonomy tech alliance and that EuroHPC fits the bill. The political prioritisation of strategic autonomy/sovereignty in this area will still have to be expressed more clearly. Consequences will have to be drawn from this in terms of partnerships. Technology anchoring will have to become more articulated. For instance, is the primary focus to have control on exascale computing or is it, rather, the intention to deploy supercomputing to support other areas of strategic importance (for example AI)? In the latter case procurement can be more open to foreign suppliers than in the first case. This changes the nature of a potential alliance.

In conclusion, strategic autonomy thinking on EU supercomputing still needs to further develop.

4.5 IoT

IoT – Internet of Things – is the collection and interconnection of devices on the Internet. This is rapidly expanding into a network of billions of more or less smart connected 'things'. IoT is becoming pervasive, supplying a wealth of data and allowing control of anything from manufacturing to road traffic to hospital operations. IoT is becoming the device-infrastructure of our economy and society, an asset that 'belongs to us', that is, a digital sovereign asset over which there should be adequate control. As for 5G, much of IoT is exclusively industry-driven. OneM2M, an industry alliance, is the main and global organisation for technical specification and standards on IoT, with important presence from India and China (next to the EU and US). India has already adopted the OneM2M standard as a national standard. The same concerns as for 5G security in 3GPP must also be raised for IoT security in OneM2M, given substantial indirect Chinese state presence. Indeed, the founder of Huawei predicted that IoT would become the next battleground after 5G security.

EU policies and programmes provide substantial support to IoT. This includes €0.5 billion in EU R&D, pre-standardisation supported by the European Union Agency for Cybersecurity (ENISA) (which may lead to certification schemes in the EU's Cyber Act) and the recent Delegated Act on security of consumer wireless devices.

The Alliance for IoT Innovation (AIOTI) was set up in 2015 – in pre-strategic-autonomy times. It could be a launchpad for a strategic autonomy alliance, but is rather indiscriminate

in its membership. As in other cases we have seen before, it cannot be expected to become a strategic autonomy tech alliance itself. Other industrial anchoring could come from the [Stakeholder Cybersecurity Certification Group](#) of the EU's CyberAct and the recently launched European Industrial Alliance on Industrial Data, Edge and Cloud. Both have potential for transatlantic and other likeminded co-operation.

Work on IoT has the potential to gain strong industrial and technological anchoring but IoT is politically under-estimated. An IoT strategic autonomy tech alliance of the EU with likeminded partners is necessary but requires stronger political recognition of IoT's importance for strategic autonomy.

4.6 Cybersecurity, secure hardware and software, confidential computing

Technologies related to digital security span a very wide area, too wide for an effective tech alliance. The EU already has a good basis in terms of policies, industry collaboration, market awareness and sizeable demand. For a strategic autonomy tech alliance, the case of cybersecurity in the ICT supply chain has already been mentioned. However, there are important areas within cybersecurity where EU control has been eroding, such as in secure hardware or where the EU has insufficient strategic control such as in confidential computing.

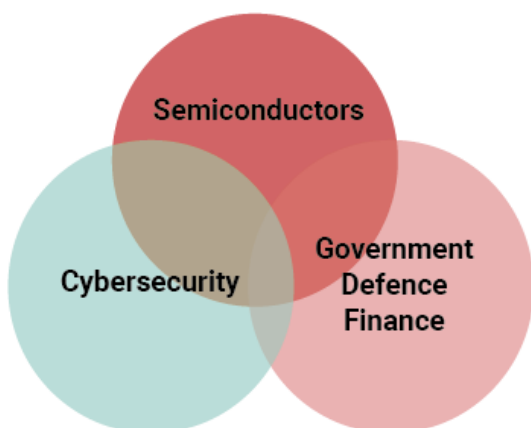### HSM – hardware security modules

Hardware security modules (HSM) are dedicated systems that physically and logically secure cryptographic keys and cryptographic processing (Thales 2020). Control of the HSM is necessary to keep a minimum of control on sensitive data, notably in the cloud. Not having control over the HSM risks exposing the core of government information and sensitive intellectual property. This therefore concerns par excellence a sovereignty challenge.[30]

The technical and market lead of European companies in the field of encryption by hardware security modules has been eroding, even if Europe has knowledge expertise in cryptography (Timmers and Dezeure 2021). In order for the EU to regain control of HSMs, alongside its existing R&D policy on cryptography it will need to consider carefully the actors involved, with a view to foreign direct investment. An HSM strategic autonomy tech alliance would be the way forward. Although there is no industry coalition for an HSM tech alliance yet, the semiconductor alliance and European industry co-operation in cyber ([ECSO](#)) may provide a launchpad. A strategic plan must describe the minimum viable market in order to assess whether public financing is necessary or whether this can become a self-standing commercial activity, as well as potential competition concerns.

HSM is at a sweet spot of intersection of interests that make an EU strategic autonomy tech alliance feasible. There could be a fruitful interplay of the political and industrial anchors of cybersecurity and semiconductors, and a strong demand, namely sovereign demand from governments and defence as well as global demand from, for example, the financial sector.

---

30   The USA's NSA advised, following the SolarWinds cyber-infiltration, to 'Strongly consider deploying a FIPS validated Hardware Security Module (HSM) to store on-premises token signing certificate private keys'.

Synergies: hardware security modules

Confidential computing

New methods of data analysis – while keeping these confidential – are developed. For example, multi-party computation and distributed homomorphic encryption, which allows the processing of data without first decrypting it. These important technologies can decouple location from data handling – in fact, may transform the data localisation challenge from a security sovereignty into an economic sovereignty issue.[31]

European researchers are active in these fields but the industrial activity is driven among others by the Confidential Computing Consortium (CCC) and moreover this consists of virtually only American and Chinese members. Confidential computing is clearly a critical technology from a strategic autonomy point of view: this is how governments and industry will process and compute sensitive information in the future. Even if the results are open source, producing them is part of an essential industrial ecosystem for strategic autonomy from which the EU cannot be excluded. In summary: while this is a strategic autonomy technology, the EU should address its weakness in the political and industrial anchoring of confidential computing.

4.7 Cloud

Cloud has become *the* infrastructure of economy, society and even democracy. No wonder that control of cloud has moved centre stage, expressed in notions such as 'sovereign cloud' or at least data sovereignty. But which kind of cloud are we talking about? Beyond basic cloud we see a rich development of functionality and architecture. In functionality what gets added are encryption, trust and assurance services and (AI-)data analytics. Distributed cloud, multi-cloud and edge cloud are new architectures that move away from the old single-provider and centralised model.

Most elements are present for a solid EU strategic autonomy tech alliance in trusted cloud. The GAIA-X cloud initiative has paved the way. Even if sometimes presented as 'taking back control' of basic cloud, its strategic orientation and its pilot projects are rather moving towards greater control of emerging added-value functionality and cloud architectures (Timmers 2021).

The European Alliance for Industrial Data, Edge and Cloud (IA-IDEC), launched in July 2021, brings an industrial ecosystem together, has membership criteria equally as strict as for the semiconductor alliance and is explicitly co-ordinating with GAIA-X. However, its strategic plan is not yet as clear in terms of expected targets and resources as the Chips Act is for semiconductors. Political, industrial and technological anchoring are all ensured with IA-IDEC, GAIA-X and the EU Cloud Strategy.
The open question is about the extent of international partnering in these initiatives. While basic cloud is US-dominated, a more balanced EU-US partnership can be envisaged in trusted cloud, edge cloud and industrial data. The IA-IDEC Alliance is clearly EU-centric

---

31   When security is no longer the main concern, having data 'close to you' may still be important to build a full data ecosystem, creating jobs, unlocking value etc.

but may consider evolving in the transatlantic relationship (for example, linked to TTC). GAIA-X, however, has also Chinese participation and questions have been raised about how credible GAIA-X is for EU strategic autonomy. A loose coupling between the Alliance and GAIA-X or compartmentalisation within GAIA-X (that is, creating an EU-core within GAIA-X) may be the way forward. Even more, GAIA-X may be a route to the globalisation of some of the EU's trusted cloud work, in other words show leadership for a global common-good approach to trusted cloud.

4.8 AI

Artificial Intelligence is another wide-sweeping label. Both the US and China aim for AI leadership, considering it indispensable for future competitiveness and national security (see for example the US National Security Commission on AI). Likely AI is indeed a foundational technology. This means that a broad presence in AI is essential for future sovereignty, even if not all of AI is of strategic autonomy importance. Such a political perspective is to some degree present in the EU's AI strategy but the EU's AI Act is based on risk management and not on strategic autonomy considerations. A European AI Alliance was set up in 2018 but it does not represent an industrial ecosystem.

Due to this limited political and industrial anchoring and a lack of technology focus, it is therefore not surprising that a strategic autonomy tech alliance on AI is not yet on the cards. When compared to the EU Chips Act, even though the EU's AI strategy[32] aims for strategic leadership in seven high-impact sectors, this is not yet accompanied by the articulation of strategic autonomy goals (in

terms of the C3 for AI in each of these seven sectors). Moreover, its strategic planning (for instance in semiconductors) is not as explicit.

At international level, the Global Partnership on Artificial Intelligence (GPAI), as a multi-stakeholder initiative (led by governments) focuses on 'trustworthy' AI consistent with human rights, fundamental freedoms, and shared democratic values. Given these requirements it is unlikely to become a fully global partnership. GPAI is not close to national security and sovereignty. It is also not addressing the whole AI industrial ecosystem.
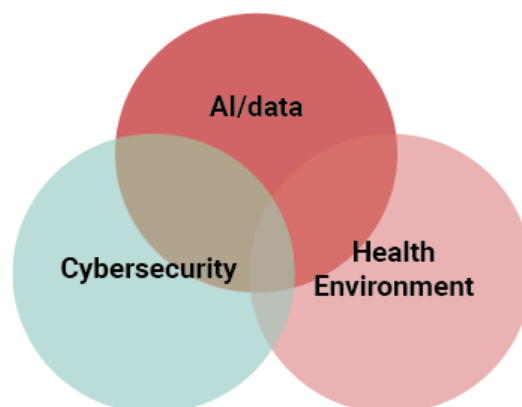
Synergies: AI for common good

It is therefore at this stage not likely that a comprehensive strategic autonomy tech alliance for AI can be launched. Nevertheless, GPAI could be a platform from which focused strategic autonomy tech alliances on AI can be spun off, for example for AI for the common good such as public health and cybersecurity, building on the GPAI work on AI and pandemic response. Here three interests can join up for which the EU could take the initiative: AI/data; cybersecurity; and public good (health, environment). Alternatively, a focused AI

---

32   European Commission, 'Build Leadership in AI. Shaping Europe's Digital Future', accessed 21 March 2022, https://digital-strategy.ec.europa.eu/en/policies/build-leadership-ai.

approach in specific sectors such as agriculture or health (both cases struggle with resilience) or in robotics may lend itself to launching a focused strategic autonomy tech alliance.

5. Conclusions and policy recommendations

It is critical for Europe's strategic autonomy to join up in key technology areas, political support and an industrial ecosystem, and to build strategic autonomy tech alliances. SATAs are the primary way in which to build and sustain the necessary capabilities, capacities and control in technology areas that are considered key for the EU's future in economy, society and democracy, that is, for sovereignty in the EU.

To launch a strategic autonomy technology alliance, it is necessary to establish strong political, industrial and technological anchoring. It is also necessary to formulate a shared strategic intent of the public and private parties involved and to agreeww on a clear strategic plan that includes mutual dependencies and to provide incentives for collaboration. The EU has embarked on the road to more strategic autonomy, notably in digital technologies. A significant number of digital technologies are essential for economy, society and democracy. It is not feasible, nor is it desirable, for the EU to become self-sufficient in each of these. The name of the game is therefore to work in partnerships or alliances, either with likeminded countries or globally. This paper analysed a number of areas where strategic autonomy tech alliances are necessary (without attempting to be complete). It also assessed the state of play, which is summarised in Table 3, below.

Currently there are only two areas where strategic autonomy tech alliances can be said to be more or less in place (semiconductors and cloud), there are several areas where strategic autonomy tech alliances should be and could be launched (cybersecurity, quantum-related,

secure 5G/6G, supercomputing), and there are areas (AI, IoT) where these should be launched but first more careful political, industrial and technological reflection must be undertaken.

A **first general recommendation** is to:

1. Pursue concrete, **focused tech alliances** that can build on political collaboration or provide political support to industry collaborations, giving much attention to government-industry balance.

For each technology area, specific recommendations on strategic autonomy technology alliances are as follows:

- **Semiconductors**: a strategic autonomy alliance is well underway thanks to the EU Chips Act. Yet, given budget constraints and the complexity of the semiconductor supply chain, the EU needs to be focused in what it aims to achieve on its own, assess what can best be achieved in partnership with the US, and develop a strategy for managing interdependencies with non-likeminded countries.

- **Trusted cloud**: a SATA is largely underway based on the Alliance for Industrial Data, Edge and Cloud and GAIA-X. However, the EU needs to make strategic choices about membership and design of GAIA-X, to reflect the extent the latter is to contribute to EU sovereignty in this domain. Finally, closer co-operation with the US can be envisaged.

- **Cybersecurity**: a SATA could be launched

for hardware security modules, and possibly also for supply chain ICT security, which could count on strong demand from government and the defence sector. In the area of confidential computing, the lack of EU presence is a concern that should be addressed.

- **Post-quantum cryptography of EU countries and likeminded partners**, for which the time is ripe to launch a strategic autonomy tech alliance, though this would require addressing issues around public procurement, risk capital and key shareholding. The same holds for an EU-only quantum communications SATA.

- **Secure 5G/6G**: before the launch of a wide-ranging SATA of EU countries and likeminded partners, it is necessary to formulate the shared intent and increase in an appropriate way the presence of EU governments in standardisation such as in 3GPP.

- **Supercomputing**: although the EuroHPC could form the basis for a SATA with likeminded partners, it was not set up for this purpose, as its open membership underlines. The EU should first decide what aspects of the technology it wants to focus on, and for which strategic objectives.

- **Artificial intelligence**: getting closer to a SATA means that the EU needs to go beyond risk-management measures and start thinking about objectives for strategic autonomy, linked to concrete technological applications and industrial ecosystems. More immediately, it could develop and take the lead on partnerships on AI for the global common good (health, environment).

- **IoT**: before a SATA can be launched with likeminded countries, there needs to be a political recognition of the importance of IoT for Europe's strategic autonomy, as well as increasing government awareness of IoT standardisation and its political relevance.

Further general recommendations are to:

2. Establish a proactive **tech alliance watch**, with **strategic policy planning** in order to systematically assess alliances for performance, strategic consistency, to fill strategic gaps and to explore opportunities.[33] Understanding the landscape of international political and business collaborations and critical technologies is a prerequisite for safeguarding sovereignty.

3. Put in place **integrated policy-by-design** for tech alliances. Mutual appreciation of policy tools across departments[34] will reinforce tech alliances or policy support for new alliances. Policymakers could have a checklist of policies that may play a mutually reinforcing role (industrial and R&D policy, standardisation, investment policy, public procurement, trade policy, international diplomacy, security policy, defence policy, etc). This would be a natural extension of current public-policy impact assessment practices.

4. Analyse, monitor and address **risks**: for emerging strategic autonomy tech alliances, short-termism, lack of focus, policy myopia and possibly protracted discussions on

---

33   See also Renda, 'Leveraging Digital Regulation for Strategic Autonomy'.
34   For instance, the rich tools of international diplomacy (dialogues, trust-building, agreements, norms, sanctions, governmental partnerships, etc) is complementary to the policy tools of digital/industrial policy (such as funding, legislation, private-public partnerships).

juste retour – that is, the idea that all member states contributing to the EU budget get a fair return – may be the most important risks. Even if a number of risks have been identified, our anticipation of risks is still limited. A constant and systematic exercise in learning lessons from collaborations is necessary. This is part of strategic monitoring for the purpose of better policymaking and not leaving important gaps (see also the information box 'Risks for strategic autonomy tech alliances', above).

Technology area	Political anchoring	Industrial anchoring	Technological anchoring	Main issues	Status (higher is more)
Semiconductors	+++	+++	+++	Budget, EU-US relation	9
Cloud	++	+++	+++	Extent of participation	8
Cybersecurity	+++	++	++	Confidential computing	7
Quantum	++	++	+++	Timing (QCI, PQC), risk capital, shareholding	7
5G/6G	++	++	++	Shared intent with likeminded partners	6
Supercomputing	+	++	++	Strategic intent	5
AI	++	+	++	Focus, strategic intent	5
Internet of Things	–	++	++	Political awareness	4

Table 3: Strategic autonomy tech alliances: state of play.

References

Aggarwal, Vinod K., and Andrew W. Reddie. 'Comparative Industrial Policy and Cybersecurity: A Framework for Analysis'. 3, no. 3 (2 September 2018): 291–305. https://doi.org/10.1080/23738871.2018.1553989.

ASML. 'EU Chips Act Position Paper', February 2022.

Baisakova, Nurzat, and Jan-Peter Kleinhans. 'The Global Semiconductor Value Chain: A Technology Primer for Policy Makers | Stiftung Neue Verantwortung (SNV)'. SNV Report, 2020. https://www.stiftung-nv.de/en/publication/global-semiconductor-value-chain-technology-primer-policy-makers.

Baron, Justus, and Olia Kanevskaia Whitaker. 'The Global Semiconductor Value Chain: A Technology Primer for Policy Makers | Stiftung Neue Verantwortung (SNV)'. SNV Report, 2020. https://www.stiftung-nv.de/en/publication/global-semiconductor-value-chain-technology-primer-policy-makers.

Baron, Justus, and Olia Kanevskaia Whitaker. 'Global Competition for Leadership Positions in Standards Development Organizations'. *Electronic Journal*, 31 March 2021. https://doi.org/10.2139/SSRN.3818143.

Beattie, Alan. 'The US's Ham-Fisted Attempts at Building a 5G Rival to China'. *Financial Times*, 2021. https://www.ft.com/content/991a739e-10a4-4a64-b872-b75b05cf2e1f.

Boston Consulting Group and Semiconductor Industry Association. 'Strengthening the Global Semiconductor Supply Chain in an Uncertain Era | BCG', 2021. https://www.bcg.com/publications/2021/strengthening-the-global-semiconductor-supply-chain.

Bradford, Anu. *The Brussels Effect : How the European Union Rules the World*, 2020.

Broeders, Dennis. 'Aligning the International Protection of "the Public Core of the Internet" with State Sovereignty and National Security'. *Journal of Cyber Policy* 2, no. 3 (2 September 2017): 366–76. https://doi.org/10.1080/23738871.2017.1403640.

'Build Leadership in AI | Shaping Europe's Digital Future'. Accessed 21 March 2022. https://digital-strategy.ec.europa.eu/en/policies/build-leadership-ai.

China State Council. 'Made in China 2025', 2015. http://english.www.gov.cn/2016special/madeinchina2025/.

Codagnone, Cristiano, Giovanni Liva, Laura Gunderson, Gianluca Misuraca, and Emanuele Rebesco. 'Europe's Digital Decade and Autonomy Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies'. *European Parliament Studies*, 2021.

European Chamber of Commerce in China. 'European Business in China Position Paper 2021/2022', 2021. https://www.europeanchamber.com.cn/en/publications-position-paper.

European Commission. 'New Approach to Enable Global Leadership of EU Standards Promoting Values and a Resilient, Green and Digital Single Market', 22 February 2022. https://ec.europa.eu/growth/news/new-approach-enable-global-leadership-eu-standards-promoting-values-and-resilient-green-and-digital-2022-02-02_en.

European Commission. 'EU-US Trade and Technology Council Inaugural Joint Statement'. Text. Accessed 21 March 2022. https://ec.europa.eu/commission/presscorner/detail/en/statement_21_4951.

European Commission. '5G Supply Market Trends', 2021. https://digital-strategy.ec.europa.eu/en/library/commission-publishes-study-future-5g-supply-ecosystem-europe.

Holslag, Jonathan. 'The Elusive Axis: Assessing the EU–China Strategic Partnership'. *JCMS: Journal of Common Market Studies* 49, no. 2 (1 March 2011): 293–313. https://doi.org/10.1111/J.1468-5965.2010.02121.X.

Kearney. 'Europe's Urgent Need to Invest in a Leading-Edge Semiconductor Ecosystem', 2021.

Kleinhans, Jan-Peter. 'The Lack of Semiconductor Manufacturing in Europe'. SNV Policy Briefs, 2021.

Lane, Nathaniel. 'The New Empirics of Industrial Policy'. J*ournal of Industry, Competition and Trade* 2020 20:2 20, no. 2 (3 January 2020): 209–34. https://doi.org/10.1007/S10842-019-00323-2.

Lee-Makiyama, Hosuk, and Florian Forsthuber. 'Open RAN: The Technology, Its Politics and Europe's Response'. ECIPE, 2020. https://ecipe.org/publications/open-ran-europes-response/.

Porter, Michael E. 'The Competitive Advantage of Nations'. *Harvard Business Review*, 1 March 1990. https://hbr.org/1990/03/the-competitive-advantage-of-nations.

Renda, Andrea. 'Leveraging Digital Regulation for Strategic Autonomy'. FEPS, 1 March 2022. https://www.feps-europe.eu/resources/publications/853-beyond-the-brussels-effect.html.

Stocker, Volker, Guenter Knieps, and Christoph Dietzel. 'The Rise and Evolution of Clouds and Private Networks – Internet Interconnection, Ecosystem Fragmentation'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 23 August 2021. https://doi.org/10.2139/ssrn.3910108.

Thales. 'An Anchor of Trust in a Digital World: Risk Management Strategies for Digital Processes', 2020.

Timmers, Paul. 'Debunking Strategic Autonomy', Directions Blog. Accessed 21 March 2022. https://directionsblog.eu/debunking-strategic-autonomy/.

Timmers, Paul. 'There Will Be No Global 6G Unless We Resolve Sovereignty Concerns in 5G Governance'. *Nature Electronics* 2020 3:1 3, no. 1 (24 January 2020): 10–12. https://doi.org/10.1038/s41928-020-0366-3.

Timmers, Paul. 'Strategic Autonomy and Cybersecurity: EU Cyber Direct'. *EUISS Research in Focus*, 2019. https://eucyberdirect.eu/research/strategic-autonomy-and-cybersecurity.

Timmers, Paul. 'The European Union's Cybersecurity Industrial Policy'. *Journal of Cyber Policy* 3, no. 3 (2 September 2018): 363–84. https://doi.org/10.1080/23738871.2018.1562560.

Timmers, Paul, and Freddy Dezeure. 'Strategic Autonomy and Cybersecurity in the Netherlands | Cyber Security Council'. Cyber Security Council, 2021. https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands.

Tyushka, Andriy, and Lucyna Czechowska. 'Strategic Partnerships, International Politics and IR Theory'. *States, International Organizations and Strategic Partnerships*, 15 July 2019, 8–43. https://doi.org/10.4337/9781788972284.00010.

Voelsen, Daniel. 'Cracks in the Internet's Foundation', SWP Research Paper 2019/RP 14. Accessed 21 March 2022. https://www.swp-berlin.org/10.18449/2019RP14/

White House. 'National Strategy for Critical and Emerging Technologies', October 2020.

About the author

PROF. DR PAUL TIMMERS

Paul Timmers is research associate at the University of Oxford, professor at European University Cyprus, visiting professor at several other universities, senior advisor EPC Brussels, board member Digital Enlightenment Forum, President of the Supervisory Board Estonian eGovernance Academy and CEO of iivii BV. He was Director at the European Commission for cybersecurity, e-ID, digital privacy, digital health, smart cities, e-government; cabinet member of European Commissioner Liikanen; manager in a large ICT company and co-founded an ICT start-up. He holds a Physics PhD from Nijmegen University, an MBA from Warwick University, an EU fellowship at UNC Chapel Hill, and a cybersecurity qualification from Harvard.

STRATEGIC AUTONOMY
pathways to progressive action

About FEPS

The Foundation for European Progressive Studies (FEPS) is the think tank of the progressive political family at EU level. Its mission is to develop innovative research, policy advice, training and debates to inspire and inform progressive politics and policies across Europe.

FEPS works in close partnership with its 68 members and other partners, including renowned universities, scholars, policymakers and activists, forging connections among stakeholders from the world of politics, academia and civil society at local, regional, national, European and global levels.

European Political Foundation - Nº 4 BE 896.230.213 | Avenue des Arts 46 1000 Brussels (Belgium)

www.feps-europe.eu | Twitter/Instagram: @FEPS_Europe | Facebook: @FEPSEurope

ON SIMILAR TOPICS

AN ARCHITECTURE FIT FOR STRATEGIC AUTONOMY

INSTITUTIONAL AND OPERATIONAL STEPS TOWARDS A MORE AUTONOMOUS EU EXTERNAL ACTION

ABSTRACT

This policy paper analyses several institutional and policymaking priorities conducive to a more strategic autonomy agenda for the whole of EU external action. It departs from two different understandings of strategic autonomy: the geopolitical understanding, on which most political efforts have been placed so far, and an institutional/operational understanding, where substantial work remains to be done. The policy paper reviews three recurrent institutional shortcomings for strategic autonomy: the political paralysis at the EU level and the need for more flexible institutional responses; the divisive and often distracting discussions on QMV in the field of foreign and security policy; and a limiting focus on security and defence when it comes to implementing strategic autonomy as a policy priority. The final section provides some policy options to advance the EU's strategic autonomy agenda, in line with its operational purposes, namely broadening the focus of discussions on strategic autonomy to the whole of EU external action; securing the buy-in of member states in processes and policies leading to more strategic autonomy; promoting thematic and regional steps forward in its operationalisation; fostering political consensus at the highest level; promoting a strategic autonomy esprit de corps; and enhancing the institutional tools, methods and capabilities for more strategic autonomy in the field of EU external action.

AUTHOR

POL MORILLAS
Director of CIDOB (Barcelona Centre for International Affairs)

FRIEDRICH EBERT STIFTUNG

Fondation Jean Jaurès

STRATEGIC AUTONOMY SERIES

BEYOND THE BRUSSELS EFFECT

LEVERAGING DIGITAL REGULATION FOR STRATEGIC AUTONOMY

ABSTRACT

The paper analyses Europe's alleged primacy in the regulation of emerging technologies and assesses whether the so-called 'Brussels effect' can help the EU achieve prominence as a global regulator in the digital space. It finds that the Brussels effect, while existing, is not only exaggerated in public debate but is also at risk of gradual erosion over the coming years. Moreover, current trends in global technology governance suggest that unilateral rule making will not be a viable strategy in the future and that the EU will be able to retain a leading role only if it develops a coalition-building strategy, as well as a self-standing, semi-open technology stack. The paper provides five policy recommendations that may help the EU thrive in an increasingly competitive and strategic terrain.

AUTHOR

ANDREA RENDA
Senior Research Fellow,
Centre for European
Policy Studies (CEPS)

FRIEDRICH EBERT STIFTUNG

Fondation Jean Jaurès

STRATEGIC AUTONOMY SERIES

CORRECTING COURSE: THE 2030 DIGITAL COMPASS

ABSTRACT

The recently proposed 2030 Digital Compass strategy by the European Commission is timely and welcome, because digital technology and infrastructures play an important strategic role in today's economy and society, and their importance will only increase.

However, the collection of metrics proposed by the European Commission to measure progress are not aligned with political objectives. Their achievement will not lead to an environmentally and socially sustainable digital transition and more digital autonomy. In addition, there is a need to better align the Compass with other strategies, notably the European Green Deal, the European Pillar of Social Rights Action Plan, and the update of the New Industrial Strategy.

The paper assesses the objectives of the four focal points of the Compass - skills, infrastructure, the digitalisation of business and the digitalisation of public services – as well as the means to implement the strategy, and points to several areas where improvement is in order. Finally, the paper provides a set of recommendations to upgrade the 2030 Digital Compass.

AUTHORS

GUILLAUME KLOSSA
Expert Consultant at FEPS and
President emeritus of the think
tank EuropaNova

JUSTIN NOGAREDE
Digital Policy Analyst at FEPS

GOVERNING ONLINE GATEKEEPERS
TAKING POWER SERIOUSLY

by Justin NOGAREDE

FRIEDRICH EBERT STIFTUNG

FUNDACIÓN PABLO IGLESIAS

Fondation Jean Jaurès

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES

FOUNDATION FOR EUROPEAN PROGRESSIVE STUDIES
FONDATION EUROPÉENNE D'ÉTUDES PROGRESSISTES

FABIAN SOCIETY

PUBLIC SERVICE FUTURES
WELFARE STATES IN THE DIGITAL AGE

Edited by
Andrew HARROP
Kate MURRAY
Justin NOGAREDE

NO DIGITALISATION WITHOUT REPRESENTATION

AN ANALYSIS OF POLICIES TO EMPOWER LABOUR IN THE DIGITAL WORKPLACE

Justin Nogarede

FRIEDRICH EBERT STIFTUNG

Fondation Jean Jaurès

FUNDACIÓN PABLO IGLESIAS

FEPS
FOUNDATION FOR EUROPEAN
PROGRESSIVE STUDIES