


ARTICLE

The Economy–Security Nexus: Risk, Strategic Autonomy and the Regulation of the Semiconductor Supply Chain

Benjamin Farrand 

Newcastle Law School, Newcastle University, Newcastle-Upon-Tyne, UK
Email: ben.farrand@ncl.ac.uk

Abstract

The EU's policies in the field of technology broadly defined are increasingly marked by a concern over strategic autonomy, and Europe's place in the world. Regulatory interventions are framed in terms of "digital sovereignty," with the Commission seeking to ensure that external dependencies are reduced with the aim of increasing the EU's resilience to geopolitical instability and external shocks. Using the case study of semiconductors, the chips that power modern electronic devices, this article explores how technology policy in the EU sits at the economy–security nexus, in which economic goals and security goals are interdependent and inseparable. Focusing on the life cycle of the semiconductor supply chain from the control over natural resources through to the cybersecurity requirements placed on the finished products, this article demonstrates the increasing security logic embedded within a burgeoning industrial technology policy.

Keywords: digital sovereignty; security; semiconductors; strategic autonomy

I. Introduction

"Digital is the make-or-break issue [and] there is no digital without chips."¹ Such was the pronouncement of Commission President von der Leyen at the 2021 EU State of the Union. EU digital policies have increasingly moved away from a binary between economy-and-internal market initiatives on the one hand, and cybersecurity initiatives on the other. The Union has seen itself increasingly beset by a range of geopolitical instabilities and global shocks, from pandemic to conflict on its borders. Its place in the world, and its responses to these insecurities, have resulted in a more assertive agenda, moving from traditional liberal economic approaches to approaches based in the merging of economic and security goals. The EU's "strategic autonomy," its ability to act independently and free of dependencies upon external actors, has expanded beyond military and defence issues to become its response to global upheaval generally, as a response to great-power rivalries reemerging, technological disruptions and the increasing use of leveraged interdependence,² in trade as much as in war. Semiconductors, the chips that power all modern

¹ Ursula von der Leyen, '2021 State of the Union Address by President von Der Leyen: Strengthening the Soul of Our Union' (European Commission 2021) SPEECH/21/4701 3–4 <https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701> accessed 17 September 2021.

² Niklas Helwig and Ville Sinkkonen, 'Strategic Autonomy and the EU as a Global Actor: The Evolution, Debate and Theory of a Contested Term' (2022) 27 *European Foreign Affairs Review* 1, 5.

electronics, and the security of their supply chains, serve as an excellent case study for exploring these dynamics, identifying the ways in which economic concerns and security concerns are brought together, justifying increased regulation on the basis of preserving and furthering strategic autonomy. This article takes an approach of considering the regulation of the semiconductor supply chain, from the harvesting of raw materials, through the research and design, manufacture, and use of these critical components. It demonstrates the economy-security nexus in EU digital policy, and how strategic autonomy as much as market integration, serves as a basis for the furthering of EU laws in technology sectors. In doing so, it serves to make a broader, generalisable case about the EU as a geopolitical actor that goes beyond the immediate case study.

II. Semiconductors, geopolitical vulnerability and strategic autonomy

In considering the merging of security and economic concerns and goals in technology governance, it is useful to begin with some definitions and explanations of the interrelated technologies at the centre of this article's analysis. The first is semiconductors. Semiconductors are materials with the capacity to conduct electricity at a value between that of traditional conductive metals such as silver or copper, and traditional insulators, such as glass (and thus have electrical resistivity above those conductors, but below that of insulators).³ Semiconductors are useful insofar as their electrical conductivity *increases* with heat, rather than *decreasing* as traditional metal conductors do.⁴ In terms of materials relevant for the microprocessor industry, the two most important semiconductors are silicon and germanium as “elemental” semiconductors, upon which the commercial processor markets depend.⁵ Central to their function is their crystalline structure, which allows for reproduction at an atomic level of their lattice composition.⁶ Ultimately, semiconductors are materials that have properties that make them essential; they are the key component in microchips, which power all modern electronics, from fridges to cars, smartphones to autonomous weapons systems. Microchips are generally described in terms of the number of transistors on a chip. The number of transistors on a chip can number in the millions or even billions – this of course requires they are incredibly small, nanometres (nm) in size. Therefore, the smaller the semiconductor transistor, the more can fit on a chip, and the more advanced the processing that the chip can perform. “Commodity” chips tend to have transistors larger than 7nm in size (and thus less can fit on a single chip), whereas high-end processing in advanced fields of computing use chips with transistors smaller than 7nm in size, with chips as small as 3nm becoming available in 2022, allowing for far greater computational capacity.⁷

The above discussion also helps to highlight why semiconductors, and by extension chips, are important. In the 21st Century, our lives are dependent upon chips. This is not hyperbole – microchips are integrated into technologies that provide water sanitisation and electricity delivery, power our medical technologies and agricultural systems, connect us in our social and professional lives, and equip our security and defence systems.

³ BG Yacobi, *Semiconductor Materials: An Introduction to Basic Principles* (Kluwer 2003) 1.

⁴ *Ibid.*, 2–3.

⁵ EJ Krol, “Silicon-Germanium” (1999) 18 IEEE Potentials 17.

⁶ Robert Pierret, *Advanced Semiconductor Fundamentals* (2nd edition, Pearson 2002) 5–6; For more on semiconductors and how they function, a very accessible text on the subject is John W Orton, *Semiconductors and the Information Revolution: Magic Crystals That Made IT Happen* (Academic Press 2009).

⁷ Lauly Li, “The Global Microchip Race: Europe’s Bid to Catch Up” *Financial Times* (13 December 2022) <<https://www.ft.com/content/b31e27fd-0781-4ffd-bb69-9af985abff41>> accessed 14 May 2024.

Historically, however, they have received comparatively little attention from social science scholars until relatively recently,⁸ and for European policymakers, their relevance even in the context of technology policies was relatively minimal. This changed dramatically, as with many things, during the COVID-19 pandemic. With supply chains facing heavy disruption due to closed factories and mining operations, while consumer demand increased substantially due to an increased desire for personal computing during periods of government-mandated home isolation,⁹ semiconductor research and supply moved from a tangential issue to technology policies more generally, to the centre of a realignment of EU strategy around ensuring security of supply.¹⁰ This has all happened, however, in the context of broader geopolitical competition. Faith in the liberal international economic order appears shaken, to the extent that we appear to be seeing a retreat from globalisation and an assumption that free and open markets are something to be desired.¹¹ The World Trade Organization appears powerless to combat the increased trade tensions and sanctions between large economic players,¹² and the increased trade nationalism and protectionism that predates Covid.¹³ This has been argued as constituting a form of de-globalisation that has significantly reconfigured global value chains, increasing levels of policy risk.¹⁴ These policy risks include the increasing fragmentation of the international order through expanding protectionist policies, efforts to sideline or minimise the influence of bodies such as the WTO, and an increased focus on regional and bilateral trade agreements.¹⁵ This is something that causes considerable consternation on the part of the EU as the two biggest trade powers signal their lack of commitment to a free-trade based order; as Friedberg has stated, “China’s rulers do not have any theoretical or moral commitment to freely functioning markets [...] economics must always be subordinate to politics.”¹⁶ China’s trade policies have been described as mercantilist,¹⁷ emphasising the link between economic activity and power, with the “plenty” of wealth providing for the power that ensures the security of the state, and the power that can be exercised externally in turn furthering the accumulation of wealth.¹⁸ As will be discussed in later sections, China has made semiconductor research and manufacture central to its technology policies. The US has engaged in similar policies, significantly increasing the

⁸ With a noticeable shift with the publication of Chris Miller, *Chip War: The Fight for the World’s Most Critical Technology* (Simon & Schuster 2022).

⁹ See for example Michael Funke and Adrian Wende, “Modeling Semiconductor Export Restrictions and the US-China Trade Conflict” (The Bank of Finland Institute for Emerging Economies 2022) 13/2022; Linda Monsees and Daniel Lambach, “Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity” (2022) 31 *European Security* 377.

¹⁰ Shawn Donnelly, “Semiconductor and ICT Industrial Policy in the US and EU: Geopolitical Threat Responses” (2023) 11 *Politics and Governance* 129.

¹¹ On this, see in particular Elisabeth Braw, *Goodbye Globalization: The Return of a Divided World* (Yale University Press 2024).

¹² Ernst-Ulrich Petersmann, “Economic Disintegration? Political, Economic, and Legal Drivers and the Need for ‘Greening Embedded Trade Liberalism’” (2020) 23 *Journal of International Economic Law* 347.

¹³ Stephen D King, *Grave New World: The End of Globalization, the Return of History* (Yale University Press 2017).

¹⁴ Nadia Zahoor and others, “De-Globalization, International Trade Protectionism, and the Reconfigurations of Global Value Chains” (2023) 63 *Management International Review* 823.

¹⁵ Daniel Bethlehem and Donald McRae, “The International Trade System – Looking to 2100” in Daniel Bethlehem and others (eds), *The Oxford Handbook of International Trade Law* (Second Edition, Oxford University Press 2022) 1070.

¹⁶ Aaron L Friedberg, *Getting China Wrong* (Polity 2022) 86.

¹⁷ Xiao Jiang, “Trade Expansion and Employment Generation: How Mercantilist Does China Have to Be?” (2013) 27 *International Review of Applied Economics* 557; Jeremy Garlick, “China’s Economic Diplomacy in Central and Eastern Europe: A Case of Offensive Mercantilism?” (2019) 71 *Europe-Asia Studies* 1390.

¹⁸ For more on this, see Lars Magnusson, *The Political Economy of Mercantilism* (Routledge 2018); as well as the key text Jacob Viner, “Power Versus Plenty as Objectives of Foreign Policy in the Seventeenth and Eighteenth Centuries” (1948) 1 *World Politics* 1.

direct subsidisation and funding of large projects in the field of semiconductor manufacture, with large new plants being built in states such as Arizona, Texas, and Ohio, based on new legislative initiatives to boost demand.¹⁹

It is in this febrile environment that the EU has revisited its approach to semiconductors, once largely non-existent, and now central to what the EU refers to as its digital or technological sovereignty.²⁰ Digital sovereignty acts in EU policy as a nexus for economic and security issues, seen as increasingly interdependent and inextricably linked. It is framed by the Commission as “ensuring the integrity and resilience of our data infrastructure, networks and communications. It requires creating the right conditions for Europe to develop and deploy its own key capacities, thereby reducing our dependency on other parts of the globe for our most crucial technologies.”²¹ Digital sovereignty is about strategic autonomy, and the ability of the EU to be self-sufficient and resilient to external shocks, motivated by a sense of vulnerability as the result of geopolitical instability and a less trusting international order.²² In particular, there is a recognition on the part of the Commission that cybersecurity goes beyond the security of end-user applications and the protection of critical infrastructure, to having relevance for the entirety of a given technology’s life-cycle, from securing of resources and know-how as discussed in Section III and IV, through to its implementation and manufacture, discussed in Section V, and eventual obsolescence, as is discussed in more detail in Section VI. The legal responses that the EU have taken can be framed as “regulatory mercantilist” in nature²³ – seeking to respond to the perceived external threats through engaging in initiatives that seek to bring security and economic interests together in order to secure strategic autonomy, with sovereignty claims lying at the basis of these initiatives. In doing so, the EU is designing an industrial policy in which objects of technological importance are attempted to be brought into the territory of the EU, and if this is not possible, by extending its regulatory influence beyond its borders. This is framed as the furthering of the EU’s “Geopolitical Union” by Commission President von der Leyen,²⁴ in which the EU exercises regulatory power as a means of securing strategic autonomy. This is being applied in a range of different sectors, such as in the approach taken to content moderation online²⁵ and the development of standards for AI.²⁶ The regulation of the semiconductor supply chain serves as another key example of the digital sovereignty initiative being put into practice,²⁷ with the linking of security and economic goals across the entire supply chain, as the next sections of this article will demonstrate. The analysis of these linkages and the creation of an economy–security nexus are operationalised through identifying how economic and security goals are aligned in the policy documents motivating regulatory initiatives in the fields of

¹⁹ A full list can be found at Michelle Adams, “Where Are All the New Semiconductor Fabs in North America & Europe?” (Z2Data, 12 September 2023) <<https://www.z2data.com/insights/new-semiconductor-fabs-in-north-america-europe>> accessed 20 June 2024; further discussion of the US legislative initiatives can be found in section V of this article.

²⁰ Terms often used interchangeably by the EU institutions – see Rocco Bellanova, Helena Carrapico and Denis Duez, “Digital/Sovereignty and European security integration: An introduction” (2022) 31 *European Security* 337.

²¹ European Commission, *Shaping Europe’s Digital Future* (2020) 3.

²² Benjamin Farrand and Helena Carrapico, “Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity” (2022) 31 *European Security* 435.

²³ *Ibid*; Benjamin Farrand, “Regulating Misleading Political Advertising on Online Platforms: An Example of Regulatory Mercantilism in Digital Policy” [2023] *Policy Studies* 1.

²⁴ Ursula von der Leyen, “2023 State of the Union Address by President von Der Leyen: Answering the Call of History” (2023) *SPEECH/23/4426*.

²⁵ Farrand (n 23).

²⁶ Andrea Calderaro and Stella Blumfelde, “Artificial Intelligence and EU security: the false promise of digital sovereignty” (2022) 31 *European Security* 415.

²⁷ Monsees and Lambach (n 9).

semiconductors, and how they then result in specific legal obligations placed upon Member States and private sector operators.

III. Regulation at the beginning of the chain: Securing strategic natural resources

The first aspect of the semiconductor supply chain to consider is the security of the natural resources from which microprocessors are built. As discussed in the preceding section, these chips require the chemical elements silicon, gallium and germanium to act as semiconductors to be able to function. The EU finds itself heavily dependent on other countries for its supply of these materials, and as such is highly vulnerable to market shocks,²⁸ impacting upon its strategic autonomy. Geopolitically, this is a concern for the EU as 71% of the world's silicon, 80% of its germanium, and 98% of its gallium is processed in China,²⁹ and the EU relies upon China for 11% of its silicon and 27% of its gallium imports, while being dependent on imports from outside the EU for 63% of its silicon, 31% of its gallium, and 100% of its lithium, which is also required for chip production.³⁰ The EU has described these vulnerabilities in explicit security terms, stating that they are central to its economic, trade, and security interests³¹ and highlighting that access to these critical raw resources is necessary for its economic competitiveness³² and the functioning of its defence industries.³³

The focus of regulation in this field is in securing the resilience of these supply chains to guarantee European access, as well as fostering relations with third countries that are key producers of desired resources. In 2023, the Commission published a Communication on a secure and sustainable supply of critical raw materials,³⁴ in which it framed the security of these supply chains as essential for its strategic autonomy. It proposed that its actions in the field should include reducing single-country dependencies for resources (thereby diversifying its supply chains), increase self-sufficiency through domestic production of critical materials where possible, and adopt a global leadership position through establishing partnerships with third countries that would serve to boost their economies while securing access to their resources for the EU.³⁵ The Commission subsequently published a Proposal for a Regulation on Critical Raw Materials,³⁶ which highlighted that the aim of this legislation would be to guarantee resources important to the European economy, framing this in terms of the geopolitical security risks that could potentially threaten supply chains.³⁷ The Critical Raw Resources Act³⁸ sets out at Article 1 that its

²⁸ Andrea Ciani and Michaela Nardo, "JRC Technical Report – The Position of the EU in the Semiconductor Value Chain: Evidence on Trade, Foreign Acquisitions, and Ownership" (European Commission 2022) JRC Working Papers in Economics and Finance, 2022/3.

²⁹ Council of the European Union, "The Semiconductor Ecosystem – Global Features and Europe's Position" 5 <<https://www.consilium.europa.eu/media/58112/220712-the-semiconductor-ecosystem-global-features-and-europe-s-position.pdf>> accessed 31 October 2023.

³⁰ European Commission, "Critical Raw Materials Resilience: Charting a Path towards Greater Security and Sustainability" (2020) COM(2020) 474 final 20–21.

³¹ European Commission, "The European Green Deal" (2019) COM(2019) 640 21.

³² *Ibid.*, 2.

³³ *Ibid.*, 8.

³⁴ European Commission, "A Secure and Sustainable Supply of Critical Raw Materials in Support of the Twin Transition" (2023) COM(2023) 165.

³⁵ *Ibid.*, 2–3.

³⁶ European Commission, "Proposal for a Regulation Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials" (2023) COM(2023) 160.

³⁷ *Ibid.*, 1.

³⁸ Regulation 2024/1252 establishing a framework for ensuring a secure and sustainable supply of critical raw materials (the Critical Raw Resources Act).

objectives are to improve the functioning of the internal market by ensuring access to a secure, resilient and sustainable supply of critical raw materials, with an emphasis on identifying and supporting strategic projects that reduce external dependencies, monitoring and mitigating supply risks. Articles 3 and 4 provide that the list of strategic raw materials (provided in Annex I, Section 1) and critical raw materials (Annex II, Section 1) shall be subject to three-yearly review, with the Commission empowered to update the lists as required. It is worth stating that all the materials listed above relevant to microprocessor development, including silicon, germanium and gallium, as well as battery-grade lithium, are all listed in the “strategic” category. Chapter 3 of the Act is titled “strengthening the union raw materials value chain” and provides for benchmarks for Union extraction capacity of at least 10% of the Union’s annual consumption of strategic raw materials, to the extent possible in light of the Union’s reserves,³⁹ Union production capacity at 40% of the Union’s annual consumption of strategic raw materials,⁴⁰ and recycling capacity of at least 25%.⁴¹ The legislation also provides for the recognition of Strategic Projects aimed at contributing to the Union’s supply of strategic raw materials,⁴² and providing for “enabling conditions” such as support in accelerating the implementation of Strategic Projects⁴³ and coordinating financing for such projects.⁴⁴ These actions link explicitly to the concept of the economy–security nexus, indicative of a regulatory mercantilist turn, exemplified in the Proposal for the Act, which stated that “it will allow Europe to boost industrial capacities [. . .] creating quality jobs and boosting growth while increasing our open strategic autonomy.”⁴⁵

Central to the economic–security nexus that these materials now represent, Chapter 4 of the Act concerns “risk monitoring and mitigation.” The Commission is required under Article 20 to monitor the risks to critical raw material access for the Union, including trade flows, demand and supply, concentration of supply, Union and global production capacities, price volatilities, bottlenecks and “potential obstacles to trade,” which can be taken to include factors that might affect supply, “including but not limited to the geopolitical situations, logistics, energy supply, workforce or natural disasters.”⁴⁶ The Commission is also expected to work with a newly created European Critical Raw Materials Board (the Board),⁴⁷ with Member States reporting to the Commission on their strategic stocks of strategic raw materials,⁴⁸ and the Commission and the Board coordinating stocks under Article 23, in order to ensure that States are holding sufficient levels of strategic raw materials. The Board is also expected to carry out coordinating functions, including for financing of Strategic Projects,⁴⁹ as well as promoting international cooperation and Strategic Partnerships with third states, “taking into account a third country’s potential reserves, extraction, processing and recycling capacities related to critical raw materials.”⁵⁰ While it is stated that any Strategic Partnerships should be consistent with the Union’s policies on emerging markets and developing economies,⁵¹ the Act

³⁹ Art 5(1)(a)(i).

⁴⁰ Art 5(1)(a)(ii).

⁴¹ Art 5(1)(a)(iii).

⁴² Art 6.

⁴³ Art 16.

⁴⁴ Art 17.

⁴⁵ European Commission, “Proposal for a Regulation Establishing a Framework for Ensuring a Secure and Sustainable Supply of Critical Raw Materials” (n 36) 2.

⁴⁶ Art 20(3)(g).

⁴⁷ Art 35.

⁴⁸ Art 22.

⁴⁹ Art 36.

⁵⁰ Art 37(1)(c)(i).

⁵¹ Art 37(1)(d).

nevertheless represents a significant shift in the EU's policies in this area; it represents moves in the direction of a technology-oriented industrial policy, triggered by "an increasingly realist and traditional security-oriented international outlook, which relies on a geopoliticization of the threat stemming from import dependencies,"⁵² highlighting a link between economic and security-oriented goals. While these moves have been made in order to mitigate against these geopolitical threats, there are some concerns that increased protectionism could in fact fuel technology-dependent states to engage in trade-based resource wars, increasing geopolitical risk⁵³ and further exacerbating risks to the liberal international trade order.⁵⁴

IV. Regulation of R&D: Keeping secrets safe from states

Assuming that critical/strategic raw resources are obtainable, or at least brought within the EU's sphere of influence, the next area of supply chain security of relevance is the protection of research and design (R&D) in microprocessor design. Tying into the previous section, and indeed linking to the next, while the EU is light on critical raw materials, and as will be discussed, lacks microchip physical production capacity, it does possess some limited expertise in R&D. R&D is considered highly relevant in the supply side of the semiconductor industry, particularly as it relates to funding, pilot lines (in which research is brought together from various actors in an industrial setting to use in production), and as it relates to innovation in node shrinkage to allow for the production of more high-end chips.⁵⁵ As such, intellectual property (IP) is of direct relevance to security in the supply chain, as companies on both the supply and demand side of semiconductor trade are involved in the selling of IP,⁵⁶ and how this IP is protected has increasingly become tied to effective cybersecurity. Protection of these IP assets in the supply chain is therefore important to economic security of private actors in these markets. When compared to other dimensions of the semiconductor supply chain, the EU's legal framework for IP protection is both relatively robust, as well as broadly comprehensive. It also allows for the discussion of an area of IP that generally receives comparatively little attention, namely the *sui generis* protection of circuit topography. The EU's approach to this is heavily modelled upon the US's Semiconductor Chip Protection Act of 1984,⁵⁷ which was heavily motivated by the US–Japan Chip War of the 1980s and concerns over the competitive edge Japanese firms were demonstrating as a result of cross-licensing agreements with US-based producers (albeit on the basis of scantily evidenced claims of "chip piracy").⁵⁸ The production of microchips on a *sui generis* basis was also in part due to questions over whether existing international frameworks such as the Berne Convention could provide protection for these specialised forms of technology.⁵⁹ In this respect, the US legislation served as a model upon which the EU designed its own regime.

⁵² Małgorzata Jakimów, Vsevolod Samokhalov and Brian Baldassarre, "Achieving European Union strategic autonomy: Circularity in critical raw materials value chains" [2024] International Affairs iiae127, 1.

⁵³ Steven E Zhang and others, "Emerging criticality: Unraveling shifting dynamics of the EU's critical raw materials and their implications on Canada and South Africa" (2023) 86 Resources Policy 104247.

⁵⁴ Andrew Glencross, "The Geopolitics of Supply Chains: EU Efforts to Ensure Security of Supply" (2024) DOI: 10.1111/1758-5899.13388 Global Policy 1.

⁵⁵ European Commission, "European Chips Survey Report" (Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Directorate-General for the Joint Research Centre 2022) 15–17.

⁵⁶ *Ibid.*, 17.

⁵⁷ 17 U.S. Code §§901–914.

⁵⁸ Thomas Hoeren, "The protection of pioneer innovations – lessons learnt from the semiconductor chip industry and its IP law framework" (2015) 32 John Marshall Journal of Information Technology and Privacy Law 151, 173–174.

⁵⁹ See for example Tana Pistorius, "The *sui generis* protection of semiconductor chips (Part 2)" (1995) 28 De Jure 113.

Directive 87/54/EEC on the legal protection of topographies of semiconductor products is as specific as the name suggests. Unlike the EU's broader IP frameworks for subjects such as copyright⁶⁰ or trademark,⁶¹ the Directive was specifically concerned with market harmonisation for the purposes of ensuring that semiconductor technologies were protected as akin to intellectual property due to their considerable investments that could be copied at a fraction of the cost needed to develop them independently. On this basis, Article 1 provided that "semiconductor products," defined as final or intermediate forms of any product consisting of a body of material which includes a layer of semiconducting material, arranged into more than one layer in accordance with a predetermined three-dimensional pattern and intended to perform an electronic function, would be protected. This protection extends to the "topography" of a semiconductor product, which constitutes the graphic representation of that pattern. This would allow for the exploitation of exclusive rights upon registration under Article 4, allowing for right-holders to prevent the unauthorised reproduction or a topography or commercial exploitation of a semiconductor product using that topography,⁶² providing an exclusive right over the topography or semiconductor product for ten years.⁶³ As a form of protection, however, the protection of semiconductor product design appears to have been of little relevance for stakeholders in the EU – according to one report in the early 21st Century, "for industry, the *function* of an integrated circuit of architecture is more valuable to protect than the design. If the function can be patented, it means broader protection than that given to [semiconductor products and topographies . . .] trademark protection may also help to some extent, as will, of course, trade secret law."⁶⁴ Hoeren is in agreement, suggesting that protection of semiconductors in IP law is really done through patents, with general approaches of cross-licensing and agreements not to sue.⁶⁵ While this is relevant to semiconductor technologies in the context of economic competition between competing firms, in terms of strategic autonomy and geopolitical vulnerabilities, this reliance on publicly disclosed patents may be less valuable.

From a security perspective, particularly *vis-à-vis* the world of geopolitical competition, trade secrecy is arguably of more direct relevance. Trade secrecy is governed in the EU under Directive 2016/943,⁶⁶ which affords protection to information that is secret in the sense that it is not generally known among or readily accessible to persons normally dealing with that kind of information, has commercial value because it is secret, and has been subject to reasonable steps to keep it secret.⁶⁷ Trade secrets have the advantages of not being timebound and can help to maintain global competitiveness, and may be preferred in the context of competition for technological dominance or on the basis of national security concerns.⁶⁸ While admittedly somewhat dated, a 2013 study by the European Commission into trade secrecy practices among firms found that in the semiconductor sector, 60% of respondents considered trade secrecy protection as an

⁶⁰ Such as Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society.

⁶¹ Regulation 2017/1001 on the European Union trade mark.

⁶² Directive 87/54/EEC, Article 5.

⁶³ Article 7(3).

⁶⁴ Gunnar WG Karnell, "Protection of layout designs (topographies) of integrated circuits: RIP?" (2001) 32 *International Review of Intellectual Property and Competition Law* 648, 652.

⁶⁵ Thomas Hoeren, "The semiconductor chip industry – the history, present and future of its IP law framework" (2016) 47 *International Review of Intellectual Property and Competition Law* 763, 791.

⁶⁶ Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

⁶⁷ Art 2(1).

⁶⁸ Mateo Aboy, Timo Minssen and Mauritz Kop, "Mapping the patent landscape of quantum technologies: Patenting trends, innovation and policy implications" (2022) 53 *International Review of Intellectual Property and Competition Law* 853, 877–79.

effective protection mechanism, compared to only 27% feeling the same way about patents.⁶⁹ In this context, however, effective protection does not only entail protection from competitor companies, but from state-based espionage, about which high-end semiconductor manufacturers demonstrate significant concern.⁷⁰ When it comes to physical products, this will be discussed in the next section. On the issue of know-how and information, effective trade secrecy protection has been linked to the issue of data sovereignty. Closely linked to the idea of digital sovereignty in the EU, data sovereignty is the understanding that “the fact that the majority of European data is stored in servers operated by non-European companies that are subject to extra-territorial legislations [sic] make such data potentially accessible by third countries.”⁷¹ Therefore, data sovereignty is intimately connected to cybersecurity, insofar as it acts as a requirement for the effective protection of data from unauthorised access facilitated through third-state attempts to access it.

In the European strategy for data,⁷² the Commission highlights its concern that “EU-based cloud providers only have a small share of the cloud market, which makes the EU highly dependent on external providers, vulnerable to external data threats.”⁷³ In addition to this, the threats identified by the US and China with regard to the processing of data (which the strategy makes clear goes beyond personal data to include industrial data) and the uncertainty of compliance with important EU rules and standards⁷⁴ is seen as requiring the creation of a European data space and new rules that would encourage the storage within the EU’s territorial and regulatory control. The implementation of the Data Governance Act⁷⁵ and Data Act⁷⁶ are the legal means by which the EU is seeking to achieve this, with the Data Governance Act seeking to establish rules concerning data possessed by public sector bodies⁷⁷ that will help to foster the creation of a European data space, including through prohibiting exclusive arrangements concerning that data⁷⁸ and facilitating reuse.⁷⁹ The Data Act is more directly relevant to protection semiconductor-related information, as Article 1 makes clear it sets rules for safeguards against unlawful third-party access to non-personal data, and that it applies to manufacturers of connected products placed on the market in the Union and providers of related services, irrespective of the place of establishment of those manufacturers and providers. Article 11 mandates the use of technical protection measures on the unauthorised use or disclosure of data, and in particular under Article 32, seeks to ensure that all data processing services shall take all adequate technical, organisational and legal measures in order to prevent international and third-country governmental access and transfer of non-personal data held in the Union. We see again the existence of an economy–security nexus – because of the value of this know-how, the EU seeks to protect it as a security interest, but through market-development means that are intended to boost the development of “domestic” providers, in turn increasing economic value within

⁶⁹ European Commission, “Study on Trade Secrets and Confidential Business Information in the Internal Market” (2013) Ref. Ares(2016)98815-08/01/2016 98.

⁷⁰ John VerWey, “Chinese semiconductor industrial policy: Past and present” (2019) 2019 *Journal of International Commerce & Economics* 1.

⁷¹ Filippo Gualtierio Blancato, “The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem” (2024) 16 *Policy & Internet* 12, 14.

⁷² European Commission, “A European strategy for data” (2020) COM(2020) 66.

⁷³ *Ibid.*, 9.

⁷⁴ *Ibid.*

⁷⁵ Regulation 2022/868 on European data governance and amending Regulation 2018/1724.

⁷⁶ Regulation 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation 2017/2394 and Directive 2020/1828.

⁷⁷ Regulation 2022/868, Art 3.

⁷⁸ Art 4.

⁷⁹ Art 5.

Europe's borders. It is hoped by the Commission that the adoption of these rules will help to facilitate the EU's strategic autonomy in the context of data sovereignty and cloud-based services, and by extension, entities possessing semiconductor-related data will need to ensure they comply with these data security requirements to prevent third state access.⁸⁰

V. Regulation of manufacture: Semiconductor security through industrial policy?

The point of the semiconductor supply chain that presents the most concern to states is in the manufacture of the microchips. This is due to twin, interrelated concerns – the first, the availability of those chips and the trade shocks that can impact this, and the second, their potential dual use functions, in which they can be used to power systems and technologies deemed security threats to other states. These concerns are interrelated, insofar as security of supply can be negatively impacted by measures aimed at ensuring broader security aims. By way of example, the US has put an increasing number of restrictions on the export of chips to China, arguing that the risks of China achieving technological supremacy in fields such as AI could present significant security risks.⁸¹ China has responded with reciprocal trade export restrictions, including on semiconductors such as gallium and germanium, which are subject to an export license.⁸² Furthermore geopolitical tensions over the status of Taiwan, home of TSMC, the world's foremost advanced chip producer, is taking place in the context of this increasingly hostile trade war.⁸³ As a result, China has announced an explicit semiconductor industrial policy,⁸⁴ with increased direct funding for semiconductor research and manufacture internally as a means of reducing dependencies on Western technology imports in the name of “technological self-reliance.”⁸⁵ Similarly, the US has invested in semiconductor industrial policy through its Chips and Science Act,⁸⁶ which provides for an industrial policy aimed at reducing dependency on semiconductors produced in Taiwan by boosting manufacturing capacity in the US, with \$280 provided billion for semiconductor research and development.⁸⁷

⁸⁰ For more on strategic autonomy as it relates to data, which is not the main focus of this article, see Oskar J Gstrein, “Data autonomy: Recalibrating strategic autonomy and digital sovereignty” (2023) 28 *European Foreign Affairs Review* 379; see also Samuele Fratini and Francesca Musiani, “Data Localization as Contested and Narrated Security in the Age of Digital Sovereignty: The Case of Switzerland” (2024) 10.1080/1369118X.2024.2362302 *Information, Communication & Society* 1.

⁸¹ AJIL Contemporary Practice of the United States, “The United States announces export controls to restrict China's ability to purchase and manufacture high-end chips” (2023) 117 *American Journal of International Law* 144.

⁸² Jing Zhang, Tamer A Soliman and Jennifer L Parry, “China Imposes New Export Controls on Two Minerals Critical to the Manufacture of Semiconductors” (*Mayer Brown*, 27 July 2023) <<https://www.mayerbrown.com/en/insights/publications/2023/07/china-imposes-new-export-controls-on-two-minerals-critical-to-the-manufacture-of-semiconductors>> accessed 19 June 2024.

⁸³ Wen-jen Hsieh, “Implications of the U.S. – China trade war for Taiwan” (2020) 19 *Asian Economic Papers* 61.

⁸⁴ Central Commission for Cybersecurity and Informatization, “Translation: 14th Five-Year Plan for National Informatization” (Rogier Creemers and others trs, 2021). <<https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/>> accessed 19 June 2024.

⁸⁵ Nikkei Asia, “Transcript: President Xi Jinping's Report to China's 2022 Party Congress” (*Nikkei Asia*, 18 October 2022) <<https://asia.nikkei.com/Politics/China-s-party-congress/Transcript-President-Xi-Jinping-s-report-to-China-s-2022-party-congress>> accessed 19 June 2024.

⁸⁶ Chips Act of 2022, Pub. L. 117–67.

⁸⁷ Justin Badlam and others, “The CHIPS and Science Act: What Is It and What Is in It?” (*McKinsey*, 4 October 2022) <<https://www.mckinsey.com/industries/public-sector/our-insights/the-chips-and-science-act-heres-whats-in-it>> accessed 31 October 2023.

It is in this context that the EU has made its own efforts at something akin to a semiconductor industrial policy. Compared to its global competitors, EU-based semiconductor manufacture is highly limited – it possesses few fabless production facilities, and no cutting-edge foundries producing chips with nodes of under 22nm.⁸⁸ The Commission has stated that while EU-based companies were heavily invested in semiconductor R&D, but there was insufficient investment in translating this into “industrial benefits [. . .] many results of European R&D are industrially deployed outside the Union.”⁸⁹ The EU only had a global market share of 10%, and largely relied upon third country suppliers.⁹⁰ In order to reduce these external dependencies, and ensure strategic autonomy, the EU has set the goal of achieving a 20% market share of worldwide production for cutting-edge chips (those of 7nm and below) by 2030.⁹¹ Increasing Europe’s manufacturing capacity is therefore a “precondition for its future competitiveness, and a matter of technological sovereignty and security,”⁹² indicative of the bringing together of economic and security goals in common policy initiatives. It therefore proposed the European Chips Act, intended to achieve the twin goals of securing the resilience of Europe’s semiconductor ecosystem, as well as increasing its global market share,⁹³ reflecting the economy-security nexus in which semiconductors now sit. The Chips Act,⁹⁴ which entered into force in September 2023, makes clear this focus in recital 1, which states that semiconductors are essential to both the Union’s economy and its security. The measures adopted in the Act therefore reflect this approach of achieving security goals through active development of industrial policy.⁹⁵

The attempt to establish an industrial policy to ensure security of supply and strategic autonomy is made clear in Chapter II, titled “Chips for Europe.” Article 3 makes clear the strategy is to be funded through the Multiannual Financial Framework and Horizon, with Article 4 stating that the objective of the strategy is to “achieve large-scale technological capacity building and support related research and innovation activities throughout the Union’s semiconductor value chain,” through capacity building for integrated semiconductor technologies, enhancing existing and developing new pilot lines, building advanced technology capacities for production, establishing a network of European competence centres including through building new facilities, and setting up a “Chips Fund” to supply capital for start-ups, scale-ups, and SMEs in the European supply chain. Chapter III complements investment with security mechanisms, reducing external dependencies through the establishment of integrated production facilities for semiconductors,⁹⁶ and “Open Foundries” to “offer production capacity to unrelated undertakings and thereby contribute to the security of supply for the internal market and the resilience of the Union’s semiconductor ecosystem.”⁹⁷ Chapter IV concerns emergency response, which entails a strategic mapping of the EU’s semiconductor sector,⁹⁸ monitoring potential

⁸⁸ For an overview, see Jan-Peter Kleinhans, “The Lack of Semiconductor Manufacturing in Europe” (Stiftung Neue Verantwortung 2021) 11–15.

⁸⁹ European Commission, “Proposal for a Regulation Establishing a Framework of Measures for Strengthening Europe’s Semiconductor Ecosystem (Chips Act)” (2022) COM(2022) 46 1.

⁹⁰ European Commission, “A Chips Act for Europe” (2022) COM(2022) 45 2.

⁹¹ *Ibid.*, 9.

⁹² *Ibid.*, 22.

⁹³ European Commission, “Proposal for a Regulation Establishing a Framework of Measures for Strengthening Europe’s Semiconductor Ecosystem (Chips Act)” (n 89) 3.

⁹⁴ Regulation 2023/1781 establishing a framework of measures for strengthening Europe’s semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act).

⁹⁵ Andrew Johnston and Robert Huggins, “Europe’s Semiconductor Industry at a Crossroads: Industrial Policy and Regional Clusters” (2023) 30 European Urban and Regional Studies 207.

⁹⁶ Chips Act, Art 13.

⁹⁷ Art 14.

⁹⁸ Art 19.

warning signs of semiconductor supply failings,⁹⁹ with the ability to enact a crisis response if supplies are deemed to be at threat,¹⁰⁰ which can include common purchase orders in order to guarantee supply for critical sectors.¹⁰¹ While these efforts are to be lauded in terms of their ambition to guarantee security, concerns have been raised concerning the ability to rapidly scale up production capacity for high-end chips,¹⁰² both in terms of the cost of doing so as well as the significant lead times in building foundries, taking approximately \$10 billion, three years, and 6,000 skilled workers to achieve.¹⁰³ Nevertheless, the EU sees these efforts as necessary in the context of what it sees as an increasingly insecure, geopolitically unstable trade system.¹⁰⁴

VI. Regulation of finished products: cybersecurity in semiconductors

A final dimension of semiconductor security entails ensuring the security of the microchips once manufactured and installed on devices. Semiconductors are not standalone items, but embedded within broader technological systems and appliances, which may be subject to cyberattacks. This of course includes the technologies used in fabless design engaged in semiconductor research and fabrication foundries used to manufacture the chips. A compromised semiconductor chip can be the vector for a system-level exploit – one such example being the “Bleeding Bit” vulnerability in Bluetooth chips, which allowed for malicious firmware to be installed on devices, or to cause a memory overflow that allows for malicious code to be run.¹⁰⁵ Mitigating and responding to cybersecurity threats have also been positioned as being central to the EU’s digital policies, linked to the threats posed by external state and non-state actors in the context of broader geopolitical tensions over the control and use of technology.¹⁰⁶ This has resulted in a raft of regulatory initiatives aimed at improving the coherence and capacities of EU cybersecurity, from updating the obligations on critical information infrastructure providers under NIS2,¹⁰⁷ and providing for a cyber-certification regime under the Cybersecurity Act,¹⁰⁸ as well as proposing Regulations on Cyber-Solidarity (which includes funding and support for joint cybersecurity initiatives)¹⁰⁹ and Cyber-Resilience

⁹⁹ Art 20.

¹⁰⁰ Art 23.

¹⁰¹ Art 27.

¹⁰² Bob Hancké and Angela Garcia Calvo, “Mister Chips goes to Brussels: On the pros and cons of a semiconductor policy in the EU” (2022) 13 *Global Policy* 585.

¹⁰³ intel, “What Does It Take to Build a Fab?” (*intel*, 2023) <<https://www.intel.com/content/dam/www/central-libraries/us/en/documents/what-does-it-take-to-build-a-fab.pdf>> accessed 28 October 2023.

¹⁰⁴ Kathleen R McNamara, “Transforming Europe? The EU’s Industrial Policy and Geopolitical Turn” (2023) 10.1080/13501763.2023.2230247 *Journal of European Public Policy* 1.

¹⁰⁵ Zack Whittaker, “A Pair of New Bluetooth Security Flaws Expose Wireless Access Points to Attack” (*TechCrunch*, 1 November 2018) <<https://techcrunch.com/2018/11/01/bleedingbit-security-flaws-bluetooth-wireless-networks/>> accessed 20 June 2024.

¹⁰⁶ European Commission and High Representative of the Union for Foreign Affairs and Security Policy, “The EU’s cybersecurity strategy for the digital decade” (2020) JOIN(2020) 18 1.

¹⁰⁷ Directive 2022/2555 on measures for a high-level common level of cybersecurity across the Union, amending Regulation 901/2014 and Directive 2018/1972, and repealing Directive 2016/1148 (NIS2 Directive).

¹⁰⁸ Regulation 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation 526/2013 (Cybersecurity Act).

¹⁰⁹ European Commission, “Proposal for a Regulation Laying down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents” (2023) COM(2023) 209.

(emphasising resilience across the entire life-cycle of software and hardware),¹¹⁰ both of which have received political agreement and are awaiting entry into the Official Journal.

For semiconductor supply chain security, obligations in the NIS2 Directive and Cybersecurity Act are particularly relevant, as are obligations that will be imposed through the Cyber-Resilience Act, once it is adopted. Under NIS2 Article 1, Member States are mandated to implement national cybersecurity strategies, with risk-management measures and reporting obligations for entities designated as operating in sectors of high criticality¹¹¹ or other critical sectors.¹¹² Under Article 3, if public or private entities are designated as operating in these types of sector, they are subject to the requirements of this legislation, which include ensuring cybersecurity governance within their structures, including providing training and upskilling under Article 20, adoption of risk-management measures under Article 21, and working with Union level bodies such as the Cooperation Group, ENISA (the EU's Cybersecurity Agency) and the Commission in order to identify risks to critical supply chains under Article 22, as well as report in the event of a cyber incident under Article 23. These entities are expected to engage with cybersecurity professionals as well as national authorities in order to develop and promote standards and best-practices in order to mitigate the risk of cyber-attacks, and ensure resilience in the event that such attacks are successful, with liability being based on the failure to report cyber incidents if they occur, or where an attack is successful due to a failure to follow industry standards of cybersecurity practice.¹¹³ In the context of R&D data concerning semiconductors, cloud service providers are listed as sectors of high criticality under Annex I.8 as providers of digital infrastructure, but in the context of manufacture and supply, semiconductor producers will be regarded as falling within the "other critical sectors" designation as manufacturers of computer, electronic and optical products under Annex II.5(b). They are therefore obliged to ensure cybersecurity resilience of their production facilities, in turn guaranteeing that supply is not impacted because of incapacity due to cyber-incident. For this reason, cybersecurity requirements permeate the entirety of the microchip development chain.

Similarly, the Cybersecurity Act creates a cybersecurity certification framework¹¹⁴ with a view to creating a digital single market for ICT products, services and processes. The purpose of the scheme is to attest that the products, services and processes have been evaluated as complying with specified security requirements, including concerning authenticity and integrity, as well as identifying and documenting known dependencies and vulnerabilities, or to verify that products, services and processes do not contain known vulnerabilities.¹¹⁵ Interestingly, an update to the certification regime which has been proposed by the Commission in 2023,¹¹⁶ while concerned with security, was adopted as a priority "for the industrial policy of the Union in the cybersecurity field,"¹¹⁷ and proposes Article 173 TFEU on the competitiveness of European industry as its legal basis,

¹¹⁰ European Commission, "Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation 2019/1020" (2022) COM(2022) 454.

¹¹¹ NIS2 Directive, Annex I.

¹¹² Annex II.

¹¹³ For more on this see Helena Carrapico and Benjamin Farrand, "Dialogue, partnership and empowerment for network and information security: The changing role of the private sector from objects of regulation to regulation shapers" (2017) 67 *Crime, Law and Social Change* 245.

¹¹⁴ Cybersecurity Act, Art 46.

¹¹⁵ Art 51.

¹¹⁶ European Commission, "Proposal for a Regulation Amending Regulation 2019/881 as Regards Managed Security Services" (2023) COM(2023).

¹¹⁷ *Ibid.*, 1.

linking its security goals with an explicitly economic legal basis. For semiconductor manufacturers, making their products available on the market will not necessarily require adherence to this certification regime, as it is voluntary unless specified by the EU or Member States under Article 56. Nevertheless, obtaining this certification may be desirable both as a demonstration of product safety, as well as potentially increasing sales in the EU. However, should the Cyber Resilience Act be adopted, this may have implications for the semiconductor industry. Under the Act, which intends to ensure that hardware and software that was not necessarily regarded as falling within existing cybersecurity rules would nevertheless be subject to regulatory control,¹¹⁸ mandatory requirements concerning cybersecurity and vulnerability handling are required by certain software and hardware producers under Article 1. If a product is designated as a critical product with digital elements,¹¹⁹ they are subject to additional requirements. Semiconductors are included in the list of critical products in Annex III, Class I.19–21 (including microprocessors not classified as Class II, microcontrollers and integrated circuits), and Class II.5, 6, 9 and 10, which are categorised as higher risk.¹²⁰ Under Article 10, manufacturers will be subject to a number of obligations, including on essential cybersecurity requirements, risk assessment, as well as ensuring regular updates to hardware and software in order to address any identified security vulnerabilities. Article 6 states that as critical products, these classes of product will be subject to conformity assessments under Article 24, and should they not be met, they will be subject to Union-level restrictions, up to and including withdrawal from the market under Article 45. This indicates that when it comes to semiconductor security, the Commission is cognisant not only of the risks to supply, but the risks of the supply. In doing so, the EU explicitly brings semiconductors into the wider cybersecurity framework, given their embedding in hardware devices that then run applications that can all create security risks, from initial development and release through to obsolescence and technology end-of-life.

VII. Conclusions

Semiconductors have moved from the periphery of EU technology policy to being at its centre, as part of the EU's growing perception of its own vulnerabilities, and its desires to be a geopolitical actor. Semiconductors sit at an economic-security nexus for the EU, where security is central to every aspect of the supply chain, from first mining of raw elements, through to incorporation into EU computing technologies, whether in commercial or military settings. This security is realised, however, through economic means that seek to boost industrial production in Europe, providing a boost for the EU economy while being driven by a desire for strategic autonomy. As part of this drive, coached in terms of digital and technological sovereignty, the EU's semiconductor regulatory framework is increasingly characterised by a regulatory mercantilist turn, in which economy and security are not distinct policy areas, but interlinked and interdependent, and essential for the EU's continued survival in the face of geopolitical instability.

Acknowledgments. I would like to take this opportunity to dedicate this paper to the memory of Professor Heike Schweitzer. Professor Schweitzer was an incredibly kind and supportive mentor during our time at the European University Institute, and it was she who encouraged me to submit my very first peer-reviewed article. It is only right that I dedicate this, my latest piece, to her.

¹¹⁸ European Commission, "Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation 2019/1020" (n 110) 1.

¹¹⁹ Listed in Annex III.

¹²⁰ European Commission, "Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation 2019/1020" (n 110) 10.

Competing interests. The author declares that there are no conflicts of interest.

Funding statement. This work was supported by the Economic and Social Research Council (ESRC) under grant number RC-MN1164X, "Digital Sovereignty by Design."